

LEGAL PROTECTION AGAINST THIRD PARTIES IN CIVIL AGREEMENTS IN THE ERA OF CONTRACT DIGITALIZATION

Rifa Jamaludin Nasir
Universitas Islam Negeri Salatiga, Indonesia
Rifa.jamaluddin@gmail.com

Abstract

The era of contract digitization has brought a major transformation in the practice of civil agreements, ranging from the use of electronic signatures, digital contract platforms, to blockchain-based smart contracts. This change not only affects the parties directly involved in the agreement, but also creates new dynamics regarding legal standing and protection for third parties. This article aims to analyze the forms, limits, and mechanisms of legal protection against third parties in digital civil agreements by integrating normative, comparative, and conceptual approaches. A study was conducted on the Civil Code, the Electronic Information and Transaction Law, regulations related to electronic signatures, and literature on smart contracts and digital contracting platforms. The results of the study show that contract digitization expands the potential for third-party involvement, both as third-party beneficiaries, parties harmed by contract violations, and parties whose data is processed in the digital ecosystem. However, Indonesia's positive legal framework still places third-party protection limited to classical concepts, so it is not fully responsive to technological risks such as *data leaks*, *automated enforcement*, and *algorithmic bias*. This article offers a model of strengthening third-party legal protection based on the principles of digital prudence, algorithmic transparency, and a functional expansion of *the principle of privity of contract*. Thus, the digitization of contracts can still take place efficiently without neglecting the rights and interests of third parties in modern civil transactions.

Keyword: Legal Protection; Civil Agreements; Contract Digitalization.

Introduction

Legal protection against third parties in civil agreements is a crucial aspect of the contract law system, especially in the era of increasingly rapid digitalization. Globalization and technological advancements have significantly changed the landscape of business transactions, with a dramatic increase in the use of digital

contracts(S. A. Hasan et al., 2024). According to data from the World Bank, more than 50% of the global population now has internet access, which has implications for the increasing potential for cross-border digital transactions(Kundu et al., 2024). In Indonesia, the growth of the digital economy reaches 11% per year, with the value of e-commerce transactions projected to reach \$130 billion by 2025(Destiani & Mufiidah, 2024). This digital transformation brings new challenges in the context of legal protection, especially for third parties who are not directly involved in the drafting of contracts but can be affected by their implementation(Sutherland, 2006).

The principle of privity of contract, which states that the contract is only binding on the parties who make it(Deakin et al., 1994), facing challenges in a digital context where the boundaries between contracting parties and third parties are becoming increasingly blurred(Chugh, 2023). Legal cases related to the protection of personal data and the responsibility of digital platforms to third-party users demonstrate the complexity of this problem(Anggraini & Wiraguna, 2025). Existing regulations, such as the Electronic Information and Transaction Law (UU ITE) No. 11 of 2008 jo. Law No. 19 of 2016, have not fully accommodated the dynamics of third-party protection in digital contracts. This creates legal uncertainty that can hinder innovation and growth in the digital economy.

Several previous studies have examined certain aspects of legal protection in digital contracts. A study by Petrov (2024) analyzed the validity of electronic signatures in online agreements (Petrov et al., 2024). Meanwhile, Thamrin's (2021) research highlights the challenges in applying conventional contract law to blockchain transactions (Thamrin et al., 2021). However, there is still a significant research gap, especially in the context of third-party protection. A comprehensive analysis of the legal implications of smart contracts on third parties, an evaluation of the effectiveness of consumer protection mechanisms in multi-stakeholder platforms, as well as a comparative study of regulatory approaches in various jurisdictions to third-party protection in digital contracts remain inadequately answered.

Given the urgency and complexity of this issue, in-depth research on "Legal Protection of Third Parties in Civil Agreements in the Era of Contract Digitalization" is highly relevant and important. This study aims to comprehensively analyze the existing legal framework, identify regulatory loopholes, and formulate recommendations for strengthening legal protection for third parties in the context of digital contracts. The results of this research are expected to make a significant contribution to the development of legal policies and practices that are more adaptive to the reality of contract digitalization, while maintaining a balance between technological innovation and legal protection for all parties involved, both directly and indirectly, in the digital contract ecosystem.

Research Method

This study uses a juridical-normative method with a statutory approach and a conceptual approach to examine legal protection for third parties in civil agreements made through a digital contract system. Analysis is carried out on the provisions of the Civil Code, the Electronic Information and Transaction Law and its amendments, as well as their derivative regulations that are relevant to the validity, validity, and legal consequences of electronic contracts. In addition, this study enriches the study by examining the doctrines of experts, the principles of contract law, and the theory of *third party protection* in modern contractual practices. To provide a more contextual empirical picture, this study uses a case approach through the analysis of court decisions related to electronic contract disputes and their implications for third parties. All data is then analyzed using descriptive-analytical techniques to build a comprehensive legal argument regarding the appropriate legal protection model in the current contract digitalization ecosystem.

Result and Discussion

Concepts, Principles, and Normative Basis for the Protection of Third Parties in Indonesian Civil Law

In the context of civil law, third parties have definitions that can be seen from two perspectives: the doctrine of civil law and the Civil Code (KUH Per). According to the doctrine of civil law, a third party is defined as a party who is not directly involved in a legal relationship or agreement. They are not the parties who made or signed the contract and have no rights and obligations arising from the agreement. Meanwhile, the Civil Code does not explicitly define a third party, but can be concluded from several articles. Article 1315 of the Civil Code implies a third party as a person who is not bound by an agreement, while Article 1340 of the Civil Code emphasizes that the agreement is only valid between the parties who make it. Characteristics of a third party include the absence of a direct interest in the agreement ([Kälin & Künzli, 2019](#)), cannot claim rights or be charged with obligations under the agreement, but can engage in the agreement through certain mechanisms such as assignment of rights (cessie). The concept of third parties is important in civil law to limit the impact of agreements, protect the interests of outside parties, and maintain justice and legal certainty in civil transactions ([Sutherland, 2006](#)).

The privity theory of contract is a doctrine in contract law that states that only the parties directly involved in the contract have rights and obligations under the contract([Sutherland, 2006](#)). In the context of Indonesian law, this principle is reflected in Article 1340 of the Civil Code (KUHPer) which states that the agreement only applies between the parties who make it. However, there are several exceptions to the principle of privity of contract in Indonesian law. One of the recognized exceptions is an agreement for a third party (*stipulatio alteri*), which is regulated in Article 1317 of the Criminal Code. This exception allows third parties to acquire rights from an agreement made by another party, even if they are not directly involved in the making of the agreement. Subrogation is another exception recognized in Indonesian law. Based on Article 1400 of the Criminal Code, a third party can replace the position of the creditor in an agreement([Zimmermann, 1996](#)). This allows for the transfer of rights and obligations to parties who were not previously involved in the original agreement.

Cessie, or assignment of receivables on behalf of the company, is also an exception to the principle of privity of contract([Samson, 2016](#)). Regulated in Article 613 of the Criminal Code, cessie allows a third party to become a new creditor in an agreement. Through this mechanism, the rights arising from the agreement can be transferred to the parties who were not involved in the creation of the original agreement([Samson, 2016](#)). In some cases, a default that is detrimental to a third party may also be an exception to the principle of privity of contract([Sutherland, 2006](#)). Although third parties are not parties to the agreement, in certain situations they may claim damages if they suffer losses due to a breach that occurs in the agreement. Collective agreements, such as collective bargaining agreements, are also an exception to the principle of privity of contract([Sutherland, 2006](#)). In this kind of agreement, the effect of the agreement may be binding on parties who are not directly involved in the making of the agreement, but belong to the group or category represented in the agreement. These exceptions indicate that Indonesian law recognizes certain situations in which the effect of an agreement may extend to a third party.

This reflects an attempt to strike a balance between the principle of privity of contract with the practical necessity and fairness of modern legal transactions([N. Hasan, 2012](#)). Developments in business practice and contract law have encouraged recognition of these exceptions. The complexity of modern transactions often involves more than two parties, and exceptions to the principle of privity of contract allow for the flexibility necessary in such situations. Despite these exceptions, the principle of privity of contract remains an important foundation in Indonesian contract law. The exceptions are applied carefully and in certain contexts to ensure legal certainty and protect the interests of the parties to the agreement([Outinen et al., 2021](#)). A deep understanding of the privity of contract theory and its exceptions is essential for legal practitioners,

business people, and the general public in Indonesia([Sutherland, 2006](#)). This helps in designing and executing effective agreements, as well as in resolving disputes that may arise related to the rights and obligations of the parties to an agreement.

Legal protection against third parties is an important aspect of the civil law system. The normative basis of this protection is reflected in the various provisions of the Civil Code (KUHPercivil) and the applicable legal principles. One of the main foundations is the concept of unlawful acts regulated in Article 1365 of the Civil Code, which states that every act that violates the law and brings harm to others obliges the person who caused the harm to compensate for the loss([Cortese, 2020](#)). Article 1366 of the Civil Code further expands this responsibility by stating that everyone is liable not only for losses caused by his actions, but also for losses caused by his negligence or lack of care. This confirms that protection against third parties includes not only adverse active actions, but also negligence that can cause losses([Jadidyah & Priyono, 2025](#)).

The principle of good faith, which is reflected in Article 1338 paragraph (3) of the Civil Code, also plays an important role in the protection of third parties. This principle obliges each party to an agreement to execute the agreement in good faith([Varbanova, 2023](#)). While it directly governs the relationship between the parties to the agreement, it also provides indirect protection to third parties by creating the standard of conduct expected in legal transactions. Article 1340 of the Civil Code emphasizes that an agreement is only valid between the parties who make it. However, Article 1317 of the Civil Code opens the possibility for third parties to obtain rights from an agreement through a promise for the benefit of third parties. It provides a legal basis for the protection of third parties in the context of a particular agreement.

In the context of property transactions, the protection of third parties in good faith is regulated in Article 1977 of the Civil Code([Molina & Preve, 2009](#)). This article states that for movable objects that are not in the form of interest or receivables that do not have to be paid to the bearer([Hutabarat, 2024](#)), then whoever controls it is considered the owner. This provides protection to third parties who acquire movable objects in good faith. Article 1977 paragraph (2) of the Civil Code further strengthens this protection by stating that a third party is not obliged to return goods that have been purchased in good faith from an unauthorized person, except in the event that the goods are lost or stolen. This provision provides legal certainty for third parties who transact in good faith.

In the context of corporate law, the protection of third parties is also reflected in the doctrine of ultra vires. Although not explicitly regulated in the Civil Code, this doctrine limits the actions of companies that exceed its authority and provides protection to

third parties who transact with companies in good faith. The principle of publicity in guarantee law also plays a role in protecting the interests of third parties. This principle requires an announcement to the public about the imposition of collateral on an object, so that a third party can find out the legal status of the object before making a transaction. Finally, the principle of *nemo plus juris transferre potest quam ipse habet* (no one can transfer rights beyond what he has) is also the basis for third-party protection. This principle limits the assignment of rights that may be detrimental to third parties and guarantees that any assignment of rights must be based on lawful ownership.

The Challenges of the Contract Digitalization Era for Third Parties

Conventional contracts have long been a cornerstone in business and legal transactions (Destiani & Mufiidah, 2024). However, along with the development of digital technology, there has been a significant shift towards electronic contracts or e-contracts (Destiani & Mufiidah, 2024). This change is driven by the need for efficiency, speed, and ease of conducting transactions in the digital era (Destiani & Mufiidah, 2024). E-contracts allow the parties involved to create, sign, and manage contracts online without the need to meet physically. This saves time, costs, and resources that would normally be required in a conventional contracting process. In addition, e-contracts also offer greater flexibility in terms of storage, filing, and access to contract documents.

The security and validity of e-contracts have also been improved through the use of technologies such as digital signatures and data encryption. This helps reduce the risk of counterfeiting and increases trust between the parties involved in the contract (Satybaldy et al., 2022). However, it should be noted that the regulations and laws governing e-contracts are still evolving in various countries (Chen et al., 2022). One of the main advantages of e-contracts is their ability to facilitate cross-border transactions more easily. This opens up new opportunities for global businesses and allows for wider collaboration between parties in different geographical locations. In addition, e-contracts also support more environmentally friendly business practices by reducing the use of paper (Judijanto et al., 2023). However, the transition from conventional to e-contracts also presents its own challenges. Issues such as data security, privacy, and regulatory differences between countries need to be addressed and addressed. Companies and individuals need to adapt to new technologies and understand the legal implications of using e-contracts (Szabo et al., 2024).

In the legal context, the recognition of e-contracts as a valid and binding document has been increasing in many jurisdictions (Douzinas, 2002). However, there is still a need for harmonization of international laws and standards governing the use of e-

contracts([Jejenywa et al., 2024](#)). This is important to ensure legal certainty and protect the interests of all parties involved. The development of blockchain technology has also begun to affect the evolution of e-contracts. Smart contracts, which are forms of e-contracts that can execute themselves under predetermined conditions, offer the potential to further increase efficiency and transparency in business transactions. Education and training on the use of e-contracts are becoming increasingly important as the technology is widely adopted. Companies, legal institutions, and educational institutions need to prepare human resources who understand the technical and legal aspects of e-contracts to optimize their benefits.

While e-contracts bring many advantages, it's important to remember that in some situations, conventional contracts may still be necessary or preferred. Therefore, the ability to manage and integrate these two forms of contracts will be a valuable skill in the future. Digital transactions are increasingly commonly used in various online transactions. However, the use of digital contracts also poses potential losses for third parties who are not directly involved in the agreement([Destiani & Mufiidah, 2024](#)). One of the main risks is the leakage or misuse of personal data collected through digital platforms. Sensitive information such as financial data or medical history can fall into the hands of unauthorized parties. Clickwrap agreements that are commonly used in online transactions also have the potential to harm consumers. Many users tend not to read the terms and conditions in detail before agreeing to them. This can result in consumers being tied to detrimental terms without them being fully aware. Digital platforms as intermediaries for transactions also pose their own risks. In the event of a security breach on the platform, the user's transaction data and personal information may be exposed. Additionally, reliance on digital platforms leaves users vulnerable to service interruptions or sudden shutdowns of platforms. The use of blockchain-based smart contracts also raises new potential losses. The code underlying such contracts may contain bugs or vulnerabilities that are exploited by irresponsible parties. This can result in financial losses for the parties involved as well as third parties. Jurisdictional issues and legal choices have also become more complex in cross-border digital contracts. An aggrieved third party may face difficulties in claiming damages in the event of a dispute, especially if it involves different jurisdictions. Digital contracts often contain arbitration clauses that limit consumers' right to bring class action lawsuits([Iryana & Mustofa, 2023](#)). This can reduce consumers' bargaining power and limit their access to justice in the event of a mass breach of contract. The use of technologies such as artificial intelligence in the drafting and execution of digital contracts also poses new risks([Destiani & Mufiidah, 2024](#)). Decisions made by automated systems may not always take into account the nuances of the situation or their impact on third parties. The lack of transparency in the algorithms used by digital platforms can result in indirect discrimination against certain groups. This has the

potential to harm third parties who do not have access or ability to make optimal use of digital services. Digital contracts also pose new challenges related to digital legacy ([Bondar et al., 2023](#)). Unclear status of a digital asset after the death of its owner can lead to disputes between the platform, heirs, and third parties who have an interest in the asset. Rapid technological developments often precede existing regulations. This legal vacuum can be exploited by irresponsible parties, while aggrieved third parties may not have adequate legal protections ([Chavali, 2024](#)). The shift from conventional contracts to e-contracts reflects a broader digital transformation in society and business. While there are still challenges to overcome, e-contracts offer great potential to improve efficiency, accessibility, and flexibility in legal and business transactions in the digital age. Existing regulations, such as the ITE Law, the Consumer Protection Law, and the Civil Code, have several limitations in providing adequate protection to third parties. One of the main limitations is the lack of a clear and comprehensive definition of third parties in the context of electronic transactions and consumer protection ([Pasaribu et al., 2025](#)). This can lead to confusion in the interpretation of the law and its application in certain cases.

The ITE Law, although it has regulated electronic transactions, still does not specifically regulate the responsibilities and rights of third parties in such transactions. These limitations can lead to legal loopholes that can be exploited by irresponsible parties, thus harming third parties involved in electronic transactions ([Anggraini & Wiraguna, 2025](#)). The Consumer Protection Law, on the other hand, focuses more on the relationship between consumers and business actors. However, these regulations do not comprehensively regulate the protection of third parties who may be involved in the distribution chain or transaction process. This can lead to difficulties for third parties to obtain adequate legal protection in the event of a dispute or loss.

The Civil Code, as the basis of civil law in Indonesia, has limitations in accommodating technological developments and the complexity of modern transactions ([Chugh, 2023](#)). Some provisions in the Civil Code may no longer be relevant or difficult to apply in the context of electronic transactions and third-party protection in the digital era. Another limitation that needs to be considered is the lack of harmonization between the three regulations. Although each regulation has a different purpose and scope, there is still potential for overlap or even contradiction in their implementation, especially when it comes to third-party protection.

In addition, law enforcement and implementation of these regulations also still face challenges. Lack of legal understanding and awareness in the community, as well as limited resources and infrastructure in law enforcement, can complicate efforts to protect third parties. Regulatory limitations are also seen in terms of data protection

and third-party privacy([Budiono et al., 2024](#)). Although the ITE Law has regulated the protection of personal data, there are still loopholes in the data protection of third parties that may be involved in a transaction or business process([Pasaribu et al., 2025](#)). In the context of cross-border transactions, existing regulations also have limitations in regulating and protecting third parties outside Indonesia's jurisdiction. This can cause difficulties in dispute resolution and law enforcement when problems arise involving third parties from other countries. Another limitation that needs to be considered is the lack of regulatory flexibility in accommodating technological developments and new business models. As technology and innovation rapidly develop in the business world, existing regulations may not be able to keep up with these changes quickly, creating gaps in third-party protection([Adelakun et al., 2024](#)).

Legal Protection Models and Mechanisms for Third Parties

Preventive protection efforts are an important step in maintaining the security and integrity of the system. The obligation of information transparency is the main foundation in this effort. Companies and organizations are required to be open about their data management policies, procedures, and practices([Destiani & Mufiidah, 2024](#)). This transparency allows users and stakeholders to understand how their information is managed and used. Notification mechanisms are the next key component in preventive protection. This system ensures that users and related parties are immediately notified in the event of a security breach or unauthorized access to their data. Fast and accurate notifications enable timely responsive action, minimizing potential data loss or misuse. Due diligence, or due diligence, is a thorough process of evaluating risks and potential issues before entering into a transaction or business partnership([S. A. Hasan et al., 2024](#)).

In the context of data protection, due diligence involves a thorough examination of the security and privacy practices of business partners, vendors, or third parties who have access to sensitive data. Implementation of information transparency obligations requires clear and accessible policies([Destiani & Mufiidah, 2024](#)). Companies must provide comprehensive information about how data is collected, stored, and used. This includes an explanation of the purpose for which the data was collected, who had access, and the security measures in place. An effective notification mechanism should include clear protocols for identifying, assessing, and reporting security incidents. This involves the establishment of a well-trained incident response team, sophisticated detection systems, and fast and secure communication channels to relay information to affected parties. The due diligence process in the context of data security involves an in-depth evaluation of the cybersecurity practices of potential partners([Maurer, 2005](#)). This includes security policy checks, regulatory compliance audits, and technology

infrastructure assessments. The goal is to ensure that all parties involved in data management meet the necessary security standards.

Information transparency also includes educating users about their rights regarding personal data([Destiani & Mufiidah, 2024](#)). This includes the right to access, correct, and delete data, as well as the right to object to the use of certain data. The Company must provide an easily accessible mechanism for users to exercise these rights. The notification mechanism should be equipped with a comprehensive response plan. This plan should include measures to address breaches, minimize impacts, and restore user trust. This may involve working with law enforcement authorities, cybersecurity service providers, and crisis communication experts. Due diligence also involves ongoing monitoring of business partners' security practices. This is not just a one-time process, but an ongoing evaluation to ensure consistent compliance with agreed safety standards. Companies must be prepared to terminate relationships with partners who fail to maintain the necessary security standards.

These preventive protection efforts must continue to be evaluated and updated in line with technological developments and new security threats. Companies must invest in ongoing research and development, participate in industry forums, and collaborate with security experts to stay ahead of the evolving data security challenges. Repressive efforts in the context of third-party lawsuits through instruments of unlawful acts or the responsibility of business actors/digital platforms are legal steps that can be taken to demand accountability for the losses experienced. This instrument is becoming important in the digital era, where transactions and interactions are increasingly taking place through online platforms([Anggraini & Wiraguna, 2025](#)). Unlawful acts, as stipulated in Article 1365 of the Civil Code, are the legal basis for third parties to file lawsuits. In the digital context, unlawful acts can include various actions such as the spread of false information, privacy violations, or failure to keep user data safe([Jadidyah & Priyono, 2025](#)). Third parties who feel aggrieved can use this instrument to claim damages. The responsibility of business actors or digital platforms is also the focus of this repressive effort. The Consumer Protection Law and regulations related to e-commerce require business actors to be responsible for the products or services they offer. This includes the obligation to provide accurate information, ensure the security of transactions, and handle consumer complaints properly([Destiani & Mufiidah, 2024](#)). In the case of digital platforms, the responsibility can extend to the management of the content uploaded by the user. Digital platforms have an obligation to ensure that the content circulating on their platform does not violate the law or harm other parties([Anggraini & Wiraguna, 2025](#)). Failure to do so may be grounds for a third party to file a lawsuit. The process of filing a lawsuit in this repressive effort generally begins with the collection of evidence that shows the existence of losses and the causal

relationship between the losses and the actions of business actors or digital platforms. This evidence can be in the form of electronic documents, transaction records, or the testimony of the parties involved. Furthermore, a third party can file a lawsuit with the competent court. In the lawsuit, the third party must be able to clearly explain the unlawful acts committed by business actors or digital platforms, as well as the losses experienced as a result of these acts. The lawsuit must also include the desired claim for damages([Bondar et al., 2023](#)). The court will then examine the lawsuit and provide an opportunity for the defendant (business actor or digital platform) to provide a response. The process of examining the case will involve evidence from both sides, where each side will present arguments and evidence that supports its position([Çetin & Eymur, 2017](#)). If the lawsuit is proven, the court can issue a judgment that requires business actors or digital platforms to provide compensation to third parties. This compensation can be in the form of compensation for material, immaterial, or even an obligation to take certain actions to restore the situation. Repressive efforts through instruments of unlawful acts or responsibility of business actors/digital platforms not only function as a means to obtain compensation, but also as a control mechanism for the behavior of business actors and digital platforms. This can encourage the creation of a safer and more responsible digital environment. However, keep in mind that the litigation process is often time-consuming and costly([Othman, 2007](#)). Therefore, this repressive effort should be used as a last resort after peaceful settlement efforts have not been successful. Third parties are advised to first try to resolve the issue through a complaint mechanism provided by the business actor or digital platform, or through mediation before deciding to file a lawsuit in court([Wellhausen, 2019](#)). Strengthening regulations related to electronic contracts needs to be carried out to accommodate technological developments and digital business practices. The revision of the Electronic Information and Transactions Act and its derivative regulations is needed to provide a more comprehensive legal framework regarding the validity and validity of electronic contracts, including provisions regarding electronic signatures, electronic seals, and timestamps([Sowmiya et al., 2021](#)). This will provide better legal certainty for the parties involved in digital contracts. The need for special arrangements regarding the protection of personal data in the context of electronic contracts. Strong regulations regarding data privacy and security will protect the interests of third parties who may be involved or affected by the performance of digital contracts. Regulations regarding the obligations of the parties to maintain the confidentiality of sensitive information as well as sanctions for violations of these provisions need to be clearly formulated. Jurisprudence related to electronic contract disputes needs to be enriched to provide guidance for judges in handling similar cases in the future. Court decisions that address aspects such as electronic proof, interpretation of digital contract clauses, and jurisdictional determination in cross-border disputes will help create legal certainty. It is also important to systematically document and publish these decisions. Strengthening

the capacity of law enforcement officials, including judges, prosecutors, and investigators, in understanding technical and legal aspects related to electronic contracts. Specialized training and certifications can be provided to enhance competence in handling cases involving digital evidence and electronic transactions. This will help ensure a fair and effective judicial process. Harmonization of national regulations with international standards related to electronic contracts needs to be carried out([Blackaby et al., 2015](#)). Adopting the principles of the UNCITRAL Model Law on Electronic Commerce or other international conventions can help create legal alignment, especially in the context of cross-border transactions. This will provide better protection for third parties who may be in different jurisdictions([Igbinenikaro & Adewusi, 2024](#)). Development of technological infrastructure that supports the security and integrity of electronic contracts. Governments need to encourage the adoption of technologies such as blockchain or distributed ledger to increase transparency and reduce the risk of digital document forgery. Regulations that support the use of such technology in a legal context also need to be formulated([Cortés, 2010](#)). Strengthening alternative dispute resolution mechanisms in accordance with the characteristics of digital transactions. The development of a legally recognized online dispute resolution (ODR) platform can provide easier and more efficient access for parties, including third parties, to resolve disputes related to electronic contracts. Regulations that govern the procedures and legal force of ODR decisions need to be established([Ortolani, 2015](#)). Increasing digital and legal literacy in the community related to electronic contracts. Public education programs need to be carried out to increase public understanding of the rights and obligations in digital transactions, as well as the risks and legal protections available([Barnett & Treleaven, 2017](#)). This will help prevent disputes and protect the interests of third parties who may lack understanding of the legal implications of digital transactions. Arrangements regarding the responsibilities of platform providers or intermediaries in the context of electronic contracts. Clarity on the roles and limitations of the responsibilities of parties facilitating digital transactions will help protect the interests of third parties. Regulations can regulate due diligence obligations, data storage, and cooperation with law enforcement for service providers. Regular regulatory evaluations and updates to keep up with technological developments([Bueno & Kaufmann, 2021](#)). The establishment of a dedicated team of legal, technological, and relevant stakeholders to conduct regular regulatory reviews will help ensure the legal framework remains relevant. An effective public consultation mechanism also needs to be held to accommodate input from various parties, including representatives of third-party interests, in the regulatory reform process.

Conclusion

The concept of third parties in Indonesian civil law, although rooted in the principle of *privity of contract*, has expanded through various exceptions such as *stipulatio alteri*, subrogation, and cessie to address the complexity of modern transactions. Legal protection against third parties is emphasized through provisions on unlawful acts, the principle of good faith, the principle of publicity, and doctrines that guarantee certainty and justice for outsiders who are harmed by a legal relationship. However, the transformation towards digital contracts presents new challenges in the form of the risk of data leakage, inequality of bargaining positions, regulatory loopholes, and regulatory disharmony involving the ITE Law, the Consumer Protection Law, and the Civil Code. Therefore, more adaptive regulatory updates to technology, improved information transparency standards, strengthening notification and *due diligence* mechanisms, and affirming the responsibility of digital platforms are needed to ensure that third-party protection remains effective in the digital era. The implications of these findings confirm that without regulatory harmonization and institutional capacity strengthening, third-party protection has the potential to become weaker, so key recommendations include the establishment of an integrated legal framework for data protection and electronic transactions, increasing digital contract literacy for the public, and stricter law enforcement against business actors or digital platforms that neglect their protection obligations.

References

- Adelakun, B., Bakare, S., Akpuokwe, C., Nembe, J., & Oguejiofor, B. (2024). Legal Frameworks And Tax Compliance In The Digital Economy: A Finance Perspective. *Engineering Science & Technology Journal*, 5(3), 844–853. <https://doi.org/10.51594/estj.v5i3.922>
- Anggraini, N., & Wiraguna, S. (2025). Tanggung Jawab Hukum Platform Pinjaman Online terhadap Penyalahgunaan dan Penyebaran Data Pribadi Konsumen secara Ilegal. *Risoma: Jurnal Riset Sosial Humaniora Dan Pendidikan*, 3(3), 144–167. <https://doi.org/10.62383/risoma.v3i3.767>
- Barnett, J., & Treleaven, P. (2017). Algorithmic Dispute Resolution—The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies. *The Computer Journal*, 61(3), 399–408. <https://doi.org/10.1093/comjnl/bxx103>

- Blackaby, N., Hunter, M., Redfern, A., & Partasides, C. (2015). *Redfern and Hunter on International Arbitration*. Oxford University.
<https://doi.org/10.1093/law/9780198714248.001.0001>
- Bondar, A., Solcan, C., Horodincu, L., & Solcan, G. (2023). Use of Spirulina platensis and Curcuma longa as Nutraceuticals in Poultry. *Agriculture*, 13(8), 1553.
<https://doi.org/10.3390/agriculture13081553>
- Budiono, A., Ngestiningrum, A., & Utami, R. (2024). Juridical Review of Legal Relationships of the Parties in Digital Marketplace Transactions (Study on Tiktok Marketplace). *International Journal of Law and Policy*, 2(5), 16–27.
<https://doi.org/10.59022/ijlp.190>
- Bueno, N., & Kaufmann, C. (2021). The Swiss Human Rights Due Diligence Legislation: Between Law and Politics. *Business and Human Rights Journal*, 6(3), 542–549.
<https://doi.org/10.1017/bhj.2021.42>
- Çetin, P. S., & Eymur, G. (2017). Developing Students' Scientific Writing and Presentation Skills through Argument Driven Inquiry: An Exploratory Study. *Journal of Chemical Education*, 94(7), 837–843. <https://doi.org/10.1021/acs.jchemed.6b00915>
- Chavali, D. P. (2024). Decentralized Intestacy Distribution: Exploring Autonomous Systems Leveraging Blockchain Technology. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, 08(04), 1–5.
<https://doi.org/10.55041/ijsem31543>
- Chen, H., Li, F., Guo, T., Luo, Z., Zhao, H., Chen, W., Yang, K., Hu, H., Qie, Y., Lin, L., Sun, B., & Pan, Y. (2022). Dynamic Anti-Counterfeiting Labels with Enhanced Multi-Level Information Encryption. *ACS Applied Materials & Interfaces*, 15(1), 2104–2111.
<https://doi.org/10.1021/acsami.2c17870>
- Chugh, U. (2023). The Evolution of Privacy Laws in the Digital Age: Challenges and Solutions. *Indian Journal of Law*, 1(1), 51–60. <https://doi.org/10.36676/ijl.2023-v1i1-07>
- Cortés, P. (2010). *Online Dispute Resolution for Consumers in the European Union*. Routledge. <https://doi.org/10.4324/9780203847756>
- Cortese, F. (2020). *The Liability of Public Administration* (pp. 61–65). Oxford University Pressoxford. <https://doi.org/10.1093/oso/9780198867555.003.0008>

Deakin, S., Lane, C., & Wilkinson, F. (1994). "Trust" or Law? Towards an Integrated Theory of Contractual Relations between Firms. *Journal of Law and Society*, 21(3), 329. <https://doi.org/10.2307/1410739>

Destiani, R. D., & Mufiidah, A. N. (2024). Era Baru Ekonomi Digital: Studi Komprehensif tentang Teknologi dan Pasar. *ADI Bisnis Digital Interdisiplin Jurnal*, 5(1), 47–50. <https://doi.org/10.34306/abdi.v5i1.1095>

Douzinas, C. (2002). Identity, Recognition, Rights or What Can Hegel Teach Us About Human Rights? *Journal of Law and Society*, 29(3), 379–405. <https://doi.org/10.1111/1467-6478.00225>

Hasan, N. (2012). Islamist Party, Electoral Politics and Dakwah Mobilization Among Youth: The Prosperous Justice Party (PKS) in Indonesia. *Journal of Indonesian Islam*, 6(1), 17. <https://doi.org/10.15642/jiis.2012.6.1.17-47>

Hasan, S. A., Al-Zahra, W. N., Maharani, D. A., Auralia, A. S., & Hidayatullah, R. (2024). Implementasi Teknologi Blockchain dalam Pengamanan Sistem Keuangan pada Perguruan Tinggi. *Jurnal Mentari: Manajemen, Pendidikan Dan Teknologi Informasi*, 3(1), 11–18. <https://doi.org/10.33050/mentari.v3i1.546>

Hutabarat, L. E. (2024). Analysis of the Internal Control System for Receivables at CV. Putra Riau Mandiri. *Luxury: Landscape of Business Administration*, 2(1), 1–25. <https://doi.org/10.61230/luxury.v2i1.65>

Igbinenikaro, E., & Adewusi, A. (2024). Developing International Policy Guidelines For Managing Cross-Border Insolvencies In The Digital Economy. *International Journal of Management & Entrepreneurship Research*, 6(4), 1034–1048. <https://doi.org/10.51594/ijmer.v6i4.983>

Iryana, W., & Mustofa, M. B. (2023). May 1998 Mass Riots in Jakarta: A Holistic and Contextual Analysis of Critical Political Communication. *Paramita: Historical Studies Journal*, 33(2). <https://doi.org/10.15294/paramita.v33i2.38022>

Jadidyah, H., & Priyono, E. A. (2025). Kajian Yuridis Terhadap Pembatalan Akta Hibah Akibat Penghibah Jatuh Miskin. *Legal Standing: Jurnal Ilmu Hukum*, 9(2), 522–531. <https://doi.org/10.24269/lis.v9i2.11710>

Jejenywa, T., Mhlongo, N., & Jejenywa, T. (2024). Conceptualizing e-Government Initiatives: Lessons Learned From Africa-Us Collaborations in Digital Governance.

International Journal of Applied Research in Social Sciences, 6(4), 759–769.
<https://doi.org/10.51594/ijarss.v6i4.1066>

Judijanto, L., Hasyim, D. M., Anurogo, D., Zani, B. N., & Ningsih, K. P. (2023). Implementation of Telemedicine in Health Services: Challenges and Opportunities. *Journal of World Future Medicine, Health and Nursing*, 2(1), 37–50.
<https://doi.org/10.70177/health.v2i1.667>

Kälin, W., & Künzli, J. (2019). *The Law of International Human Rights Protection*. Oxford University. <https://doi.org/10.1093/law/9780198825685.001.0001>

Kundu, S., Rayhan, Z., Rahman, M. A., Debi, K. R., & Faruq, O. (2024). E-commerce development in Bangladesh: marketing improvement based personalized recommendation service. *Информатика. Экономика. Управление - Informatics. Economics. Management*, 3(4), 0218–0240. <https://doi.org/10.47813/2782-5280-2024-3-4-0218-0240>

Maurer, B. (2005). Due Diligence and “Reasonable Man,” Offshore. *Cultural Anthropology*, 20(4), 474–505. <https://doi.org/10.1525/can.2005.20.4.474>

Molina, C. A., & Preve, L. A. (2009). Trade Receivables Policy of Distressed Firms and Its Effect on the Costs of Financial Distress. *Financial Management*, 38(3), 663–686.
<https://doi.org/10.1111/j.1755-053x.2009.01051.x>

Ortolani, P. (2015). Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin. *Oxford Journal of Legal Studies*, 36(3), 595–629. <https://doi.org/10.1093/ojls/gqv036>

Othman, A. (2007). “And Amicable Settlement Is Best”: Sulh and Dispute Resolution in Islamic Law. *Arab Law Quarterly*, 21(1), 64–90. <https://doi.org/10.1163/026805507x197857>

Outinen, O., Bailey, S. A., Broeg, K., Chasse, J., Clarke, S., Daigle, R. M., Gollasch, S., Kakkonen, J. E., Lehtiniemi, M., Normant-Sarembe, M., Ogilvie, D., & Viard, F. (2021). Exceptions and exemptions under the ballast water management convention – Sustainable alternatives for ballast water management? *Journal of Environmental Management*, 293, 112823. <https://doi.org/10.1016/j.jenvman.2021.112823>

Pasaribu, A. S., Taun, T., Saputra, M., & Prayogo, I. (2025). Analisis Yuridis Perbedaan Kritik Dengan Pencemaran Nama Baik Dalam Kuhp Dan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik (ITE). *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 4(2), 220–232. <https://doi.org/10.55606/jurrish.v3i2.4748>

- Petrov, V., Dubois, X., & Anugrah, R. (2024). Transformasi Sosial: Perubahan Kehidupan Masyarakat melalui Penyebaran Jaringan Komputer. *ADI Pengabdian Kepada Masyarakat*, 4(2), 50–56. <https://doi.org/10.34306/adimas.v4i2.1093>
- Samson, C. (2016). Canada's Strategy of Dispossession: Aboriginal Land and Rights Cessions in Comprehensive Land Claims. *Canadian Journal of Law and Society / Revue Canadienne Droit et Société*, 31(01), 87–110. <https://doi.org/10.1017/cls.2016.2>
- Satybaldy, A., Subedi, A., & Nowostawski, M. (2022). A Framework for Online Document Verification Using Self-Sovereign Identity Technology. *Sensors (Basel, Switzerland)*, 22(21), 8408. <https://doi.org/10.3390/s22218408>
- Sowmiya, B., Ramana, K., Poovammal, E., Singh, S., & Yoon, B. (2021). Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server. *IEEE Access*, 9, 138245–138253. <https://doi.org/10.1109/access.2021.3115238>
- Sutherland, P. (2006). *Third-Party Contracts* (pp. 203–229). Edinburgh University. <https://doi.org/10.3366/edinburgh/9780748624256.003.0008>
- Szabo, J., Philip, L., & Bernard, C. (2024). Legal Implications and Challenges of Blockchain Technology and Smart Contracts. *Computer Life*, 12(2), 6–10. <https://doi.org/10.54097/ztn2w848>
- Thamrin, R. M., Zelina, K., Faturahman, A., Khoirunisa, A., & Harahap, E. P. (2021). Blockchain-based Land Certificate Management in Indonesia. *ADI Journal on Recent Innovation (AJRI)*, 2(2), 232–252. <https://doi.org/10.34306/ajri.v2i2.339>
- Varbanova, G. (2023). Legal Nature of Smart Contracts: Contract or Program Code? *Journal of Digital Technologies and Law*, 1(4), 1028–1041. <https://doi.org/10.21202/jdtl.2023.44>
- Wellhausen, R. L. (2019). International Investment Law and Foreign Direct Reinvestment. *International Organization*, 73(4), 839–858. <https://doi.org/10.1017/s0020818319000225>
- Zimmermann, R. (1996). *The Law of Obligations Roman Foundations of the Civilian Tradition*. Oxford University. <https://doi.org/10.1093/acprof:oso/9780198764267.001.0001>