YUDHISTIRA

Jurnal Yurisprudensi, Hukum dan Peradilan

Volume 3 Nomor 1 Tahun 2025

E-ISSN : 2988-7658

DOI : 10.59966/yudhistira.v3i1.1775

Article 28 of the ITE Law as a Pillar of Consumer Protection in Online Transactions

Siti Nurkhalifah Kaharu[1], Mohamad Rusdiyanto U Puluhulawa[2], Mohamad Hidayat Muhtar[3]

Universitas Negeri Gorontalo[1,2,3]

kaharunur746@gmail.com[2], rusdiyantop@gmail.com[2], hidayatmuhtar21@ung.ac.id[3]

Diserahkan tanggal 30 Januari 2025 | Diterima tanggal 31 Januari 2025 | Diterbitkan tanggal 30 Maret 2025

Abstract:

The development of online buying and selling transactions has also given rise to a rise in fraud cases that are detrimental to consumers. Article 28 paragraph (1) of Law Number 19 of 2016 concerning ITE needs to be legally reviewed to determine the extent to which these provisions are able to provide protection for consumers from fraudulent acts in online transactions. Therefore, this study aims to legally analyze the provisions of Article 28 paragraph (1) of Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE) as a form of legal protection for consumers in dealing with the rampant fraud in online buying and selling transactions. The main problems in this study include how the concept of legal protection for consumers is formulated in the article and what are the legal implications for perpetrators of fraud. This study uses a normative method with a legislative, conceptual, and case approach. Data were obtained from primary, secondary, and tertiary legal materials through literature studies. The results of the study indicate that Article 28 paragraph (1) of the ITE Law provides legal protection through a prohibition on the dissemination of false information that is detrimental to consumers in electronic transactions, with a maximum prison sentence of six years and/or a fine of up to one billion rupiah as regulated in Article 45A paragraph (1). In addition to being a repressive instrument, this provision is also preventive in nature by demanding that sellers be responsible for conveying honest and accurate information. This study emphasizes the urgency of law enforcement and digital literacy in strengthening consumer protection amidst the rapid growth of e-commerce.

Keywords: *consumer protection, electronic transactions, online fraud.*

Abstrak *:*

Perkembangan transaksi jual beli secara daring turut memunculkan maraknya kasus penipuan yang merugikan konsumen. Pasal 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang ITE perlu dikaji secara hukum untuk mengetahui sejauh mana ketentuan tersebut mampu memberikan perlindungan bagi konsumen dari tindakan penipuan dalam transaksi daring. Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara hukum ketentuan Pasal 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai bentuk perlindungan hukum bagi konsumen dalam menghadapi maraknya penipuan dalam transaksi jual beli secara daring. Pokok permasalahan dalam penelitian ini meliputi bagaimana konsep perlindungan hukum bagi konsumen yang dirumuskan dalam pasal tersebut dan apa saja implikasi hukum bagi pelaku penipuan. Penelitian ini menggunakan metode normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Data diperoleh dari bahan hukum primer, sekunder, dan tersier melalui studi kepustakaan. Hasil penelitian menunjukkan bahwa Pasal 28 ayat (1) UU ITE memberikan perlindungan hukum melalui larangan penyebaran informasi palsu yang merugikan konsumen dalam transaksi elektronik, dengan ancaman pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah sebagaimana diatur dalam Pasal 45A ayat (1). Selain bersifat represif, ketentuan ini juga bersifat preventif dengan menuntut agar penjual bertanggung jawab menyampaikan informasi yang jujur dan benar. Studi ini menekankan urgensi penegakan hukum dan literasi digital dalam memperkuat perlindungan konsumen di tengah pesatnya pertumbuhan e-commerce.

Kata Kunci: perlindungan konsumen, penipuan daring, transaksi elektronik.

INTRODUCTION

The advancement of information technology in the last two decades has given birth to a fundamental transformation in the social, economic, and legal life of global society, including Indonesia. (Abqa et al, 2023) The Internet is no longer just a means of communication, but has become the main medium in carrying out economic activities, especially trade. Trade through electronic systems or what is known as e-commerce has grown rapidly, allowing business actors and consumers to interact without geographical and time boundaries. However, behind the benefits of efficiency and convenience offered, e-commerce also opens up a wide space for deviations and criminal acts, especially fraud committed through digital media. This reality places the law in a challenging position, because it must be able to adapt to the new dynamics caused by the use of information technology. (Rahman et al, 2024)

The phenomenon of fraud in electronic transactions or digital fraud is not a sudden symptom, but a logical consequence of the shift in the pattern of community interaction. If in conventional trade the relationship between sellers and buyers is built through physical interaction and direct trust, then in e-commerce the interaction takes place virtually and is highly dependent on trust in the information displayed digitally. This is where the vulnerability lies. (Pensiunulawa et al, 2023) Unclear business actors' identities, misleading product information, and other manipulative practices provide loopholes for criminals to exploit consumers. In many cases, consumers are harmed because the goods purchased are not appropriate, not sent, or even the sales site is a fictitious entity. Such practices are increasingly complex because they involve technological elements and are often cross-jurisdictional.

In the context of Indonesian law, the crime of fraud has actually been regulated in Article 378 of the Criminal Code which regulates acts of deception by using a false name, false dignity, trickery, or a series of lies. However, this article was designed in the context of an analog society, not a digital one. Therefore, with the birth of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) and then amended through Law Number 19 of 2016, the state began to present legal norms that respond to more contemporary forms of cybercrime. Article 28 paragraph (1) of the ITE Law explicitly mentions the prohibition of the spread of false and misleading news that results in consumer losses in electronic transactions. (Dewi et al, 2021) Thus, this provision can be understood as an expansion of the concept of fraud in the digital dimension, which substantially strengthens legal protection for consumers.

However, the implementation of the norms in the ITE Law still presents a number of problems. One of the most striking is the issue of proof and classification of the crime. Article 28 paragraph (1) is a material crime, which means that the element of loss must be proven concretely. In practice, this makes it difficult for law enforcement because not all losses are visible, especially if they are related to non-material losses such as loss of trust or damage to reputation. In addition, the disparity in understanding among law enforcement officers regarding the boundaries between false information and the right to express oneself also raises doubts in prosecuting perpetrators. This is exacerbated by the fact that not all officers have adequate competence in the field of information technology, which makes the investigation and proof process in digital fraud cases less than optimal.

Concrete incidents such as those experienced by a journalist with the initials PIS who suffered losses of up to tens of millions of rupiah due to fictitious purchase transactions, or endorsements by public figures such as Marissya Icha for online stores that turned out to be problematic, show that digital crime not only impacts individuals, but also has the potential to create collective losses. Victims in cases like this often experience not only economic losses, but also psychological ones, because they feel cheated in a space that should provide a sense of security and trust.

Another problem lies in the legal-structural dimension. Normatively, there is an overlap between criminal norms in the Criminal Code and the ITE Law, as well as implementing regulations such as Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems. This regulation stipulates the obligation to identify business actors and fairly detailed administrative requirements, but in reality, many business actors in the digital sector have not or do not comply with these provisions. Not a few actors operate without a clear legal identity, are not registered, and cannot be traced, so that when a violation occurs, the law enforcement process becomes very difficult. (Rohmy et al, 2021) This vague identity of the perpetrator is a major obstacle in enforcing the law in the digital space, which is anonymous and easily manipulated.

On the other hand, consumer protection is also regulated in Law Number 8 of 1999 concerning Consumer Protection. In the context of electronic transactions, consumers are individuals who purchase goods or services for personal interests and not for resale. This means that legal protection in digital transactions is explicitly only given to end consumers, and does not include intermediary business actors or distributors. This raises its own problems, especially when digital consumers are not aware of their legal status in the transaction and ultimately have no legal basis to demand justice.

Furthermore, digital fraud crimes also challenge cross-border jurisdiction and enforcement aspects. In many cases, perpetrators and victims are in different jurisdictions, or transactions are conducted through platforms operating abroad. This makes law enforcement against perpetrators hampered due to limited cooperation between countries and other technical obstacles. Therefore, although legal norms have been presented, their effectiveness is highly dependent on the capacity of institutions to prosecute violations and overcome transnational barriers. (Pakaya et al, 2024)

By considering these dynamics, it can be concluded that fraud in digital transactions is a complex form of contemporary crime, not only in terms of the mode and technology used, but also from a legal, structural, and cultural perspective. This complexity demands a legal approach that is not only responsive, but also able to capture the development of forms of crime that continue to evolve in cyberspace. Ultimately, the existence of regulations such as the Criminal Code, the ITE Law, the Consumer Protection Law, and the PMSE PP are important foundations in building a responsible digital legal order, although the challenges of implementation and supervision remain crucial issues that need to be continuously studied in the context of legal protection for consumers in cyberspace.

Formulation of the problem

1. What is the legal protection for consumers in cases of online fraud according to Article 28 paragraph (1) of Law Number 19 of 2016 concerning Information and Electronic Transactions?
2. What are the legal implications arising from violations of Article 28 paragraph (1) of the ITE Law in online buying and selling practices?

Research Purposes

1. To find out the legal protection for consumers in cases of online fraud according to Article 28 paragraph (1) of Law Number 19 of 2016 concerning Information and Electronic Transactions
2. To find out the legal implications arising from violations of Article 28 paragraph (1) of the ITE Law in online buying and selling practices.

RESEARCH METHODS

This study uses a doctrinal or normative approach that focuses on positive law, emphasizing the study of legal norms written in laws and legal doctrines. Normative legal research aims to identify, interpret, and evaluate applicable legal rules in order to obtain a systematic and

comprehensive understanding of the legal issues discussed. The normative approach was chosen because it allows researchers to deeply analyze the provisions of positive law that regulate fraud in online buying and selling, and to relate them to legal theory, especially the theory of punishment and the theory of legal protection. Compared to the empirical approach that emphasizes field data, the normative approach is more relevant in the context of this study because its main focus lies in the exploration of legal texts and developing legal thinking. (Syarif et al, 2024)

In conducting the research, three types of approaches were used, namely the legislative approach, the conceptual approach, and the case approach. The legislative approach was carried out by critically reviewing all relevant laws and regulations, including the Criminal Code, Law Number 11 of 2008 concerning Information and Electronic Transactions which has been amended by Law Number 19 of 2016, and other implementing regulations relating to consumer protection and electronic commerce. The conceptual approach was used to understand the developing framework of thought in legal science regarding digital fraud and consumer protection in electronic transactions. Meanwhile, the case approach was carried out by reviewing court decisions relating to the crime of online fraud as a case study that can provide a concrete picture of the application of positive law.

The sources of legal materials in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include binding laws and regulations, including the Criminal Code and Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions. Secondary legal materials include doctrines or literature that provide explanations of primary legal materials, such as books, scientific journals, articles, and opinions of relevant legal experts. Meanwhile, tertiary legal materials include legal encyclopedias, legal dictionaries, and indexes that help explain or facilitate the search for primary and secondary legal materials.

The technique of collecting legal materials is carried out through a literature study using the literary method. Researchers trace, read, and evaluate various legal sources related to the issue of fraud in online buying and selling and consumer protection in electronic transactions. This process involves searching for legal sources in books, journals, electronic documents, and expert opinions in order to build a strong and relevant basis for analysis. In addition, a study was conducted on the perspectives of criminal law and information law experts in understanding and interpreting legal provisions related to digital fraud crimes.

In analyzing the legal materials that have been collected, a qualitative analysis method is used, namely by interpreting relevant laws and doctrines without using statistical data or figures. This analysis is carried out by linking applicable legal norms with the legal reality found in practice, as well as by examining the consistency and suitability between legal provisions and their application in real cases. The purpose of this analysis is to produce a comprehensive understanding of legal protection for consumers who are victims of online fraud based on criminal provisions in the Criminal Code and the Electronic Information and Transactions Law.

DISCUSSION

1. Protection Concept of Article 28 Paragraph 1 of Law Number 19 of 2016 concerning Electronic Transaction Information Against Online Buying and Selling Fraud

The variety of criminal acts in Indonesian society shows a significant increase, one of which is fraud, which is increasingly complex both in terms of the modus operandi and the media used. (Harahap et al, 2023) Fraud is no longer only carried out conventionally, but also develops in digital form along with advances in information technology. The general definition of fraud refers to an act carried out intentionally using misleading information or false material facts to obtain financial gain. In many cases, fraud begins with the perpetrator's attempt to gain the victim's trust. (Muhtar et al, 2023) The trust that the perpetrator has successfully instilled is ultimately used to carry out manipulative actions that result in losses. From a criminal law perspective, fraud is an unlawful act

that can be subject to criminal sanctions, as regulated in various statutory provisions. (Arief et al, 2023)

Trade is a strategic sector in Indonesia's economic growth, so fraudulent acts in the trade space, including digital trade, have broad implications not only for individuals, but also for national economic stability. With the increasing use of digital systems in buying and selling transactions, new forms of fraud have emerged. In this context, positive law is required to be able to anticipate and regulate various crimes that occur in cyberspace. (Widodo et al, 2023) Fraud committed in digital transactions or known as online fraud is part of cybercrime, especially in the category of illegal content. This category includes acts of spreading false, immoral, or misleading information through electronic media that can result in losses for other parties. The mode of fraud in electronic commerce is often disguised in the form of product promotions, big discounts, or the use of fake accounts that appear convincing.

Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), is present as a state response to legal challenges in the digital realm. One of the important provisions in the ITE Law that is relevant to digital fraud is Article 28 paragraph (1), which states that anyone who intentionally and without the right to spread false and misleading news that results in consumer losses in electronic transactions can be punished. (Yanuaria & Rongalaha, 2019) The criminal threat stipulated in Article 45A paragraph (1) of the same Law is a maximum imprisonment of six years and/or a maximum fine of one billion rupiah. This norm aims to provide legal protection to consumers while providing legal certainty regarding the legality of transactions carried out electronically.

Article 28 paragraph (1) of the ITE Law has the characteristics of a material crime, meaning that the element of loss is an absolute requirement for the act to be qualified as a criminal act. Thus, the burden of proof of the existence of real losses becomes important in the law enforcement process. This also distinguishes this provision from formal crimes which are sufficient only by proving the existence of an act without the need to prove the consequences. In practice, it is not uncommon for law enforcement against digital fraud crimes to be hampered by the difficulty of proof, especially if the perpetrators use fake identities or disguise their digital footprints. In addition, cross-border jurisdictions that often occur in electronic transactions are a challenge in prosecuting perpetrators who are abroad.

Real cases that occurred in Indonesia show how high the risks faced by consumers in online transactions are. In the case of a journalist with the initials PIS, a loss of Rp66.3 million was experienced after buying imported clothes from a fictitious seller. The goods were never received, and the perpetrator asked for additional money under the pretext of a refund . This is a classic form of digital fraud that exploits consumer weaknesses in terms of verifying information and trust in digital displays. Another case that has emerged is the case of Marissya Icha, a public figure who gave an endorsement to an online store that turned out to deceive consumers. Although not directly the perpetrator, endorsements from public figures have great persuasive power, raising legal questions regarding the accountability of parties who indirectly contribute to consumer losses.

From a criminal law perspective, Article 28 paragraph (1) of the ITE Law and Article 378 of the Criminal Code can be seen as two norms that regulate the crime of fraud from different perspectives. Article 378 of the Criminal Code regulates fraud as an act of using a false name , false dignity, trickery, or a series of lies to obtain goods or benefits. This norm is general and has been in effect for a long time, while Article 28 paragraph (1) of the ITE Law more specifically regulates fraud in the context of electronic transactions with an emphasis on the dissemination of misleading information through digital media. (Rusdiyanto et al, 2024) In this case, the principle of lex specialis derogat legi generalis applies, where special provisions in the ITE Law override general provisions in the Criminal Code if there is a conflict or overlapping regulation.

In addition to the Criminal Code and the ITE Law, consumer protection is also regulated in Law Number 8 of 1999 concerning Consumer Protection, which provides a legal basis for

consumers to claim their rights over purchased products and services. The definition of consumer in this law refers to the end consumer, namely the party who uses the product for personal interests and not for commercialization. This means that legal protection in the context of Article 28 paragraph (1) of the ITE Law only applies to end consumers and does not include business actors who use the product as part of the production process.

Fraud in online buying and selling transactions takes various forms, ranging from goods that do not match the description, the use of fake identities by business actors, to unreasonable price offers that attract consumers emotionally. Criminals take advantage of system weaknesses and the lack of identity verification by e-commerce platforms to carry out their actions. The absence of a strong system in verifying the identity of business actors and consumers makes it easy for perpetrators to cover their tracks and escape the law. In this case, the existence of digital contracts and transaction proof mechanisms is very important as a legal tool that can strengthen the position of consumers.

Although the ITE Law provides strict criminal sanctions against fraudsters, there are no explicit regulations regarding the rights of victims to compensation or restitution in cases of online fraud. This creates a legal vacuum that has an impact on the unclear mechanism for restoring consumer rights. In practice, victims must take civil legal action to obtain compensation, even though not all victims have the resources or sufficient legal understanding to do so. Therefore, legal protection for victims must not only cover criminal aspects, but also civil aspects, especially in terms of recovering financial losses.

The online motorcycle fraud case uncovered by the West Java Regional Police confirms that the perpetrators' modus operandi is increasingly sophisticated and targeting the wider community. The perpetrators offer vehicles at low prices through social media and e-commerce platforms, and after the victim makes payment, the goods are not sent. The perpetrators disappear and are difficult to track. This case shows that Article 28 paragraph (1) of the ITE Law can be applied because there is an element of spreading false information that causes real losses to consumers. The success of uncovering the case by the police also shows the importance of digital literacy and public vigilance in online transactions.

From the perspective of legal philosophy, the principle of legal protection as stated by Philipus M. Hadjon emphasizes the importance of the state in guaranteeing human dignity through the recognition and protection of human rights. (Muhtar, 2023) In this context, the state through its legal instruments is obliged to provide a sense of security to digital consumers who are vulnerable to information misuse. When the law fails to carry out this protective function, public trust in the legal system will decline, and the space for criminals to grow will be wider.

Overall, Article 28 paragraph (1) of the ITE Law is a special norm that is relevant in responding to legal challenges in the digital era, especially in protecting consumers from fraudulent practices that utilize electronic transactions. Although not yet perfect in its regulations, this article provides a strong foundation for law enforcement and consumer protection efforts. However, the effectiveness of its implementation is highly dependent on the capacity of law enforcement officers, public awareness, and synergy between applicable regulations. The conflict of norms between the ITE Law and the Criminal Code in regulating fraud must be resolved through the principle of lex specialis derogat legi generalis, where the ITE Law is the main basis for dealing with digital fraud because of its more specific and contextual nature. Proper implementation of this article will not only strengthen the national legal system in dealing with cybercrime , but also be a concrete manifestation of the state's protection of its citizens in the increasingly complex and vulnerable digital space.

2. Legal Implications of Online Purchase and Sale Violations Reviewed from Article 28 Paragraph 1 of the Electronic Transaction Information Law

As a country of law, Indonesia upholds the principle that every citizen since birth has basic rights guaranteed by the constitution. This is as stated in the 1945 Constitution of the Republic of

Indonesia which states that the rights of citizens must be protected by the state. (Pujayanti et al, 2024) In the modern context, these rights also include protection of citizens' activities in the digital space. The development of information and communication technology has created a new paradigm in social and economic interactions in society, including online buying and selling transactions. However, this progress not only brings benefits, but also raises new challenges in the form of cybercrime, one of which is online buying and selling fraud which is now one of the most disturbing forms of crime for society in the digital era.

Fraud in online transactions is a form of adaptation of conventional fraud into cyberspace. If previously the crime was committed through direct interaction, now simply through electronic devices, the perpetrator can commit the crime remotely, without face-to-face, and with a relatively smaller risk of being caught. Online fraud occurs when the perpetrator spreads false information about a product or service through digital media, with the aim of misleading consumers and obtaining illegal profits. In practice, the perpetrator takes advantage of the victim's trust, consumer negligence, and the weakness of the legal protection system in the digital ecosystem to carry out his actions. This has an impact not only economically on the victim, but also damages the ecosystem of trust in electronic transactions. (Aryani & Susanti, 2022)

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) is present as a legal response to various forms of crime that use information technology as a medium. Article 28 paragraph (1) of the ITE Law explicitly stipulates that anyone who intentionally and without the right to spread false and misleading news that results in consumer losses in electronic transactions can be punished. This provision is very important because it provides a legal basis for law enforcement officers in prosecuting online fraud perpetrators, as well as providing legal protection to consumers as the most vulnerable party in electronic transactions. The criminal threat as stated in Article 45A paragraph (1) is a maximum imprisonment of six years and/or a maximum fine of one billion rupiah.

Online fraud often occurs due to underlying factors, such as economic pressure, low levels of education, the influence of the social environment, and weaknesses in law enforcement. Many perpetrators take advantage of legal loopholes and system vulnerabilities to carry out their actions. They use fake identities, fictitious accounts, and information manipulation techniques to convince victims. Victims also come from various backgrounds of age , gender, education level, and economic conditions, making it difficult to map the profile of the most vulnerable consumers. In many cases, victims not only experience material losses, but also psychological losses because they feel cheated and humiliated. (Fauzi et al, 2023)

The legal implications of violating Article 28 paragraph (1) of the ITE Law are very significant. First, from the consumer protection perspective, this article provides firm legal guarantees to people who conduct electronic transactions. This protection is not only in the form of criminal threats against perpetrators, but also reflects the state's commitment to creating a safe and trustworthy digital transaction ecosystem. With legal certainty, consumers can feel more at ease in making online purchases. Second, from the seller's perspective, this article demands greater responsibility to convey honest, accurate, and non-misleading information. Sellers who are proven to have provided false information can be subject to criminal sanctions, which ultimately fosters ethical awareness in business and encourages healthy business practices.

Third, from the aspect of law enforcement, Article 28 paragraph (1) provides a strong legal basis for investigators to carry out legal proceedings against perpetrators of digital fraud. In this case, electronic evidence such as instant messaging conversations, emails, transaction screenshots, and digital recordings can be used as valid evidence in court. This provides flexibility for law enforcement to access and verify evidence more efficiently. However, it is undeniable that law enforcement against cybercrime, especially online fraud, still faces various obstacles, ranging from

tracking the identity of the perpetrator, limited human resources who have expertise in the field of digital forensics, to the lack of coordination between related institutions.

From a normative perspective, Article 28 paragraph (1) of the ITE Law has advantages compared to Article 378 of the Criminal Code which regulates fraud in general. While Article 378 of the Criminal Code requires trickery or a series of lies that cause the victim to hand over something, Article 28 paragraph (1) of the ITE Law specifically highlights the spread of false information in the context of electronic transactions. Thus, this provision can be viewed as lex specialis to Article 378 of the Criminal Code in terms of digital media-based fraud. The clarity of the elements of the crime in Article 28 paragraph (1) is an important instrument in supporting the process of criminalizing the perpetrator, especially in proving the element of intent and the existence of real losses experienced by consumers.

In practice, the effectiveness of Article 28 paragraph (1) of the ITE Law in protecting consumers depends on the ability of the legal system to prosecute violations. Many cases of online fraud do not reach the court process due to reporting constraints, victims' ignorance of legal procedures, or because the perpetrators are difficult to identify. Therefore, efforts are needed to improve the digital legal literacy of the community, as well as strengthening consumer protection institutions that can provide legal assistance to victims. In addition, the involvement of e-commerce platform organizers as parties who are also responsible for the validity of user data and activities is also crucial. Digital platforms must have clear policies regarding seller identification and verification, and provide dispute resolution mechanisms that are easily accessible to consumers.

Law enforcement against digital fraud must also pay attention to the principle of restorative justice, which does not only focus on punishing the perpetrator, but also on restoring the victim's losses. In this case, the state can encourage a model of compensation (restitution) as part of the court's decision, so that the victim does not just accept the perpetrator being punished, but also receives compensation for the losses suffered. This principle of justice is the spirit of legal protection in modern society. Meanwhile, from the perspective of criminal theory, the existence of criminal sanctions in the article shows the repressive function of criminal law, namely providing a deterrent effect on the perpetrator and preventing other people from committing the same act . The imposition of criminal sanctions in digital crimes is not only intended to punish, but also to emphasize the social norm that the spread of false information is a despicable act that is contrary to the public interest.

Thus, it can be concluded that Article 28 paragraph (1) of the ITE Law plays a strategic role in combating online fraudulent transactions. This provision not only provides legal protection to consumers, but also strengthens the national legal system in responding to the challenges of technology-based crimes. However, the effectiveness of this article is highly dependent on the synergy between clear regulations, strong law enforcement, the active role of digital platforms, and public participation in building a technology-aware legal culture. In the context of a state of law, the existence of legal instruments such as Article 28 paragraph (1) of the ITE Law is a concrete form of the state's role in guaranteeing citizens' rights and creating legal order in the digital era.

CONCLUSION

Article 28 paragraph (1) of the Electronic Information and Transactions Law (UU ITE) provides a strong legal basis for consumer protection in dealing with fraudulent practices in online transactions. This provision confirms that anyone who intentionally spreads false news that causes losses to consumers can be subject to criminal sanctions, thus functioning as a legal umbrella to prevent misuse of information in e-commerce. The legal protection provided includes the seller's responsibility to provide accurate and non-misleading information, as well as the consumer's right to claim compensation if they become victims. Thus, Article 28 paragraph (1) is not only repressive through the threat of imprisonment and fines, but also preventive in creating a transparent and ethical digital transaction climate. The legal implications include providing a deterrent effect for

perpetrators of fraud, increasing seller caution, and empowering consumers in demanding their rights legally.

In supporting the effectiveness of these norms , integrated efforts from various parties are needed. The government and related institutions should increase the intensity of public education regarding consumer rights in online transactions so that the public is more aware and alert to the potential for fraud. Supervision of e-commerce platforms must also be strengthened to ensure that all digital business actors comply with applicable regulations. In addition, increasing the capacity of law enforcement officers is important so that handling online fraud cases is more professional and responsive. On the other hand, e-commerce platform organizers also have a responsibility to develop transaction security systems, such as escrow or money back guarantees, to provide additional protection for consumers and increase trust in the digital trading ecosystem.

DAFTAR PUSTAKA

Abqa, MAR, Hutabarat, SA, Suhariyanto, D., Fauziah, NM, Khilmi, EF, Meliana, Y., & Muhtar, MH (2023). *Constitutional law: A basic concept in organizing the nation* . PT. Sonpedia Publishing Indonesia.

Arief, S., Muhtar, MH, & Saragih, GM (2023). Self-defense efforts in the perspective of equality before the law. *Judicial Journal* , 16(1), 25–47. https://doi.org/10.29123/jy.v16i1.475

Aryani, AP, & Susanti, LE (2022). The Importance of Consumer Personal Data Protection in Online Transactions on Marketplaces for Consumer Satisfaction. Ahmad Dahlan Legal Perspective , 2(1), 20–29. https://doi.org/10.12928/adlp.v2i1.5610

Dewi, EK, Dewi, AASL, & Widyantara, IMM (2021). Legal consequences of the implementation of online arisan based on Law Number 19 of 2016. *Journal of Legal Construction* , 2(2), 296–302. https://doi.org/10.22225/jkh.2.2.3226.296-302

Fauzi, A., Fikri, AWN, Marhadi, A., Prabaswara, BA, Situmorang, BB, Piliyanto, EA, Nasution, IA, & Nugraha, RE (2023). Online fraudulent buying and selling crimes through social media. *Journal of Information Systems Management Economics* , 4(6), 968–974. https://doi.org/10.31933/jemsi.v4i6.1615

Harahap, TK, Prayuti, Y., Latianingsih, N., Damanik, A., Maheni, T., Farida, I., & Muhtar, MH Mustaqim. (2023). *Introduction to legal science* . Publisher Tahta Media.

Muhtar, MH (2023). Definition and scope of legal theory. *In Basics of constitutional law theory: Perspectives and practices* . Sada Kurnia Pustaka.

Muhtar, MH, Tribakti, I., Salim, A., Tuhumury, HA, Ubaidillah, MH, Imran, SY, Laka, I., Hasiah, GMS, Iping, B., Amin, F., Amalia, M., Syamsiah, N., Riza, K., Widodo, MFS, & Churniawan, E. (2023). *Indonesian legal concept* . PT Global Executive Technology.

Pakaya, D., Dungga, WA, & Muhtar, MH (2024). Dynamics of online arisan (legal protection and manager responsibility in the case of Decision Number 1/Pdt.GS/2021/PN TRT). *SINERGI: Scientific Research Journal* , 1(12), 1307–1318. https://doi.org/10.62335/rafzke95

Pujayanti, LPVA, Nugrahayu, ZZ, Rahim, EI, Muhtar, MH, & Yassine, C. (2024). Indonesia's Constitutional Court: Bastion of law enforcement and protector of human rights in the reform era. *Journal of Speech: Scientific Journal of the University of Trunojoyo* , 17(1), 35–49. https://doi.org/10.21107/pamator.v17i1.24128

Puluhulawa, J., Muhtar, MH, Towadi, M., & Swarianata, V. (2023). The concept of cyber insurance as a loss guarantee on data protection hacking in Indonesia. *Law, State & Telecommunications Review/Journal of Law, State and Telecommunications* , 15(2).

Rahman, I., Muhtar, MH, Mongdong, NM, Setiawan, R., Setiawan, B., & Siburian, HK (2024). Harmonization of digital laws and adaptation strategies in Indonesia focusing on e-commerce and digital transactions. *Innovative: Journal of Social Science Research* , 4(1), 4314–4327.

Rohmy, AM, Suratman, T., & Nihayaty, AI (2021). ITE Law in the perspective of the development of information and communication technology. *Dakwatuna: Journal of Islamic Dakwah and Communication* , 7(2), 309. https://doi.org/10.54471/dakwatuna.v7i2.1202

Rusdiyanto, D., Siwi, DR, Fitriana, G., Fitri, A., & Jainah, ZO (2024). Fraud using internet media in the form of online buying and selling. *Iqtishaduna: Scientific Journal of Islamic Economic Law Students* , 277–285. https://doi.org/10.24252/iqtishaduna.vi.43808

Syarif, M., Ramadhani, R., Graha, MAW, Yanuaria, T., Muhtar, MH, Asmah, N., Syahril, MAF, Utami, RD, Rustan, A., Nasution, HS, Putera, A., Wilhelmus, K., & Jannah, M. (2024). *Legal research methods* . GET Press Indonesia.

Widodo, IS, Muhtar, MH, Suhariyanto, D., Permana, DY, Bariah, C., Widodo, MF S ., ... & Susmayanti, R. (2023). *Constitutional law* . Sada Kurnia Library.

Yanuaria, T., & Rongalaha, J. (2019). Implementation of IPTEKS Law Number 19 of 2016 concerning Electronic Information and Transactions. *Papua Community Service Journal*, 2(3). https://doi.org/10.31957/.v2i3.655