Al-battar: Jurnal Pamungkas Hukum
DOI: https://doi.org/10.63142/al-battar.v2i3.440
Volume 2 Nomor 3, Desember 2025
e-ISSN 3063-8895 | p-ISSN - | Hal. 270-280

State Responsibility in Safeguarding the Integrity of Digital Land Records against Manipulation and Cyber Attacks

***Rikky Fermana, Septa Agung Rahayu Basuki, Fajar Kurniawan, Muhammad Zarnudin**
Universitas Darul Ulum Islamic Centre Sudirman Guppi
*Email: rikkyfermana@gmail.com, septaagung09@gmail.com, fajargiboy@gmail.com, mzundaris@gmail.com

Received:	Revised:	Accepted:	Available Online:	Published:
10/10/2025	24/12/2025	25/12/2025	25/12/2025	25/12/2025

Abstract

The digital transformation of land administration in Indonesia enhances efficiency and transparency, particularly through the implementation of electronic land certificates by the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (ATR/BPN). However, the shift to digital land records also raises serious legal challenges related to data integrity and authenticity amid increasing risks of manipulation and cyber attacks. Existing legal scholarship has predominantly addressed the formal validity of electronic documents and procedural aspects of digital land registration, while insufficient attention has been given to the state's legal responsibility in safeguarding the integrity of digital land records within an integrated framework of land law, information technology law, and data protection. This study aims to examine the scope of state responsibility in protecting digital land records from cyber threats and to assess the adequacy of the prevailing regulatory framework in ensuring legal certainty of land rights. Using normative legal research with statutory and conceptual approaches, this study analyzes key regulations, including the Electronic Information and Transactions Law, the Personal Data Protection Law, Government Regulation Number 18 of 2021, and the Regulation of the Minister of ATR/BPN on Electronic Certificates. The findings indicate that the state has a constitutional obligation to ensure the integrity of digital land records as part of citizens' right to legal certainty under Article 28D paragraph (1) of the 1945 Constitution. Nevertheless, challenges persist in regulatory harmonization, institutional coordination, cybersecurity preparedness, and human resource capacity. Therefore, strengthening state responsibility requires coherent regulatory integration, effective inter-agency coordination, enhanced cybersecurity measures, and the adoption of advanced technologies such as blockchain to maintain the integrity and authenticity of digital land records in a sustainable manner.

Keywords: *State Accountability, Digital Land Data, Authenticity, Cybersecurity, Legal Protection.*

Abstrak

Transformasi digital administrasi pertanahan di Indonesia meningkatkan efisiensi dan transparansi, khususnya melalui penerapan sertifikat pertanahan elektronik oleh Kementerian Agraria dan Tata Ruang/Badan Pertanahan Nasional (ATR/BPN). Namun, peralihan ke catatan tanah digital juga menimbulkan tantangan hukum serius terkait integritas dan keaslian data di tengah meningkatnya risiko manipulasi dan serangan siber. Keilmuan hukum yang ada sebagian besar membahas validitas formal dokumen elektronik dan aspek prosedural pendaftaran tanah digital, sementara perhatian yang tidak memadai diberikan pada tanggung jawab hukum negara dalam menjaga integritas catatan tanah digital dalam kerangka terpadu hukum pertanahan, hukum

teknologi informasi, dan perlindungan data. Penelitian ini bertujuan untuk mengkaji ruang lingkup tanggung jawab negara dalam melindungi catatan tanah digital dari ancaman siber dan untuk menilai kecukupan kerangka peraturan yang berlaku dalam memastikan kepastian hukum hak atas tanah. Dengan menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, penelitian ini menganalisis regulasi utama, termasuk UU Informasi dan Transaksi Elektronik, UU Perlindungan Data Pribadi, Peraturan Pemerintah Nomor 18 Tahun 2021, dan Peraturan Menteri ATR/BPN tentang Sertifikat Elektronik. Temuan tersebut menunjukkan bahwa negara memiliki kewajiban konstitusional untuk memastikan integritas catatan tanah digital sebagai bagian dari hak warga negara atas kepastian hukum berdasarkan Pasal 28D ayat (1) UUD 1945. Namun demikian, tantangan tetap ada dalam harmonisasi regulasi, koordinasi kelembagaan, kesiapsiagaan keamanan siber, dan kapasitas sumber daya manusia. Oleh karena itu, memperkuat tanggung jawab negara membutuhkan integrasi peraturan yang koheren, koordinasi antar-lembaga yang efektif, langkah-langkah keamanan siber yang ditingkatkan, dan adopsi teknologi canggih seperti blockchain untuk menjaga integritas dan keaslian catatan tanah digital secara berkelanjutan.

Kata Kunci: Akuntabilitas Negara, Data Tanah Digital, Keaslian, Keamanan Siber, Perlindungan Hukum.

INTRODUCTION

Land digitization is a key component of the government's agenda to achieve more effective, transparent, and efficient public services.[1] The adoption of electronic certificates by the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (ATR/BPN) is indicative of this change.[2] Digital land data not only serves as an administrative tool but also serves as an instrument to ensure legal certainty regarding land rights.[3] The existence of an electronic system allows faster access to land information while reducing the potential for abuse of authority in managing physical data.[4] The shift from a manual to a digital system requires stronger legal certainty to protect public rights.[5]

The risk of manipulation and cyberattacks poses a significant challenge to implementing an electronic land system. Cases such as digital document forgery, system hacking, and data theft demonstrate clear vulnerabilities.[6] Systems lacking high-standard security layers have the potential to open up loopholes for cybercriminals to misuse.[7] The impacts can be significant, including overlapping land rights and a decline in public trust in the land administration system. Land data security must be viewed as an integral part of protecting land ownership rights.

---

[1] Riswan Erfa, "Digitalisasi Administrasi Pertanahan Untuk Mewujudkan Percepatan Pembangunan Nasional Perspektif Kebijakan Hukum (Legal Policy)," *Jurnal Pertanahan* 10, no. 1 (2020).

[2] Kurnia Rheza Randy Adinegoro, "Tantangan Implementasi Sertipikat Tanah Elektronik Di Kementerian Agraria Dan Tata Ruang/Badan Pertanahan Nasional Republik Indonesia," *Jurnal Ilmu Kenotariatan* 4, no. 2 (2023): 130–43.

[3] Indri Fogar Susilowati, "Tinjauan Yuridis Sertifikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Tanah Di Indonesia," *Novum: Jurnal Hukum* 1, no. 1 (2024): 57–71.

[4] I Kadek Dewi Sasih Adnyani et al., "Pentingnya Sertifikat Tanah Elektronik Di Era Digital Sebagai Bukti Hak Kepemilikan Tanah," *Jurnal Komunitas Yustisia* 7, no. 2 (2024): 121–29.

[5] I Kadek Dewi Sasih Adnyani et al., "Pentingnya Sertifikat Tanah Elektronik Di Era Digital Sebagai Bukti Hak Kepemilikan Tanah," *Jurnal Komunitas Yustisia* 7, no. 2 (2024): 121–29.

[6] Syarifaatul Hidayah et al., "Tantangan Dan Peluang Sertifikat Elektronik Dalam Reformasi Pendaftaran Tanah Di Era Digital.," *Jurnal Ilmiah Nusantara* 1, no. 6 (2024): 186–99.

[7] Risma Siti Maesaroh, "Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital," *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 255–74.

Legal certainty over land has long been regulated through Article 19 of the Basic Agrarian Law (UUPA) No. 5 of 1960. This article emphasizes the importance of land registration as a basis for guaranteeing community rights.[8] Land registration, which was previously based on physical documents, has now shifted to an electronic system. This change requires affirmation that the principle of legal certainty remains valid despite the difference in storage media. The validity of digital land data must have the same legal value as physical documents for its authenticity to be legally recognized.[9]

The definition of digital land data encompasses all information regarding the status, rights, and land use that is stored and managed through an electronic system.[10] This data includes certificates, land plot maps, and other legal and technical information previously recorded manually. The transition to digital format is intended to increase service efficiency while reducing the potential for bureaucratic red tape.[11] This coverage also allows for integration with other information systems, such as regional taxes and spatial planning. Thus, the existence of digital land data confirms the role of technology in supporting the principle of legal certainty.

The principle of legal certainty in land matters relates not only to ownership but also to the comprehensive protection of community rights.[12] Articles 3 and 19 of the Basic Agrarian Law emphasize that land registration aims to guarantee legal certainty for rights holders. Integrated digital land data must reflect this principle by providing clarity, accuracy, and guaranteed access.[13] A well-designed system will minimize the potential for land disputes that often arise from data asymmetry. Legal certainty is key to ensuring public confidence in the legality of digital data provided by the state.

The authenticity of electronic data is strictly regulated by Law Number 11 of 2008 concerning Electronic Information and Transactions, which was later amended by Law Number 19 of 2016. Authenticity is defined as the assurance that an electronic document truly originates from an authorized party and has not undergone unauthorized changes.[14] This principle is crucial for digital land data to be applied because it directly relates to individual ownership rights. Without guaranteed authenticity, electronic certificates are vulnerable to forgery or manipulation. Positive law has established that electronic data that meets certain requirements is valid evidence, making it relevant for application in land administration.[15]

---

[8] Lisnadia Nur Avivah et al., "Pentingnya Pendaftaran Tanah Untuk Pertama Kali Dalam Rangka Perlindungan Hukum Kepemilikan Sertifikat Tanah," *Tunas Agraria* 5, no. 3 (2022): 197–210.

[9] Michelle Priscilla et al., "-Keabsahan Hukum Penerbitan Sertipikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Hak Atas Tanah Di Persidangan:-," *UIR Law Review* 8, no. 2 (2024): 68–84.

[10] Muh Arif Suhattanto et al., "Kualitas Data Pertanahan Menuju Pelayanan Sertifikat Tanah Elektronik," *Widya Bhumi* 1, no. 2 (2021): 87–100.

[11] Aslan Noor et al., "Implications of the Use of Electronic Certificates in Proving Land Rights According to the Civil Procedure Law," *Electronic Journal of Education, Social Economics and Technology* 5, no. 2 (2024): 276–81.

[12] Desy Tejawati, "Asas Kepastian Hukum Dalam Kedudukan Girik Terhadap Sertipikat Hak Atas Tanah," *Jurnal Suara Hukum* 3, no. 2 (2021): 251–73.

[13] Deva Sakti Susmana, "Transformasi Digital Dalam Administrasi Pertanahan: Analisis Yuridis Terhadap Sertipikat Tanah Elektronik," *Jurnal Impresi Indonesia* 4, no. 6 (2025): 2063–70.

[14] Gabriel Amadeus Sitompul and Albert Lodewyk Sentosa Siahaan, "Analisis Terhadap Pembuatan Surat Pernyataan Keabsahan Dan Kebenaran Dokumen Elektronik Pada Sertifikat Hak Tanggungan," *Media Hukum Indonesia (MHI)* 2, no. 4 (2024): 20–33.

[15] Yuzi Afif and Muhammad Afif Mahfud, "Kepastian Hukum Terhadap Sertifikat Elektronik Hak Milik Atas Tanah," *Unes Law Review* 6, no. 2 (2023): 7605–11.

Instruments that guarantee the authenticity of electronic data include electronic signatures and electronic certificates. Articles 5 through 12 of the ITE Law explain that electronic signatures have legal force and valid legal consequences as long as they meet technical and procedural requirements.[16] In the land context, the use of electronic signatures ensures that digital documents can only be accessed or modified by authorized parties. Electronic certificates issued by authorized electronic certification providers serve as additional validation.[17] The implementation of these instruments provides an extra layer of protection for the validity of digital land data.

The concept of a state based on the rule of law, or rechtsstaat, provides a philosophical basis that the state has an obligation to guarantee legal certainty for all its citizens.[18] The implementation of a digital land system cannot be separated from this principle, as it concerns the community's fundamental right to land. The state is required to provide adequate legal instruments to prevent the public from being disadvantaged due to system weaknesses. The existence of clear, consistent regulations that respond to technological developments is one indicator of the strength of the rule of law principle. Thus, legality and justice are maintained despite digitalization.

The theory of state responsibility asserts that the state can be held accountable for violations or negligence that harm the public.[19] In the case of digital land data, the state has an obligation to prevent manipulation and cyberattacks through regulations and concrete actions. If data leaks or losses occur due to weak oversight, the state must provide redress to affected parties. This accountability encompasses administrative, civil, and criminal aspects, depending on the nature of the violation. This theory positions the state as a legal subject that not only has authority but also must be responsible.

Information security theory, which encompasses confidentiality, integrity, and availability, is relevant for application in digital land systems.[20] Confidentiality ensures that land data can only be accessed by authorized parties. Integrity ensures that the data has not undergone unauthorized changes since it was first recorded. Availability ensures that data remains available to the public and agencies that require it whenever needed.[21] These three principles are the main foundation for ensuring the authenticity of digital land data. Without the application of information security theory, the reliability of the digital land system will continue to be questioned.

RESEARCH METHODS

This study employs normative legal research to examine legal norms governing the protection of digital land records and the state's responsibility in safeguarding their integrity against manipulation and cyber attacks. The research applies a statutory

[16] Indah Julitah Pelapu, "Kepastian Hukum Penggunaan Tanda Tangan Elektronik Dalam Akta Notaris," *LEX PRIVATUM* 14, no. 2 (2024).

[17] Dini Ernawati et al., "Perlindungan Hukum Bagi Pemegang Sertipikat Tanah Elektronik," *Journal of Innovation Research and Knowledge* 4, no. 9 (2025): 7213–28.

[18] SH Selfianus Laritmas and SH Ahmad Rosidi, *Teori-Teori Negara Hukum* (Prenada Media, 2024).

[19] Ainuddin Samsul and Ikhsan Kamil, "Analisa Yuridis Pertanggungjawaban Badan Pertanahan Nasional Dalam Penyimpanan Dan Pengelolaan Sertifikat Tanah Elektronik: Studi Kasus Di Kantor Pertanahan Kabupaten Lombok Barat," *SIMPUL: Jurnal Ilmu Politik Dan Hukum* 1, no. 2 (2025): 43–48.

[20] RG Guntur Alam et al., *Manajemen Risiko Keamanan Informasi* (PT. Sonpedia Publishing Indonesia, 2025).

[21] Joshua Paskah Nugraha et al., "Penerapan Blockchain Untuk Pencegahan Sertipikat Tanah Ganda Di Kementerian Agraria Dan Tata Ruang/Badan Pertanahan Nasional," *Widya Bhumi* 2, no. 2 (2022): 123–35.

approach and a conceptual approach in an integrated manner. The statutory approach is used to analyze binding legal instruments, including Law Number 11 of 2008 on Electronic Information and Transactions as amended by Law Number 19 of 2016, Law Number 27 of 2022 on Personal Data Protection, Government Regulation Number 18 of 2021 on Management Rights, Land Rights, Apartment Units, and Land Registration, and Regulation of the Minister of Agrarian Affairs and Spatial Planning/National Land Agency Number 1 of 2021 on Electronic Certificates, in order to assess their coherence, consistency, and adequacy in ensuring the authenticity, integrity, and legal certainty of digital land records. Meanwhile, the conceptual approach examines relevant legal doctrines and principles, including the rule of law (rechtsstaat), the theory of state responsibility, and information security principles of confidentiality, integrity, and availability, to evaluate how normative obligations imposed on the state translate into concrete legal accountability in digital land administration. The study relies on primary, secondary, and tertiary legal materials, which are analyzed qualitatively using prescriptive and analytical methods to identify normative gaps, regulatory overlaps, and institutional weaknesses, thereby ensuring methodological transparency and enabling the formulation of normative recommendations for strengthening state responsibility in protecting the integrity of digital land records.

RESULTS AND DISCUSSION

Review of Regulations and State Obligations in Guaranteeing the Authenticity of Digital Land Data

Indonesian land law is primarily based on the Basic Agrarian Law (UUPA) No. 5 of 1960. To maintain legal clarity, Article 19 of the UUPA requires the government to set up land registration across the Republic of Indonesia. This registration covers bookkeeping, mapping, and land measurement, certificate issuance, and data storage related to land rights. This article affirms the state's legal obligation to regulate an accurate and reliable land registration system. The transformation to a digital system does not eliminate this fundamental principle but rather requires new methods to ensure the goal of legal certainty is achieved.

The enforcement of land registration requirements is strengthened by Government Regulation No. 18 of 2021 concerning Management Rights, Land Rights, Apartment Units, and Land Registration. This regulation's Article 84 states that land registration may be done online, including the recording of rights, bookkeeping, and certificate issuance. This provision represents a legal breakthrough that provides strong legitimacy to a digital-based land system. The article also mandates the use of information technology in land administration to accelerate public services. This regulation serves as the basis for the transition from a manual system to an electronic system with equal legal force.

Regulation No. 1 of 2021 of the National Land Agency (ATR/BPN) and the Minister of Agrarian Affairs and Spatial Planning pertaining to Electronic Certificates specifically regulates the mechanism for issuing digital land title certificates. Article 2 of this regulation states that land registration can produce electronic land certificates as a replacement for conventional land certificates. Article 6 also confirms that electronic certificates have the same legal force as physical certificates. This provision ensures that digital documents are recognized as valid and binding proof of rights. This regulation also encourages the modernization of land services while upholding the principle of data authenticity.

The most recent piece of legislation pertaining to digital land data is Law No. 27 of 2022 respecting Personal Data Protection (PDP). Any information pertaining to an

identifiable or identified person is considered personal data under Article 1, number 1 of the PDP Law. Personal data subjects have rights under Article 4, including the right to data security and confidentiality. Articles 57 to 67 regulate administrative and criminal sanctions for violations of personal data management. This provision is highly relevant because digital land data often contains sensitive information regarding landowners, the confidentiality of which must be maintained by the state.

The legitimacy of electronic papers is validated by Law No. 19 of 2016, which amends Law No. 11 of 2008 respecting Electronic Information and Transactions. According to the ITE Law's Article 5, paragraph (1), electronic records and/or information, along with their printouts, constitute valid legal evidence. Article 12 emphasizes the validity of electronic signatures as a means of strengthening the authenticity of data. Article 35 imposes criminal penalties on anyone who intentionally and without authority manipulates, creates, changes, deletes, or destroys electronic information. The regulation strengthens the protection of the authenticity of digital land data to prevent it from being easily manipulated.

The National Cyber and Crypto Agency (BSSN) plays a significant role in securing electronic data, including land data. BSSN Head Regulation No. 10 of 2020 concerning Information Security establishes standards and guidelines for protecting electronic systems from cyber threats. Article 4 of this regulation stipulates that every agency is required to implement information security management, encompassing policies, organization, access control, and technical controls. Article 7 stipulates the obligation to conduct regular information security audits. Thus, BSSN ensures that digital land systems maintain an adequate level of security in accordance with national standards.

The Ministry of Agrarian Affairs and Spatial Planning/BPN, as the land authority, has primary authority over digital land data management. Article 2 of ATR/BPN Regulation No. 1 of 2021 emphasizes that the administration of electronic certificates falls under the authority of the ministry. This function encompasses data management, storage, issuance, and cancellation of electronic land certificates. This authority must be exercised with due care to ensure the accuracy of all recorded data. The BPN's role is crucial, as the success of land digitization depends on the integrity of the systems they manage.

The Ministry of Communication and Informatics (Kominfo) serves as the supervisory authority for the implementation of electronic systems. Article 40, paragraph (2) of the ITE Law mandates Kominfo to regulate, foster, and supervise electronic system providers. Article 46 of the PDP Law also authorizes the supervisory authority, in this case Kominfo, to ensure compliance by personal data controllers. This supervisory function includes enforcing administrative sanctions for parties who violate data protection obligations. Thus, Kominfo acts as both a regulator and an external supervisor of the implementation of digital land data.

The National Cyber Security Agency (BSSN) exercises its authority as the agency responsible for national cybersecurity, which is also closely related to digital land data. Article 3 of Presidential Regulation No. 53 of 2017 concerning BSSN states that BSSN is tasked with implementing national cybersecurity. Article 4 emphasizes that BSSN's function is to formulate and establish technical policies for electronic system security and to control cyber incidents. This task includes protecting land information systems from hacking and data manipulation. BSSN's authority is crucial because the success of the digital land system depends heavily on the strength of its cyber protection.

Synergy between the ATR/BPN, the Ministry of Communication and Information Technology, and the BSSN is key to the success of digital land data protection. ATR/BPN functions as a data manager, the Ministry of Communication and Information Technology oversees electronic systems and personal data compliance, and the BSSN safeguards cybersecurity. These three institutions have a clear legal basis for exercising their authority. Collaboration between these state institutions is necessary to ensure the authenticity of digital land data. Without strong coordination, the threat of manipulation and cyberattacks will be difficult to address, even if regulations are in place.

Challenges and Law Enforcement Strategies in Protecting Digital Land Data from the Threat of Manipulation and Cyber Attacks

The state's responsibility for protecting digital land data can take the form of preventive accountability, emphasizing the obligation to establish regulations and system security standards. Good regulations include establishing data security policies, developing technical guidelines, and requiring regular audits of electronic land systems. Article 3 of Law No. 27 of 2022 concerning Personal Data Protection (PDP) stipulates that every data controller is obliged to protect the personal data they manage. This preventive obligation aims to ensure that the state not only reacts after a breach occurs, but also anticipates it from the outset. Established security standards serve as the first line of defense against the threat of manipulation or cyberattacks.

Repressive accountability is another equally important form of accountability, particularly when digital land data leaks or manipulation occur. Article 12 of the PDP Law grants data subjects the right to compensation in the event of a data management breach. The state, through the managing agency, is obliged to provide a recovery mechanism, including data correction, financial compensation, and restoration of affected land rights. This repressive mechanism demonstrates that the state cannot abdicate when the public suffers losses due to system weaknesses. Recovery is a manifestation of the state's responsibility to maintain public trust in digital land administration.

Administrative, civil, and criminal aspects also form part of the state's accountability. Administrative consequences, such as written warnings, temporary activity suspension, and data deletion if data protection responsibilities are not fulfilled, are governed by Article 57 of the PDP Law. The PDP Law's Articles 65 to 67 indicate that anyone who willfully divulge personal information face jail time and fines. Article 35 of the ITE Law stipulates criminal penalties for anyone who intentionally and without authority manipulates or changes electronic documents. These provisions demonstrate that legal instruments are available to prosecute violations, whether committed by individuals or institutions.

The most obvious threat to digital land data is the occurrence of duplicate certificates, which can harm more than one landowner. Duplicate certificates can arise from data manipulation, data theft, or security vulnerabilities in electronic systems. This incident is not merely an administrative issue but also has the potential to lead to prolonged legal disputes. Article 32, paragraph (1) of the ITE Law stipulates that any person who intentionally and without authority changes, adds to, reduces, transmits, damages, removes, or renders electronic information unusable is subject to criminal penalties. Threats such as this demonstrate the need for a robust security system to prevent the recurrence of duplicate certificate cases.

Another increasing issue is data theft and land system hacking. According to the ITE Law's Article 30, paragraph (1), anyone who willfully and without authorization gains access to another person's computer or electronic system faces criminal charges.

Article 30, paragraph (2) further emphasizes the criminal penalties for those who exceed their authority with the intent of obtaining electronic information. This crime can have a systemic impact because stolen land data can be sold, falsified, or exploited for specific purposes. The state is obliged to provide serious protection because the land system concerns broad public interests.

Regulatory weaknesses are a major obstacle to ensuring state accountability. The lack of synchronization between the PDP Law, There is insufficient legal protection due to the ITE Law and land rules like Government Regulation No. Law No. 18 of 2021 and Regulation of the Minister of Agrarian Affairs and Spatial Planning/National Land Agency No. 1 of 2021. Each regulation stands alone without a clear coordination mechanism between agencies. This leads to confusion in the application of sanctions when violations occur. For example, the Personal Data Protection Law regulates sanctions against personal data controllers but does not specifically address land institutions as legal entities. This lack of coordination highlights the need for regulatory harmonization to eliminate legal loopholes.

The lack of administrative sanctions for state institutions that fail to protect land data also poses a serious problem. The PDP Law places greater emphasis on the responsibility of data controllers, which is generally directed at businesses or private parties. Article 57 of the PDP Law regulates administrative sanctions, but its implementation in government agencies is often ineffective. State officials are rarely given firm sanctions even when data leaks occur due to negligence. This situation demonstrates the disparity between the legal obligations that should be inherent in the state and the reality of law enforcement.

The low level of digital literacy among some land officials is another contributing factor. The electronic land system requires high technical expertise to operate and maintain its security effectively. Without adequate skills, officials often become a weak point easily exploited by cybercriminals. The PDP Law does provide data controllers with the right and obligation to undergo training, but this provision is not always optimally implemented. The low digital literacy of officials means that the potential for human error remains a serious threat to data authenticity.

International practices can serve as a reference to strengthen state legal accountability. The 1996 UNCITRAL Model Law on Electronic Commerce provides basic principles for recognizing electronic data as legitimate documents possessing authenticity. These principles emphasize the need for system integrity, data security, and the protection of data subjects' rights. Several countries have adopted these principles by developing more comprehensive cybersecurity regulations. Indonesia can learn from this experience to strengthen its digital land legal framework to become more resilient in the face of global threats.

The relevance of implementing international practices in Indonesia is significant, given that the digital land system is closely linked to developments in global information technology. International data security principles, such as confidentiality, integrity, and availability, can be integrated with the national legal system. This integration will help Indonesia develop regulations that are not only local but also compliant with global standards. Implementing these principles will strengthen the legal standing of digital land data, enabling it to face the challenges of manipulation and cyberattacks. In this way, the state's responsibility is not only formally realized but also operationally implemented in practice.

CONCLUSION

The state has a constitutional and legal obligation to guarantee the protection of the authenticity of digital land data from the threat of manipulation and cyber attacks. This is founded on the state's obligation to control and defend citizens' ownership rights as well as the legal certainty concept included in Article 28D, paragraph (1) of the 1945 Constitution. Government Regulation Number 18 of 2021 concerning Management Rights, Land Rights, Apartment Units, and Land Registration, Regulation of the Minister of ATR/BPN Number 1 of 2021 concerning Electronic Certificates, and other sectoral provisions, along with pertinent legal instruments like Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), provide the main legal foundation.. However, although these regulations have provided an adequate normative framework, major challenges remain in the aspects of synchronization between regulations, the readiness of cybersecurity infrastructure, and weak coordination between authorized institutions. The condition opens up the potential for data manipulation, hacking, and the loss of integrity of the digital land administration system, which could have serious implications for land ownership security and public trust in the state.

Therefore, targeted strategic steps are needed, both in terms of regulation and technical implementation. Regulatory harmonization between the ITE Law, the PDP Law, and land regulations is essential to avoid overlapping authority and to clarify the legal responsibilities of each party. Furthermore, strengthening the role of relevant institutions, such as the ATR/BPN as land data managers, the Ministry of Communication and Informatics (Kominfo) as the telematics regulator, and the National Cyber and Crypto Agency (BSSN) as the cybersecurity authority, is crucial for building transparent, accountable, and secure data governance. The use of blockchain technology, or distributed ledger technology, can be an effective alternative to guarantee data integrity and authenticity verified by the system that cannot be manipulated. Furthermore, increasing human resource capacity and digital security literacy within agencies and the community is a crucial prerequisite for ensuring system security relies not only on technology but also on the readiness of the actors operating it. Thus, legal protection for digital land data can be realized comprehensively while strengthening public trust in digital transformation in the land sector.

ACKNOWLEDGMENTS

This section contains acknowledgments to institutions and individuals who have contributed to the implementation of the research and the preparation of this manuscript. The authors would like to express their sincere gratitude to all parties who have provided support, guidance, and assistance throughout the research process, including academic advisors, funding institutions, and other individuals or organizations whose contributions were invaluable to the completion of this study.

FUNDING INFORMATION

None.

CONFLICTING INTEREST STATEMENT

The authors state that there is no conflict of interest in the publication of this article.

BIBLIOGRAPHY

Adinegoro, Kurnia Rheza Randy. "Tantangan Implementasi Sertipikat Tanah Elektronik Di Kementerian Agraria Dan Tata Ruang/Badan Pertanahan Nasional Republik Indonesia." *Jurnal Ilmu Kenotariatan* 4, no. 2 (2023): 130–43.

Adnyani, I Kadek Dewi Sasih, Ratna Artha Windari, and Muhamad Jodi Setianto. "Pentingnya Sertifikat Tanah Elektronik Di Era Digital Sebagai Bukti Hak Kepemilikan Tanah." *Jurnal Komunitas Yustisia* 7, no. 2 (2024): 121–29.

Adnyani, I Kadek Dewi Sasih, Ratna Artha Windari, and Muhamad Jodi Setianto. "Pentingnya Sertifikat Tanah Elektronik Di Era Digital Sebagai Bukti Hak Kepemilikan Tanah." *Jurnal Komunitas Yustisia* 7, no. 2 (2024): 121–29.

Afif, Yuzi, and Muhammad Afif Mahfud. "Kepastian Hukum Terhadap Sertifikat Elektronik Hak Milik Atas Tanah." *Unes Law Review* 6, no. 2 (2023): 7605–11.

Alam, RG Guntur, Agung Kharisma Hidayah, Gunawan Gunawan, Ardi Wijaya, and Dedy Abdullah. *Manajemen Risiko Keamanan Informasi*. PT. Sonpedia Publishing Indonesia, 2025.

Avivah, Lisnadia Nur, Sutaryono Sutaryono, and Dwi Wulan Titik Andari. "Pentingnya Pendaftaran Tanah Untuk Pertama Kali Dalam Rangka Perlindungan Hukum Kepemilikan Sertifikat Tanah." *Tunas Agraria* 5, no. 3 (2022): 197–210.

Erfa, Riswan. "Digitalisasi Administrasi Pertanahan Untuk Mewujudkan Percepatan Pembangunan Nasional Perspektif Kebijakan Hukum (Legal Policy)." *Jurnal Pertanahan* 10, no. 1 (2020).

Ernawati, Dini, Asri Wijayanti, and Fajar Rachmad Dwi Miarsa. "Perlindungan Hukum Bagi Pemegang Sertipikat Tanah Elektronik." *Journal of Innovation Research and Knowledge* 4, no. 9 (2025): 7213–28.

Hidayah, Syarifaatul, Evi Hariyani, Lilis Mukarromah, Aprila Niravita, and M Adymas Hikal Fikri. "Tantangan Dan Peluang Sertifikat Elektronik Dalam Reformasi Pendaftaran Tanah Di Era Digital." *Jurnal Ilmiah Nusantara* 1, no. 6 (2024): 186–99.

Maesaroh, Risma Siti. "Tantangan Keamanan Siber Dan Implikasinya Terhadap Hukum Kenegaraan: Tinjauan Atas Peran Negara Dalam Menjamin Ketahanan Digital." *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 2 (2024): 255–74.

Noor, Aslan, Bekawita Wassir, Ira Anggraini, and Erlin Rahmaniah. "Implications of the Use of Electronic Certificates in Proving Land Rights According to the Civil Procedure Law." *Electronic Journal of Education, Social Economics and Technology* 5, no. 2 (2024): 276–81.

Nugraha, Joshua Paskah, Aris Prasetyo Kurniawan, Indriana Diani Putri, Ryan Kunto Wicaksono, and Tarisa Tarisa. "Penerapan Blockchain Untuk Pencegahan Sertipikat Tanah Ganda Di Kementerian Agraria Dan Tata Ruang/Badan Pertanahan Nasional." *Widya Bhumi* 2, no. 2 (2022): 123–35.

Pelapu, Indah Julitah. "Kepastian Hukum Penggunaan Tanda Tangan Elektronik Dalam Akta Notaris." *LEX PRIVATUM* 14, no. 2 (2024).

Priscilla, Michelle, Dini Laelatul Nova, and Septi Naelina Fajriah. "-Keabsahan Hukum Penerbitan Sertipikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Hak Atas Tanah Di Persidangan:-." *UIR Law Review* 8, no. 2 (2024): 68–84.

Samsul, Ainuddin, and Ikhsan Kamil. "Analisa Yuridis Pertanggungjawaban Badan Pertanahan Nasional Dalam Penyimpanan Dan Pengelolaan Sertifikat Tanah Elektronik: Studi Kasus Di Kantor Pertanahan Kabupaten Lombok Barat." *SIMPUL: Jurnal Ilmu Politik Dan Hukum* 1, no. 2 (2025): 43–48.

Selfianus Laritmas, SH, and SH Ahmad Rosidi. *Teori-Teori Negara Hukum*. Prenada Media, 2024.

Sitompul, Gabriel Amadeus, and Albert Lodewyk Sentosa Siahaan. "Analisis Terhadap Pembuatan Surat Pernyataan Keabsahan Dan Kebenaran Dokumen Elektronik Pada Sertifikat Hak Tanggungan." *Media Hukum Indonesia (MHI)* 2, no. 4 (2024): 20–33.

Suhattanto, Muh Arif, Sarjita Sarjita, Sukayadi Sukayadi, and Dian Aries Mujiburohman. "Kualitas Data Pertanahan Menuju Pelayanan Sertifikat Tanah Elektronik." *Widya Bhumi* 1, no. 2 (2021): 87–100.

Susilowati, Indri Fogar. "Tinjauan Yuridis Sertifikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Tanah Di Indonesia." *Novum: Jurnal Hukum* 1, no. 1 (2024): 57–71.

Susmana, Deva Sakti. "Transformasi Digital Dalam Administrasi Pertanahan: Analisis Yuridis Terhadap Sertipikat Tanah Elektronik." *Jurnal Impresi Indonesia* 4, no. 6 (2025): 2063–70.

Tejawati, Desy. "Asas Kepastian Hukum Dalam Kedudukan Girik Terhadap Sertipikat Hak Atas Tanah." *Jurnal Suara Hukum* 3, no. 2 (2021): 251–73.