

Legal Certainty of Biometric-Based Electronic Contracts under Indonesian Contract Law

Rahmawati Sabila¹, Wiwin Widiyaningsih², Zuraidah³

¹Faculty of Law, Majalengka University, Indonesia. E-mail: rahmawati.sabila2@gmail.com

²Faculty of Law, Majalengka University, Indonesia. E-mail: wiwin@unma.ac.id

³Faculty of Law, Majalengka University, Indonesia. E-mail: zuraidah@unma.ac.id

Abstract: The development of information technology has encouraged the extensive use of electronic contracts, including the application of biometric methods as mechanisms for authentication and consent. Although biometrics provide efficiency and enhanced security, their use in electronic contracts raises legal issues concerning contractual validity and legal certainty. This study aims to analyze the legal certainty of biometric-based electronic contracts in relation to Article 1320 of the Indonesian Civil Code and the Law on Information and Electronic Transactions (ITE Law). This research employs a normative legal research method using statutory and conceptual approaches, supported by library-based analysis of relevant legal materials. The findings indicate that biometric-based electronic contracts may, in principle, be considered legally valid provided that the legal requirements for a valid contract particularly mutual consent are fulfilled. However, legal certainty remains limited due to the absence of explicit regulation governing the legal status of biometrics as a form of electronic authentication or electronic signature, as well as challenges related to the protection of biometric data as sensitive personal data. This study contributes by identifying normative gaps in the regulation of biometric authentication and proposing regulatory harmonization to enhance legal certainty and personal data protection

Keywords: Article 1320 Civil Code, Biometrics, Electronic Contract, Legal Certainty

1. Introduction

The development of information and communication technology has brought significant changes to various aspects of society, including in the field of contract law. Transactions that were previously conducted conventionally have now shifted to digital form through electronic contracts (*e-contracts*). Electronic contracts offer convenience, efficiency, and speed in the process of forming agreements, especially in electronic commerce (*e-commerce*) activities. However, this progress has also given rise to new legal issues, particularly those related to legal certainty and the protection of the parties involved.¹

One of the main issues in electronic contracts is the aspect of validity and proof of identity of the parties. In practice, electronic contracts often use digital authentication methods, one of which is through biometric technology, such as fingerprints, facial recognition, or iris scanning.² Biometric methods are considered to have a higher level of security than conventional signatures or ordinary electronic signatures, because biometric characteristics are unique and inherent to a particular individual. Nevertheless, the use of

¹ Wahyu Taufiq and Abdul Aziz, "Analisis Yuridis Penggunaan Blockchain Technology Dalam Penerapan E-Residency" 1, no. 1 (2025): 1–16.

² Rian Rambu Raya et al., "Urgensi Perancangan Kontrak Elektronik Dalam Menjamin Kepastian Hukum Transaksi E-Commerce The Urgency Of Designing Electronic Contracts To Ensure Legal Certainty Of E-Commerce Transactions In Indonesia," 2025, 18173–83.

biometric methods in electronic contracts still raises debates from a civil law perspective, particularly in relation to the fulfillment of the requirements for a valid agreement.³

The development of information and communication technology in Indonesia has experienced rapid growth in line with the increasing use of the internet, digital financial services, and electronic trading platforms.⁴ This digitalization has driven changes in legal relationships within society, particularly in the area of agreements, which are now often conducted through electronic contracts (*e-contracts*). Electronic contracts have become common practice in various sectors in Indonesia, such as digital banking, fintech, marketplaces, online transportation services, and electronic-based government administration. This phenomenon shows that electronic contracts are no longer just an alternative, but have become a necessity in national legal and economic activities.

In practice in Indonesia, the use of biometric authentication methods in electronic contracts is becoming increasingly widespread. Various financial institutions, financial technology (fintech) service providers, and digital platforms have implemented biometric verification, such as face recognition and fingerprint scanning, for account registration, digital credit agreement approval, and electronic document signing. The application of biometrics is considered capable of increasing transaction security and preventing identity fraud. However, this phenomenon also raises legal issues, especially when disputes arise regarding the validity of contracts or repudiation by one of the parties to an agreement made electronically.⁵

Previous studies have extensively discussed the validity of electronic contracts and electronic signatures from the perspective of civil law and the Electronic Information and Transactions Law (ITE Law). For example, Sutedi (2019) analyzes the legal validity of electronic contracts in Indonesia and concludes that electronic contracts are legally binding as long as they fulfill the requirements stipulated in Article 1320 of the Civil Code, namely consent, legal capacity, a certain subject matter, and a lawful cause, as well as the formal requirements under the ITE Law. Similarly, Sjahdeini (2020) emphasizes that electronic contracts are recognized under Indonesian law, particularly when electronic signatures are used in accordance with Article 11 of the ITE Law.

Furthermore, Hutabarat (2021) examines the evidentiary strength of electronic signatures and highlights that electronic signatures based on digital certificates issued by certified electronic certification providers offer strong legal certainty. Other studies, such as Pratama and Wijaya (2022), focus on the use of one-time passwords (OTP) as a form of electronic authentication and conclude that OTP-based verification can serve as valid evidence of consent, provided that it is supported by reliable electronic systems.

However, despite the growing discussion on electronic contracts and electronic signatures, most existing studies remain limited to conventional electronic signature mechanisms, such as digital certificates and OTP-based authentication. Very few studies specifically address the use of biometric methods such as fingerprints, facial recognition, or iris scanning as a means of expressing and proving consent in electronic contracts. In particular, prior research has not comprehensively analyzed whether biometric-based consent satisfies the element of “agreement” under Article 1320 of the Civil Code, nor how

³ Lompoh Egia Et Al., “Keabsahan Perjanjian Arisan Online Ditinjau Dari Pasal 1320 Kitab Undang-Undang Hukum Perdata Universitas Pendidikan Ganesha E-Journal Komunikasi Yustisia Universitas Pendidikan Ganesha” 5, No. November (2022): 47–57.

⁴ Yudistira Kusuma Wardana, “Analisis Aspek Hukum Dan Implikasi Kontrak Elektronik Dalam Perjanjian Bisnis” 1, no. 1 (2023): 776–86.

⁵ Reghina Miftahuljannah Hambali, Mutya Cherawaty Thalib, and Nurul Fazri Elfikri, “Pembatalan Dalam Perjanjian Jual Beli : Telaah Pasal 1320 KUHPPerdata Dan Putusan Pengadilan” 1, no. 3 (2025): 838–45.

such methods align with the legal framework of the ITE Law regarding electronic signatures and electronic evidence.

This limitation indicates a clear research gap concerning the legal certainty of electronic contracts that utilize biometric technology. Given the increasing adoption of biometric authentication in digital transactions, there is a pressing need for a normative legal analysis that examines the compatibility of biometric methods with the requirements of Article 1320 of the Civil Code and the provisions of the ITE Law. Therefore, this research seeks to fill that gap by analyzing the extent to which biometric methods can provide legal certainty in electronic contracts under Indonesian law.

Based on these conditions, this study aims to analyze the legal certainty of electronic contracts using biometric methods in relation to the provisions of Article 1320 of the Civil Code and the ITE Law. This study is expected to explain whether the use of biometrics in electronic contracts has fulfilled the requirements for a valid agreement and how it stands in the Indonesian legal system. The scientific value and uniqueness of this article lies in its focus on biometric technology as a method of authenticating electronic contracts, which is still relatively rarely discussed comprehensively, so it is expected to contribute theoretically and practically to the development of civil law and information technology law in Indonesia.

2. Method

This study uses a normative legal research method (doctrinal research) that focuses on examining positive legal norms and relevant legal principles. This method was chosen because the study aims to analyze the legal certainty of electronic contracts using biometric methods based on Article 1320 of the Civil Code and the Electronic Information and Transactions Law, without examining empirical aspects. The approaches used include a legislative approach and a conceptual approach. The legislative approach was carried out by examining the Civil Code, the ITE Law, and related regulations, while the conceptual approach was used to examine the concepts of agreement, competence, evidence, and legal certainty in biometric-based electronic contracts.

The legal materials consist of primary, secondary, and tertiary legal materials collected through literature studies. The analysis of legal materials was conducted qualitatively using prescriptive and argumentative methods to formulate conclusions regarding the legal certainty of the use of biometrics in electronic contracts..

3. Results and Discussion

3.1 The Position of Electronic Contracts with Biometric Methods in Indonesian Contract Law

The results of the study show that electronic contracts using biometric methods can normatively be considered valid and binding agreements under the Indonesian civil law system. This is in line with the principle of consensualism, which affirms that an agreement is formed upon the parties reaching an agreement, without requiring a specific formal form, unless otherwise specified by law. In this context, electronic contracts including those using biometric authentication still fulfill the principle of consensualism as long as there is consensus ad idem between the parties.⁶ Biometric methods serve as a technological means

⁶ Undang Nomer, Tahun Tentang, and Informasi Dan, "E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha Program Studi Ilmu Hukum (Volume 4 Nomor 2 Agustus 2021) e-Journal Komunitas Yustisia Universitas Pendidikan Ganesha Program Studi Ilmu Hukum (Volume 4 Nomor 2 Agustus 2021)" 4 (2021): 617–25.

to express and confirm the will of the parties in the digital space. Authentication through fingerprints or facial recognition can be viewed as a modern form of expression of intent, which is essentially no different from a conventional signature. Thus, from the perspective of the principle of consensualism, the use of biometrics does not change the nature of the agreement, but only changes the medium of conveying consent.⁷

In addition to the principle of consensualism, the existence of biometric electronic contracts must also be analyzed within the framework of the principle of freedom of contract, which gives the parties the authority to determine the content, form, and manner of making agreements as long as they do not conflict with the law, morality, and public order. The use of biometric methods as a means of authentication is essentially a manifestation of the parties' freedom to choose the most efficient and secure mechanism for forming an agreement. Therefore, in theory, there is no legal prohibition for the parties to agree on the use of biometrics in electronic contracts.⁸

However, the application of the principle of freedom of contract in biometric electronic contracts cannot be separated from the reality of practice in Indonesia, where most electronic contracts are in the form of standard contracts prepared unilaterally by electronic system operators. In this situation, freedom of contract tends to be illusory, because users do not have a real opportunity to negotiate the content of the agreement or the authentication method used. The use of biometrics in standard contracts has the potential to strengthen the dominance of business actors and weaken the position of consumers, raising questions about the fulfillment of free will as an essential condition of the agreement.⁹

Furthermore, although the principles of consensualism and freedom of contract provide theoretical legitimacy for biometric electronic contracts, the absence of explicit regulations regarding the status of biometrics in legislation creates legal uncertainty. Normatively, biometrics have not been explicitly positioned as a form of electronic signature, but rather as a means of authentication in electronic systems. As a result, in the event of a dispute, the assessment of the validity and evidentiary value of biometric electronic contracts is highly dependent on the interpretation of the judge, which has the potential to result in inconsistent decisions.

In this context, the principle of good faith plays a central role in assessing the validity and appropriateness of biometric electronic contracts. This principle requires the parties to act honestly, openly, and not abuse technological advantages in the process of forming and implementing agreements. The use of biometrics without adequate explanation of its functions, risks, and legal consequences may be considered contrary to good faith, as it has the potential to mislead or harm other parties. Thus, good faith serves as a normative instrument for assessing whether consent given through biometrics truly reflects the free will of the parties.¹⁰

From a consumer protection perspective, the use of biometrics should not only be viewed as a tool for efficiency and security, but should also guarantee consumers' rights to convenience, security, and safety in transactions. If biometric data is misused or managed irresponsibly, consumers could potentially suffer serious and irreparable losses. Therefore,

⁷ Mulan Kasisty Anami et al., "Analisis Hukum Perdata Pada Perlindungan Hukum Bagi Para Pihak Dalam Kontrak Digital : Studi Kasus Sengketa Saldo DANA" 2, no. 5 (2025): 338–44.

⁸ Monika Esterina Situmorang and Abdul Salam, "Lex Patrimonium Analisis Aspek Hukum Kontrak Pintar Dalam Transaksi Kebendaan Digital : Tantangan Anonimitas Dan Peran Identitas Digital Analisis Aspek Hukum Kontrak Pintar Dalam Transaksi Kebendaan Digital : Tantangan Anonimitas Dan Peran Identitas Digital" 4, no. 1 (2025).

⁹ R Oetomo Hermawan, Huala Adolf, and Edy Santoso, "Kajian Hukum Penerapan Pasal Dalam Kontrak Elektronik" 5, no. 2 (2024): 141–64.

¹⁰ Muhammad Kandriana, Sri Atika, and Muhammad Wildan, "Unes Law Review" 8, no. 1 (2025): 221–28.

the principle of consumer protection reinforces the argument that the legal certainty of biometric electronic contracts is not only determined by the validity of the agreement, but also by the existence of effective legal protection for the weaker party. Based on the principles of consensualism, freedom of contract, good faith, and consumer protection, it can be concluded that electronic contracts using biometric methods are theoretically valid and acceptable, but normatively still require regulatory reinforcement. The absence of specific regulations regarding biometrics has the potential to open up opportunities for abuse and weaken consumer protection, thereby contradicting the legal objectives of creating certainty, justice, and benefit. Therefore, affirming the legal status of biometrics is an urgent necessity in order to ensure a balance of rights and obligations for the parties in electronic contracts in Indonesia.¹¹

In Indonesian contract law, the validity of an agreement is fundamentally determined by the fulfillment of the requirements set forth in Article 1320 of the Civil Code, particularly the element of consent (*kesepakatan*). Consent in civil law doctrine is understood not merely as a mechanical act, but as a meeting of the wills (*consensus ad idem*) between legally capable parties, expressed freely and without defects of will such as mistake, coercion, or fraud.

The use of biometric methods such as fingerprint scanning, facial recognition, or iris recognition in electronic contracts raises a critical legal question: does biometric scanning always represent “consent” in the sense required by civil law? From a technological perspective, biometric authentication functions as a means of identity verification, ensuring that the person accessing or approving a transaction is the legitimate user. However, from a legal perspective, identity verification does not automatically equate to the expression of contractual intent.

Biometric systems are inherently passive in nature. The act of scanning a fingerprint or face may occur automatically or as part of a system requirement, without the user fully understanding the legal consequences of such action. This condition potentially weakens the assumption that biometric authentication reflects a conscious and voluntary agreement. In contrast, conventional electronic signatures such as digital signatures or OTP-based confirmations generally require an active and deliberate action, such as clicking an approval button or entering a verification code, which more clearly demonstrates intent.

Moreover, biometric data can be compromised, replicated, or misused without the knowledge of the data subject. Unlike passwords or OTPs, biometric identifiers cannot be changed once exposed. This characteristic raises concerns regarding the possibility of consent being attributed to a party without their actual will, thereby conflicting with the civil law principle that consent must be genuine and attributable to the contracting party.

From the perspective of the ITE Law, biometric methods may fall within the broader concept of electronic authentication or electronic signatures if they meet the requirements of reliability, integrity, and accountability of the electronic system. However, the ITE Law does not explicitly regulate biometric consent mechanisms, nor does it provide clear standards to assess whether biometric authentication sufficiently represents contractual agreement under Article 1320 of the Civil Code.

Therefore, while electronic contracts using biometric methods may offer efficiency and security in verifying identity, their position in Indonesian contract law remains legally debatable, particularly regarding the fulfillment of the element of consent. Legal certainty can only be achieved if biometric authentication is accompanied by clear procedural safeguards, such as explicit consent notices, confirmation mechanisms, and system logs that demonstrate the conscious intention of the parties to be bound by the contract.

¹¹ Universitas Udayana, Dauh Puri Klod, and Kota Denpasar, “Keabsahan Perjanjian Elektronik Dalam Perjanjian Jual Beli Ditinjau Dari Prespektif Hukum Perdata” 3, no. 9 (2025).

Thus, from the perspective of contract law theory, electronic contracts using biometric methods do not, in principle, conflict with the principles of consensualism and freedom of contract, but normatively remain in a gray area due to the limitations of positive law regulations. This condition highlights the need for regulatory updates and affirmations to ensure that the application of biometric technology in electronic contracts is not only theoretically valid, but also provides legal certainty and fair protection for the parties involved.

3.2 Fulfillment of Valid Requirements for Agreements under Article 1320 of the Civil Code in Biometric Electronic Contracts

Agreements in biometric-based electronic contracts can be considered to meet the requirements of Article 1320 of the Civil Code if biometrics are actually used as an instrument of conscious and free consent, supported by a transparent process, and there is sufficient electronic evidence. However, in the practice of standard digital contracts, biometrics has the potential to create agreements that only appear to be technically sound but are vulnerable to legal challenges if the consent process does not meet the standards of good faith and does not provide adequate protection for consumers.¹²

The agreement of the parties is the most essential subjective requirement in Article 1320 of the Civil Code because it forms the basis for the creation of an agreement. In the context of electronic contracts using biometric methods, the agreement is no longer manifested through conventional signatures, but rather through electronic actions verified using certain biological characteristics, such as fingerprints or facial recognition. Conceptually, these biometric actions can be viewed as a declaration of intent, as they are consciously performed by legal subjects to agree to a contract. Thus, agreement in biometric electronic contracts can in principle be considered to have occurred as long as the biometric authentication truly reflects the parties' agreement to the content of the contract.¹³ However, normatively, it is necessary to clearly distinguish between the function of biometrics as a means of identity authentication and the function of consent as a legal declaration of intent. Biometrics essentially only ensures that a particular action is performed by the individual concerned, but does not necessarily prove that the individual understands and agrees to the substance of the agreement. In the practice of electronic contracts in Indonesia, biometric authentication is often combined with the login or account verification process, thus creating the potential for error when authentication actions are considered a form of contractual consent. This condition opens up room for dispute as to whether an agreement as referred to in Article 1320 of the Civil Code has actually been reached.¹⁴

In addition, agreements in biometric electronic contracts must also be tested for possible defects of consent, such as mistake, fraud, or coercion, which in the digital context can take on new forms. Mistake can occur when users assume that biometrics are only used for system security purposes, not to agree to a specific contract. Fraud can arise through the presentation of non-transparent or misleading contract information, such as important clauses hidden in a format that is difficult to understand. Meanwhile, coercion in its modern form can occur

¹² Ni Luh et al., "Kekuatan Hukum Perjanjian Elektronik Dalam Perspektif KUH Perdata Dan UU ITE," no. 4 (2025): 1–10.

¹³ Scolastika Vebriani et al., "Keabsahan Hukum Perjanjian Jual Beli Melalui E-Commerce Di Indonesia : Perlindungan Konsumen Dan Uu Ite" 13, no. 10 (2008).

¹⁴ Muhammad Wafi Amrillah and Putri Sahara Herlina, "Analisis Yuridis Terhadap Kontrak Perjanjian Praktik Layanan Pembukaan IMEI iPhone Berdasarkan Kitab Undang-Undang Hukum Perdata Dan ITE" 1, no. 2 (2025): 259–67.

when users have no choice but to agree to a standard biometric-based contract in order to access certain services, thereby calling into question their free will.¹⁵

The principle of good faith is an important parameter in assessing the validity of agreements in biometric electronic contracts. Electronic system operators are required to act honestly and transparently by providing clear information about biometric functions, the content of agreements, and the legal consequences of the consent given.¹⁶ If biometrics are used without adequate explanation or are designed in such a way as to expedite consent without sufficient understanding, this may be considered contrary to the principle of good faith. In such circumstances, even if biometric authentication technically exists, the resulting agreement may be legally challenged.¹⁷

Furthermore, from a consumer protection perspective, agreements in biometric electronic contracts should not only be assessed formally, but also substantively. The majority of electronic contracts in Indonesia are in the form of standard contracts drafted unilaterally by business actors, placing consumers in a weak position. The use of biometrics has the potential to strengthen the position of business actors because the agreement appears to be very strong technically, even though consumers have no room to negotiate or fully understand the contents of the agreement. Therefore, biometrics should not be used as a tool to lock in agreements that are detrimental to consumers. Thus, agreements between parties in electronic contracts using biometric methods can be considered to meet the requirements of Article 1320 of the Civil Code if the consent is given consciously, freely, and supported by a transparent and legally provable process. Conversely, if biometrics are only used as a technical authentication tool without ensuring understanding and free will, the agreement formed becomes normatively weak and has the potential to cause legal uncertainty in the settlement of electronic contract disputes in Indonesia.¹⁸

3.3 Legal Certainty of Electronic Contracts Using Biometric Methods in the Perspective of the Electronic Information and Transactions Law

The legal certainty of electronic contracts using biometric methods in the Indonesian legal system is normatively based on the provisions of the Electronic Information and Transactions Law (EIT Law) and its implementing regulations, namely Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). Article 5 paragraphs (1) and (2) of the ITE Law emphasize that electronic information and/or electronic documents and their printouts are valid legal evidence and have the same legal force as conventional evidence.¹⁹ This provision forms the basis for the legal recognition of electronic contracts as valid agreements in the Indonesian legal system. Furthermore, Article 11 of the ITE Law stipulates that electronic signatures have legal force and legal consequences as long as they meet certain requirements, including those related to the identity of the signatory, control over the data used to create the signature, and the connection between the signature and the electronic information being signed. In this context, biometric methods can functionally fulfill the aspect of authenticating

¹⁵ Yanuar Joko Susilo, "Implementasi Kontrak Elektronik Dalam Bisnis : Melihat Tantangan Dan Risiko Di Era Digital" 2, no. 2 (2025): 280–86.

¹⁶ Nataneila Astya et al., "Kontrak Elektronik Dalam Bisnis Online : Kajian Terhadap Bentuk , Keabsahan , Dan Perlindungan Hukum Bagi Para Pihak" 1, no. 2 (2025): 201–10.

¹⁷ Kosmas Dohu Amajihono and Universitas Nias Raya, "Kekuatan Hukum Kontrak Elektronik" 1 (2022): 128–39.

¹⁸ Ni Kadek et al., "Keabsahan Syarat Dan Ketentuan Flash Sale Dalam Kontrak Elektronik Pada Platform," 2025, 7825–34.

¹⁹ Ikhlashul Sholah et al., "Kontrak Elektronik Dalam Mekanisme Hukum Di Indonesia" 6, no. 3 (2024): 8068–73.

the identity of the signatory.²⁰ However, the ITE Law does not explicitly mention biometrics as a form of electronic signature, but only recognizes electronic signatures in general. The absence of explicit regulations has led to normative uncertainty as to whether biometrics can be positioned as an electronic signature or only as a supporting authentication mechanism.

The PSTE Government Regulation reinforces the principles of electronic system implementation that are prerequisites for the legal certainty of electronic contracts. Article 3 of the PSTE Government Regulation stipulates that the implementation of electronic systems must be based on the principles of prudence, security, reliability, and accountability.²¹ Furthermore, Article 4 of PP PSTE requires Electronic System Operators (PSE) to be responsible for the reliable and secure operation of electronic systems. In the context of biometric electronic contracts, this provision means that the use of biometrics must be supported by a system that is capable of ensuring data integrity, preventing manipulation, and providing an electronic audit trail that is legally accountable.²²

The aspect of legal certainty is also closely related to the protection of biometric data as part of personal data. PP PSTE, specifically Articles 26 to 28, regulates the obligations of PSE to protect personal data managed in electronic systems. Biometric data, which is unique and sensitive, requires a higher level of protection, as misuse or leakage of such data can have a direct impact on the validity of electronic contracts and the rights of data subjects. If the management of biometric data does not meet the protection standards as stipulated in PP PSTE, the reliability of biometric electronic contracts can be questioned, both in terms of evidence and legal liability.²³

In the event of a dispute, the absence of regulations that explicitly equate biometrics with electronic signatures means that judges must interpret the relationship between Article 11 of the ITE Law and the biometric authentication mechanism used. The judge's assessment will not only focus on the compatibility of biometric data, but also on compliance with the principles of electronic system reliability as stipulated in the PP PSTE. This situation opens up room for differences in interpretation and has the potential to produce inconsistent decisions, thereby weakening the principle of legal certainty.²⁴

This legal uncertainty becomes even more significant when a dispute arises and one of the parties denies ever having given consent to the electronic contract in question. In such circumstances, judges must assess whether biometric authentication can be considered valid evidence of an agreement between the parties. Without clear normative standards in the ITE Law regarding the use of biometrics, such assessments are highly dependent on the judge's interpretation and other supporting evidence submitted. This has the potential to lead to differing verdicts in similar cases, thereby undermining the principle of legal certainty that should be guaranteed by the legal system.²⁵

By linking the PDP Law with the ITE Law and the PSTE Government Regulation, it can be concluded that the legal certainty of electronic contracts using biometric methods is multidimensional, covering aspects of agreement validity, electronic system reliability, and

²⁰ Deden Saputra, "JUKAHU: Jurnal Kajian Hukum Kekuatan Pembuktian Kontrak Elektronik Dalam Perspektif Hukum Perdata" 1, no. 1 (2025): 32–40.

²¹ Hellen S De Lima, Jupryanto Purba, and Diana Napitupulu, "Analisis Hukum Kontrak Dalam Sistem Hukum Indonesia: Perlindungan, Wanprestasi, Dan Tantangan Era Digital" 11, no. 71 (2025): 190–204.

²² Ditiya Salsabila and Budi Ispriyarso, "Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif Di Indonesia" 5, no. 2 (2023): 1343–54, <https://doi.org/10.37680/almanhaj.v5i2.3085>.

²³ Nadia Florensia Tarigan Et Al., "Legalitas Hukum Pembuatan Kontrak Kerja Sama Di Bidang Perdagangan Yang Dilakukan Secara Digital" 3, No. 10 (2025).

²⁴ u I N Sunan Et Al., "Elektronik (E- Contract) Dan Arbitrase Elektronik (E- Arbitration) Dalam Satu Platform Digital" 15 (2025).

²⁵ Paul Hans Kakisina Et Al., "Paulhans0109@Gmail.Com," No. 04 (2023).

personal data protection.²⁶ The lack of clear harmonization between these three legal regimes means that the use of biometrics in electronic contracts remains in a normative gray area. Therefore, strengthening regulations that explicitly integrate electronic contract arrangements, biometric authentication, and personal data protection is an urgent need to ensure legal certainty, protection of data subjects' rights, and fairness for parties in electronic transactions in Indonesia.

3.4. Data Protection Challenges and Risks of Biometric Misuse in Electronic Contracts

The use of biometric methods in electronic contracts poses serious challenges in terms of personal data protection and the risk of data misuse. Unlike ordinary identity data, biometric data such as fingerprints and facial recognition has unique, permanent, and unchangeable characteristics. If biometric data is misused or leaked, data subjects do not have the possibility to “replace” the data as they would replace a password or identity number. Therefore, the use of biometrics in electronic contracts poses greater legal risks than other authentication methods, especially when it comes to legal certainty and the protection of data subjects' rights.²⁷ One of the main challenges is the centralization and storage of biometric data by electronic system operators. In practice, many digital platforms store users' biometric data in centralized databases for repeated authentication purposes. If the security system is inadequate, this biometric data could potentially be targeted for leaks or hacking. For example, in digital financial services, biometric data used to approve electronic credit agreements can be misused by unauthorized parties to conduct transactions or bind data subjects to other contracts without their knowledge. This condition not only violates the PDP Law, but also raises disputes regarding the validity of the contracts formed.²⁸

The next challenge is the use of biometrics beyond its original purpose (*function creep*). Biometric data that was originally collected for the purpose of authenticating electronic contracts can be reused for other purposes, such as user behavior analysis, marketing, or shared with third parties without clear consent. For example, facial recognition data used to verify contract approval on digital platforms can be used to map user preferences or submitted to business partners. Such practices contradict the principle of purpose limitation in the PDP Law and have the potential to undermine the validity of consent, as data subjects never consciously consented to the use of their biometrics for such purposes.²⁹

Based on various data protection challenges and risks of biometric misuse in electronic contracts, concrete normative recommendations are needed to strengthen legal certainty and protection for all parties. First, strict and verified audit trail standards need to be established in every biometric-based electronic contract. The audit trail must include information regarding the time of approval, the stages of the approval process, the version of the document approved, and evidence of the link between biometric authentication and contractual approval actions. The existence of a clear audit trail will facilitate evidence in court and prevent unilateral denial of agreements that have been made.³⁰

²⁶ Universitas Selamat Sri, “JA: Jurnal Al-Wasath 3 No.2: 105-112” 6160, No. 2 (2022): 105–11, <https://doi.org/10.47776/Alwasath.V2i2.213>.

²⁷ Niswatu Filmadina et al., “Pengembangan Hukum Perjanjian Dalam Era Digitalisasi Di Ekonomi Indonesia,” 2025, 5889–98.

²⁸ Maulia Nurfadillah, “Hukum Kontrak Di Era Digital : Adaptasi Teknik Pembuatan Kontrak Dalam Transaksi Online” 2, no. 1 (2025): 185–93.

²⁹ Fras Gandhi Hidayatullah, Fakultas Hukum, and Universitas Narotama, “Prinsip Hukum Kontrak Elektronik Dalam Perjanjian Bisnis Legal Principles of Electronic Contracts in Business Agreements” 8 (2024): 452–62.

³⁰ Battuta Jurnal et al., “Analisis Keabsahan Kontrak Elektronik Dalam Transaksi E-Commerce Di Indonesia” 1, no. 11 (2025): 16–21.

The application of the principle of data minimization must be a normative obligation for electronic system operators. The collection and storage of biometric data must be limited to only the type and amount of data that is absolutely necessary for the purpose of contract authentication, and its use for other purposes without a valid legal basis is prohibited.³¹ This principle is not only in line with the Personal Data Protection Law, but also serves to prevent the misuse of biometric data that could affect the validity of electronic contracts. A separate consent mechanism (*separate and explicit consent*) must be implemented between consent to the contract and consent to the processing of biometric data. Consent to the use of biometrics should not be implicitly equated or combined with contractual consent. With separate consent, data subjects gain clarity regarding the scope of use of their biometrics, while electronic contracts retain a strong basis of agreement that is not mixed with consent to the processing of personal data.

These normative recommendations indicate that legal certainty in electronic contracts using biometric methods cannot be achieved solely through recognition of the technology, but must be built through comprehensive legal regulations that are oriented towards protecting the rights of data subjects and ensuring a balance of interests between the parties. On this basis, the conclusion section of this study will formulate the main findings and directions for legal reforms needed to ensure that the use of biometrics in electronic contracts is fair, secure, and provides legal certainty in Indonesia.³²

Thus, the use of biometrics in electronic contracts faces serious challenges related to personal data protection and the risk of misuse. Without strict regulation and oversight, biometrics has the potential to become a new source of disputes that undermine legal certainty. Therefore, biometric data protection must be positioned as an integral part of the validity of electronic contracts, not merely a technical issue, so that the use of biometric technology truly provides security, fairness, and legal certainty for the parties involved.

3.5. Critical Analysis of Legal Certainty and the Need for Regulatory Reform of Biometric-Based Electronic Contracts

One of the main objectives of this study, as stated in the background, is to analyze the legal certainty of electronic contracts using biometric methods and to identify the limitations of existing legal regulations. The results of the study show that although biometric-based electronic contracts are widely used in practice in Indonesia, the legal framework governing them is still fragmented and does not provide optimal legal certainty. The current legal certainty is more implicit and depends on the interpretation of general norms in Article 1320 of the Civil Code, the ITE Law, the PSTE Government Regulation, and the Personal Data Protection Law, without any specific regulations that explicitly regulate the position of biometrics in electronic contracts.³³

Normatively, biometric electronic contracts can be considered valid because they fulfill the elements of agreement and recognition of electronic documents. However, the absence of a clear definition and classification of biometrics as a means of authentication or electronic signature creates legal uncertainty in terms of evidence. For example, in an online loan contract dispute, a business actor can submit biometric authentication evidence as proof that the consumer has agreed to the agreement. Conversely, consumers may deny such consent

³¹ Peraturan Perundang-undangan Di et al., “Analisis Perlindungan Data Pribadi Dalam Kontrak Elektronik Berdasarkan Indonesia” 13, no. 11 (n.d.).

³² Hizkia Ivan Nugroho et al., “Tinjauan Keabsahan Pelaksanaan Kontrak Elektronik Indonesia Ditinjau Dari Sistem Hukum Positif Indonesia” 6, no. 2 (2023): 4302–7.

³³ Irene Puteri A S Sinaga et al., “Kedudukan Hukum Kontrak Baku Dalam Perlindungan Konsumen Di Indonesia,” 2025, 248–59.

on the grounds that biometrics were only used for identity verification or that their biometric data was misused. In this situation, judges must interpret the evidentiary weight of biometrics themselves because there are no clear normative standards, potentially resulting in different rulings for similar cases.³⁴

Another example can be seen in the use of biometrics in digital banking and fintech services. Facial verification is often used to approve changes to terms of service or new contract agreements. If such consent is combined with a login or application update process without adequate explanation, the question arises as to whether consumers have actually given valid consent. This situation highlights the gap between technological practices and legal norms, which is one of the key issues in the background of this research.

In addition to the aspect of proof, the need for regulatory reform is also related to the protection of weaker parties, particularly consumers. As analyzed earlier, biometric electronic contracts are generally in the form of standard contracts that are drafted unilaterally by business actors. The use of biometrics in standard contracts has the potential to strengthen the position of business actors because it gives the impression of strong technical approval, even though consumers do not have the opportunity to negotiate or fully understand the contents of the agreement. For example, consumers of e-commerce or online transportation services are often required to agree to updates to terms and conditions through biometric verification, with no alternative methods of consent available. This practice can weaken consumer protection and runs counter to the legal objective of creating balance between the parties.

The need for regulatory updates is also evident in the management and protection of biometric data. The Personal Data Protection Law has classified biometrics as specific personal data, but has not specifically regulated its implications for the validity of electronic contracts. For example, if consumers withdraw their consent to the processing of biometric data after the contract has been agreed upon, legal questions arise regarding the validity of the contract. The absence of clear regulations regarding the relationship between consent to biometric data processing and contractual consent indicates a need for regulatory harmonization, as identified in the research objectives.

Based on these examples, it can be concluded that the legal certainty of biometric-based electronic contracts in Indonesia is still relative and does not yet provide optimal legal protection. This condition is in line with the research objectives in the background, namely to identify the limitations of previous research and regulations and to offer new analyses to address legal gaps. Therefore, regulatory updates are urgently needed, either through affirming the position of biometrics in the ITE Law, drafting technical standards in the PSTE Government Regulation, or harmonization with the Personal Data Protection Law.

Thus, critical analysis of legal certainty and the need for regulatory reform not only answers the research objectives formulated in the introduction, but also confirms the scientific value and uniqueness of this article, namely linking the development of biometric technology with the basic principles of contract law and legal protection in the Indonesian legal system.

4. Conclusion

This study concludes that electronic contracts using biometric methods can in principle be recognized as valid and binding agreements as long as they meet the requirements of Article 1320 of the Civil Code, because the principles of consensualism and freedom of

³⁴ Vanza Rifky Octavian, "Teknik Dasar Pembuatan Kontrak Hukum : Melindungi Hak Dan Kewajiban" 2, no. 6 (2024): 567–73.

contract do not limit the form of expression of intent to conventional media. However, the legal certainty of biometric-based electronic contracts in Indonesia is still relative, given that the Electronic Information and Transactions Law and the Electronic Signatures Regulation do not explicitly regulate the position of biometrics as a means of authentication or electronic signature with clear standards of proof. On the other hand, the use of biometrics also poses serious challenges in the protection of personal data, given that biometrics are specific personal data as regulated in the Personal Data Protection Law, so that the unclear relationship between consent to biometric data processing and contractual consent has the potential to weaken the validity of the agreement. In addition, the practice of biometric electronic contracts, which is dominated by standard contracts, risks reinforcing the legal imbalance between businesses and consumers if it is not accompanied by the application of the principles of good faith and consumer protection. Therefore, it is necessary to strengthen and harmonize regulations that explicitly regulate the use of biometrics in electronic contracts, establish standards for proof and system security, and integrate personal data protection to ensure legal certainty, fairness, and protection of the rights of parties in electronic transactions in Indonesia.

References

- Amajihono, Kosmas Dohu, And Universitas Nias Raya. “Kekuatan Hukum Kontrak Elektronik” 1 (2022): 128–39.
- Amrillah, Muhammad Wafi, And Putri Sahara Herlina. “Analisis Yuridis Terhadap Kontrak Perjanjian Praktik Layanan Pembukaan IMEI Iphone Berdasarkan Kitab Undang-Undang Hukum Perdata Dan ITE” 1, No. 2 (2025): 259–67.
- Anami, Mulan Kasisty, Alvina Maretia Lidowati, Rachel Netanya Panjaitan, Rasya Aika, Diana Febri, And Nauli Purba. “Analisis Hukum Perdata Pada Perlindungan Hukum Bagi Para Pihak Dalam Kontrak Digital : Studi Kasus Sengketa Saldo DANA” 2, No. 5 (2025): 338–44.
- Astya, Nataneila, Putri Asmana, Aisyah Nabila Ramandhani, And Regina Agnesia. “Kontrak Elektronik Dalam Bisnis Online : Kajian Terhadap Bentuk , Keabsahan , Dan Perlindungan Hukum Bagi Para Pihak” 1, No. 2 (2025): 201–10.
- Di, Peraturan Perundang-Undangan, Eveline Vania Sirait, Fakultas Hukum, And Universitas Udayana. “Analisis Perlindungan Data Pribadi Dalam Kontrak Elektronik Berdasarkan Indonesia” 13, No. 11 (N.D.).
- Egia, Lompoh, Nuansa Pinem, Ketut Sari Adnyani, And Muhammad Jodi Setianto. “Keabsahan Perjanjian Arisan Online Ditinjau Dari Pasal 1320 Kitab Undang-Undang Hukum Perdata Universitas Pendidikan Ganesha E-Journal Komunikasi Yustisia Universitas Pendidikan Ganesha” 5, No. November (2022): 47–57.
- Filmadina, Niswatu, Tasya Monica, Fendy Setiawan, And Firman Floranta Adonara. “Pengembangan Hukum Perjanjian Dalam Era Digitalisasi Di Ekonomi Indonesia,” 2025, 5889–98.
- Hambali, Reghina Miftahuljannah, Mutya Cherawaty Thalib, And Nurul Fazri Elfikri.

- “Pembatalan Dalam Perjanjian Jual Beli : Telaah Pasal 1320 Kuhperdata Dan Putusan Pengadilan” 1, No. 3 (2025): 838–45.
- Hermawan, R Oetomo, Huala Adolf, And Edy Santoso. “Kajian Hukum Penerapan Pasal Dalam Kontrak Elektronik” 5, No. 2 (2024): 141–64.
- Hidayatullah, Fras Gandhi, Fakultas Hukum, And Universitas Narotama. “Prinsip Hukum Kontrak Elektronik Dalam Perjanjian Bisnis Legal Principles Of Electronic Contracts In Business Agreements” 8 (2024): 452–62.
- Jurnal, Battuta, Ilmu Hukum, Irma Herliza Rizki, And Mela Novita Rizki. “Analisis Keabsahan Kontrak Elektronik Dalam Transaksi E-Commerce Di Indonesia” 1, No. 11 (2025): 16–21.
- Kadek, Ni, Intan Diah, Kadek Januarsa, And Adi Sudharma. “Keabsahan Syarat Dan Ketentuan Flash Sale Dalam Kontrak Elektronik Pada Platform,” 2025, 7825–34.
- Kakisina, Paul Hans, Vecky Yani Gosal, Nurhikmah Nachrawy, A Latar Belakang, Dalam Kitab, And Undang-Undang Hukum Perdata. “Paulhans0109@Gmail.Com,” No. 04 (2023).
- Kandriana, Muhammad, Sri Atika, And Muhammad Wildan. “Unes Law Review” 8, No. 1 (2025): 221–28.
- Lima, Hellen S De, Jupryanto Purba, And Diana Napitupulu. “Analisis Hukum Kontrak Dalam Sistem Hukum Indonesia : Perlindungan , Wanprestasi , Dan Tantangan Era Digital” 11, No. 71 (2025): 190–204.
- Luh, Ni, Gede Mella, Ni Made, And Puspautari Ujianti. “Kekuatan Hukum Perjanjian Elektronik Dalam Perspektif KUH Perdata Dan UU ITE,” No. 4 (2025): 1–10.
- Nomer, Undang, Tahun Tentang, And Informasi Dan. “E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha Program Studi Ilmu Hukum (Volume 4 Nomor 2 Agustus 2021) E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha Program Studi Ilmu Hukum (Volume 4 Nomor 2 Agustus 2021)” 4 (2021): 617–25.
- Nugroho, Hizkia Ivan, Ariawan Gunadi, Fakultas Hukum, And Universitas Tarumanagara. “Tinjauan Keabsahan Pelaksanaan Kontrak Elektronik Indonesia Ditinjau Dari Sistem Hukum Positif Indonesia” 6, No. 2 (2023): 4302–7.
- Nurfadillah, Maulia. “Hukum Kontrak Di Era Digital : Adaptasi Teknik Pembuatan Kontrak Dalam Transaksi Online” 2, No. 1 (2025): 185–93.
- Octavian, Vanza Rifky. “Teknik Dasar Pembuatan Kontrak Hukum : Melindungi Hak Dan Kewajiban” 2, No. 6 (2024): 567–73.
- Raya, Rian Rambu, Fadlan Nur Azizil, Rizal Al Birra, And Rayi Kharisma Rajib. “Urgensi Perancangan Kontrak Elektronik Dalam Menjamin Kepastian Hukum Transaksi E-Commerce The Urgency Of Designing Electronic Contracts To Ensure Legal Certainty Of E-Commerce Transactions In Indonesia,” 2025, 18173–83.

- Salsabila, Ditiya, And Budi Ispriyarso. “Efektivitas Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif Di Indonesia” 5, No. 2 (2023): 1343–54. <https://doi.org/10.37680/Almanhaj.V5i2.3085>.
- Saputra, Deden. “JUKAHU : Jurnal Kajian Hukum Kekuatan Pembuktian Kontrak Elektronik Dalam Perspektif Hukum Perdata” 1, No. 1 (2025): 32–40.
- Sholah, Ikhlasul, Kusuma Wardani, Alya Safirah, And Alfika Salsa Qurrotulaini. “Kontrak Elektronik Dalam Mekanisme Hukum Di Indonesia” 6, No. 3 (2024): 8068–73.
- Sinaga, Irene Puteri A S, Felicia Jacinta, Ivanka Anter, And Vivi Anjelika. “Kedudukan Hukum Kontrak Baku Dalam Perlindungan Konsumen Di Indonesia,” 2025, 248–59.
- Situmorang, Monika Esterina, And Abdul Salam. “Lex Patrimonium Analisis Aspek Hukum Kontrak Pintar Dalam Transaksi Kebendaan Digital : Tantangan Anonimitas Dan Peran Identitas Digital Analisis Aspek Hukum Kontrak Pintar Dalam Transaksi Kebendaan Digital : Tantangan Anonimitas Dan Peran Identitas Digital” 4, No. 1 (2025).
- Sri, Universitas Selamat. “JA: Jurnal Al-Wasath 3 No.2: 105-112” 6160, No. 2 (2022): 105–11. <https://doi.org/10.47776/Alwasath.V2i2.213>.
- Sunan, U I N, Gunung Djati, U I N Sunan, And Gunung Djati. “Elektronik (E- Contract) Dan Arbitrase Elektronik (E- Arbitration) Dalam Satu Platform Digital” 15 (2025).
- Susilo, Yanuar Joko. “Implementasi Kontrak Elektronik Dalam Bisnis : Melihat Tantangan Dan Risiko Di Era Digital” 2, No. 2 (2025): 280–86.
- Tarigan, Nadia Florensia, Dewa Ayu, Dian Sawitri, Universitas Udayana, Dauh Puri Klod, And Kota Denpasar. “Legalitas Hukum Pembuatan Kontrak Kerja Sama Di Bidang Perdagangan Yang Dilakukan Secara Digital” 3, No. 10 (2025).
- Taufiq, Wahyu, And Abdul Aziz. “Analisis Yuridis Penggunaan Blockchain Technology Dalam Penerapan E-Residency” 1, No. 1 (2025): 1–16.
- Udayana, Universitas, Dauh Puri Klod, And Kota Denpasar. “Keabsahan Perjanjian Elektronik Dalam Perjanjian Jual Beli Ditinjau Dari Prespektif Hukum Perdata” 3, No. 9 (2025).
- Vebriani, Scolastika, Fakultas Hukum, Universitas Udayana, Ayu Putu, Laksmi Danyathi, Fakultas Hukum, And Universitas Udayana. “Keabsahan Hukum Perjanjian Jual Beli Melalui E-Commerce Di Indonesia : Perlindungan Konsumen Dan Uu Ite” 13, No. 10 (2008).
- Wardana, Yudistira Kusuma. “Analisis Aspek Hukum Dan Implikasi Kontrak Elektronik Dalam Perjanjian Bisnis” 1, No. 1 (2023): 776–86.