

**ANALISIS KEPASTIAN HUKUM PENDAFTARAN TANAH DIGITAL:
STUDI KOMPARATIF INDONESIA, ESTONIA DAN SINGAPURA
LEGAL CERTAINTY ANALYSIS OF DIGITAL LAND REGISTRATION:
A COMPARATIVE STUDY OF INDONESIA, ESTONIA, AND SINGAPORE**

Andhika Purnama Seta

**Program Studi Magister Ilmu Hukum Fakultas Hukum
Universitas Al Azhar Indonesia**

Korespondensi Penulis : purseta@gmail.com

Citation Structure Recommendation :

Seta, Andhika Purnama. *Analisis Kepastian Hukum Pendaftaran Tanah Digital: Studi Komparatif Indonesia, Estonia dan Singapura*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.7. No.1 (2026).

ABSTRAK

Pendaftaran tanah digital di Indonesia menghadapi tantangan kepastian hukum akibat kerentanan integritas data dan keandalan sistem elektronik. Penelitian hukum normatif ini menganalisis kepastian hukum pendaftaran tanah digital melalui studi komparatif Indonesia, Estonia dan Singapura dengan pendekatan perundang-undangan, perbandingan, dan konseptual. Hasil penelitian menunjukkan regulasi Indonesia belum mengakomodasi keamanan siber secara komprehensif, sementara Estonia menjamin kepastian hukum melalui keterlacakan data berbasis *Keyless Signature Infrastructure* (KSI) *Blockchain* dan Singapura memperkuat akuntabilitas hukum melalui pengendalian *Zero Trust Architecture*. Penelitian ini merekomendasikan rekonstruksi regulasi Indonesia berbasis prinsip integritas data Estonia dan pengendalian akses Singapura guna menjamin kepastian hukum.

Kata Kunci: Hukum Komparatif, Keamanan Siber, Kepastian Hukum, Pendaftaran Tanah Digital

ABSTRACT

Digital land registration in Indonesia faces challenges regarding legal certainty due to vulnerabilities in data integrity and the reliability of electronic systems. This normative legal study analyses the legal certainty of digital land registration through a comparative study of Indonesia, Estonia and Singapore, employing legislative, comparative and conceptual approaches. The findings indicate that Indonesian regulations have not yet comprehensively addressed cybersecurity, whilst Estonia ensures legal certainty through data traceability based on the *Keyless Signature Infrastructure* (KSI) *Blockchain*, and Singapore strengthens legal accountability through *Zero Trust Architecture* controls. This study recommends a restructuring of Indonesian regulations based on Estonia's data integrity principles and Singapore's access controls to ensure legal certainty.

Keywords: Comparative Law, Cybersecurity, Legal Certainty, Digital Land Registration

A. PENDAHULUAN

Implementasi layanan pertanahan berbasis digital menandai fase penting perkembangan transformasi digital administrasi publik di Indonesia. Kondisi ini bertujuan untuk memodernisasi layanan pertanahan guna meningkatkan efisiensi, transparansi, serta mempercepat proses validasi data secara *real-time*. Perubahan sistem fisik menjadi sistem elektronik merupakan upaya pemerintah untuk meminimalisasi birokrasi yang rumit dan mempersempit ruang gerak mafia tanah yang selama ini memanfaatkan celah dalam administrasi dokumen berbasis kertas.¹ Namun, transisi tersebut memunculkan tantangan fundamental yang belum sepenuhnya teratasi, yaitu jaminan keamanan data pribadi dan integritas sistem informasi pertanahan dalam menghadapi ancaman siber yang semakin kompleks.²

Pada sektor pertanahan nasional, kebocoran data pribadi seperti nomor induk kependudukan (NIK), koordinat spasial dan riwayat kepemilikan bukan hanya sekadar masalah privasi, melainkan ancaman langsung terhadap kepastian hukum kepemilikan aset yang dapat memicu sengketa pertanahan di masa depan.³ Beberapa penelitian sebelumnya telah melakukan kajian tentang perlindungan hukum untuk masalah pendaftaran tanah secara digital. Hasilnya, bila dilihat secara umum dari kasus-kasus yang terjadi di dalam negeri, diperlukan penguatan aspek legal terhadap digitalisasi administrasi, peran institusi seperti Kementerian Agraria dan Tata Ruang (ATR)/Badan Pertanahan Nasional (BPN), serta efektivitas sistem sertipikat elektronik.⁴

Berdasarkan kepada laporan Badan Siber dan Sandi Negara (BSSN), Indonesia mencatatkan adanya anomali siber yang melampaui angka 330 juta kejadian pada tahun 2024 dan deteksi kebocoran data sebesar 241 dugaan, dengan sektor pemerintahan sebagai sasaran utamanya (183 dugaan atau 75,93%).⁵

¹ Indonesia, *Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Republik Indonesia tentang Sertipikat Elektronik*, Permen ATR/KBPN No.1 Tahun 2021, BN RI Tahun 2021 No.12.

² Suci Febrianti, *Perlindungan Hukum terhadap Pemegang Sertipikat Hak atas Tanah Elektronik*, Indonesian Notary, Vol.3, No.3 (September 2021), p.205.

³ Juliyanti Ni Kadek, I Made Dharsana dan Ni Made Ujianti, *Perlindungan Hukum terhadap Pemegang Sertifikat Tanah Digital Dikaitkan dengan Keamanan Data Pribadi*, Jurnal Preferensi Hukum, Vol.4, No.1 (Maret 2022), p.92.

⁴ Duma Indah Sari Lubis, Hakim Andi Lubis dan Rodiatun Adawiyah, *Analisis Yuridis Peranan Kantor ATR/BPN terhadap Penyelesaian Permasalahan Sengketa Batas Tanah*, Law Jurnal, Vol.1, No.1 (Juli 2024), p.47.

⁵ Badan Siber dan Sandi Negara, *Lanskap Keamanan Siber Indonesia 2024*, Badan Siber dan Sandi Negara, Jakarta, 2024, p.16.

Dominasi insiden kebocoran data di sektor publik mempertegas kebutuhan mendesak akan keamanan siber yang tangguh. Kondisi ini menunjukkan bahwa infrastruktur digital nasional masih memiliki kerentanan yang signifikan, terlebih dengan adanya insiden serangan *ransomware* di Pusat Data Nasional (PDN) pada tahun 2024 yang sempat melumpuhkan beberapa layanan publik.⁶

Implementasi digital pada dasarnya mempermudah dan mempercepat proses penerbitan dokumen pertanahan guna mewujudkan kepastian hukum.⁷ Namun, keberlanjutan kepastian hukum atas dokumen elektronik tersebut sangat bergantung pada keandalan sistem dan integritas pangkalan data pertanahan.⁸ Mengingat ancaman siber bersifat lintas batas (*borderless threats*), kerentanan pada infrastruktur digital di tingkat domestik berpotensi membuka celah manipulasi data.⁹ Oleh karena itu, penguatan arsitektur keamanan siber menjadi krusial bukan untuk menghambat digitalisasi, melainkan untuk melindungi integritas pangkalan data agar kepastian hukum yang telah tercipta melalui penerbitan dokumen elektronik tetap terjaga dari risiko perubahan tanpa hak. Upaya penguatan hukum yang mampu menyelaraskan standar teknologi global dengan perlindungan hak privasi merupakan syarat mutlak bagi keberhasilan digitalisasi pendaftaran tanah digital.¹⁶

Kondisi keamanan siber di Indonesia saat ini tampak kontras apabila dibandingkan dengan negara-negara pionir pendaftaran tanah digital seperti Estonia dan Singapura. Estonia dan Singapura menempati posisi 3 teratas negara paling digital di dunia, sementara negara Indonesia berada di posisi 64 secara global.¹⁰

⁶ Nurul Syafitri dan Hendrawarman, *Legal Review of Cyber Crime: Case of Attack On Center Data National Temporary 2*, Critical Legal Review, Vol.2, No.3 (Agustus 2025), p.43.

⁷ Silvia Theresia Abigail, dkk., *Efektivitas Digitalisasi Sistem Pendaftaran Tanah terhadap Peningkatan Pelayanan Publik dan Kepastian Hukum*, Jurnal Ilmiah Wahana Pendidikan, Vol.12, No.5D (Mei 2026), p.188.

⁸ Arifin Habibi, Ghally Sukma Prambudi, Tuti Trisnawati dan Ratna Wulandari, *Transformasi Digital Administrasi Pertanahan: Implementasi dan Tantangan Sertipikat Elektronik di Indonesia*, Rio Law, Vol.6, No.1 (Februari 2025).

⁹ Imanuel Toding Bua dan Nur Isdah Idris, *Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024*, Asosiasi Seni Desain dan Komunikasi Visual Indonesia) Desentralisasi : Jurnal Hukum, Kebijakan Publik dan Pemerintahan, Vol.2, No.2 (Mei 2025).

¹⁰ United Nations, *E-Government Survey 2024 Accelerating Digital Transformation for Sustainable Development With the addendum on Artificial Intelligence*, United Nations, New York, 2024, p.22.

Estonia merupakan pelopor tata kelola digital dunia yang berhasil mengamankan sistem *e-Land Register* melalui pemanfaatan teknologi *Keyless Signature Infrastructure (KSI) Blockchain*.¹¹ Pendekatan desentralisasi ini terbukti mampu memitigasi risiko manipulasi data dan menjamin integritas sertipikat tanah elektronik dari serangan luar.¹²

Singapura merupakan representasi terbaik di kawasan regional *Association of Southeast Asian Nations (ASEAN)* yang menempati peringkat teratas dalam *Global Cybersecurity Index*.⁷ Melalui *Cyber Security Agency (CSA)*, Singapura menerapkan strategi keamanan siber terpusat yang mewajibkan sistem pengelolaan data publik, termasuk administrasi pertanahan digital oleh *Singapore Land Authority*, dikategorikan sebagai *Critical Information Infrastructure (CII)* berdasarkan *Cybersecurity Act*. Dalam implementasinya, Singapura mengadopsi *Zero Trust Architecture (ZTA)* yang menerapkan prinsip *never trust, always verify*, sehingga setiap pengguna, perangkat dan aplikasi harus melalui proses autentikasi dan otorisasi secara berkelanjutan sebelum memperoleh akses ke sistem. Pendekatan ini memperkuat perlindungan terhadap ancaman siber, baik dari pihak eksternal maupun penyalahgunaan akses oleh pihak internal.¹³

Melalui pendekatan perbandingan hukum, penelitian ini menganalisis kesenjangan regulasi dan arsitektur keamanan siber dalam penyelenggaraan pendaftaran tanah digital di Indonesia dengan membandingkan praktik terbaik Estonia dan Singapura. Perbandingan tersebut dilakukan untuk merumuskan kerangka penguatan hukum yang mampu mengintegrasikan standar keamanan siber dalam rangka menjamin integritas data, keandalan sistem dan kepastian hukum pendaftaran tanah digital. Penguatan hukum dilakukan berdasarkan Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Republik Indonesia Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah.

¹¹ Meelis Kitsing, *Alternative Futures for Digital Governance*, ACM International Conference Proceeding Series, New York, 2019, p.48.

¹² Clare Sullivan dan Eric Burger, *E-Residency and Blockchain*, *Computer Law and Security Review*, Vol.33, No.4 (Agustus 2017), p.13.

¹³ Cybersecurity Agency of Singapore, *The Singapore Cybersecurity Strategy 2021*, Cyber Security Agency of Singapore, Singapura, 2021, p.17.

Berbeda dengan penelitian terdahulu yang umumnya berfokus pada aspek perlindungan hukum sertipikat elektronik atau perlindungan data pribadi, banyak kajian yang menganalisis keterkaitan antara tata kelola keamanan siber dan kepastian hukum dalam penyelenggaraan pendaftaran tanah digital melalui pendekatan perbandingan hukum.¹⁴ Penelitian ini menawarkan analisis komparatif Indonesia, Estonia dan Singapura untuk merumuskan model penguatan regulasi yang mewajibkan penerapan teknologi keamanan siber sebagai instrumen hukum dalam melindungi integritas data dan meningkatkan kepastian hukum ekosistem pendaftaran tanah digital Indonesia. Berdasarkan latar belakang tersebut, rumusan masalah dari penelitian yang diberi judul "Analisis Kepastian Hukum Pendaftaran Tanah Digital: Studi Komparatif Indonesia, Estonia, dan Singapura" adalah:

1. Bagaimana pengaturan dan kerentanan regulasi keamanan siber dalam pendaftaran tanah digital di Indonesia dalam menjamin kepastian hukum?
2. Bagaimana penguatan regulasi keamanan siber dalam pendaftaran tanah digital di Indonesia dapat dilakukan melalui studi komparatif dengan Estonia dan Singapura?

B. PEMBAHASAN

1. Pengaturan Hukum Keamanan Siber dalam Sistem Pendaftaran Tanah Digital di Indonesia dan Implikasinya terhadap Kepastian Hukum

Transformasi penyelenggaraan pendaftaran tanah dari sistem konvensional menuju sistem elektronik merupakan bagian dari reformasi administrasi pertanahan di Indonesia yang bertujuan untuk meningkatkan kualitas pelayanan publik sekaligus memberikan kepastian hukum atas hak atas tanah. Landasan hukum transformasi tersebut pada awalnya diatur melalui Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 1 Tahun 2021 tentang Sertipikat Elektronik, yang kemudian disempurnakan melalui Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah.¹⁵

¹⁴ Arum Puspa Pradhipta dan I Gusti Nyoman Krisnadi Yudiantara, *Analisis Regulasi Perlindungan Data Pribadi terhadap Kasus Kebocoran Data di Indonesia*, Jurnal Media Akademik, Vol.3, No.7 (Juli 2025).

Kedua peraturan tersebut mengatur penggunaan dokumen elektronik, tanda tangan elektronik dan sistem elektronik dalam penyelenggaraan pendaftaran tanah sebagai bagian dari upaya meningkatkan efisiensi pelayanan, akuntabilitas administrasi, serta keandalan pengelolaan data pertanahan. Namun, penyelenggaraan pendaftaran tanah berbasis elektronik juga menimbulkan konsekuensi hukum berupa kebutuhan akan pengaturan keamanan siber yang mampu menjamin kerahasiaan, integritas dan ketersediaan data pertanahan. Dengan demikian, kepastian hukum atas hak atas tanah dalam era digital tidak lagi semata-mata ditentukan oleh pengakuan normatif terhadap dokumen elektronik, tetapi juga oleh efektivitas pengaturan keamanan siber yang menjamin kendala sistem elektronik sebagai media penyelenggaraan pendaftaran tanah.²

Kebutuhan akan pengaturan keamanan siber dalam penyelenggaraan pendaftaran tanah digital tidak dapat dipisahkan dari konsep kepastian hukum dalam hukum pertanahan. Kepastian hukum tidak hanya dimaknai sebagai adanya norma yang mengatur hak atas tanah, tetapi juga sebagai jaminan bahwa data mengenai subjek hukum, objek hukum dan status hak atas tanah memiliki keaslian, integritas, serta dapat dipertanggungjawabkan secara hukum.¹⁵ Dalam penyelenggaraan pendaftaran tanah berbasis elektronik, kepastian hukum tidak lagi hanya bergantung pada validitas dokumen elektronik, tetapi juga pada kemampuan penyelenggara sistem elektronik untuk menjamin kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) informasi sebagaimana dikenal dalam konsep CIA Triad. Ketiga prinsip tersebut merupakan fondasi keamanan informasi sekaligus menjadi praktik terbaik yang diadopsi dalam standar ISO/IEC 27001 tentang *Information Security Management System* (ISMS), sehingga dapat digunakan sebagai parameter untuk menilai kecukupan pengaturan hukum keamanan siber dalam penyelenggaraan pendaftaran tanah digital.¹⁶

Urgensi penerapan keamanan siber dalam penyelenggaraan pendaftaran tanah digital semakin nyata apabila dikaitkan dengan kondisi keamanan siber nasional.

¹⁵ Ni Komang, dkk., *Analisis Kepastian Hukum terhadap Standar Keamanan Sertifikat Elektronik dalam Kepemilikan Tanah*, Sarana Komunikasi Dosen dan Mahasiswa, Vol.20, No.1 (Maret 2026), p.67.

¹⁶ International Organization for Standardization (ISO), *Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements (ISO/IEC 27001:2022)*, ISO, Geneva, 2022.

Berdasarkan *Lanskap Keamanan Siber Indonesia Tahun 2024* yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), jumlah maupun kompleksitas serangan siber terhadap infrastruktur digital nasional terus mengalami peningkatan.⁵ Salah satu peristiwa yang menunjukkan kerentanan tersebut adalah serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) pada tahun 2024 yang mengakibatkan terganggunya berbagai layanan publik berbasis elektronik. Meskipun serangan tersebut tidak secara langsung menyasar sistem pendaftaran tanah, peristiwa tersebut menunjukkan bahwa penyelenggaraan layanan publik berbasis sistem elektronik memiliki tingkat kerentanan yang dapat mengganggu keandalan data, kontinuitas layanan, serta perlindungan hak-hak keperdataan masyarakat jika tidak didukung oleh pengaturan keamanan siber yang memadai.⁹

Kerentanan sistem elektronik sebagaimana tercermin dalam berbagai insiden keamanan siber menunjukkan bahwa ancaman terhadap penyelenggaraan pendaftaran tanah digital dapat berasal dari berbagai sumber. Secara umum, risiko keamanan siber dalam sistem pendaftaran tanah digital dapat diklasifikasikan menjadi dua bentuk utama, yaitu serangan eksternal (*external cyber attacks*) dan ancaman internal (*insider threats*). Serangan eksternal dapat berupa akses tanpa otorisasi terhadap basis data pertanahan, manipulasi data kepemilikan tanah, perubahan data spasial, maupun penerbitan sertifikat elektronik secara tidak sah.^{17,18} Ancaman tersebut berpotensi mengganggu keandalan data elektronik yang menjadi dasar penerbitan sertifikat hak atas tanah serta menimbulkan sengketa mengenai keabsahan data pertanahan. Oleh karena itu, efektivitas perlindungan hukum terhadap sertifikat elektronik tidak hanya bergantung pada pengakuan normatif terhadap dokumen elektronik, tetapi juga pada kecukupan pengaturan keamanan siber yang mampu melindungi sistem elektronik dari akses tanpa hak, manipulasi data dan gangguan terhadap integritas informasi pertanahan.¹⁹

¹⁷ Ach Farhan Arif, Herowati Poesoko dan Miftahul Munir, *Mitigasi Risiko Keamanan Data dalam Implementasi Sertifikat Tanah Elektronik Untuk Mewujudkan Kepastian Hukum bagi Pemegang Hak atas Tanah*, Jurnal Hukum Pelita, Vol.6, No.1 (Mei 2025), p.84.

¹⁸ Azis Budianto, *Land Certificate Forgery Methods and the Structure of Criminal Networks as Well as Legal Reform Efforts to Strengthen Rights Certainty and Law Enforcement*, Greenation International Journal of Law and Social Sciences, Vol.3, No.3 (November 2025), p.1332.

¹⁹ Achmad M. Fitriady dan A. I. Wisnubroto, *Dampak Yuridis, Teknis dan Sosial Penerapan E-Sertifikat dalam Sertifikat Tanah di Penajam Paser Utara Tidak ada entri indeks yang ditemukan*, Al-Zayn: Jurnal Ilmu Sosial, Vol.4, No.1 (Desember 2025), p.5440.

Perlindungan hukum atas risiko serangan eksternal dalam penyelenggaraan pendaftaran tanah digital diatur dalam Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah. Pasal 3 ayat (1) mewajibkan penyelenggaraan sistem elektronik yang andal, aman dan bertanggung jawab. Selanjutnya, Pasal 4 ayat (2) dan ayat (3) mengatur bahwa dokumen elektronik harus memuat data yang valid dan autentik serta disimpan dalam pangkalan data sistem elektronik, sedang Pasal 5 ayat (2) mewajibkan penggunaan tanda tangan elektronik. Ketentuan tersebut menjadi dasar hukum dalam menjaga keaslian, integritas dan autentisitas dokumen elektronik serta mencegah pemalsuan dan manipulasi data pertanahan.²⁰ Meskipun demikian, Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023 belum mengatur secara eksplisit standar keamanan siber yang wajib diterapkan, seperti pengendalian akses berbasis risiko, audit keamanan informasi, maupun mekanisme pemantauan ancaman siber secara berkelanjutan. Akibatnya, efektivitas perlindungan hukum terhadap serangan eksternal masih bergantung pada implementasi teknis oleh penyelenggara sistem elektronik, sehingga belum sepenuhnya memberikan jaminan preventif terhadap ancaman siber maupun kepastian hukum atas keandalan data pertanahan.

Ancaman internal merupakan risiko yang timbul ketika pejabat atau pegawai yang memiliki hak akses sistem informasi menyalahgunakan kewenangannya untuk mengubah, menghapus, atau membocorkan data pertanahan demi kepentingan tertentu. Berbeda dengan serangan eksternal yang berasal dari pihak di luar sistem, ancaman ini berasal dari pengguna yang memiliki otorisasi sehingga lebih sulit dideteksi dan berpotensi memengaruhi integritas data pertanahan.¹⁶ Risiko tersebut semakin meningkat apabila pengaturan mengenai tata kelola keamanan informasi, pengendalian hak akses dan mekanisme pengawasan terhadap penggunaan sistem elektronik belum diterapkan secara memadai. Kondisi ini dapat mengurangi keabsahan data pertanahan yang menjadi dasar penerbitan sertifikat elektronik serta berimplikasi pada berkurangnya kepastian hukum bagi pemegang hak atas tanah.²¹

²⁰ Indonesia, *Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah*, Permen ATR/Kepala BPN No.3 Tahun 2023, BN Tahun 2023 No.461.

²¹ Muhammad Sahal Fikri dan Ratih Damayanti, *Sistem Keamanan pada Digitalisasi Pendaftaran Tanah di Indonesia*, UNNES Pres, Semarang, 2025, p.610.

Dalam konteks ancaman internal, Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023 juga memberikan dasar hukum untuk menjaga akuntabilitas pengelolaan dokumen elektronik. Kewajiban penyelenggaraan sistem elektronik yang andal dan aman, penggunaan dokumen elektronik yang valid dan autentik, serta pengesahan melalui tanda tangan elektronik sebagaimana diatur dalam Pasal 3 ayat (1), Pasal 4 ayat (2) dan ayat (3), serta Pasal 5 ayat (2), memungkinkan setiap perubahan data dilakukan melalui mekanisme yang dapat diverifikasi dan dipertanggungjawabkan. Dengan demikian, ketentuan tersebut berfungsi membatasi peluang penyalahgunaan kewenangan oleh pengguna yang memiliki hak akses terhadap sistem elektronik.

Meskipun demikian, Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023 belum mengatur secara eksplisit mekanisme pengendalian terhadap ancaman internal, seperti pembatasan hak akses berdasarkan tingkat kewenangan (*role-based access control*), pencatatan aktivitas pengguna (*audit trail*), pemisahan fungsi (*segregation of duties*), maupun audit keamanan informasi secara berkala. Akibatnya, pencegahan terhadap penyalahgunaan hak akses masih bergantung pada kebijakan teknis penyelenggara sistem elektronik dan belum memberikan perlindungan hukum yang optimal terhadap integritas data pertanahan. Kondisi tersebut berpotensi memengaruhi keabsahan data yang menjadi dasar penerbitan sertifikat elektronik serta mengurangi kepastian hukum bagi pemegang hak.

Berdasarkan uraian tersebut, dapat dipahami bahwa pengaturan hukum keamanan siber dalam penyelenggaraan pendaftaran tanah digital di Indonesia telah memberikan landasan normatif melalui pengaturan mengenai penyelenggaraan sistem elektronik yang andal, penggunaan dokumen elektronik yang valid dan autentik, serta penerapan tanda tangan elektronik. Pengaturan tersebut telah menyediakan kerangka perlindungan hukum terhadap risiko serangan eksternal maupun ancaman internal sebagai bagian dari upaya mewujudkan kepastian hukum dalam penyelenggaraan pendaftaran tanah digital. Namun demikian, pengaturan yang berlaku masih bersifat umum dan belum mengatur secara spesifik standar keamanan siber yang komprehensif, seperti pengendalian akses berbasis risiko (*risk-based access control*), pencatatan aktivitas (*audit trail*), pemantauan ancaman siber berkelanjutan, maupun pengelolaan hak akses berdasarkan tingkat kewenangan.

Keterbatasan tersebut menunjukkan bahwa kepastian hukum dalam pendaftaran tanah digital tidak hanya bergantung pada pengakuan normatif terhadap dokumen elektronik, tetapi juga pada kecukupan pengaturan keamanan siber yang mampu menjamin integritas, keandalan dan akuntabilitas sistem elektronik. Oleh karena itu, diperlukan analisis komparatif terhadap pengaturan keamanan siber dalam sistem pendaftaran tanah digital di Indonesia, Estonia dan Singapura untuk menilai kecukupan pengaturan hukum yang berlaku serta mengidentifikasi praktik terbaik yang dapat menjadi dasar penguatan pengaturan hukum di Indonesia.

2. Analisis Komparatif Pengaturan dan Arsitektur Keamanan Siber Pendaftaran Tanah Digital Indonesia, Estonia dan Singapura terhadap Kepastian Hukum

Analisis komparatif dalam penelitian ini dilakukan untuk menilai kecukupan pengaturan keamanan siber dalam penyelenggaraan pendaftaran tanah digital di Indonesia melalui perbandingan dengan Estonia dan Singapura. Kedua negara dipilih karena telah mengembangkan sistem pendaftaran tanah digital yang didukung oleh kerangka keamanan siber yang berbeda. Estonia menerapkan pengamanan berbasis *Keyless Signature Infrastructure (KSI) Blockchain* yang menitikberatkan pada perlindungan integritas data dan jejak audit (*audit trail*), sedangkan Singapura mengembangkan pendekatan *Zero Trust Architecture (ZTA)* yang berfokus pada verifikasi akses secara berkelanjutan dan pengendalian hak akses berbasis risiko. Mengingat penelitian ini menggunakan pendekatan hukum komparatif, perbandingan dilakukan berdasarkan beberapa aspek hukum dan keamanan siber yang berkaitan dengan penyelenggaraan pendaftaran tanah digital sebagaimana disajikan pada Tabel 1.

Aspek	Indonesia	Estonia	Singapura
Dasar Hukum	Permen ATR/BPN No. 3 Tahun 2023	<i>Land Register Act, Cybersecurity Act, Public Information Act</i> ²²	<i>Land Titles Act, Cybersecurity Act 2018, Personal Data Protection Act 2012 (PDPA)</i> ²³

²² Riigi Teataja, *Ligipäasetavus*, diakses dari <https://www.riigiteataja.ee/et>, diakses pada 27 Juni 2026, jam 22.15 WIB.

²³ A Singapore Government Agency Website, *Singapore Statutes Online*, diakses dari <https://sso.agc.gov.sg/Act>, diakses pada 27 Juni 2026, jam 23.41 WIB.

Model Keamanan Siber	Sistem elektronik dengan dokumen dan tanda tangan elektronik ¹⁹	KSI <i>Blockchain</i> ⁸	<i>Zero Trust Architecture</i> ¹⁰
Perlindungan Integritas Data	Validasi dokumen elektronik dan tanda tangan elektronik ¹⁹	<i>Hash chaining, KSI Blockchain, audit trail</i> ⁸	<i>Continuous verification dan data integrity control</i> ¹⁰
Pengendalian Hak Akses	Diatur secara umum ¹⁹	<i>Digital identity dan role-based authorization</i> ⁸	<i>Least privilege, multi-factor authentication, Zero Trust</i> ¹⁰
Audit dan Pemantauan	Belum diatur secara spesifik dalam Permen ATR/BPN No. 3 Tahun 2023	<i>Audit trail permanen dan verifikasi integritas</i> ²¹	<i>Continuous monitoring dan security analytics</i> ²²
Implikasi Terhadap Kepastian Hukum	Menjamin keabsahan dokumen elektronik, tetapi belum mengatur standar keamanan siber secara spesifik	Menjamin integritas data dan keterlacakan perubahan sehingga memperkuat kepastian hukum	Menjamin autentikasi, pengendalian akses, dan akuntabilitas sistem sehingga memperkuat kepastian hukum

Tabel 1. Parameter Analisis Komparatif

Sumber: Kreasi Penulis diolah dari berbagai sumber

Analisis berdasarkan parameter komparasi pada Tabel 1 dilakukan secara sistematis terhadap pengaturan keamanan siber dalam penyelenggaraan pendaftaran tanah digital di Indonesia, Estonia dan Singapura. Pembahasan diawali dengan Indonesia sebagai dasar pembandingan (*baseline*) untuk menilai sejauh mana pengaturan hukum nasional telah mengakomodasi perlindungan terhadap data pertanahan dalam sistem elektronik.

Selanjutnya, analisis diarahkan pada Estonia dan Singapura sebagai negara yang telah mengembangkan tata kelola keamanan siber yang lebih maju melalui penerapan KSI *Blockchain* dan ZTA. Perbandingan tersebut difokuskan pada ruang lingkup pengaturan hukum, mekanisme perlindungan data, pengendalian akses, audit keamanan, serta implikasinya terhadap terwujudnya kepastian hukum dalam penyelenggaraan pendaftaran tanah digital.

Indonesia telah memiliki landasan hukum yang mengatur penyelenggaraan pendaftaran tanah digital melalui Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah.

Pengaturan tersebut memberikan dasar hukum bagi penggunaan dokumen elektronik, tanda tangan elektronik dan penyelenggaraan sistem elektronik dalam kegiatan pendaftaran tanah sebagai bentuk modernisasi administrasi pertanahan yang mendukung kepastian hukum. Meskipun demikian, apabila dibandingkan dengan parameter analisis pada Tabel 1, pengaturan hukum di Indonesia masih berfokus pada legalitas penyelenggaraan sistem elektronik dan keabsahan dokumen elektronik.

Peraturan tersebut belum mengatur secara khusus standar keamanan siber yang wajib diterapkan dalam sistem pendaftaran tanah digital, seperti mekanisme *risk-based access control*, *audit trail*, *continuous security monitoring*, maupun pengamanan integritas data melalui teknologi tertentu. Akibatnya, perlindungan terhadap data pertanahan masih bergantung pada implementasi teknis oleh penyelenggara sistem elektronik dan belum sepenuhnya dibangun melalui pengaturan hukum yang komprehensif. Kondisi tersebut menunjukkan bahwa pengaturan hukum di Indonesia telah memberikan legitimasi terhadap penyelenggaraan pendaftaran tanah digital, tetapi belum mengintegrasikan pengaturan keamanan siber sebagai instrumen yang secara khusus menjamin integritas, autentisitas dan akuntabilitas data pertanahan. Oleh karena itu, diperlukan perbandingan dengan negara yang telah mengembangkan pengaturan keamanan siber secara lebih komprehensif dalam sistem pendaftaran tanah digital, yaitu Estonia dan Singapura.

Estonia merupakan salah satu negara yang paling maju dalam pemerintahan digital (*e-Government*), termasuk di dalam sistem pendaftaran tanah digital.

Berbeda dengan Indonesia yang mengatur keamanan sistem elektronik secara umum, Estonia membangun sistem pendaftaran tanah digital melalui kerangka hukum yang mengintegrasikan pengaturan administrasi pertanahan berdasarkan *Land Register Act*, keamanan siber berdasarkan *Cybersecurity Act* (*Küberturvalisuse seadus*), serta tata kelola informasi publik berdasarkan *Public Information Act*. Ketiga regulasi tersebut secara bersama-sama menjadi dasar penyelenggaraan layanan publik digital yang aman, andal dan akuntabel. Pengaturan tersebut menempatkan keamanan siber sebagai bagian yang tidak terpisahkan dari penyelenggaraan administrasi publik, sehingga perlindungan terhadap data pertanahan memperoleh legitimasi hukum yang kuat.

Land Register Act mengatur penyelenggaraan registrasi hak atas tanah secara elektronik dengan menekankan keakuratan, keabsahan dan keterbukaan data pertanahan. Sementara itu, *Cybersecurity Act* mengatur kewajiban penyelenggara layanan digital untuk menerapkan langkah-langkah keamanan terhadap sistem informasi yang digunakan dalam penyelenggaraan layanan publik, termasuk pengelolaan risiko keamanan siber, pelaporan insiden, serta perlindungan terhadap infrastruktur informasi yang bersifat penting. Di sisi lain, *Public Information Act* mengatur tata kelola informasi publik berbasis elektronik yang menekankan integritas, ketersediaan dan keandalan data dalam sistem pemerintahan digital. Ketiga regulasi tersebut menunjukkan bahwa keamanan informasi dalam pendaftaran tanah digital Estonia tidak hanya dipandang sebagai aspek teknis, tetapi juga sebagai bagian dari tata kelola hukum administrasi publik.

Berbeda dengan Indonesia yang belum menentukan model keamanan siber tertentu dalam regulasi pendaftaran tanah, Estonia mengintegrasikan KSI *Blockchain* sebagai mekanisme verifikasi integritas data dalam ekosistem pemerintahan digital yang mendukung keandalan layanan registrasi pertanahan. KSI *Blockchain* tidak berfungsi sebagai media penyimpanan data pertanahan, melainkan sebagai mekanisme kriptografi yang menghasilkan nilai *hash* terhadap perubahan data sehingga setiap modifikasi dapat diverifikasi dan ditelusuri (*audit trail*) tanpa mengubah data asli. Dengan mekanisme tersebut, setiap perubahan terhadap data pertanahan dapat diketahui apabila terjadi manipulasi atau akses yang tidak sah sehingga meningkatkan keandalan sistem elektronik.

Dari perspektif kepastian hukum, pengaturan tersebut memberikan perlindungan yang lebih komprehensif dibandingkan dengan Indonesia. Integrasi antara *Land Register Act*, *Cybersecurity Act*, serta penerapan KSI *Blockchain* sebagai mekanisme pengamanan digital tidak hanya memperkuat penyelenggaraan pendaftaran tanah digital, tetapi juga memastikan bahwa setiap perubahan data memiliki mekanisme verifikasi dan keterlacakan yang dapat dipertanggungjawabkan secara hukum. Dengan demikian, keabsahan data pertanahan tidak hanya bergantung pada pengakuan terhadap dokumen elektronik, tetapi juga pada mekanisme keamanan siber yang mampu mencegah manipulasi data serta memperkuat kepercayaan terhadap sistem pendaftaran tanah digital.

Singapura merupakan salah satu negara dengan tingkat kematangan transformasi digital tertinggi di kawasan Asia Tenggara yang menjadikan keamanan siber sebagai elemen utama dalam penyelenggaraan pemerintahan digital (*e-Government*). Berbeda dengan Estonia yang membangun keamanan sistem pendaftaran tanah digital melalui integrasi antara regulasi administrasi pertanahan, keamanan siber dan mekanisme verifikasi integritas data berbasis KSI *Blockchain*, Singapura mengembangkan pendekatan keamanan siber yang berorientasi pada pengelolaan risiko, perlindungan infrastruktur digital kritis dan pengendalian akses terhadap sistem elektronik. Pendekatan tersebut menempatkan keamanan siber bukan hanya sebagai perlindungan teknis terhadap ancaman digital, tetapi juga sebagai bagian dari tata kelola pemerintahan digital untuk menjamin keandalan, kerahasiaan, integritas dan ketersediaan informasi.

Kerangka hukum keamanan siber Singapura terutama dibangun melalui *Cybersecurity Act 2018* yang memberikan dasar kewenangan kepada Cyber Security Agency of Singapore (CSA) untuk mengatur, mengawasi dan meningkatkan ketahanan sistem informasi yang memiliki kepentingan strategis bagi negara. Melalui pengaturan tersebut, Singapura menetapkan kewajiban bagi penyelenggara *Critical Information Infrastructure* (CII) untuk menerapkan langkah-langkah pengamanan, melakukan pengelolaan risiko keamanan siber, serta melaporkan insiden keamanan yang dapat memengaruhi keberlangsungan layanan digital.

Selain itu, perlindungan terhadap informasi elektronik juga diperkuat melalui *Personal Data Protection Act 2012* (PDPA), yang mengatur kewajiban organisasi dalam melakukan pengumpulan, penggunaan, penyimpanan dan perlindungan data pribadi secara bertanggung jawab. Integrasi antara regulasi keamanan siber dan perlindungan data tersebut membentuk kerangka hukum yang mendukung penyelenggaraan layanan publik digital secara aman dan terpercaya.

Dalam konteks administrasi pertanahan digital, Singapura menyelenggarakan layanan pertanahan melalui sistem elektronik yang dikelola oleh *Singapore Land Authority* (SLA) sebagai bagian dari ekosistem pemerintahan digital nasional. Berbeda dengan Estonia yang secara eksplisit menggunakan KSI *Blockchain* untuk memperkuat keterlacakan perubahan data, Singapura lebih menekankan penerapan prinsip keamanan berlapis (*defence-in-depth*) dan pengelolaan risiko untuk memastikan bahwa sistem digital pemerintahan tetap tersedia dan terlindungi dari berbagai bentuk ancaman siber. Pendekatan tersebut sejalan dengan kebijakan keamanan siber nasional Singapura yang menempatkan perlindungan infrastruktur digital sebagai komponen penting dalam menjaga kepercayaan publik terhadap layanan pemerintahan berbasis elektronik.

Salah satu pendekatan utama yang dikembangkan dalam penguatan keamanan siber Singapura adalah penerapan *Zero Trust Architecture* (ZTA). Berbeda dengan pendekatan keamanan tradisional yang mengandalkan batas keamanan jaringan (*perimeter-based security*), ZTA menerapkan prinsip bahwa setiap pengguna, perangkat, maupun koneksi tidak dapat secara otomatis dipercaya dan harus selalu melalui proses verifikasi sebelum memperoleh akses terhadap sumber daya digital. Prinsip “*never trust, always verify*” tersebut diwujudkan melalui mekanisme autentikasi berlapis, pengendalian akses berbasis identitas dan risiko, pemantauan aktivitas secara berkelanjutan, serta segmentasi sistem untuk membatasi dampak apabila terjadi kompromi keamanan.

Penerapan *Zero Trust Architecture* memiliki relevansi yang kuat terhadap penyelenggaraan pendaftaran tanah digital karena sistem pertanahan menyimpan data yang memiliki nilai hukum dan ekonomi yang tinggi. Melalui pendekatan tersebut, perlindungan data pertanahan tidak hanya dilakukan setelah terjadi pelanggaran keamanan, tetapi dimulai sejak proses pemberian akses terhadap sistem.

Setiap permintaan akses diverifikasi berdasarkan identitas pengguna, kewenangan, kondisi perangkat, serta tingkat risiko, sehingga potensi penyalahgunaan akses internal maupun eksternal dapat diminimalkan. Dengan demikian, keamanan siber berfungsi sebagai instrumen preventif yang mendukung perlindungan terhadap integritas dan kerahasiaan data pertanahan.

Dari perspektif kepastian hukum, pendekatan Singapura menunjukkan bahwa keamanan sistem pendaftaran tanah digital tidak hanya bergantung pada pengakuan hukum terhadap dokumen elektronik, tetapi juga pada kemampuan sistem dalam mencegah, mendeteksi dan merespons ancaman siber. Integrasi antara *Cybersecurity Act*, regulasi perlindungan data, serta penerapan prinsip ZTA memberikan mekanisme pengendalian yang memastikan bahwa akses dan pemrosesan data dilakukan secara sah, terverifikasi dan dapat dipertanggungjawabkan. Oleh karena itu, berbeda dengan Estonia yang memperkuat kepastian hukum melalui jaminan integritas dan keterlacakan perubahan data, Singapura memperkuat kepastian hukum melalui mekanisme pengendalian akses dan manajemen risiko keamanan siber yang berkelanjutan.

Berdasarkan analisis komparatif tersebut, terlihat bahwa perbedaan utama antara Indonesia, Estonia dan Singapura terletak pada tingkat integrasi antara regulasi dan arsitektur keamanan siber dalam mendukung pendaftaran tanah digital. Indonesia telah memiliki dasar hukum penyelenggaraan sistem elektronik, namun belum secara spesifik menetapkan model keamanan siber sebagai instrumen perlindungan data pertanahan. Sebaliknya, Estonia memperkuat kepastian hukum melalui jaminan integritas dan keterlacakan data berbasis KSI *Blockchain*, sedangkan Singapura menekankan pengendalian akses dan manajemen risiko melalui pendekatan ZTA. Dengan demikian, kepastian hukum dalam pendaftaran tanah digital tidak hanya bergantung pada pengakuan terhadap dokumen elektronik, tetapi juga pada penerapan mekanisme keamanan siber yang mampu menjamin integritas, autentisitas dan perlindungan data secara berkelanjutan.

3. Rekonstruksi Penguatan Regulasi Keamanan Siber dalam Pendaftaran Tanah Digital di Indonesia melalui Adopsi Model Estonia dan Singapura

Berdasarkan hasil analisis komparatif, kelemahan utama pengaturan keamanan siber pendaftaran tanah digital di Indonesia terletak pada belum adanya

pengaturan yang secara spesifik menghubungkan aspek hukum pertanahan dengan arsitektur keamanan siber. Regulasi yang berlaku saat ini telah memberikan dasar hukum terhadap penggunaan dokumen elektronik dan penyelenggaraan sistem elektronik, tetapi belum menjadikan keamanan siber sebagai bagian integral dari jaminan kepastian hukum atas data pertanahan. Akibatnya, perlindungan terhadap data pertanahan masih lebih berorientasi pada validitas administratif, sementara aspek pencegahan manipulasi data, keterlacakan perubahan, dan pengendalian akses belum diatur secara komprehensif. Oleh karena itu, rekonstruksi regulasi keamanan siber pendaftaran tanah digital Indonesia perlu diarahkan pada pembentukan kerangka hukum yang menempatkan keamanan siber sebagai unsur substantif dalam penyelenggaraan administrasi pertanahan digital. Rekonstruksi tersebut tidak dimaksudkan untuk menggantikan regulasi yang telah ada, tetapi untuk memperkuatnya melalui pengaturan khusus mengenai standar keamanan data pertanahan, kewajiban pengelolaan risiko, mekanisme audit keamanan, pelaporan insiden, serta akuntabilitas pihak yang memiliki kewenangan terhadap sistem elektronik pertanahan.

Dalam aspek teknis hukum, model rekonstruksi perlu mengadopsi prinsip jaminan integritas data dari Estonia dengan memastikan bahwa setiap perubahan terhadap data pertanahan memiliki mekanisme verifikasi dan jejak digital yang dapat ditelusuri. Penerapan teknologi seperti *cryptographic hashing* dan *immutable audit trail* dapat menjadi lapisan pengamanan tambahan untuk memperkuat autentisitas serta mencegah perubahan data tanpa kewenangan. Dengan demikian, kepastian hukum tidak hanya didasarkan pada penerbitan sertifikat elektronik, tetapi juga pada kemampuan sistem untuk membuktikan keutuhan dan riwayat perubahan data.

Selain integritas data, rekonstruksi juga perlu mengadopsi prinsip pengendalian akses berbasis risiko dari Singapura melalui penerapan pendekatan *Zero Trust Architecture*. Dalam konteks pendaftaran tanah digital, setiap akses terhadap data harus didasarkan pada verifikasi identitas, kewenangan dan tingkat risiko pengguna. Pendekatan ini diperlukan untuk mengurangi potensi penyalahgunaan akses, baik dari pihak eksternal maupun internal, sehingga keamanan data pertanahan tidak hanya bergantung pada perlindungan infrastruktur,

tetapi juga pada tata kelola akses yang terukur. Dengan demikian, model rekonstruksi keamanan siber pendaftaran tanah digital Indonesia perlu dibangun melalui integrasi tiga aspek utama, yaitu penguatan regulasi khusus keamanan siber pertanahan, mekanisme jaminan integritas data, dan pengendalian akses berbasis risiko. Integrasi tersebut menjadikan keamanan siber sebagai instrumen hukum preventif yang memperkuat asas kepastian hukum dalam pendaftaran tanah digital, karena keabsahan data elektronik tidak hanya ditentukan oleh pengakuan normatif, tetapi juga oleh kemampuan sistem dalam menjamin keamanan, keterlacakan dan pertanggungjawaban setiap proses pengelolaan data pertanahan.

C. PENUTUP

Pembahasan yang telah diuraikan menjawab rumusan masalah mengenai pengaturan keamanan siber dalam pendaftaran tanah digital di Indonesia melalui perbandingan dengan Estonia dan Singapura serta arah penguatan regulasi untuk menjamin kepastian hukum. Analisis tersebut menunjukkan perlunya integrasi keamanan siber sebagai bagian dari sistem hukum pendaftaran tanah digital. Kesimpulan dan rekomendasi penelitian disajikan sebagai berikut:

Pengaturan keamanan siber dalam pendaftaran tanah digital di Indonesia telah memiliki dasar hukum melalui berbagai peraturan perundang-undangan, termasuk Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023. Namun, pengaturannya masih berfokus pada legalitas sistem dan dokumen elektronik sehingga belum mengatur secara komprehensif standar keamanan siber yang menjamin integritas data, pengendalian akses dan mitigasi ancaman siber. Hasil studi komparatif menunjukkan bahwa Estonia dan Singapura telah mengintegrasikan keamanan siber sebagai bagian dari penyelenggaraan pendaftaran tanah digital. Estonia memperkuat kepastian hukum melalui jaminan integritas dan keterlacakan data, sedangkan Singapura melalui pengendalian akses berbasis *Zero Trust Architecture*.

Perbandingan tersebut menunjukkan bahwa keamanan siber di kedua negara telah menjadi instrumen hukum yang mendukung kepastian hukum secara lebih komprehensif. Penguatan kepastian hukum pendaftaran tanah digital di Indonesia memerlukan rekonstruksi regulasi yang mengintegrasikan keamanan siber sebagai

bagian substantif penyelenggaraan administrasi pertanahan. Rekonstruksi tersebut perlu mengadopsi praktik terbaik Estonia dan Singapura melalui pengaturan mengenai jaminan integritas data, pengendalian akses berbasis risiko, audit keamanan dan pemantauan ancaman siber secara berkelanjutan.



DAFTAR PUSTAKA

Buku

- Fikri, Muhammad Sahal dan Ratih Damayanti. 2025. *Sistem Keamanan pada Digitalisasi Pendaftaran Tanah di Indonesia*. (Semarang: UNNES Pres).
- Kitsing, Meelis. 2019. *Alternative Futures for Digital Governance*. (New York: ACM International Conference Proceeding Series).

Publikasi

- Abigail, Silvia Theresia, dkk. *Efektivitas Digitalisasi Sistem Pendaftaran Tanah terhadap Peningkatan Pelayanan Publik dan Kepastian Hukum*. Jurnal Ilmiah Wahana Pendidikan. Vol.12. No.5D (Mei 2026).
- Arif, Ach Farhan, Herowati Poesoko dan Miftahul Munir. *Mitigasi Risiko Keamanan Data dalam Implementasi Sertifikat Tanah Elektronik untuk Mewujudkan Kepastian Hukum bagi Pemegang Hak atas Tanah*. Jurnal Hukum Pelita. Vol.6. No.1 (Mei 2025).
- Bua, Imanuel Toding dan Nur Isdah Idris. *Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024*. Desentralisasi: Jurnal Hukum, Kebijakan Publik dan Pemerintahan. Vol.2. No.2 (Mei 2025).
- Budianto, Azis. *Land Certificate Forgery Methods and the Structure of Criminal Networks as Well as Legal Reform Efforts to Strengthen Rights Certainty and Law Enforcement*. Greenation International Journal of Law and Social Sciences. Vol.3. No.3 (November 2025).
- Febrianti, Suci. *Perlindungan Hukum terhadap Pemegang Sertipikat Hak atas Tanah Elektronik*. Indonesian Notary. Vol.3. No.3 (September 2021).
- Fitriady, Achmad M. dan A. I. Wisnubroto. *Dampak Yuridis, Teknis dan Sosial Penerapan E-Sertifikat dalam Sertifikat Tanah di Penajam Paser Utara*. Al-Zayn: Jurnal Ilmu Sosial. Vol.4. No.1 (Desember 2025).
- Habibi, Arifin, Ghally Sukma Prambudi, Tuti Trisnawati dan Ratna Wulandari. *Transformasi Digital Administrasi Pertanahan: Implementasi dan Tantangan Sertipikat Elektronik di Indonesia*. Rio Law. Vol.6. No.1 (Februari 2025).
- Juliyanti, Ni Kadek, I Made Dharsana dan Ni Made Ujianti. *Perlindungan Hukum terhadap Pemegang Sertifikat Tanah Digital Dikaitkan dengan Kemanan Data Pribadi*. Jurnal Preferensi Hukum. Vol.4. No.1 (Maret 2022).
- Lubis, Duma Indah Sari, Hakim Andi Lubis dan Rodiatun Adawiyah. *Analisis Yuridis Peranan Kantor ATR/BPN terhadap Penyelesaian Permasalahan Sengketa Batas Tanah*. Law Jurnal. Vol.1. No.1 (Juli 2024).
- Pradhipta, Arum Puspa dan I Gusti Nyoman Krisnadi Yudiantara. *Analisis Regulasi Perlindungan Data Pribadi terhadap Kasus Kebocoran Data di Indonesia*. Jurnal Media Akademik. Vol.3. No.7 (Juli 2025).
- Pramesti, Ni Komang Arinda Sastra, Made Mulyawan Subawa dan Deli Bunga Saravistha. *Analisis Kepastian Hukum terhadap Standar Keamanan Sertifikat Elektronik dalam Kepemilikan Tanah*. Kertha Wicaksana: Sarana Komunikasi Dosen dan Mahasiswa. Vol.20. No.1 (Maret 2026).
- Sullivan, Clare dan Eric Burger. *E-Residency and Blockchain*. Computer Law & Security Review. Vol.33. No.4 (Agustus 2017).

Syafitri, Nurul dan Hendrawarman. *Legal Review of Cyber Crime: Case of Attack On Center Data National Temporary 2*. Critical Legal Review. Vol.2. No.3 (Agustus 2025).

Website

A Singapore Government Agency Website. *Singapore Statutes Online*, diakses dari <https://sso.agc.gov.sg/Act>. diakses pada 27 Juni 2026.

Riigi Teataja. *Ligipäätavus*, diakses dari <https://www.riigiteataja.ee/et>. diakses pada 27 Juni 2026.

Sumber Hukum

Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Republik Indonesia Nomor 1 Tahun 2021 tentang Sertipikat Elektronik. Berita Negara Republik Indonesia Tahun 2021 Nomor 12.

Peraturan Menteri Agraria dan Tata Ruang/Kepala Badan Pertanahan Nasional Nomor 3 Tahun 2023 tentang Penerbitan Dokumen Elektronik dalam Kegiatan Pendaftaran Tanah. Berita Negara Tahun 2023 Nomor 461.

Sumber Lain

Badan Siber dan Sandi Negara. 2024. *Lanskap Keamanan Siber Indonesia 2024*. (Jakarta: Badan Siber dan Sandi Negara).

Cybersecurity Agency of Singapore. 2021. *The Singapore Cybersecurity Strategy 2021*. (Singapura: Cyber Security Agency of Singapore).

International Organization for Standardization (ISO). 2022. *Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements (ISO/IEC 27001:2022)*. (Geneva: ISO).

United Nations. 2024. *E-Government Survey 2024 Accelerating Digital Transformation for Sustainable Development With the addendum on Artificial Intelligence*. (New York: United Nations).