Nusantara: Journal of Law and Islamic Law
Published by Yayasan Cerdas Pedia Indonesia
Volume 1 Issue 3, 2026 ISSN (Online) ***3110-8415***
Journal Homepage: **https://jurnal.smartpedia.co.id/index.php/nusantara**

Strengthening Data Security Systems in the Cyber Notary to Ensure Legal Certainty

Penguatan Sistem Keamanan Data dalam Cyber Notary untuk Menjamin Kepastian Hukum

Alisya Rahma Saebani
Faculty of Law, Doctoral Program in Law, Universitas Pembangunan Nasional 'Veteran' Jakarta, Indonesia

Article Info

Corresponding Author:
Alisya Rahma Saebani
✉alisyarahma51@gmail.com

History:
Submitted: 25-02-2026
Revised: 01-05-2026
Accepted: 17-05-2026

Keyword:
Cyber Notary; Personal Data Protection; Legal Certainty; Privacy by Design; Regulatory Harmonization.

Kata Kunci:
Cyber Notary; Perlindungan Data Pribadi; Kepastian Hukum; *Privacy by Design*; Harmonisasi Regulasi.

https://doi.org/10.65101/nusantara.v1i3.291

Abstract

The implementation of cyber notary practices in Indonesia currently encounters profound regulatory fragmentation among the Law on Notary Public Office, Electronic Information and Transactions Law, and Personal Data Protection Law. This fundamental normative vacuum triggers significant legal uncertainty in securing clients' electronic data. This normative legal research aims to comprehensively analyze the interconnection of positive legal instruments regarding privacy protection within the digital notarial ecosystem. Utilizing statutory, conceptual, and comparative approaches, this study critically evaluates the obligations of notaries who now transform into personal data controllers bearing absolute liability. The research findings demonstrate that the absence of uniform information security standards substantially elevates the risks of system hacking and digital identity breaches. Therefore, this research concludes the urgency for regulatory harmonization that strictly mandates the implementation of privacy by design principles alongside the standardization of encrypted information security systems. This legal measure constitutes an imperative directive to mitigate cybercrime threats.

Abstrak

Pelaksanaan *cyber notary* di Indonesia saat ini masih dihadapkan pada tantangan fragmentasi regulasi antara Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi. Kekosongan norma fundamental tersebut memicu ketidakpastian hukum yang signifikan dalam proses pengamanan data elektronik klien. Penelitian hukum normatif ini bertujuan untuk menganalisis interkoneksi instrumen hukum positif secara komprehensif terkait perlindungan privasi dalam ekosistem digital kenotariatan. Menggunakan pendekatan perundang-undangan, konseptual, dan perbandingan hukum, studi ini mengevaluasi secara kritis kewajiban notaris yang kini bertransformasi menjadi pengendali data pribadi dengan tanggung jawab mutlak. Hasil penelitian mendemonstrasikan bahwa ketiadaan standar keamanan informasi yang seragam sangat meningkatkan risiko peretasan sistem dan kebocoran identitas digital. Oleh karena itu, penelitian ini menyimpulkan urgensi harmonisasi peraturan yang secara tegas mewajibkan implementasi prinsip *privacy by design* serta standardisasi sistem keamanan informasi terenkripsi. Langkah hukum ini merupakan instruksi imperatif untuk memitigasi kejahatan siber, menjamin kepastian hukum, dan melindungi hak asasi privasi warga negara.

A. PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi informasi mendorong perubahan besar dalam layanan hukum, termasuk praktik kenotariatan. Konsep cyber notary mulai dikenal sebagai bentuk adaptasi notaris terhadap kebutuhan masyarakat yang menginginkan layanan cepat dan berbasis digital. Proses pembuatan, penyimpanan, dan pengiriman dokumen kini tidak lagi bergantung pada bentuk fisik, semua bergerak ke arah sistem elektronik.[1] Meski begitu, pengaturan mengenai cyber notary di Indonesia masih belum tersusun secara menyeluruh. Kondisi ini menimbulkan ketidakjelasan dalam praktik dan berpotensi mengganggu kepastian hukum.[2] Dampaknya, perlindungan hukum bagi para pihak dalam transaksi elektronik belum sepenuhnya terjamin. Situasi ini menunjukkan perlunya pembentukan regulasi yang lebih jelas dan terarah agar keabsahan dokumen elektronik dapat diakui, kepercayaan publik meningkat, dan sistem hukum nasional mampu beradaptasi dengan perkembangan digital.[3]

Kepastian hukum memegang peran penting dalam pembuatan akta autentik oleh Notaris. Tanpa kepastian tersebut, para pihak berpotensi mengalami kerugian karena tidak adanya jaminan perlindungan hukum yang memadai. Kondisi ini juga dapat menempatkan Notaris pada risiko persoalan hukum, terutama ketika akta dibuat dalam bentuk elektronik tanpa dasar pengaturan yang jelas. Dalam praktiknya, Notaris memerlukan pedoman yang tegas saat menyusun akta secara elektronik. Pedoman ini berfungsi sebagai acuan agar setiap tindakan yang dilakukan tetap berada dalam koridor hukum. Acuan tersebut harus bersumber dari aturan yang ditetapkan oleh otoritas yang berwenang. Dengan adanya norma yang jelas, Notaris memiliki dasar yang pasti dalam menjalankan kewenangannya serta dapat memberikan kepastian dan perlindungan hukum bagi para pihak yang terlibat.[4]

---

[1] Stefan Koos, "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany," *The Indonesian Journal of Socio-Legal Studies* 2, no. 2 (March 25, 2023): 1–16, https://doi.org/10.54828/ijsls.2023v2n2.1.

[2] Ikhsan Lubis et al., "Cyber Notary as A Mean of Indonesian Economic Law Development," *Sriwijaya Law Review* 7, no. 1 (January 26, 2023): 62–72, https://doi.org/10.28946/slrev.Vol7.Iss1.1972.pp62-72.

[3] Henry Aspan et al., "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling," *Journal of Law and Sustainable Development* 11, no. 10 (October 26, 2023): e1801, https://doi.org/10.55908/sdgs.v11i10.1801.

[4] Deny Fernaldi Chastra, "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris," *Indonesian Notary* 3, no. 2 (2021): 248–67, https://scholarhub.ui.ac.id/notary/vol3/iss2/17/.

Di Indonesia, dasar hukum yang berkaitan dengan praktik cyber notary masih mengacu pada beberapa peraturan, yaitu Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi. Ketiga aturan ini memang sudah memberikan landasan, namun belum saling terhubung secara utuh. Kondisi ini menimbulkan ruang kosong dalam pengaturan, terutama terkait perlindungan data pribadi yang berada dalam pengelolaan notaris. Dalam pelaksanaannya, notaris menangani berbagai data klien yang bersifat sensitif. Data tersebut memiliki tingkat risiko tinggi terhadap kebocoran maupun penggunaan tanpa izin. Walaupun aturan mengenai perlindungan data sudah tersedia, penerapannya dalam layanan kenotariatan berbasis elektronik belum berjalan konsisten. Perbedaan kesiapan teknologi di tiap daerah juga mempengaruhi. Sistem keamanan informasi, metode autentikasi elektronik, dan mekanisme sertifikasi belum memiliki standar yang seragam.[5]

Studi komparatif lintas yurisdiksi mengonfirmasi adanya disparitas fundamental dalam kodifikasi dan implementasi doktrin *cyber notary*. Negara penganut sistem *civil law* seperti Jerman secara rigid menempatkan perlindungan hak atas privasi dan keamanan data terstruktur sebagai prioritas konstitusional tertinggi dalam digitalisasi kenotariatan. Sebaliknya, yurisdiksi *common law* seperti Amerika Serikat mengadopsi pendekatan pragmatis-pasar melalui akselerasi *remote online notarization* (RON) guna memenuhi tuntutan efisiensi layanan hukum yang inklusif dan mudah diakses. Eksplorasi komparatif ini jamak dijadikan acuan formal dalam memetakan proyeksi transisi digitalisasi notaris di Indonesia, sebagaimana dielaborasi dalam studi terdahulu yang berfokus pada analisis peluang dan tantangan umum adopsi teknologi informasi dalam institusi kenotariatan nasional.[6,7,8,9]

[5] Asriannor et al., "Tantangan Dan Peluang Profesi Notaris Diera Digital," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (June 24, 2025): 2040–46, https://doi.org/10.62976/ijijel.v3i2.1205.
[6] Maria Debora Alamanda and Sri Laksmi Anindita, "Tantangan Dan Prospek Cyber Notary Di Indonesia," *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 5 (May 22, 2025): 4751–66, https://doi.org/10.36418/syntax-literate.v10i5.58183.
[7] Koos, "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany."
[8] Satrio Abdillah, Norhasliza Ghapa, and Maheran Makhtar, "Regulatory Challenges and Social Dynamics of Online Notary Practices: A Comparative Legal Study of Indonesia and Malaysia," *Mawaddah: Jurnal Hukum Keluarga Islam* 4, no. 1 (2026): 376–409, https://doi.org/10.52496/mjhki.v4i1.46.
[9] Ikhsan Lubis et al., "Comparison of Civil Law Regarding The Implementation of Cyber Notary in Countries With Common Law and Civil Law Traditions," *Jurnal IUS Kajian Hukum Dan Keadilan* 10, no. 1 (April 23, 2022): 1–11, https://doi.org/10.29303/ius.v10i1.981.

Di tingkat domestik, pengundangan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai paradigma baru dalam memperkuat jaminan hak privasi masyarakat secara konstitusional. Kendati demikian, operasionalisasi UU PDP dalam ekosistem digital kenotariatan memicu antinomi norma yang pelik ketika disandingkan dengan Undang-Undang Jabatan Notaris (UUJN) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Ketidakselarasan ini bermuara pada ambiguitas dogmatik mengenai determinasi kedudukan hukum notaris: apakah diklasifikasikan sebagai pengendali data (*data controller*) yang memikul tanggung jawab penuh, atau sekadar pemroses data (*data processor*). Guna mengurai problem tersebut, beberapa kajian mencoba menawarkan pisau analisis hukum responsif untuk mengintegrasikan perlindungan privasi pasca-UU PDP. Studi tersebut menekankan urgensi internalisasi prinsip *privacy by design* dan *privacy by default* agar mitigasi risiko kebocoran data tidak terreduksi menjadi formalitas administratif belaka, melainkan tertanam secara inheren dalam arsitektur sistem informasi kenotariatan.[10,11,12,13]

Meskipun diskursus mengenai harmonisasi regulasi dan perlindungan data siber telah diinisiasi oleh literatur terdahulu, masih terdapat *research gap* (celah penelitian) yang signifikan terkait penyelesaian benturan norma (*conflict of norms*) konkret antara kewajiban kerahasiaan jabatan (*notarial secrecy*) dalam UUJN dengan asas akuntabilitas pemrosesan data siber dalam UU ITE dan UU PDP. Mayoritas studi terdahulu terjebak pada tataran deskriptif-makro mengenai tantangan teknologi dan perlindungan privasi secara umum tanpa menyentuh aspek rekonstruksi pertanggungjawaban hukum perdata dan administratif notaris secara spesifik saat sistem elektronik mengalami interseptasi ilegal (*hacking*). Oleh karena itu, *novelty* (kebaruan ilmiah) dari penelitian ini terletak pada formulasi model pertanggungjawaban hukum doktrinal yang menempatkan notaris secara tegas sebagai *data controller* berkewajiban mutlak (*absolute liability*), yang

[10] Emerentia Nathawira, M. Sudirman, and Benny Djaja, "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi," *Jurnal Sosial Dan Sains* 5, no. 12 (December 8, 2025): 759–770, https://doi.org/10.59188/jurnalsosains.v5i12.32612.
[11] Naurah Humam Alkatiri, Mohamad Fajri Mekka Putra, and Kyle Ongko, "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era," *Jambura Law Review* 5, no. 2 (June 30, 2023): 332–55, https://doi.org/10.33756/jlr.v5i2.19221.
[12] Satrio Abdillah, Norhasliza Ghapa, and Maheran Makhtar, "Cyber Notary: Adaptation to Changes in Notary Practices in Indonesia," *Jambura Law Review* 8, no. 1 (January 19, 2026): 76–96, https://doi.org/10.33756/jlr.v1i1.32490.
[13] Dwi Suryahartati and Jefri Mahardika, "Reforming the Legal Framework of Notary Supervision in Indonesia: Towards a Digital Governance Model," *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (June 30, 2025): 89–110, https://doi.org/10.14421/2xx8sn14.

diintegrasikan dengan kerangka operasional teknis *privacy by design* terenkripsi berskala internasional. Temuan masalah utama berupa ketidakpastian hukum akibat vakuat norma operasional ini mendesak untuk dipecahkan karena berpotensi merugikan hak asasi privasi warga negara serta mengikis legitimasi akta autentik itu sendiri. Berdasarkan hal tersebut, artikel ini bertujuan untuk merekonstruksi batas-batas yurisdiksi, hak, dan kewajiban hukum notaris guna menghasilkan landasan preskriptif yang kokoh dalam ekosistem *cyber notary* di Indonesia.

2. Perumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Bagaimana ketentuan hukum yang mengatur perlindungan dan keamanan data dalam pelaksanaan cyber notary di Indonesia saat ini?
b. Bagaimana bentuk pertanggungjawaban notaris atas potensi kebocoran maupun penyalahgunaan data dalam praktik cyber notary?

3. Metode Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif (doktrinal) yang berfokus pada analisis interkoneksi dan koherensi instrumen hukum positif. Pemilihan metode doktrinal didasarkan pada alasan fundamental bahwa persoalan inti dalam pelaksanaan *cyber notary* di Indonesia saat ini bukan bermuara pada aspek empiris atau sosiologis, melainkan pada kekosongan norma (*vacuum of norm*) dan fragmentasi regulasi antara Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi. Melalui metode ini, penelitian difokuskan untuk menemukan landasan preskriptif guna menjamin kepastian hukum dan merumuskan model pertanggungjawaban notaris dalam mengelola data elektronik.[14]

Untuk mencapai analisis yang komprehensif dan mendalam, penelitian ini mengaplikasikan tiga pendekatan utama dengan justifikasi sebagai berikut:

[14] Tunggul Ansari Setia Negara, "Normative Legal Research in Indonesia: Its Originis and Approaches," *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (February 2, 2023): 1–9, https://doi.org/10.22219/aclj.v4i1.24855.

a. Pendekatan Perundang-undangan (*Statute Approach*): Pendekatan ini merupakan instrumen primer yang dipilih untuk membedah arsitektur hukum nasional secara hierarkis dan sistematis. Pendekatan ini esensial untuk menganalisis sinkronisasi atau benturan norma (*conflict of norms*) antara kewajiban kerahasiaan akta dalam UU Jabatan Notaris dengan kewajiban pengamanan sistem elektronik dalam UU ITE dan UU Perlindungan Data Pribadi.
b. Pendekatan Konseptual (*Conceptual Approach*): Pendekatan ini digunakan untuk membangun kerangka teoretis dengan menelaah konsep *privacy by design*, *privacy by default*, serta doktrin pertanggungjawaban pengendali data (*data controller*). Alasan kuat penggunaan pendekatan ini adalah karena terminologi perlindungan data dalam *cyber notary* merupakan isu kontemporer yang menuntut interpretasi filosofis baru mengenai kedudukan notaris, tidak sekadar sebagai pejabat umum, tetapi juga sebagai entitas pemroses data berskala sensitif.
c. Pendekatan Perbandingan Hukum (*Comparative Approach*): Guna menawarkan kebaruan (*novelty*) yang berstandar global, penelitian ini melakukan komparasi makro terhadap yurisdiksi *civil law* (seperti Jerman yang memprioritaskan privasi terstruktur) dan *common law* (seperti Amerika Serikat dengan *remote online notarization* yang pragmatis). Pemilihan komparasi lintas sistem hukum ini memiliki justifikasi kuat untuk menemukan formula jalan tengah (*best practices*) yang paling kompatibel untuk diadaptasi ke dalam sistem tata hukum Indonesia tanpa mereduksi aspek keamanan data.

Data yang digunakan berpijak pada data sekunder yang terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup regulasi perundang-undangan terkait. Bahan hukum sekunder diperoleh melalui penelusuran literatur yang ketat (*systematic literature review*) dari artikel jurnal internasional bereputasi (terindeks Scopus) dan jurnal nasional terakreditasi, guna memastikan aktualitas dan validitas perdebatan akademik terkait kejahatan siber dan *cyber notary*.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*documentary research*). Seluruh bahan hukum yang terkumpul kemudian dianalisis menggunakan metode kualitatif dengan teknik interpretasi sistematis dan teleologis. Alasan pemilihan teknik analisis ini adalah untuk menghindari pembacaan teks undang-

undang secara kaku (*textualist*). Melalui interpretasi sistematis, peneliti akan merekonstruksi benang merah penafsiran antara berbagai peraturan perundang-undangan agar menghasilkan konklusi yang preskriptif, terukur, dan mampu memberikan solusi atas celah keamanan data pribadi dalam ekosistem digital kenotariatan di Indonesia.

B. PEMBAHASAN

1. Perlindungan dan Keamanan Data dalam Pelaksanaan *Cyber Notary* di Indonesia

Perkembangan teknologi yang sangat cepat membawa berbagai tantangan baru, salah satunya adalah munculnya kejahatan siber atau *cyber crime* yang berpotensi mengancam keamanan baik di tingkat nasional maupun global. Dalam kondisi ini, notaris memiliki peran penting dalam menjaga kepastian hukum sekaligus mendukung terciptanya keamanan dalam kehidupan bermasyarakat. Kejahatan siber merupakan tindakan melawan hukum yang terjadi melalui sistem elektronik tanpa interaksi langsung dengan korban. Pelaku dapat menjalankan aksinya dari mana saja dengan memanfaatkan celah dalam sistem digital. Motif yang sering muncul berkaitan dengan keuntungan ekonomi. Salah satu bentuk kejahatan tersebut adalah serangan terhadap data pribadi. Tindakan seperti peretasan sistem atau akses ilegal menjadi contoh nyata yang dapat merugikan pemilik data.[15]

Cyber crime merujuk pada tindakan melawan hukum yang memanfaatkan komputer dan jaringan internet, seperti peretasan, penyebaran malware, pencurian identitas, pelecehan daring, hingga praktik skimming.[16] Saat ini, hampir seluruh aktivitas dan informasi pribadi tersimpan dalam sistem digital, sehingga membuka peluang besar bagi pihak tidak bertanggung jawab untuk mengakses dan menyalahgunakan data tersebut. Pengambilan data pribadi tanpa izin termasuk dalam kategori perbuatan melawan hukum. Walaupun belum terdapat regulasi khusus yang secara komprehensif mengatur cyber law, ketentuan mengenai perlindungan data telah diakomodasi dalam beberapa peraturan, terutama dalam Undang-Undang Informasi dan Transaksi Elektronik. Dalam

[15] Russel Butarbutar, "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal* 2, no. 2 (August 24, 2023): 299–317, https://doi.org/10.21143/TELJ.vol2.no2.1043.
[16] Venny Febriyanti Puspita, Ningrum, and Ufran, "Perlindungan Hukum Terhadap Korban Cyber Sexual Harassment Dalam Media Sosial," *Iuris Notitia: Jurnal Ilmu Hukum* 1, no. 2 (October 25, 2023): 51–55, https://doi.org/10.69916/iuris.v1i2.65.

aturan tersebut ditegaskan bahwa setiap pelanggaran terhadap ketentuan Pasal 26 dapat menimbulkan tanggung jawab hukum berupa gugatan atas kerugian yang dialami oleh pihak yang dirugikan

Perkembangan teknologi dan informasi tidak hanya membawa kemudahan, tetapi juga membuka peluang terjadinya kejahatan dengan cara yang lebih cepat dan terorganisir. Kondisi ini turut berdampak pada pengelolaan data dan informasi, terutama data pribadi yang memerlukan perlindungan khusus. Kemajuan teknologi komunikasi membuat batas privasi semakin kabur, sehingga data pribadi menjadi lebih rentan untuk diakses dan disebarluaskan. Peningkatan kasus terkait perlindungan data menunjukkan bahwa isu ini tidak bisa dianggap sepele. Penyalahgunaan data pribadi dapat menimbulkan berbagai risiko, termasuk kebocoran informasi yang merugikan individu. Data seperti NIK, nama, alamat email, dan nomor telepon memiliki nilai ekonomi tinggi dan sering menjadi target dalam berbagai aktivitas ilegal.

Terdapat penerapan asas kemanfaatan dapat dilihat dari penggunaan konsep cyber notary dalam proses sertifikasi yang membantu notaris menjalankan tugasnya secara lebih praktis. Sistem ini mendorong efisiensi karena berbagai proses dapat dilakukan secara digital. Dalam praktiknya, layanan berbasis elektronik membutuhkan dokumen publik dalam format digital, termasuk penggunaan tanda tangan elektronik oleh notaris. Dalam proses verifikasi para pihak, notaris umumnya menggunakan identitas seperti KTP, SIM, atau paspor. Dengan adanya cyber notary, metode ini berkembang dengan memanfaatkan Electronic Identity atau e-ID sebagai sarana pengenalan. e-ID merupakan bagian dari penerapan e-government, yaitu penggunaan teknologi informasi oleh pemerintah untuk meningkatkan kualitas layanan publik dan penyampaian informasi. Karena identitas memuat data pribadi yang bersifat sensitif, pengelolaannya harus dilakukan secara ketat. Akses yang tidak terbatas berpotensi membuka peluang penyalahgunaan, terutama oleh pihak yang melakukan kejahatan siber. Oleh sebab itu, setiap individu sebagai pemilik data harus mendapatkan perlindungan hukum, termasuk terhadap data biometrik yang tersimpan dalam sistem digital.[17]

Dalam pembahasan mengenai konsep cyber notary, aspek yang perlu mendapat perhatian adalah perlindungan hukum terhadap identitas para pihak yang terlibat.

[17] Litha Nabilla Mallolongan and Hendry Julian Noor, "Peluang Penerapan Penyimpanan Minuta Akta Secara Elektronik Menuju Era E-Notary Berdasarkan Undang- Undang No. 2 Tahun 2014 Tentang Jabatan Notaris," *Notary Law Journal* 2, no. 1 (January 23, 2023): 54–81, https://doi.org/10.32801/nolaj.v2i1.39.

Identitas ini menjadi elemen penting karena berfungsi sebagai pembeda antara satu individu dengan individu lainnya. Sebelum masuk ke pembahasan identitas elektronik atau e-ID, perlu dipahami bahwa identitas pada dasarnya merupakan tanda pengenal yang melekat pada seseorang. Sementara itu, e-ID merujuk pada bentuk identitas yang disajikan melalui media elektronik dan berisi data pribadi individu. Kebutuhan akan data pribadi di era digital semakin meningkat. Data tersebut digunakan untuk mendukung berbagai aktivitas, termasuk mencegah terjadinya kejahatan berbasis teknologi.

Ancaman dalam ruang digital terus berkembang, salah satunya adalah peretasan sistem komputer. Peretasan merupakan tindakan akses tanpa izin ke dalam perangkat atau jaringan dengan tujuan tertentu, biasanya untuk memperoleh keuntungan. Dalam konteks praktik cyber notary, risiko ini menjadi serius ketika perangkat atau sistem yang digunakan notaris mengalami peretasan. Dokumen seperti draf akta yang tersimpan secara digital dapat terekspos. Kondisi ini berpotensi menimbulkan beberapa dampak, antara lain penggunaan data pribadi para pihak tanpa izin, terbukanya informasi yang seharusnya bersifat rahasia, serta perubahan isi data yang dapat merugikan para pihak maupun notaris itu sendiri.[18]

Pengaturan mengenai tindakan peretasan telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik. Peretasan dipandang sebagai bentuk kejahatan siber yang menyerang sistem elektronik secara melawan hukum. Dalam Undang-Undang Informasi dan Transaksi Elektronik, khususnya Pasal 30, dijelaskan bahwa:

(1) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan."

[18] Jenny Divia Fitcanisa and Busyra Azheri, "Keabsahan Tanda Tangan Elektronik Pada Akta Notaris," *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 2, no. 5 (April 30, 2023): 1449–58, https://doi.org/10.54443/sibatik.v2i5.809.

Ketentuan pidana atas pelanggaran tersebut diatur dalam Pasal 46 UU ITE. Seseorang yang terbukti melakukan akses ilegal sebagaimana dimaksud dalam Pasal 30 ayat (1) dapat dikenakan pidana penjara hingga 6 tahun dan/atau denda maksimal Rp600.000.000. Jika akses tersebut dilakukan dengan tujuan memperoleh informasi atau dokumen elektronik sebagaimana ayat (2), ancaman pidananya meningkat menjadi penjara paling lama 7 tahun dan/atau denda maksimal Rp700.000.000. Sementara itu, apabila tindakan dilakukan dengan cara menerobos atau merusak sistem pengamanan sebagaimana ayat (3), pelaku dapat dijatuhi pidana penjara hingga 8 tahun dan/atau denda paling banyak Rp800.000.000.

Ancaman terhadap data pribadi dalam praktik cyber notary menjadi permasalahan yang serius. Perkembangan layanan kenotariatan berbasis digital membuat bentuk ancaman terhadap keamanan informasi semakin beragam. Notaris berada pada posisi yang rawan karena mengelola data klien yang bersifat sensitif. Tanpa sistem perlindungan yang kuat, risiko penyalahgunaan maupun terbukanya data menjadi sangat besar. Salah satu ancaman yang sering terjadi adalah akses ilegal melalui serangan siber. Peretasan pada sistem atau media penyimpanan dapat membuka jalan bagi pihak luar untuk memperoleh informasi penting, seperti data identitas, dokumen hukum, dan informasi keuangan. Dampaknya tidak hanya dirasakan oleh klien yang dirugikan, tetapi juga mempengaruhi tingkat kepercayaan masyarakat terhadap profesi notaris.

Walaupun Undang-Undang Perlindungan Data Pribadi, Undang-Undang Jabatan Notaris, dan Undang-Undang Informasi dan Transaksi Elektronik telah memberikan dasar pengaturan, keselarasan antar aturan tersebut masih belum tercapai. Perbedaan pengaturan ini menimbulkan ketidakpastian dalam praktik, terutama saat notaris harus menyesuaikan diri dengan perkembangan layanan digital melalui konsep cyber notary. Undang-Undang Jabatan Notaris memang menegaskan kewajiban notaris untuk menjaga kerahasiaan akta sebagai bagian dari tanggung jawab profesi. Namun, ketentuan tersebut belum menjangkau secara rinci perlindungan data dalam bentuk elektronik. Padahal, penggunaan sistem digital menuntut adanya standar yang jelas terkait cara penyimpanan, pengamanan, dan pengendalian akses terhadap data agar kerahasiaannya tetap terjaga.[19]

[19] Nathawira, Sudirman, and Djaja, "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi."

2. Pertanggungjawaban Notaris atas Potensi Kebocoran Maupun Penyalahgunaan Data dalam Praktik *Cyber Notary*

Dengan diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, tanggung jawab notaris dalam menjaga kerahasiaan data klien menjadi semakin ketat, terutama dalam penggunaan sistem elektronik. Dalam Pasal 1 angka 1, dijelaskan bahwa data pribadi merupakan setiap informasi yang dapat mengidentifikasi seseorang, baik secara langsung maupun melalui kombinasi dengan data lain, yang diproses melalui sistem elektronik atau non-elektronik. Dalam praktik kenotariatan, isi akta hampir selalu memuat informasi pribadi para pihak. Data tersebut mencakup identitas, kondisi keuangan, hingga dokumen hukum yang berkaitan dengan badan usaha. Bahkan, sebagian data tersebut masuk dalam kategori data spesifik, seperti yang diatur dalam Pasal 4 ayat (2) huruf b, yang meliputi informasi keuangan pribadi. Kondisi ini menempatkan notaris pada posisi yang tidak hanya terbatas sebagai pejabat pembuat akta. Notaris juga memiliki peran dalam mengelola dan memproses data pribadi. Peran ini sejalan dengan konsep pengendali dan pemroses data dalam rezim perlindungan data pribadi.[20]

Ketentuan ini selaras dengan Pasal 16 ayat (1) huruf f UU Jabatan Notaris yang mengharuskan notaris menjaga kerahasiaan seluruh isi akta serta informasi yang diperoleh dalam proses pembuatannya sesuai dengan sumpah jabatan. Kewajiban tersebut tidak lagi hanya berada pada ranah etik dan profesional, tetapi telah diperkuat melalui rezim perlindungan data pribadi yang memuat konsekuensi hukum berupa sanksi administratif dan pidana. Dalam kerangka Undang-Undang Perlindungan Data Pribadi, pihak yang terlibat dalam pemrosesan data dibedakan menjadi dua kategori, yaitu pengendali data pribadi dan prosesor data pribadi. Berdasarkan Pasal 1 angka 4 dan 5, pengendali data pribadi merupakan pihak yang menetapkan tujuan serta memiliki kendali atas pemrosesan data pribadi. Sementara itu, prosesor data pribadi adalah pihak yang melakukan pemrosesan data atas dasar instruksi atau untuk kepentingan pengendali data pribadi.[21]

[20] Intan Permata Mipon and Mohamad Fajri Putra, "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Hukum & Pembangunan* 53, no. 3 (September 30, 2023): 479–92, https://doi.org/10.21143/jhp.vol53.no3.1576.
[21] Pingkan Chandra Dewi Tamaka, "Prinsip Kepastian Hukum Profesi Notaris Terhadap Amanah Dalam Sumpah Atau Janji Jabatan Notaris," *Al Qodiri : Jurnal Pendidikan, Sosial Dan Keagamaan* 22, no. 1 (September 2024): 71–92, https://doi.org/10.53515/qodiri.2024.22.1.71-92.

Peran notaris dapat ditempatkan sebagai pengendali data pribadi karena notaris menentukan tujuan serta cara penggunaan data dalam proses pembuatan akta autentik. Konsekuensinya, notaris memikul tanggung jawab langsung atas keamanan, kerahasiaan, dan akuntabilitas dalam setiap tahapan pemrosesan data milik klien. Kewajiban tersebut ditegaskan dalam Pasal 20 ayat (1) Undang-Undang Perlindungan Data Pribadi yang mengatur bahwa pengendali data pribadi harus memproses data berdasarkan prinsip keabsahan dasar pemrosesan, pembatasan tujuan, keterbukaan, akurasi, pembatasan penyimpanan, integritas dan kerahasiaan, serta akuntabilitas. Dalam praktik cyber notary, ketentuan ini mengharuskan notaris memastikan setiap akta elektronik yang dibuat, disimpan, dan dikirim telah dilindungi melalui sistem keamanan informasi yang memadai, seperti enkripsi, autentikasi, dan mekanisme audit.

Di sisi lain, Undang-Undang Informasi dan Transaksi Elektronik memberikan legitimasi terhadap penggunaan tanda tangan elektronik dalam dokumen digital. Pasal 11 ayat (1) menegaskan bahwa tanda tangan elektronik memiliki kekuatan hukum yang sah. Selanjutnya, Pasal 12 ayat (1) menyatakan bahwa tanda tangan elektronik memiliki kekuatan pembuktian yang setara dengan tanda tangan konvensional sepanjang memenuhi persyaratan tertentu, antara lain terikat secara eksklusif dengan penanda tangan, data pembuatannya berada dalam kendali penanda tangan, setiap perubahan terhadap tanda tangan dapat terdeteksi, serta setiap perubahan terhadap informasi elektronik yang terkait juga dapat diketahui

Tanggung jawab tersebut menuntut notaris untuk memastikan bahwa setiap akta elektronik yang dibuat, disimpan, dan dikirim telah melalui sistem pengamanan yang memadai. Sistem ini harus mencakup standar enkripsi, proses autentikasi yang jelas, serta mekanisme audit yang dapat menelusuri setiap aktivitas terhadap data. Dalam kerangka hukum, Undang-Undang Informasi dan Transaksi Elektronik memberikan landasan atas penggunaan tanda tangan elektronik dalam dokumen digital. Pada Pasal 11 ayat (1) ditegaskan bahwa tanda tangan elektronik memiliki kekuatan hukum dan menimbulkan akibat hukum yang sah. Selanjutnya, Pasal 12 ayat (1) menyatakan bahwa tanda tangan elektronik memiliki kekuatan pembuktian yang setara dengan tanda tangan konvensional selama memenuhi persyaratan tertentu. Persyaratan tersebut meliputi keterkaitan langsung dengan penanda tangan, penguasaan data pembuatan tanda tangan oleh penanda tangan, kemampuan untuk mendeteksi setiap perubahan pada tanda tangan elektronik, serta kemampuan untuk mengetahui perubahan pada informasi

elektronik yang berkaitan.

Dalam praktik cyber notary, penggunaan tanda tangan elektronik tersertifikasi menjadi hal yang wajib agar akta elektronik dapat diakui secara hukum. Tanda tangan ini memberikan jaminan keaslian identitas serta integritas dokumen yang digunakan dalam transaksi. Selain itu, Pasal 15 ayat (1) UU ITE mengatur bahwa setiap penyelenggara sistem elektronik wajib mengoperasikan sistem yang andal, aman, dan bertanggung jawab. Sistem tersebut harus mampu menjamin ketersediaan, keutuhan, kerahasiaan, serta aksesibilitas data pribadi. Dalam konteks ini, sistem yang digunakan dalam cyber notary juga harus memenuhi standar tersebut. Oleh karena itu, notaris sebagai pihak yang menggunakan sistem memiliki kewajiban untuk memastikan bahwa sistem manajemen keamanan informasi yang diterapkan telah memenuhi standar yang diakui, baik secara nasional maupun internasional, seperti ISO atau standar keamanan informasi lainnya. Hal ini penting untuk menjaga kepercayaan para pihak serta memastikan perlindungan hukum terhadap data yang dikelola.[22]

Secara etika, kedudukan notaris sebagai pejabat umum yang dipercaya masyarakat menuntut standar integritas yang lebih tinggi dibanding profesi hukum lain. Peran notaris tidak berhenti pada pengesahan dokumen, tetapi juga merepresentasikan kepercayaan publik terhadap negara. Ketika notaris tidak mampu menjaga kerahasiaan data pribadi, dampaknya tidak hanya merugikan klien, tetapi juga mengganggu legitimasi negara dalam menjamin kepastian hukum. Dalam perspektif filsafat hukum, persoalan ini berkaitan dengan perlindungan hak privasi sebagai bagian dari hak asasi manusia. Pasal 28G ayat 1 UUD 1945 menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, serta harta benda yang berada dalam penguasaannya. Setiap orang juga berhak atas rasa aman dan perlindungan dari ancaman yang membatasi kebebasannya dalam bertindak. Dengan demikian, cyber notary tidak dapat dipandang sekadar sebagai isu administratif atau teknis. Isu ini berkaitan langsung dengan tanggung jawab konstitusional negara dalam menjamin dan melindungi hak privasi warga negara.

[22] Dinda Cantik Senantya, Fany Rahmasari, and Intan Glarita Zodies Liusyadi, "Analisis Transformasi Pelayanan Notaris Di Era Digital : Studi Tentang Tanda Tangan Elektronik Dalam Akta Otentik," *Jurnal Ilmu Multidisiplin* 4, no. 2 (June 19, 2025): 823–31, https://doi.org/10.38035/jim.v4i2.959.

C. KESIMPULAN

Pelaksanaan *cyber notary* di Indonesia saat ini masih dihadapkan pada fragmentasi regulasi antara Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi, yang memicu ketidakpastian hukum dalam mengamankan data elektronik klien. Dalam konstruksi hukum pelindungan data, kedudukan notaris kini bertransformasi menjadi pengendali data pribadi yang memikul tanggung jawab mutlak atas setiap kebocoran atau penyalahgunaan identitas digital dalam proses pembuatan akta autentik. Oleh karena itu, diperlukan harmonisasi peraturan yang secara tegas mewajibkan penerapan prinsip *privacy by design* dan standardisasi sistem keamanan informasi terenkripsi dalam setiap tahapan layanan kenotariatan berbasis digital. Langkah komprehensif ini merupakan instruksi imperatif tidak hanya untuk memitigasi ancaman kejahatan siber, tetapi juga demi menjamin kepastian hukum dan melindungi hak asasi privasi masyarakat secara konstitusional.

DAFTAR PUSTAKA

Abdillah, Satrio, Norhasliza Ghapa, and Maheran Makhtar. "Cyber Notary: Adaptation to Changes in Notary Practices in Indonesia." *Jambura Law Review* 8, no. 1 (January 19, 2026): 76–96. https://doi.org/10.33756/jlr.v1i1.32490.

———. "Regulatory Challenges and Social Dynamics of Online Notary Practices: A Comparative Legal Study of Indonesia and Malaysia." *Mawaddah: Jurnal Hukum Keluarga Islam* 4, no. 1 (2026): 376–409. https://doi.org/10.52496/mjhki.v4i1.46.

Alamanda, Maria Debora, and Sri Laksmi Anindita. "Tantangan Dan Prospek Cyber Notary Di Indonesia." *Syntax Literate ; Jurnal Ilmiah Indonesia* 10, no. 5 (May 22, 2025): 4751–66. https://doi.org/10.36418/syntax-literate.v10i5.58183.

Alkatiri, Naurah Humam, Mohamad Fajri Mekka Putra, and Kyle Ongko. "A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era." *Jambura Law Review* 5, no. 2 (June 30, 2023): 332–55. https://doi.org/10.33756/jlr.v5i2.19221.

Aspan, Henry, Abdi Setiawan, Irawan, Etty Sri Wahyuni, Ari Prabowo, and Ami Natuz Zahara. "Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online Selling." *Journal of Law and Sustainable Development* 11, no. 10 (October 26, 2023): e1801. https://doi.org/10.55908/sdgs.v11i10.1801.

Asriannor, Muhammad Afdal Zikri, Muhammad Indra Gazali, and Riski Dwi Nugraha. "Tantangan Dan Peluang Profesi Notaris Diera Digital." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (June 24, 2025): 2040–46. https://doi.org/10.62976/ijijel.v3i2.1205.

Butarbutar, Russel. "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya." *Technology and Economics Law Journal* 2, no. 2 (August 24, 2023):

299–317. https://doi.org/10.21143/TELJ.vol2.no2.1043.

Chastra, Deny Fernaldi. "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris." *Indonesian Notary* 3, no. 2 (2021): 248–67. https://scholarhub.ui.ac.id/notary/vol3/iss2/17/.

Divia Fitcanisa, Jenny, and Busyra Azheri. "Keabsahan Tanda Tangan Elektronik Pada Akta Notaris." *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan* 2, no. 5 (April 30, 2023): 1449–58. https://doi.org/10.54443/sibatik.v2i5.809.

Koos, Stefan. "The Digitization of Notarial Tasks - A Comparative Overview and Outlook of 'Cyber Notary' In Indonesia and Germany." *The Indonesian Journal of Socio-Legal Studies* 2, no. 2 (March 25, 2023): 1–16. https://doi.org/10.54828/ijsls.2023v2n2.1.

Lubis, Ikhsan, Tarsisius Murwadji, Mahmul Siregar, Detania Sukarja, Robert Robert, Dedi Harianto, and Mariane Magda Ketaren. "Comparison of Civil Law Regarding The Implementation of Cyber Notary in Countries With Common Law and Civil Law Traditions." *Jurnal IUS Kajian Hukum Dan Keadilan* 10, no. 1 (April 23, 2022): 1–11. https://doi.org/10.29303/ius.v10i1.981.

Lubis, Ikhsan, Tarsisius Murwadji, Sunarmi Sunarmi, and Detania Sukarja. "Cyber Notary as A Mean of Indonesian Economic Law Development." *Sriwijaya Law Review* 7, no. 1 (January 26, 2023): 62–72. https://doi.org/10.28946/slrev.Vol7.Iss1.1972.pp62-72.

Mallolongan, Litha Nabilla, and Hendry Julian Noor. "Peluang Penerapan Penyimpanan Minuta Akta Secara Elektronik Menuju Era E-Notary Berdasarkan Undang- Undang No. 2 Tahun 2014 Tentang Jabatan Notaris." *Notary Law Journal* 2, no. 1 (January 23, 2023): 54–81. https://doi.org/10.32801/nolaj.v2i1.39.

Mipon, Intan Permata, and Mohamad Fajri Putra. "Penyelenggaraan Pelindungan Data Pribadi Oleh Notaris Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Hukum & Pembangunan* 53, no. 3 (September 30, 2023): 479–92. https://doi.org/10.21143/jhp.vol53.no3.1576.

Nathawira, Emerentia, M. Sudirman, and Benny Djaja. "Implementasi Cyber Notary Di Indonesia: Harmonisasi Regulasi Dan Perlindungan Data Pribadi Pasca Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dalam Kerangka Teori Hukum Responsif Dan Hak Privasi." *Jurnal Sosial Dan Sains* 5, no. 12 (December 8, 2025): 759–770. https://doi.org/10.59188/jurnalsosains.v5i12.32612.

Negara, Tunggul Ansari Setia. "Normative Legal Research in Indonesia: Its Originis and Approaches." *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (February 2, 2023): 1–9. https://doi.org/10.22219/aclj.v4i1.24855.

Pingkan Chandra Dewi Tamaka. "Prinsip Kepastian Hukum Profesi Notaris Terhadap Amanah Dalam Sumpah Atau Janji Jabatan Notaris." *Al Qodiri : Jurnal Pendidikan, Sosial Dan Keagamaan* 22, no. 1 (September 2024): 71–92. https://doi.org/10.53515/qodiri.2024.22.1.71-92.

Puspita, Venny Febriyanti, Ningrum, and Ufran. "Perlindungan Hukum Terhadap Korban Cyber Sexual Harassment Dalam Media Sosial." *Iuris Notitia: Jurnal Ilmu Hukum* 1, no. 2 (October 25, 2023): 51–55. https://doi.org/10.69916/iuris.v1i2.65.

Senantya, Dinda Cantik, Fany Rahmasari, and Intan Glarita Zodies Liusyadi. "Analisis

Transformasi Pelayanan Notaris Di Era Digital : Studi Tentang Tanda Tangan Elektronik Dalam Akta Otentik." *Jurnal Ilmu Multidisiplin* 4, no. 2 (June 19, 2025): 823–31. https://doi.org/10.38035/jim.v4i2.959.

Suryahartati, Dwi, and Jefri Mahardika. "Reforming the Legal Framework of Notary Supervision in Indonesia: Towards a Digital Governance Model." *Supremasi Hukum: Jurnal Kajian Ilmu Hukum* 14, no. 1 (June 30, 2025): 89–110. https://doi.org/10.14421/2xx8sn14.