Journal of Social Science Studies Vol. 4, No. 2, July 2024, pages 503 – 516

Legal Construction and Enforcement Challenges of Credit Card Data Hacking Crimes in E-Commerce Systems

Phintar Charry Hartana, Rahayu Mardikaningsih, Siti Nur Halizah

Universitas Sunan Giri Surabaya, Indonesia

A R T I C L E I N F O

Article history:
Received 17 May 2024
Revised 03 June 2024
Accepted 06 June 2024

Key words:
Cybercrime,
Hacking,
E-Commerce,
Data Theft,
ITE Law,
Law Enforcement,
Digital Evidence.

ABSTRACT

This literature study examines the legal construction and law enforcement challenges regarding the crime of hacking e-commerce security systems to steal customer credit card data. Using a normative juridical method, the analysis focuses on the evolution of Indonesia's Electronic Information and Transactions Law (ITE Law), from its inception in Law No. 11 of 2008, amended by Law No. 19 of 2016, and most recently revised by Law No. 1 of 2024. The study finds that the ITE Law constructs the crime through offenses of unauthorized access (Article 30) and acts against data integrity (Article 32), with an increasingly robust approach to personal data protection. The relationship between the ITE Law as lex specialis and the Indonesian Criminal Code as lex generalis is integrative; the ITE Law addresses the digital method of the crime, while the Criminal Code qualifies its object and consequences under traditional offenses like theft or fraud. However, significant enforcement challenges persist, primarily related to the volatile and technical nature of digital evidence, cross-jurisdictional obstacles, limited technical capacity of law enforcement agencies, and the need for harmonization with newer regulations such as the Personal Data Protection Law (PDP Law). The study concludes that while the legal framework is substantively adequate, its effectiveness hinges on overcoming these practical, procedural, and international cooperation hurdles.

INTRODUCTION

Digital transformation has reshaped the global economic landscape, with e-commerce becoming the backbone of modern consumer transactions. E-commerce platforms serve as intermediaries of trust that process and store vast amounts of sensitive user data, including personal and financial information (Gardi & Darmawan, 2022). The success of this business model depends heavily on the platform's ability to guarantee the confidentiality, integrity, and availability of that data (Mardikaningsih et al., 2020). In a hyper-connected digital ecosystem, credit card data represents a highly liquid and valuable asset (Sinambela & Darmawan, 2022). The economic value of this data on the black market fuels organized cybercrime, which aims to exploit security gaps for illegal financial gain (Novriano et al., 2022; Mujisulistyo et al., 2024). Furthermore, in this era of information openness, social media is being massively utilized to simultaneously expand the reach of online business promotions (Infante & Mardikaningsih, 2022). Wall (2007) identified how cyberspace creates new opportunities for traditional crimes while spawning entirely new *modi operandi* that often transcend national jurisdictional boundaries.

Hacking e-commerce company systems to steal credit card data is a manifestation of cybercrime that carries a dual impact. On one hand, this act constitutes a violation of protected computer systems, which in many jurisdictions is categorized as a crime against property or electronic systems (Rahman et al., 2024). On the other hand, the theft of financial data is a crime against economic assets that can be directly converted into financial losses for cardholders, banking institutions, and the e-commerce company itself (Firmanto et al., 2024). According to Graham (2008), although not addressing legal aspects specifically, the motivations of hackers vary widely, ranging from intellectual challenges to pure economic profit. In cases of credit card data theft, economic motive is almost always the primary driver, placing this act in the category of

* *Corresponding author, email address:* ***rahayumardikaningsih@gmail.com***

cyber-enabled financial crime (Suwiknyo, 2021).

In Indonesia, the rapid development of the digital economy has not been fully matched by a specific and comprehensive criminal legal framework regarding cybercrime in the early 2000s. The primary regulation used as a reference was the Criminal Code, which was not designed to handle the complexity of the digital realm. The need for specialized law led to the birth of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). This law was a fundamental step as it recognized electronic documents as valid evidence and regulated criminal acts related to illegal access, illegal interception, interference with data, and misuse of devices (Putri & Miru, 2020). Articles 30, 31, and 32 of the ITE Law specifically criminalize actions that attack the availability, integrity, and confidentiality of electronic systems and data, providing the legal basis for prosecuting hacking activities.

However, stealing credit card data through hacking e-commerce companies raises complex legal questions. This act often involves a series of actions that can be qualified under several articles simultaneously, both in the ITE Law and the Criminal Code, such as theft (Article 362 Criminal Code), embezzlement (Article 372 Criminal Code), or fraud (Article 378 Criminal Code). The fundamental question is how criminal law construction frames the material act of hacking a system with the intent to steal intangible financial asset data. Is the legal object the electronic system, the electronic data, or the economic value of that data? Brenner (2007) argued that law often lags behind technology, creating a gap between actual occurrences and the legal ability to adequately define and reach those acts.

Therefore, this literature study focuses on the analysis of criminal law construction regarding the breach of security systems (hacking) of e-commerce companies with the specific intent to steal customer credit card data. This research seeks to trace how Indonesian legislation, especially the ITE Law and its amendments, defines and prosecutes this complex series of actions. The study will also examine how elements of criminal acts such as intent (*mens rea*), material action (*actus reus*), and the resulting damages are shaped within the existing legal framework. A thorough understanding of this legal construction is important to evaluate the effectiveness and shortcomings of current regulations, as well as to provide a foundation for developing more targeted policies and law enforcement in facing cybercrime threats in the digital economy sector.

Legal construction regarding hacking to steal credit card data faces problems due to the intangible and cross-border nature of the data itself. Credit card data, despite having very high economic value, is not a physical object or good as intended in the provisions of conventional theft in the Criminal Code. Article 362 Criminal Code requires the taking of "goods" belonging to another. Courts and legal experts are then faced with the issue of whether digital data can be equated to those "goods." Although the ITE Law recognizes electronic information as valid evidence, it does not explicitly construct data theft as the act of taking "goods." The absence of a firm definition creates legal ambiguity and the potential for divergent interpretations that can affect the prosecution and sentencing process. Brenner (2007) noted that the greatest challenge in cyber law is applying traditional legal concepts built for the physical world into an abstract and fluid digital reality, often resulting in conceptual incompatibility.

The second problem lies in the technical complexity of the crime's *modus operandi*, which hinders the proof of causal relationships and perpetrator fault. Hacking into secure e-commerce systems is rarely a single, simple event (Ulandari & Salsabila, 2022). Perpetrators may use a series of techniques such as SQL injection, exploitation of zero-day vulnerabilities, phishing attacks against employees, or the installation of malware to create backdoors. Each stage in this attack can be carried out from different jurisdictions, using proxy servers, and with masked identities. To convincingly prove the *mens rea* and *actus reus* of the principal perpetrator in court, law enforcement officials require high-level technical digital forensic expertise and access to electronic evidence that may be stored abroad. Therefore, increasing human resource capabilities in data analysis mastery is a key factor for legal decision-making accuracy (Khairi & Darmawan, 2022). Wall (2007) highlighted that the global character of cybercrime often clashes with the highly territorial nature of criminal law, posing significant obstacles in investigations and prosecutions.

Third, there is a gap in regulations governing the responsibility and security obligations of electronic system providers, in this case, e-commerce companies. While the ITE Law prosecutes hackers, the question regarding security standards that companies must fulfill to protect customer data has not been regulated comprehensively and specifically in the early development of the ITE Law (Sulistiono et al., 2024). The absence of clear provisions regarding *duty of care* or the obligation to implement adequate security measures (*security by design*) can

implicate the difficulty in assessing whether a company's negligence in securing its system contributed to the success of an attack. This touches upon aspects of corporate criminal liability and the division of responsibility between the perpetrator of the crime and the entity that is the target. The reconstruction of robust legal mechanisms is absolutely necessary to guarantee the restoration of consumer rights in the event of personal data leaks (Mujisulistyo et al., 2024). Analysis of this regulatory gap is necessary to understand the extent to which criminal law can drive an increase in cybersecurity standards on the service provider side.

The exponential growth of e-commerce transactions in Indonesia, accelerated by digital technology adoption and post-pandemic consumer behavior changes, has made this sector a critical infrastructure for the national economy. To maintain this ecosystem, ensuring the effectiveness of consumer protection in every electronic transaction is a fundamental legal instrument (Irfan & Negara, 2023). Any disruption to security and trust in the e-commerce ecosystem not only harms business players and individual consumers but potentially disrupts the stability of the financial sector and lowers public trust in the digital economy as a whole. Direct financial losses from credit card data theft can be followed by indirect costs such as reputation recovery, legal damages, and increased cyber insurance premiums. Furthermore, this aspect of legal protection must also be expanded to various other digital economic instruments such as online-based lending services and digital *arisan* (community savings) activities (Faridi et al., 2023; Negara & Darmawan, 2023). Therefore, a proper understanding of criminal law construction to prosecute perpetrators is a prerequisite for effective law enforcement, which in turn serves as a deterrent for potential criminals and affirms the state's commitment to protecting digital economic activities.

The highly dynamic development of cybercrime technology also demands constant evaluation of the adequacy of existing regulations. The methods and tools used to hack e-commerce systems five or ten years ago may be very different from those used today. Criminal law regulations must be sufficiently flexible and futuristic to reach new *modi operandi* without needing regular revisions. Examining the legal construction in the ITE Law and its relation to the Criminal Code is important to test its reach against the variations of cybercrime techniques that continue to evolve. In addition to cybercrime aspects, the optimization of the manufacturing industry supply chain through digital transformation as well as the structuring of value-added tax regulations on digital economic transactions also require aligned legal adjustments (Putra & Arifin, 2021; Nurhadi et al., 2023). Such studies can identify whether the formulation of offenses in the law is *technology-neutral* and focuses on the essence of unlawful acts, so that it remains relevant even as technology changes.

At the international level, pressure for the harmonization of cyber law and cross-border law enforcement cooperation is increasingly emerging. Indonesia is involved in various regional and global forums and initiatives related to cybersecurity. The urgency of global collaboration is a necessity to create resilient personal data protection in the digital age (Gardi & Eddine, 2023). Having a domestic criminal legal framework that is clear, strong, and aligned with international principles will facilitate *mutual legal assistance*, extradition, and the exchange of electronic evidence with other countries. This holistic legal construction also includes the dynamism of anti-money laundering regulations in tech company governance as well as law enforcement against trademark counterfeiting crimes (Fiana et al., 2024; Isnaeni et al., 2023). Without a solid and recognized legal construction, legal processes against transnational cybercriminals will be hindered. Thus, this academic review is not only valuable for the development of criminal law science in Indonesia but also for strengthening Indonesia's position in global cybersecurity governance and protecting its digital sovereignty.

The objective of this research is to critically analyze the criminal law construction regarding the breach of e-commerce company security systems for the purpose of stealing customer credit card data. Specifically, the research seeks to delineate and evaluate how the ITE Law (Electronic Information and Transactions Law) defines and covers acts of hacking and electronic data theft, to analyze the complementary or overlapping relationship between offenses in the ITE Law and traditional offenses in the Criminal Code (such as theft, fraud, and embezzlement) in responding to these crimes, and to identify and discuss the substantive and procedural challenges in proof and law enforcement, particularly concerning technical aspects of digital forensics, cross-jurisdictional issues, and international cooperation. The theoretical contribution of this research is expected to enrich the discourse on cyber criminal law in Indonesia, particularly regarding the construction of offenses and the integration of legal systems. Practically, the results of this study can provide input for legislators, law enforcement officials

(police, prosecutors, judges), and practitioners in the fields of information technology and cybersecurity in understanding the prevailing legal framework and the aspects that need to be strengthened for more effective law enforcement.

RESEARCH METHOD

This research is designed as a qualitative legal literature study employing a normative approach. Normative research in legal science focuses on discovering and analyzing legal principles, positive norms, and the prevailing legal system to address specific legal problems (Soekanto & Mamudji, 2001). The qualitative approach was chosen because the characteristics of the problem require an interpretative understanding of legal texts, court decisions, and academic discourse, rather than statistical measurement. This research is descriptive-analytical in nature, aiming to systematically describe the criminal law construction regarding hacking and credit card data theft, and subsequently analyze the relationships, gaps, and implications of such construction in a deep and comprehensive manner.

The data used consists entirely of secondary data, grouped into three main categories according to their hierarchy. The first category is primary legal material, encompassing legislation such as the Criminal Code, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments, as well as other relevant implementing regulations. The second category is secondary legal material, consisting of criminal law and cyber law textbooks, national and international scientific journal articles, legal scholars' commentaries, and legal dictionaries that provide explanations for the primary materials. The third category is tertiary legal material, in the form of indices, bibliographies, and online legal sites that facilitate the search for and tracing of the previous two categories of material.

The analysis technique applied is qualitative content analysis and juridical-normative analysis. Content analysis is used to systematically examine written materials such as legislative texts, court decisions, and academic literature by identifying key concepts, argumentation patterns, and developments in thought (Krippendorff, 2004). The process involves gathering materials, coding text based on the themes of the research questions, presenting data narratively, and drawing analytical conclusions. Juridical-normative analysis is conducted by applying methods of legal interpretation, such as grammatical (linguistic), systematic (in relation to other articles), teleological (according to the purpose of the law), and comparative interpretations regarding existing decisions. This technique allows the researcher to construct the meaning of applicable norms and evaluate their conformity with the complex and dynamic reality of cybercrime.

RESULT AND DISCUSSION

Criminal Law Construction of Hacking and Data Theft in the ITE Law

The criminal law construction for the act of breaching an e-commerce company's security system to steal credit card data was built incrementally through the evolution of the Electronic Information and Transactions Law. The original ITE Law, Law Number 11 of 2008, served as the initial foundation by recognizing the existence and legal force of electronic information and transactions. The ITE Law constitutes a legal framework governing electronic transactions, personal data protection, electronic transaction security, as well as copyright and intellectual property in the digital world (Ramadhani, 2023). In line with these developments, the acceleration of digitalization also reaches various small and medium industrial sectors, which demands the strengthening of innovation orientation and internet-based marketing strategies to optimize business performance (Darmawan et al., 2023). In relation to cybercrime, this law introduced specific offenses previously non-existent in the Criminal Code. Article 30 paragraph (1) of the 2008 ITE Law regulates unauthorized access, stating that any person who intentionally and without rights or unlawfully accesses a computer and/or electronic system belonging to another is subject to criminal penalties. This formulation became the main pillar for prosecuting the initial stage of hacking: the act of entering or accessing an e-commerce company's computer system without permission. However, this initial formulation remained general and focused on the access itself, without explicitly linking such access to the specific intent of data theft. The initial ITE Law formulation prosecuted illegal access, although it did not explicitly address data theft.

Article 32 of the 2008 ITE Law provides a construction more relevant to actions occurring after access is obtained. This article criminalizes the act of intentionally and without rights or unlawfully changing, removing, damaging, or transferring electronic information and/or electronic documents. In the context of credit card data theft, the act of downloading or copying data from an e-commerce company's database can be qualified as the "transfer of electronic information" in an

unlawful manner. Although the original data may not disappear from the server, the act of taking or duplicating it without permission has violated the confidentiality and ownership of the data. The legal construction at this stage began to reach the essence of the crime, namely the acquisition of digital assets with economic value. However, the approach of the 2008 ITE Law still appeared to separate illegal access (Article 30) from actions against data (Article 32), even though in practice, these two acts constitute a single continuous sequence. Article 32 prosecutes data transfer, complementing the illegal access offense.

The 2016 ITE Law revision expands the scope of cybercrime offenses. The first amendment through Law Number 19 of 2016 brought significant improvements, although it did not radically change the basic construction. This revision focused more on adjusting sanctions and clarifying several provisions. However, in the framework of prosecuting data theft, the change to Article 32 became important. The 2016 ITE Law clarified the scope of criminal acts by mentioning "changing, adding, reducing, erasing, damaging, moving, hiding" electronic information. The addition of the word "hiding" expanded the interpretation of the perpetrator's actions who might attempt to cover the tracks of their data theft. This revision demonstrated legislative awareness regarding the complexity of techniques used by cybercriminals. On the other hand, the dynamics of business management in the digital space also trigger various new legal challenges, including the risk of breach of contract in commercial marketplace-based digital business space leases (Anggoro et al., 2024). Nevertheless, the legal construction still did not fully unify illegal access with the economic objectives of that access. The law still regarded them as two separate acts, each of which could be prosecuted. This revision affirmed the complexity of the perpetrator's techniques, although the offenses remained separate.

The 2024 ITE Law presents substantive reforms to address modern cybercrime. The most substantive reform occurred with the enactment of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law. This law provides a more comprehensive and robust legal framework to respond to contemporary cybercrime dynamics, including structured financial data theft. First, the 2024 ITE Law strengthens and clarifies the "without rights" element in illegal access. More detailed explanations regarding what is meant by unauthorized access, including attempts to bypass authentication security mechanisms, provide clearer guidance for law enforcement and judges. Second, and most crucially, is the strengthening of personal data protection embodied in more integrated provisions. This strengthening step is crucial considering that the effectiveness of personal data protection in the financial technology sector and the supervision of compliance on various online platforms still require high attention (Aziz et al., 2023; Baraja et al., 2023). Although the Personal Data Protection Law stands alone, the 2024 ITE Law functions as *lex specialis* that regulates its criminal aspects specifically within the realm of electronic systems. The 2024 ITE Law clarifies illegal access and strengthens personal data protection.

The 2024 ITE Law unites illegal access and data theft offenses into an integrated construction. The legal construction in the 2024 ITE Law to reach credit card data theft via hacking can be analyzed through a more integrated approach. No longer merely viewing illegal access and data transfer as two separate offenses, law enforcement can build a construction that connects both as a complete scheme of crime. Unauthorized access (Article 30) is the method or path to achieve the goal, while the transfer of credit card data (as part of protected electronic information) is the goal as well as the consequence of that access, which is regulated in Article 32. Its legal qualification becomes sharper because credit card data can be specifically categorized as personal data that is confidential and sensitive, so violations against it receive greater attention and stricter penalty threats. The urgency of this data protection is not only crucial for consumers but also for internal companies regarding employee data protection, which is now beginning to be directed toward the utilization of blockchain-based technology (da Costa et al., 2023). This integrated construction affirms credit card data theft as a serious cybercrime.

The 2024 ITE Law closes loopholes by regulating the misuse of stolen data. Furthermore, the 2024 ITE Law includes more explicit provisions regarding the misuse of access or data obtained illegally. This is important in credit card data theft cases, because such data rarely ends up in the hands of the first hacker; data is usually traded or used to commit further fraud. Misuse of data in electronic transactions is also vulnerable to causing layered losses for consumers (Amin et al., 2023; Anugroh et al., 2023). Provisions regarding the misuse of electronic information obtained unlawfully, including for self-enrichment or

unlawfully benefiting others, close loopholes that might be exploited by perpetrators who argue that they only accessed and took the data, not used it. This construction ensures the chain of crime, from hacking to the utilization of stolen data, can be prosecuted more thoroughly. This provision ensures the entire chain of cybercrime can be penalized.

The 2024 ITE Law strengthens the legitimacy of electronic evidence in cyber cases. This criminal law construction is also reinforced by the increasingly mature recognition of electronic evidence. Article 5 of the 2024 ITE Law reaffirms and strengthens the position of electronic information as valid evidence in accordance with applicable procedural law. In the practice of law enforcement against hacking, this means server logs, network logs, digital forensic examination results on hardware and software, as well as electronic transaction metadata can be used as strong evidence in court. The ability to prove the causal link between illegal access from a specific IP address and data downloading activity from a specific database is key in building a solid indictment. All these digital evidentiary instruments ultimately lead to the strengthening of management optimization for the accuracy of managerial decision-making and the formulation of accountable business strategies (Journal of Social Science Studies, 2023). The validity of electronic evidence eliminates legal doubts that might have arisen in the early era of ITE Law implementation. The recognition of electronic evidence ensures that hacking indictments can be constructed robustly.

The 2024 ITE Law affirms corporate criminal liability in cybercrime. The aspect of corporate criminal liability also receives affirmation in the revised ITE Law framework. If hacking against an e-commerce company is carried out by or involves a corporation, for example as part of industrial espionage or unhealthy business competition, then that corporation can be held criminally liable. Cybercrime developments give birth to new facts that corporations can be perpetrators of criminal acts, therefore criminal liability against corporations needs to be enforced (Rahayu & Lukitasari, 2021). Aside from the purely cyber realm, this expansion of corporate legal responsibility is also in line with the strict anti-money laundering regulations applied in the governance of financial technology companies today (Fiana et al., 2024). This construction is in line with the development of modern criminal law which recognizes that organized crime, including large-scale cybercrime, often involves corporate structures. Regulations regarding corporate liability allow law enforcement to reach not only individual technical perpetrators (hackers), but also parties providing orders, funding, or facilities to perform such hacking. This regulation expands the reach of the law to the corporate level.

The 2024 ITE Law revision marks a shift in legal protection focus from systems to data. From a philosophical legal perspective, the construction in the ITE Law, especially after the 2024 revision, shows a shift from protection focused on systems (system-centric) toward protection that also focuses on data and its impacts (data-impact-centric). The law no longer solely protects electronic system integrity from access interference, but explicitly protects the substantive interests behind those systems, namely the personal and financial data of citizens along with the economic and social consequences of their theft. The urgency of this enforcement is in line with the increasing demand for global-scale collaboration to create cybersecurity and resilient personal data protection in the digital age (Gardi & Eddine, 2023). This shift is highly relevant to credit card data theft cases, where the main loss does not lie in the damage to the e-commerce system, but in the misuse of stolen data for consumer financial loss and disturbances to the digital trust ecosystem. This shift affirms the orientation of the law toward data protection and its socio-economic impacts.

The 2024 ITE Law establishes a comprehensive criminal construction against data theft. Overall, the criminal law framework within the ITE Law, which reached its most current form in Law Number 1 of 2024, has formed a sufficiently comprehensive structure to reach and qualify the criminal act of breaching e-commerce systems to steal credit card data. This framework is built upon the foundational element of unauthorized access, expanded to include actions against the integrity and confidentiality of electronic data, strengthened by specific protections for sensitive personal data, and supported by the recognition of electronic evidence and corporate liability. This construction enables law enforcement to not only prosecute individual perpetrators but also to unravel the entire chain of organized cybercrime, providing a robust legal basis for protecting digital assets in the modern economy. This construction ensures that the protection of digital assets and public trust remain upheld.

The Integration of Offences under the ITE Act and the Criminal Code within the Framework of Cybercrime

The relationship between the Electronic Information and Transactions Law (ITE Law) and the Criminal Code in prosecuting hacking and credit card data theft is not substitutive, but integrative and layered. The legal principle of *lex specialis derogat legi generali* serves as the primary framework. In this regard, the ITE Law acts as special law (*lex specialis*) that specifically regulates criminal acts related to electronic systems and information. Meanwhile, the Criminal Code functions as general law (*lex generalis*) that regulates conventional criminal acts. This integrative construction aligns with the development of technology-based legal violation patterns that demand continuous renewal in aspects of legal liability and cyber evidence procedures (Sutanto et al., 2023). For acts with a digital dimension, these two legal frameworks complement each other and can be applied cumulatively or alternatively, depending on which aspect of the act the public prosecutor wishes to emphasize. This integration allows for a charge construction that reflects the entire scheme of the crime, from the method of the act to the resulting consequences. Integration of *lex specialis* and *lex generalis* strengthens cybercrime charges.

Substantively, the ITE Law defines and criminalizes attacks on the system itself. Article 30 of the ITE Law in all its versions (2008, 2016, 2024) regulates unauthorized access to electronic systems, which serves as the foundation for prosecuting the initial act of a hacker breaching an e-commerce company's security. Article 32 regulates acts against electronic data, such as data transfer or destruction, which are relevant to the stage of acquiring credit card data from a database. This condition affirms the need for balanced digital regulation adaptation to keep pace with the dynamics of social interaction in a virtual society, ensuring that every illegal act in online communication remains reachable by law (Darmawan, 2021). These provisions fill the legal void in the Criminal Code, which does not regulate illegal access to computer systems or digital data transfer at all. Without the ITE Law, the act of breaching a system and downloading data might be difficult to qualify as a standalone criminal act under the Criminal Code, as the object is not a physical item that can be taken. The ITE Law makes hacking and digital data theft clearly punishable.

On the other hand, the Criminal Code provides a legal construction to assess successfully stolen credit card data as an object of crime with economic value. This is where integration becomes important. After the ITE Law prosecutes the "how" of the data acquisition (through illegal access and transfer), the Criminal Code enters to prosecute "what" is done with that data and the value of the object taken. Credit card data, although digital, contains very real financial value because it can be used to make purchases or withdraw funds. Therefore, the act of taking this data can be analogous to or subsumed into the theft offense under Article 362 of the Criminal Code. The conceptualization of these intangible assets is increasingly crucial to ensuring big data management optimization in supporting accurate managerial decision-making and business strategy in the digital economy era (Ali & Darmawan, 2023). The legal argument is that theft is no longer limited to taking tangible items, but includes taking everything containing economic value, including electronic data that serves as an instrument for obtaining wealth. This integration confirms digital data as an object of theft with economic value.

This integrative approach is further strengthened by the presence of fraud offenses in the Criminal Code, specifically Article 378. Crime schemes often do not stop at mere data theft. Stolen credit card data is usually used to conduct fictitious transactions or fund withdrawals without the cardholder's consent. This stage of utilizing stolen data for financial gain is what can be directly qualified as fraud. The ITE Law, through provisions such as Article 35 regarding misleading electronic information, can also reach this aspect of fraud, but its construction in the Criminal Code is more mature and has a long-standing jurisprudence. Additionally, data misuse in commercial transactions often intersects with issues of fulfilling the principles of justice, promotion, and service quality to maintain trust from the public as financial service users (Mardikaningsih & Hastriana, 2024). Thus, the sequence of acts can be unraveled: the ITE Law prosecutes unlawful data acquisition, while the Criminal Code (Article 378) prosecutes the use of that data to deceive other parties (merchants, banks) for gain. This integration ensures the entire sequence of cybercrime can be prosecuted in its entirety.

The integration of these two regulations is also very clear in terms of proof and evidence. The Criminal Code, as an older material criminal procedure law, does not specifically regulate electronic evidence. The ITE Law exists to fill this

crucial procedural void. Article 5 of the ITE Law, which remains maintained and reinforced in every revision, establishes that electronic information and/or electronic documents and their printouts are valid legal evidence. In presenting electronic evidence as valid and standalone evidence, it must be ensured that the recording or data runs in accordance with applicable provisions (Hasnawati & Safrin, 2023). These provisions act as an enabler for the use of digital evidence in judicial processes based on the Criminal Code. Without recognition from the ITE Law, server logs recording hacking activity, IP address traces, or digital forensic files might be rejected or have their validity debated in court. The validity of digital proof also becomes a vital instrument in guaranteeing legal certainty and digital literacy for modern society, especially among the younger generation who are highly active in consuming digital content (Kurniawan et al., 2021). Thus, the ITE Law modernizes and expands the evidence that can be used to prove criminal acts regulated both in the ITE Law itself and in the Criminal Code. Recognition of digital proof strengthens indictment construction in cyber cases.

Online fraud criminal acts via cyberspace have fulfilled the elements of sentencing (Rahman et al., 2023). In the realm of criminal liability and sanctions, integration creates flexibility in prosecution strategies that can be adjusted to the severity of the consequences and the *modus operandi*. A hacker who "only" accesses a system and takes data without directly utilizing it can be prosecuted based on Article 30 and/or 32 of the ITE Law. However, if that perpetrator also sells the data on the black market or uses it to transact, then the charge can be aggravated by adding Article 362 of the Criminal Code (theft) or Article 378 of the Criminal Code (fraud). This phenomenon of utilizing digital technology also reflects the dynamics of self-identity formation and individual social perception through massive interaction on various social media platforms today (Darmawan & de Jesus Isaac, 2022). The criminal threats can also be accumulated or the heaviest one selected. This cumulative approach allows the judiciary to provide a sentence that is more proportional to the total loss incurred, which includes system damage, privacy violations, and the victim's financial loss. A cumulative approach ensures sanctions are commensurate with the total loss.

As technology advances, crime also continues to develop, requiring law enforcement to possess more effective ways to handle complex cybercrime (Widijowati, 2022). The revision of the ITE Law through Law Number 1 of 2024 further tightens this integration by introducing norms that are more aligned with the concept of property crimes in the Criminal Code. Regulatory alignment is crucial considering that digital proficiency and adequate access to technology are the main pillars in bridging the opportunity gap in the modern industrial era (Arifin & Darmawan, 2021). With the increasing recognition of the economic value of personal data, legal construction has begun to view data not just as information, but as an asset. This perspective brings certain offenses in the ITE Law closer to the spirit of offenses in the Criminal Code. For instance, illegal data transfer is no longer seen solely as a violation of system confidentiality, but also as an acquisition of a valuable asset. This development makes it easier for law enforcement and judges to perform legal interpretations that directly link an act in the ITE Law to a specific offense in the Criminal Code, as there is a meeting point regarding the protected legal object: ownership and economic value. This integration confirms personal data as a valuable asset protected by law.

In law enforcement practice, this integration has been acknowledged by public prosecutors and the courts. Police and prosecutors, when preparing case files, often use layered articles (based on the ITE Law and the Criminal Code) to anticipate the possibility of one article not being proven or to describe the entire scope of the crime. The complex *modus operandi* of cybercrime even demands law enforcement vigilance equal to handling disinformation in the digital democratic space to comprehensively protect the rights of the public (Rojak, 2023). Judges, in their legal considerations, also frequently refer to both legal frameworks. They might use the ITE Law to prove the material element of hacking and taking data, then use the Criminal Code to assess the magnitude of the material and moral losses incurred, as well as to determine the severity of the sentence. Such jurisprudence demonstrates that integration is not just a theory, but has become standard practice in handling complex cybercrime cases. This layered integration has now become standard jurisprudence in cyber cases.

The existence of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) adds another dimension to this legal integration. The PDP Law specifically regulates the obligations of data controllers and the rights of data subjects, including administrative and criminal sanctions

for serious violations. In hacking cases, the PDP Law can be used to assess the negligence of e-commerce companies in protecting customer data (administrative and civil law aspects), while the ITE Law and the Criminal Code focus on criminal acts committed by hackers. The urgency of dividing these responsibility clusters aligns with the need for a robust legal mechanism reconstruction to guarantee the restoration of consumer rights due to personal data leaks in the financial technology sector (Mujisulistyo et al., 2024). However, the criminal provisions in the PDP Law can also be integrated, as credit card data theft is clearly an unlawful acquisition of personal data. This creates a triad of legal integration: the ITE Law for system and access aspects, the Criminal Code for theft and asset fraud aspects, and the PDP Law for privacy and specific personal data violation aspects. The triad of ITE Law, Criminal Code, and PDP Law strengthens legal protection over personal data.

Philosophically, the integration of the ITE Law and the Criminal Code reflects the ability of the law to adapt without abandoning existing foundations. The Criminal Code as a 19th-century legal product remains relevant because the basic principles of justice it regulates, such as the prohibition of taking other people's rights and fraud, are universal and apply across eras. The ITE Law functions as an adapter and translator that makes these universal principles applicable in the new digital reality. This adaptation includes the alignment of various new sectoral rules, such as digital credit regulation in business law and the arrangement of consumer protection instruments in community online rotating savings and credit associations (Negara & Darmawan, 2023; Yuristiawan et al., 2024). Successful integration is marked by the absence of contradiction between the two regulations, but rather a relationship of complementing and strengthening one another. The resulting legal construction becomes more robust and comprehensive, capable of reaching all stages of a modern cybercrime, from technical hacking in cyberspace to very real financial losses in the physical world. This integration makes the law more resilient in facing modern cybercrime.

The proof challenge in hacking criminal acts to steal credit card data arises primarily from the nature of the evidence itself, which is volatile, technical, and easily manipulated. The Electronic Information and Transactions Law (ITE Law), although revised until 2024, provides principled recognition of electronic evidence in Article 5. However, this normative recognition has not necessarily been followed by technical capacity and standard operating procedures across all stages of the legal process. Key evidence such as server access logs, firewall records, memory dumps, or malware traces are data that are very easily altered, deleted, or damaged due to a lack of understanding in initial handling. This empirical reality proves the existence of highly specific digital technology-based legal violation patterns, making the handling of legal obligations and the accuracy of cyber proof crucial (Sutanto et al., 2023). Strict digital evidence handling procedures, from *chain of custody* to forensic imaging methods, are often not understood evenly by investigators at the sectoral police level. Consequently, evidence submitted to court is vulnerable to being rejected because it is considered not to meet integrity and authenticity standards, thus collapsing the entire indictment construction built on that evidence. Without strict forensic standards, cyber indictments easily collapse in court.

The next challenge stems from the technical complexity of attacks, which complicates proving the causal link between the perpetrator, the action, and the loss. Modern hacking is rarely a direct attack from point A to point B. Perpetrators can use botnet networks, proxy servers in various countries, or lateral movement techniques within the victim's breached network. The ITE Law, specifically Article 30 on unauthorized access, requires proof that such access indeed originated from the prosecuted perpetrator. This complexity of the digital chain also demands the meticulousness of authorities in mapping public information circulation to suppress the rate of disinformation that has the potential to harm the digital democratic climate (Rojak, 2023). Tracing digital footprints that have passed through several layers of disguise requires skills in tracing analysis and cooperation with internet service providers in various jurisdictions a slow, expensive process often stalled by the absence of an effective Mutual Legal Assistance Treaty (MLAT) with the country where the intermediate server is located. Without the ability to prove this access path, the "performing access" element in the indictment becomes weak. Without clear causal evidence, hacking indictments are easily broken.

The jurisdictional aspect poses the most thorny law enforcement challenge. The cross-border nature of cybercrime inherently conflicts with the principle of territoriality in Indonesian criminal law. Article 2 paragraph (1) of the ITE Law indeed states the applicability of Indonesian law to every act that has

consequences in Indonesia, which can serve as a jurisdictional basis. However, executing this jurisdiction practically is a different matter. Arrests, seizure of digital assets on foreign servers, or compelling testimony from foreign service providers are almost impossible to carry out without solid international cooperation. Moreover, cases of transnational privacy violations on social media are proven to erode interpersonal trust between younger generations widely if left without sanctions (Negara et al., 2022). Indonesia is not a party to the Budapest Convention on Cybercrime, which is the main multilateral agreement facilitating such cooperation. Existing cooperation is still *ad hoc* and bilateral, with processes that are highly bureaucratic and unsuited to the speed required in cybercrime investigations where evidence can vanish within hours. Without effective international cooperation, cyber jurisdiction is difficult to enforce.

Another relevant regulation, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), may actually create a procedural dilemma in investigation. On one hand, the PDP Law requires e-commerce companies as data controllers to protect customer data and report data breaches. On the other hand, the investigation process by authorities against victim companies to collect digital evidence may intersect with provisions within the PDP Law itself. Investigators requesting full access to logs and databases for forensic analysis must contend with the company's obligation to maintain the confidentiality of other customers' data. This compliance conflict requires high managerial caution to remain aligned with the ethical principles of financial management and investment risk mitigation in the corporate ecosystem (Putra & Arifin, 2023). The lack of clear protocols or implementing regulations governing the procedure for requesting data for criminal investigation purposes based on the ITE Law within the PDP Law framework has the potential to cause compliance conflicts and slow down evidence collection. Without clear protocols, the PDP Law potentially slows down cyber investigation.

The proof challenge also concerns the difficulty in quantifying and proving losses legally. Stolen credit card data has a dual value: intrinsic value as confidential data, and extrinsic value as a tool to commit financial fraud. Proving material loss in a theft indictment (Criminal Code Article 362) or fraud (Criminal Code Article 378) requires converting the stolen data into a rupiah value acceptable to the court. This asset valuation dilemma is a major challenge, akin to measuring the level of satisfaction and perception of the ease of use of digital payment instruments in the current financial market (Kemarauwana & Darmawan, 2020). Is the value based on the selling price of data in dark web forums, based on credit card limits, or based on the actual loss suffered by the cardholder? Non-uniformity in assessing these losses can cause very wide variations in sentencing and difficulties in building a solid indictment regarding the magnitude of state or other parties' losses. Without a loss valuation standard, cyber indictments risk losing legal certainty.

The capacity of human resources in law enforcement agencies remains a fundamental structural obstacle. Although there are special units such as the Cyber Crime Directorate of the Criminal Investigation Agency of the Indonesian National Police or the Financial Transaction Reports and Analysis Center (PPATK), the number and expertise of investigators mastering advanced digital forensics, malware analysis, and network investigation remain limited compared to the volume and complexity of crimes occurring. Investment risk mitigation efforts in cyber assets on inclusive financial platforms, such as peer-to-peer lending, are also often constrained by the limited early detection capacity of law enforcement (Sahid et al., 2023). Existing training is often unable to keep pace with the speed of hacking technique evolution. This limitation results in a heavy reliance on third parties, such as private cybersecurity firms or independent experts, whose costs are high and whose report status in the hierarchy of evidence is sometimes still questioned in court. Without strengthening internal human resources, cyber law enforcement will continue to rely on external parties.

The speed of technological change is indeed accommodated by the technology-neutral nature of the ITE Law formulation. However, this technology neutrality is a double-edged sword. On one hand, it keeps the law from becoming quickly obsolete. On the other, it demands a very broad and bold interpretation from judges. New hacking techniques such as supply chain exploitation, fileless malware, or the misuse of artificial intelligence for social engineering must be able to be subsumed into existing ITE Law articles. The need for adaptive law is similar to the urgency of strengthening fair competition principles implemented by the KPPU to realize economic justice in the digital era (Wibowo et al., 2023). The ability of judges to understand the

essence of these new techniques and link them to legal elements such as "unauthorized access" or "data transfer" is very decisive. Without adequate technical understanding or strong expert assistance, there is a risk of failure in performing proper legal qualification. Without adaptive interpretation, the ITE Law risks falling behind the evolution of cybercrime.

Coordination and fragmentation of authority between state institutions also hinder effective law enforcement. Handling a single credit card data theft hacking case can involve the Police (as investigator of general criminal acts/ITE Law), the National Cyber and Crypto Agency (BSSN) (as national cyber security coordinator), the Financial Services Authority (because it concerns financial data), and the PPATK (to track crime proceeds flow). Each institution has its own mandate, priorities, and database. This fragmented nature of law enforcement must be immediately rectified through a commitment to eradicating corrupt practices in digital business activities to create clean investment certainty (Saputra et al., 2021). The absence of a single integrated command or a real-time information-sharing platform often causes investigations to run piecemeal, result in duplication of efforts, or even cause information leaks that interfere with the smoothness of the investigation. Without integrated coordination, cyber investigations are prone to being fragmented and ineffective.

Regulatory harmonization presents a crucial prospective challenge. The final prospective challenge concerns the harmonization of regulations. The revised ITE Law, the new PDP (Personal Data Protection) Law, and the Criminal Code must synergize without gaps. Currently, there remains potential for overlap and ambiguity. For instance, criminal sanctions for severe personal data violations are regulated both in the PDP Law and may also be applicable under the ITE Law (regarding the hacking aspect). The choice of which article to invoke can influence the burden of proof and the severity of the sentence. There is a need for prosecution guidelines or consistent jurisprudence from the Supreme Court to provide certainty for law enforcement at the lower levels, thus preventing disparities in case handling that would weaken the deterrent effect of the law itself. Consistent guidelines from the Supreme Court are necessary to ensure that regulatory harmonization is truly effective.

CONCLUSION

Based on the in-depth analysis conducted, it can be concluded that law enforcement against the criminal act of breaching e-commerce security systems to steal customer credit card data relies on a complex and layered legal framework. The primary criminal law construction is built upon the Law on Electronic Information and Transactions (ITE Law), which has undergone significant evolution from Law Number 11 of 2008, was revised by Law Number 19 of 2016, and reached its most current form in Law Number 1 of 2024. The ITE Law successfully captures and qualifies hacking acts through offenses of unauthorized access (Article 30) and actions against the integrity of electronic data (Article 32), with an approach that increasingly strengthens the protection of personal data. The relationship between the ITE Law as *lex specialis* and the Criminal Code as *lex generalis* is integrative and complementary. The ITE Law regulates the methods of crime in the digital world, while the Criminal Code provides qualifications regarding the objects and consequences of those crimes, such as theft or fraud, enabling comprehensive prosecution. However, the effectiveness of this legal construction is still faced with a number of substantive challenges in proof and law enforcement, particularly concerning the volatility and complexity of digital evidence, cross-border jurisdictional constraints, limitations in the technical capacity of officials, and the need for harmonization with new regulations such as the Personal Data Protection (*PDP*) Law.

The findings of this research carry important implications for various stakeholders. For legislators and policymakers, the implication that arises is the need for continuous evaluation and adjustment of technical regulations under the ITE Law and the PDP Law, particularly implementing regulations that govern investigation procedures, digital forensics standards, and inter-agency cooperation protocols. Coherence between the ITE Law, the Criminal Code, and the PDP Law must be maintained to prevent overlap and legal uncertainty. For law enforcement officials (police, prosecutors), the most direct implication is the necessity to make continuous investments in human resource capacity and technological upgrades. The establishment and strengthening of specialized cyber units equipped with state-of-the-art digital forensics tools and expertise have become a necessity. Furthermore, it is necessary to develop standardized investigation and prosecution guidelines for cybercrime cases, including integrated coordination mechanisms

between the National Cyber and Crypto Agency (*BSSN*), the National Police (*Polri*), the Attorney General's Office, and the Financial Transaction Reports and Analysis Center. For the business sector, particularly e-commerce companies, the implications of this research emphasize the obligation to implement adequate cybersecurity measures (*security by design and by default*) as mandated by the PDP Law, as negligence can worsen the impact of attacks and potentially lead to legal liability.

Based on these conclusions and implications, several strategic recommendations are proposed. First, the ratification of the Budapest Convention on Cybercrime or the formation of more effective bilateral and multilateral treaties is necessary to facilitate international cooperation in investigations, extradition, and the blocking of cross-border digital assets. Second, the Supreme Court needs to issue a Supreme Court Regulation or a Circular containing guidelines on the application of electronic evidence and evidentiary standards in cybercrime, in order to create certainty and uniformity of practice at all levels of the judiciary. Third, intensive education and training regarding digital forensics, cyber law, and financial investigation must become mandatory and continuous programs for investigators, prosecutors, and judges. Collaboration with universities and the cybersecurity industry can enrich these training curricula. Fourth, the government needs to encourage or require the e-commerce and fintech sectors to adopt high-level data security standards (such as tokenization, end-to-end encryption) and conduct penetration testing (*pentest*) and security audits periodically. Fiscal incentives can be provided to companies that achieve specific security certifications. Fifth, massive socialization to the public regarding the importance of protecting personal data, recognizing digital fraud *modi operandi*, and the mechanism for reporting if one becomes a victim of cybercrime must be aggressively carried out to create collective awareness as the first layer of defense.

REFERENCES

Ali, R., & Darmawan, D. (2023). Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies,* 3(2), 139-144.

Amin, M. N., Herisasono, A., Mujito, Khayru, R. K., & Zakki, M. (2023). Legal Protection of Consumers in Online Transactions for Counterfeit Halal Products on E-Commerce Platforms. *Journal of Social Science Studies*, 3(1), 53-58.

Anggoro, F., Saputra, R., Wibowo, A. S., Putra, A. R., & Wijaya, K. (2024). Consequences of Default in Commercial Marketplace-Based Digital Business Space Leases. *Journal of Social Science Studies*, 4(1), 483-498.

Anugroh, Y. G., Hardyansah, R., Darmawan, D., Khayru, R. K., Putra, A. R., & Putra, A. R. (2023). Consumer Protection and Responsibilities of E-commerce Platforms in Ensuring the Smooth Process of Returning Goods in COD Transactions. *Journal of Social Science Studies*, 3(2), 89-94.

Arifin, S., & Darmawan, D. (2021). Technology Access and Digital Skills: Bridging the Gaps in Education and Employment Opportunities in the Age of Technology 4.0. *Journal of Social Science Studies*, *1*(1), 163-168.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector. *Journal of Social Science Studies*, 3(1), 23-28.

Baraja, M. U., Saputra, R., Saktiawan, P., Dirgantara, F., & Waskito, S. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms. *Journal of Social Science Studies,* 3(1), 101-108.

Brenner, S. W. (2007). *Law in an Era of "Smart" Technology.* Oxford University Press, Oxford.

costa, S. da., Darmawan, D., & Isaac, A. de J. (2023). Safeguarding Employee Data with Blockchain in HR. *International Journal of Service Science, Management, Engineering, and Technology,* 4(3), 41–46.

Darmawan, D. (2021). Social Interaction in Digital Society: Changes in Online Communication Patterns and Dynamics of Virtual Communities, *Studi Ilmu Sosial Indonesia,* 1(1), 325-350.

Darmawan, D., & de Jesus Isaac, A. (2022). Self-identity formation and social perception of individuals through interaction on social media in a digital world. *Journal of Social Science Studies*, *2*(2), 273-278.

Darmawan, D., P. N. L. Sari, J. Jahroni, S. N. Halizah & R. Mardikaningsih. (2023). Digitalization of Kedai Industry: Analysis of The Role of Internet Marketing Orientation and Innovation on Marketing Performance.

Sustainable Environmental and Optimizing Industry Journal, 5(1), 21-31.

Faridi, F., Darmawan, D., Hardyansah, R., Putra, A. R., & Wibowo, A. S. (2023). Legal Protection for Online-Based Lending Consumers. *International Journal of Service Science, Management, Engineering, and Technology,* 4(2), 34–38.

Fiana, A., A. R. Putra, & A. S. Wibowo. (2024). The Dynamics of Anti-Money Laundering Regulation in the Governance of Fintech and E-Commerce Companies in Indonesia, *Journal of Social Science Studies*, 4(2), 397-412.

Firmanto, R., Hardyansah, R., & Darmawan, D. (2024). Responsibility of Banks in Preventing Name Abuse in Credit Applications. *Bulletin of Science, Technology and Society*, 3(3), 14-19.

Gardi, B., & Darmawan, D. (2022). Study of Shopping Lifestyle, Sales Promotion and Impulsive Buying Behavior. *Journal of Marketing and Business Research (MARK),* 2(2), 125-134.

Gardi, B., & Eddine, B. A. S. (2023). Cyber Security and Personal Data Protection in the Digital Age: Challenges, Impacts, and Urgency of Global Collaboration. *Bulletin of Science, Technology and Society,* 2(3), 58–63.

Graham, P. (2008). *Hackers & Painters: Big Ideas from the Computer Age.* O'Reilly Media, USA.

Hasnawati, H., & Safrin, M. (2023). Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, 5(2), 1207-1214.

Infante, A. & R. Mardikaningsih. (2022). The Potential of Social Media as a Means of Online Business Promotion. *Journal of Social Science Studies*, 2(2), 45-48.

Irfan, M., & Negara, D. S. (2023). The Effectiveness of Consumer Protection Arrangements in E-Commerce Transactions on the Shopee Marketplace Platform in Indonesia. *Journal of Social Science Studies,* 3(2), 115-120.

Isnaeni, M., Darmawan, D., Sutriyono, S., Sulistiono, D., & Octavianto, A. D. (2023). The Crime of Brand Counterfeiting in Commerce. *Studi Ilmu Sosial Indonesia*, 3(2), 101-118.

Kemarauwana, M., & Darmawan, D. (2020). Perceived Ease of Use Contribution to Behavioral Intention in Digital Payment. *Journal of Science, Technology and Society (SICO)*, 1(1), 1–4.

Khairi, M., & Darmawan, D. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations. *Journal of Social Science Studies,* 2(1), 223-228.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Sage Publications, Thousand Oaks.

Kurniawan, Y. & R. K. Khayru. (2021). Popular Culture and Youth: Value, Attitude, and Behavior Formation Through Music, Film, and Digital Content, *Studi Ilmu Sosial Indonesia,* 1(1), 303-324.

Kurniawan, Y., D. Darmawan, & R. K. Khayru. (2021). Social Media and Contemporary Youth Digital Literature, *Studi Ilmu Sosial Indonesia*, 1(2), 109-124.

Mardikaningsih, R., & Hastriana, A. Z. (2024). The Influence of Service Quality, Brand Equity, Promotion, and Perception of Justice on Customer Trust of Sharia Pawnshop Service Users. *Alkasb: Journal of Islamic Economics*, *3*(2), 234-251.

Mardikaningsih, R., Sinambela, E. A., Darmawan, D., & Nurmalasari, D. (2020). Hubungan Perilaku Konsumtif dan Minat Mahasiswa Menggunakan Jasa Pinjaman Online. *Jurnal Simki Pedagogia*, 3(6), 98-110.

Mujisulistyo, Y. F., Darmawan, D., & Dirgantara, F. (2024). Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia. *Journal of Social Science Studies*, 4(1), 75-84.

Mujisulistyo, Y. F., Darmawan, D., & Dirgantara, F. (2024). Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia. *Journal of Social Science Studies,* 4(1), 75-84.

Negara, D. S., & Darmawan, D. (2023). Digital Empowerment: Ensuring Legal Protections for Online Arisan Engagements. *Bulletin of Science, Technology and Society*, 2(2), 13-19.

Negara, D. S., Darmawan, D., & Saktiawan, P. (2022). Privacy Violations on Social Media and Interpersonal Trust Among Young Generations. *Journal of Social Science Studies*, 2(2), 151-156.

Novriano, F., Makarao, T., & Mawadi, H. (2022). Penegakan Hukum Tindak Pidana Peretasan Data Pribadi Konsumen Kartu Kredit Menurut Undang-Undang Informasi dan

Transaksi Elektronik Nomor 19 Tahun 2016. *Jurnal Hukum Jurisdictie*, 4(2), 167-190.

Nurhadi, Wibowo, A. S., Darmawan, D., Negara, D. S., & Hardyansah, R. (2023). Analysis of Value Added Tax Application on Electronic Commerce Transaction in Digital Economy System in Indonesia. *Journal of Social Science Studies*, 3(2), 83-88.

Putra, A. R., & Arifin, S. (2021). Supply Chain Management Optimization in the Manufacturing Industry through Digital Transformation: The Role of Big Data, Artificial Intelligence, and the Internet of Things. *Journal of Social Science Studies,* 1(2), 161-166.

Putra, A. R., & Arifin, S. (2023). Ethical Principles in Corporate Financial Management: A Literature Study on Investment and Risk. *Journal of Social Science Studies*, 3(2), 221-226.

Putri, A. P. Y., & Miru, A. (2020). Praktik Penyalahgunaan Fitur Kredit (Paylater) oleh Pihak Ketiga melalui Aplikasi Belanja Online. *Amanna Gappa*, 101-116.

Rahayu, H. S., & Lukitasari, D. (2021). The Concept of Corporate Criminal Liability in the Law on Information and Electronic Transactions. *Indonesian Journal of Criminal Law Studies*, 6(1), 83-92.

Rahman, A., Darmawan, D., & Saputra, R. (2024). Analysis of Cross-border Payment Regulation and its Impact on Consumers in Indonesia. *Bulletin of Science, Technology and Society*, 3(2), 23-28.

Rahman, M. A., Renggong, R., & Oner, B. (2023). Analisis Tindak Pidana Penipuan Online di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan. *Clavia*, 21(2), 357-370.

Ramadhani, F. (2023). Dinamika UU ITE sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, 1(1), 89-97.

Republik Indonesia. (1915). *Kitab Undang-Undang Hukum Pidana (KUHP/Wetboek van Strafrecht)*. Staatsblad Tahun 1915 Nomor 732. Sekretariat Negara Republik Indonesia. Jakarta.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843. Sekretariat Negara Republik Indonesia. Jakarta.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952. Sekretariat Negara Republik Indonesia. Jakarta.

Rojak, J. A. (2023). The Role and Risk of Citizen Journalism in the Digital Democracy Era: A Literature Study on Participation and Disinformation. *Studi Ilmu Sosial Indonesia*, 3(2), 421-440.

Sahid, R. R., Hardyansah, R., Darmawan, D., Negara, D. S., & Khayru, R. K. (2023). Legal Perspective of Investment Risk Mitigation on Peer-to-peer Lending Platforms. *Journal of Social Science Studies*, 3(1), 177-184.

Saputra, R., Hardyansah, R., & Saktiawan, P. (2021). Preventing Corrupt Practices in Business and Investment through Effective Law Enforcement. *Journal of Social Science Studies*, 1(2), 25-28.

Sutanto, H., R. Saputra, & D. Darmawan. (2023). Legal Violation Patterns in Digital Technology on Liability and Proof, *Studi Ilmu Sosial Indonesia*, 3(2), 277-308.

Wibowo, A. S., Darmawan, D., Halizah, S. N., & Mardikaningsih, R. (2023). Optimizing the Principles of Healthy Business Competition and the Role of KPPU for a Fair Economy in the Digital Era. *Journal of Social Science Studies*, 3(1), 95-100.

Widijowati, D. (2022). Legal Complexity in Dealing with Cyber Crime in Indonesia. *Research Horizon*, 2(6), 597-606.

Yuristiawan, A., Darmawan, D., & Hardyansah, R. (2024). Digital Credit Regulations in Business Law and Financial Markets. *Journal of Social Science Studies*, *4*(1), 371-380.

***Hartana, P. C., R. Mardikanigsih, & S. N. Halizah. (2024). Legal Construction and Enforcement Challenges of Credit Card Data Hacking Crimes in E-Commerce Systems, *Journal of Social Science Studies* 4(2), 503 – 516.**