JURNAL

JURNAL SOSIAL DAN SAINS

VOLUME 5 NOMOR 12 2023

P-ISSN 2774-7018, E-ISSN 2774-700X

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

Emerentia Nathawira , M. Sudirman , Benny Djaja

Universitas Tarumanagara, Indonesia

Email: emerentia.217242046@stu.untar.ac.id , m.sudirman321@gmail.com, bennyd@fh.untar.ac.id

Kata kunci

Cyber Notary, Perlindungan Data Pribadi, Privasi, Hukum Responsif, Indonesia

Abstrak

Penelitian ini bertujuan untuk menganalisis implementasi cyber notary di Indonesia dalam kaitannya dengan perlindungan data pribadi, khususnya setelah berlakunya Undang-Undang Perlindungan Data Pribadi (UU PDP). Dengan menggunakan metode penelitian hukum normatif, penelitian ini mengkaji bahan hukum primer seperti UU ITE, UU PDP, dan UUJN, serta bahan hukum sekunder berupa literatur hukum dan studi perbandingan antara yurisdiksi civil law dan common law. Temuan penelitian menunjukkan bahwa meskipun cyber notary menawarkan efisiensi dan aksesibilitas melalui akta elektronik dan otentikasi digital, namun hal tersebut juga menimbulkan tantangan serius terkait privasi data, risiko keamanan, serta disharmonisasi regulasi. Notaris berpotensi berperan sebagai pengendali maupun pemroses data, sehingga memerlukan kewajiban hukum yang jelas serta perlindungan teknologi untuk mencegah penyalahgunaan atau kebocoran data pribadi. Penelitian ini menyimpulkan bahwa Implementasi cyber notary di Indonesia masih menghadapi berbagai kendala, seperti ketidakharmonisan aturan, ketidakjelasan status akta elektronik, dan risiko pelanggaran data pribadi. Perbedaan antara KUH Perdata, UU Jabatan Notaris, dan UU ITE membuat penerapan akta digital belum sejalan. Selain itu, keterbatasan aturan dalam UUJN menyulitkan notaris beradaptasi dengan era digital, sementara UU Perlindungan Data Pribadi menambah tanggung jawab baru tanpa mekanisme yang jelas bagi notaris.masa depan cyber notary di Indonesia sangat bergantung pada harmonisasi peraturan perundang-undangan, penerapan prinsip hukum responsif, serta penguatan peran notaris sebagai penjaga privasi. Lebih lanjut, integrasi mekanisme regulatory sandbox, standar teknis nasional, dan pengawasan bersama oleh lembaga negara serta asosiasi profesi merupakan langkah esensial untuk memastikan bahwa digitalisasi di bidang kenotariatan sejalan dengan kepastian hukum sekaligus hak privasi warga negara.

Keywords

Cyber Notary, Personal Data Protection, Privacy, Responsive Law, Indonesia.

Abstract

This study aims to analyze the implementation of cyber notary in Indonesia in relation to personal data protection, particularly after the enactment of the Personal Data Protection Act (UU PDP). Using a normative legal research method, the study examines primary legal materials such as UU ITE, UU PDP, and UUJN, as well as secondary sources from legal literature and comparative studies between civil law and common law jurisdictions. The findings show that although cyber notary offers efficiency and accessibility through electronic deeds and digital authentication, it also raises serious challenges regarding data privacy, security risks, and regulatory disharmony. Notaries potentially act as both data controllers and processors, requiring clear legal obligations and technological safeguards to prevent misuse or leakage of personal data. The study concludes that the future of cyber notary in Indonesia depends on harmonizing relevant laws, adopting responsive law principles, and reinforcing notaries' role as guardians of privacy. Furthermore, the

integration of regulatory sandbox mechanisms, national technical standards, and joint supervision by state institutions and professional associations is essential to ensure that digitalization in the notarial field aligns with both legal certainty and citizens' right to privacy.

PENDAHULUAN

Digitalisasi di bidang hukum telah menjadi kebutuhan strategis seiring dengan meningkatnya tuntutan masyarakat akan layanan yang cepat, transparan, dan efisien (Choirunnisa et al., 2023; Meranggi & Lukman, 2024; Wirawan, 2020). Perkembangan pesat teknologi informasi mendorong transformasi layanan kenotariatan menuju bentuk elektronik yang dikenal dengan istilah cyber notary (Andriani et al., 2025; Ferryanto et al., 2024; Mayana & Santika, 2021; Rizkia et al., 2022). Konsep ini memunculkan berbagai pertanyaan mendasar terkait keabsahan akta elektronik, kekuatan pembuktiannya, serta kesiapan regulasi dalam menjamin kepastian hukum dan perlindungan hak-hak individu, khususnya perlindungan data pribadi.

Di Indonesia, pengaturan hubungan antara praktik cyber notary masih bertumpu pada beberapa regulasi utama seperti Undang-Undang Jabatan Notaris (UUJN), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Undang-Undang Perlindungan Data Pribadi (UU PDP) (Bayumurti et al., 2025; Rukmana et al., 2021). Meski masing-masing memberikan kerangka hukum, integrasi antar ketiga undang-undang ini masih belum mencukupi, sehingga menimbulkan celah hukum khususnya terkait dengan perlindungan data pribadi yang dikelola oleh notaris (Lubis et al., 2025). Dalam praktiknya, notaris memproses data sensitif klien dengan risiko tinggi terhadap kebocoran dan penyalahgunaan (Asriannor et al., 2025; Jasmine et al., 2024; Sitaresmi & Ristawati, 2025). Meskipun UU PDP memberikan standar hukum perlindungan data, penerapannya dalam praktik kenotariatan elektronik belum sepenuhnya jelas dan merata, apalagi dengan kesiapan infrastruktur digital seperti sistem keamanan informasi, autentikasi elektronik, dan sertifikasi yang masih bervariasi di berbagai daerah.

Pengalaman internasional menampilkan perbedaan pendekatan yang signifikan dalam implementasi cyber notary (Alamanda & Anindita, 2025; Mahyuddin & Saleh, 2025; Rizkianti et al., 2025). Negara-negara dengan sistem hukum civil law, seperti Jerman, memandang penting perlindungan privasi secara hati-hati dan sistematis dalam menanggapi digitalisasi. Sementara itu, negara common law seperti Amerika Serikat cenderung lebih cepat mengadopsi konsep remote online notarization, sebagai respons cepat terhadap kebutuhan akses layanan. Perbandingan ini memberikan pelajaran penting bagi Indonesia agar memilih model digitalisasi kenotariatan yang sesuai dengan karakteristik sistem hukumnya dan sekaligus mampu melindungi hak privasi warganya.

Sejumlah penelitian terdahulu telah banyak membahas aspek digitalisasi kenotariatan (Eli & Rasji, 2025). Studi-studi seperti Prasetyo (2021) dan Nugroho (2023) lebih berfokus pada aspek efisiensi dan peluang digitalisasi, serta tantangan keabsahan akta elektronik dalam sistem *civil law*. Sementara itu, penelitian Arifin (2025) dan Junaidi (2025) mulai menyoroti tanggung jawab notaris dalam perlindungan data pribadi pasca UU PDP. Namun, penelitian-penelitian tersebut cenderung terfragmentasi—antara yang mengkaji aspek regulasi, teknologi, atau perlindungan data secara terpisah. **Kebaruan penelitian ini** terletak pada upaya **analisis integratif** yang menghubungkan tiga kerangka regulasi utama (UUJN, UU ITE, UU PDP) dengan pendekatan teori hukum responsif dan hak privasi untuk mengkaji implementasi *cyber notary*. Penelitian ini tidak hanya mengidentifikasi disharmoni regulasi, tetapi juga

menganalisis posisi ganda notaris sebagai pengendali dan pemroses data, serta merumuskan rekomendasi harmonisasi yang responsif terhadap perkembangan teknologi sekaligus protektif terhadap hak privasi warga negara.

Sejumlah penelitian sebelumnya lebih banyak berfokus pada aspek efisiensi dan peluang digitalisasi kenotariatan, sementara studi yang mengkaji keterkaitan antara cyber notary dengan perlindungan data pribadi serta peran notaris sebagai data controller dan data processor masih sangat terbatas. Oleh sebab itu, penelitian ini hadir dengan pendekatan yang menganalisis keselarasan cyber notary dengan hak privasi melalui dua kerangka teori utama, yaitu Teori Hukum Responsif dan Teori Hak Privasi. Pendekatan ini bertujuan untuk memberikan rekomendasi normatif bagi harmonisasi regulasi dan arah kebijakan digitalisasi kenotariatan di Indonesia secara lebih komprehensif.

Teori Hukum Responsif, yang dikembangkan oleh Philippe Nonet dan Philip Selznick, membagi evolusi hukum ke dalam tiga tahap: hukum represif, hukum otonom, dan hukum responsif. Tahap terakhir ini menekankan bahwa hukum tidak cukup hanya mempertahankan kepastian formal, tetapi harus melayani tujuan sosial dengan merespons nilai-nilai masyarakat yang dinamis. Hukum responsif menolak pandangan hukum sebagai sistem tertutup yang kaku, dan sebaliknya memandang hukum sebagai instrumen sosial yang harus mampu beradaptasi dengan perubahan zaman dan perkembangan teknologi. Dalam konteks digitalisasi kenotariatan, hukum responsif memastikan notaris bisa tetap menjalankan fungsi autentikasi dan perlindungan hukum, namun dengan prosedur yang menyesuaikan perkembangan teknologi, seperti tanda tangan elektronik dan enkripsi data.

Selain itu, hukum responsif harus berjalan seiring dengan prinsip perlindungan data pribadi. Adaptasi regulasi tidak cukup mengejar efisiensi digitalisasi, tetapi juga wajib memperhatikan hak privasi warga negara. Oleh karena itu, penyusunan regulasi cyber notary seharusnya melibatkan multipihak seperti notaris, ahli teknologi informasi, regulator perlindungan data, dan masyarakat umum agar menghasilkan regulasi yang tidak hanya efisien, tetapi juga menjamin kerahasiaan informasi sekaligus kepastian hukum. Konsep ini menegaskan pentingnya adaptabilitas, institusionalisasi reformasi kelembagaan, partisipasi pemangku kepentingan, keseimbangan antara kepastian dan fleksibilitas hukum, serta fokus pada tujuan hukum yang melayani keadilan dan keamanan masyarakat digital.

Dalam konteks perlindungan data, sejumlah indikator menjadi tolok ukur penting dalam menilai praktik cyber notary, antara lain: adanya dasar hukum yang jelas untuk pemrosesan data oleh notaris, penerapan keamanan teknis seperti enkripsi dan autentikasi multifaktor, kebijakan transparan terkait retensi dan penghapusan data, mekanisme penyampaian hak subjek data, pelaksanaan Data Protection Impact Assessment (DPIA) khusus notaris elektronik, penetapan ranah kewenangan notaris sebagai data controller ataupun data processor, serta pengawasan yang efektif oleh otoritas perlindungan data pribadi dengan sanksi yang tegas.

Teori Hak Privasi yang diperkenalkan oleh Warren dan Brandeis (1890) menggarisbawahi hak individu untuk "being let alone", yaitu kebebasan dari gangguan eksternal dan perlindungan terhadap intervensi terhadap kehidupan pribadi. Perkembangan lebih lanjut mengubah konsep ini menjadi hak atas perlindungan data pribadi yang meliputi kontrol atas bagaimana data dikumpulkan, dipakai, disimpan, dan dibagikan. Di era digital dan khususnya dalam praktik cyber notary, konsep hak privasi ini menjadi sangat relevan karena notaris memproses data pribadi yang sangat sensitif, mulai dari identitas hingga dokumen rahasia. Oleh karena itu, notaris harus mematuhi prinsip-prinsip perlindungan data dengan menjaga kerahasiaan, integritas, dan keamanan data melalui teknologi seperti enkripsi, autentikasi berlapis, dan mekanisme audit.

UU PDP di Indonesia merepresentasikan usaha hukum nasional dalam menginstitutionalisasi perlindungan hak privasi. Namun, tantangan besar masih muncul dalam pelaksanaan yang harmonis dengan UU Jabatan Notaris dan UU ITE, terutama dalam

menentukan posisi hukum notaris sebagai pengendali atau pemroses data pribadi. Di sinilah prinsip privacy by design dan privacy by default sangat krusial untuk diterapkan dalam pembangunan sistem kenotariatan digital agar tidak hanya memenuhi aspek administratif, tetapi juga substantif dalam menjamin perlindungan hak dasar warga negara.

Selain konsep kompetensi hukum, pengembangan cyber notary dan perlindungan data pribadi juga memerlukan perubahan kelembagaan, prosedur kerja, serta kapasitas sumber daya manusia. Regulasi yang responsif hukumnya harus melibatkan berbagai pemangku kepentingan dan senantiasa mengimbangi antara kepastian hukum dan ruang untuk inovasi agar tercapai keadilan, keamanan, dan aksesibilitas layanan kenotariatan dalam era digital.

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah penelitian sebagai berikut: Bagaimana harmonisasi regulasi antara Undang-Undang Jabatan Notaris (UUJN), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam mendukung implementasi cyber notary di Indonesia? Bagaimanakah peran dan tanggung jawab notaris dalam melindungi data pribadi klien sebagai data controller atau data processor dalam praktik cyber notary sesuai dengan prinsip hukum responsif dan hak privasi? Berdasarkan identifikasi kesenjangan dalam penelitian terdahulu dan kebaruan yang diusung, penelitian ini secara umum bertujuan untuk menganalisis implementasi *cyber notary* di Indonesia dalam kaitannya dengan harmonisasi regulasi dan perlindungan data pribadi pasca berlakunya UU PDP. Secara spesifik, penelitian ini dirancang untuk mengkaji keselarasan dan disharmoni antara UUJN, UU ITE, dan UU PDP; menganalisis peran dan tanggung jawab notaris sebagai pengendali atau pemroses data pribadi dalam kerangka teori hukum responsif dan hak privasi; serta merumuskan rekomendasi normatif bagi harmonisasi regulasi dan penguatan perlindungan data dalam praktik *cyber notary*. Dari segi manfaat, penelitian ini diharapkan dapat memberikan kontribusi akademis dengan memperkaya literatur hukum digital yang interdisipliner, khususnya pada persimpangan hukum kenotariatan, teknologi informasi, dan perlindungan data pribadi. Secara praktis, temuan penelitian dapat menjadi bahan pertimbangan bagi regulator, Ikatan Notaris Indonesia (INI), dan pemangku kepentingan terkait dalam menyusun kebijakan, standar teknis, dan kode etik yang mendukung digitalisasi kenotariatan yang aman, akuntabel, dan sesuai dengan prinsip perlindungan hak asasi warga negara.

METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini adalah metode penelitian hukum normatif dengan pendekatan studi kepustakaan (*library research*). Pendekatan ini bertujuan untuk menganalisis dan memahami konsep hukum serta peraturan perundang-undangan yang terkait dengan implementasi cyber notary dan perlindungan data pribadi dalam sistem hukum Indonesia. Penelitian ini menggunakan tiga jenis bahan hukum sebagai sumber utama: Bahan hukum primer, yang meliputi peraturan perundang-undangan langsung terkait praktik kenotariatan dan perlindungan data pribadi, seperti: Undang-Undang Nomor 30 Tahun 2004 tentang Jabatan Notaris beserta perubahan-perubahannya (UU Nomor 2 Tahun 2014), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Bahan primer ini menjadi dasar utama dalam menelaah kerangka hukum dan ketidakharmonisan regulasi yang berdampak pada praktik cyber notary. Bahan hukum sekunder, yaitu literatur pendukung seperti pendapat para ahli, hasil penelitian terdahulu, buku akademik, dan artikel jurnal yang relevan. Bahan ini berfungsi memperkuat analisis dengan perspektif teori dan interpretasi hukum yang lebih luas. Bahan hukum tersier, berupa kamus hukum, ensiklopedia,

dan sumber referensi lain yang digunakan untuk memperjelas istilah dan konsep teknis dalam penelitian.

Dalam analisis, penelitian ini menggunakan beberapa pendekatan: Statute Approach (Pendekatan Perundang-Undangan) Pendekatan ini menelaah secara sistematis isi, tujuan, dan hubungan antara peraturan yang mengatur jabatan notaris, perlindungan data pribadi, dan transaksi elektronik. Analisis ini bertujuan mengidentifikasi kesesuaian dan kekurangan regulasi terkait cyber notary di Indonesia. Conceptual Approach (Pendekatan Konseptual) Pendekatan ini berfokus pada pemahaman mendalam terhadap konsep-konsep penting seperti cyber notary, perlindungan data pribadi, dan prinsip kerahasiaan informasi dalam praktik kenotariatan digital. Dengan pendekatan ini, konsep hukum dapat diformulasikan secara sistematis sebagai dasar analisis dan rekomendasi. Metode ini dipilih untuk memberikan pemahaman yang mendalam dan komprehensif mengenai aspek hukum formal dan substantif di balik implementasi cyber notary serta tanggung jawab notaris dalam perlindungan data pribadi, sehingga dapat memberikan rekomendasi normatif yang sesuai dengan perkembangan teknologi dan kebutuhan hukum Indonesia.

HASIL DAN PEMBAHASAN

Harmonisasi Regulasi dalam Mendukung Implementasi *Cyber Notary* di Indonesia

Secara konseptual, notaris adalah pejabat umum yang diberi kewenangan oleh negara untuk membuat akta otentik dan kewenangan lain sebagaimana ditentukan dalam peraturan perundang-undangan. Hal ini ditegaskan dalam Pasal 1 angka 1 UUJN: "Notaris adalah pejabat umum yang berwenang untuk membuat akta autentik dan memiliki kewenangan lainnya sebagaimana dimaksud dalam Undang-Undang ini." Keberadaan cyber notary pada hakikatnya merupakan transformasi fungsi notaris dalam dunia digital, tanpa mengurangi prinsip dasar notariat yaitu kehadiran negara dalam memberikan jaminan kepastian hukum atas akta. Oleh karena itu, pembahasan mengenai harmonisasi regulasi cyber notary tidak hanya menyentuh aspek teknologi, tetapi juga menyangkut legitimasi akta sebagai produk hukum.

Emma Nurita menyatakan bahwa cyber notary adalah notaris yang menjalankan tugas atau kewenangannya berbasis teknologi informasi, khususnya dalam pembuatan akta. Sementara Brian Amy Prastyo menegaskan bahwa konsep cyber notary masih bersifat konseptual karena belum ada pengaturan eksplisit dalam hukum positif Indonesia. Konsep ini menemukan relevansinya karena perubahan gaya hidup masyarakat yang semakin digital, sebagaimana tercermin dalam meningkatnya penggunaan transaksi elektronik. Bahkan, data Bank Indonesia tahun 2024 menunjukkan nilai transaksi digital banking tumbuh lebih dari 11% setiap tahun. Perkembangan ini menuntut adanya instrumen hukum yang mampu menjamin keamanan, kepastian, dan perlindungan hukum, salah satunya melalui cyber notary. Secara normatif, Pasal 15 ayat (3) UUJN memberi peluang bagi perluasan kewenangan notaris: "Selain kewenangan sebagaimana dimaksud pada ayat (1) dan ayat (2), Notaris mempunyai kewenangan lain yang diatur dalam peraturan perundang-undangan."

Namun dalam praktiknya, kewenangan tersebut belum secara tegas diarahkan pada pembuatan akta dalam bentuk elektronik. Hal ini karena paradigma UUJN masih bertumpu pada kehadiran fisik para pihak di hadapan notaris. Ketentuan ini selaras dengan doktrin bahwa akta otentik harus dibuat di hadapan pejabat umum dengan bentuk formal tertentu. Pasal 1868 KUHPerdata memberikan definisi akta otentik: "Suatu akta otentik ialah suatu akta yang dibuat dalam bentuk yang ditentukan undang-undang oleh atau di hadapan pejabat umum yang berkuasa untuk itu di tempat akta itu dibuat." Masalah timbul karena akta elektronik, yang dibuat tanpa kehadiran fisik para pihak, sulit memenuhi unsur "di hadapan pejabat umum" tersebut.

Di Amerika Serikat, Remote Online Notarization (RON) telah dilegalkan di lebih dari 30 negara bagian, dengan dasar hukum bahwa kehadiran virtual melalui video conference

dianggap sah sebagai pengganti kehadiran fisik. Sedangkan di Jerman, Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) 2021 memberi ruang pembuatan akta notaris secara online untuk jenis akta tertentu, misalnya pendirian perseroan terbatas. Indonesia, sebaliknya, masih menghadapi disharmoni regulasi. UUJN dan KUHPerdata berorientasi pada model konvensional, sementara UU ITE memberi pengakuan pada dokumen elektronik sebagai alat bukti sah. Pasal 5 ayat (1) UU ITE: "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah." Kemudian ditegaskan dalam Pasal 11 ayat (1) UU ITE: "Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah." Ketentuan ini menegaskan bahwa secara umum, dokumen elektronik diakui sebagai alat bukti hukum. Namun, permasalahannya adalah UU ITE tidak membedakan antara dokumen elektronik biasa dan akta otentik elektronik.

Akibatnya, akta elektronik yang dibuat notaris bisa diakui sebagai bukti hukum, tetapi statusnya sebagai akta otentik masih diperdebatkan karena bertentangan dengan Pasal 1868 KUHPerdata. Selain itu, pelaksanaan cyber notary harus memenuhi prinsip penyelenggaraan sistem elektronik sebagaimana diatur dalam Pasal 15 ayat (1) UU ITE jo. Pasal 3 PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang mewajibkan penyelenggara sistem elektronik menjamin: Kerahasiaan, keutuhan, ketersediaan, autentikasi, dan aksesibilitas data.

Dengan demikian, cyber notary juga tunduk pada rezim hukum keamanan siber. Notaris menyimpan dan memproses data pribadi dalam jumlah besar, mulai dari identitas diri, dokumen perusahaan, hingga data keuangan. Oleh karena itu, cyber notary juga harus tunduk pada UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Pasal 4 ayat (2) huruf b UU PDP menyatakan: "Data Pribadi yang bersifat spesifik meliputi data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan."

Jika dikaitkan dengan praktik notaris, hampir seluruh akta memuat data yang bersifat spesifik, terutama data keuangan dan identitas hukum subjek. Hal ini berarti notaris wajib mematuhi prinsip-prinsip pemrosesan data, termasuk privacy by design dan privacy by default (Pasal 29 UU PDP). Lebih lanjut, notaris berpotensi ditempatkan dalam posisi sebagai data controller (penentu tujuan dan kendali pemrosesan data) maupun data processor (pemroses data untuk kepentingan pihak lain). Kepastian hukum mengenai posisi ini menjadi penting agar kewajiban administratif notaris, seperti penyusunan Data Protection Impact Assessment (DPIA), pencatatan aktivitas pemrosesan, hingga penunjukan pejabat perlindungan data, dapat dijalankan dengan jelas.

Dari uraian di atas, dapat diidentifikasi setidaknya terdapat tiga bentuk disharmoni regulasi utama dalam penerapan konsep cyber notary di Indonesia. Pertama, terdapat kontradiksi antara Pasal 1868 KUHPerdata dengan Pasal 5 UU ITE. KUHPerdata secara tegas mensyaratkan kehadiran fisik para pihak di hadapan notaris serta bentuk formal akta sebagai syarat sahnya suatu akta autentik. Sementara itu, UU ITE justru memberikan pengakuan bahwa dokumen elektronik dan tanda tangan elektronik dapat memiliki kekuatan hukum yang sama dengan dokumen kertas. Perbedaan mendasar ini menimbulkan kerancuan mengenai legalitas akta elektronik yang dibuat dalam konteks kenotariatan.

Kedua, keterbatasan yang terdapat dalam Undang-Undang Jabatan Notaris (UUJN). Secara normatif, UUJN belum mengakomodasi praktik pembuatan akta secara elektronik. Meskipun Pasal 15 ayat (3) UUJN membuka peluang adanya kewenangan baru bagi notaris sepanjang diatur dalam peraturan perundang-undangan, namun sampai saat ini belum ada pengaturan yang secara eksplisit mengatur mekanisme pembuatan akta elektronik.

Kekosongan norma ini menyebabkan notaris berada dalam posisi serba sulit, karena di satu sisi ada kebutuhan modernisasi layanan, tetapi di sisi lain belum ada landasan hukum yang jelas.

Ketiga, potensi konflik dengan Undang-Undang Perlindungan Data Pribadi (UU PDP). Cyber notary melibatkan pengelolaan data sensitif yang mencakup identitas pribadi, informasi keuangan, maupun dokumen hukum para pihak. Namun hingga saat ini, belum ada mekanisme khusus dalam regulasi kenotariatan yang mengatur secara detail tata cara penyimpanan, pemrosesan, serta perlindungan data pribadi tersebut. Padahal, UU PDP mewajibkan setiap pengendali data, termasuk notaris, untuk menjamin keamanan, kerahasiaan, dan integritas data yang dikelola. Kondisi ini menimbulkan risiko tumpang tindih tanggung jawab apabila terjadi kebocoran atau penyalahgunaan data pribadi dalam praktik cyber notary.

Dari perspektif teori hukum responsif yang dikemukakan oleh Nonet dan Selznick, hukum seharusnya mampu menyesuaikan diri dengan dinamika masyarakat. Hukum tidak boleh kaku dan statis, melainkan harus mampu memberikan jawaban terhadap perkembangan teknologi dan kebutuhan publik. Namun demikian, responsivitas hukum yang berlebihan juga mengandung risiko. Salah satunya adalah regulatory capture, yaitu kondisi ketika kekuatan besar, seperti perusahaan teknologi raksasa (big tech), justru mendikte arah regulasi sesuai dengan kepentingan mereka. Situasi ini tentu berbahaya karena dapat menggeser orientasi hukum dari kepentingan publik menuju kepentingan korporasi.

Dalam kerangka reformasi hukum kenotariatan, perlu ada keseimbangan antara tiga aspek utama. Pertama adalah kepastian hukum, yaitu jaminan bahwa akta yang dibuat secara elektronik tetap memiliki otentisitas dan kekuatan pembuktian yang sama dengan akta konvensional. Kedua adalah perlindungan hukum, khususnya yang berkaitan dengan keamanan serta kerahasiaan data pribadi klien yang dikelola notaris. Ketiga adalah efisiensi layanan publik, yang merupakan salah satu tujuan utama digitalisasi kenotariatan melalui cyber notary. Dengan demikian, hukum tidak hanya responsif terhadap perkembangan teknologi, tetapi juga tetap menjaga esensi perlindungan kepentingan masyarakat.

Untuk mewujudkan hal tersebut, terdapat sejumlah langkah konkret yang dapat ditempuh. Pertama, amandemen UU Jabatan Notaris (UUJN) diperlukan dengan menambahkan bab khusus mengenai akta elektronik dan mekanisme kehadiran virtual. Kedua, perlu dilakukan integrasi antara UUJN dan UU ITE melalui aturan turunan, misalnya dalam bentuk Peraturan Pemerintah yang secara spesifik mengatur praktik cyber notary. Ketiga, Kementerian Komunikasi dan Informatika bersama Ditjen AHU Kementerian Hukum dan HAM harus menetapkan standar keamanan siber yang wajib dipatuhi oleh setiap notaris. Keempat, peran Ikatan Notaris Indonesia (INI) perlu diperkuat, baik dalam hal pengawasan maupun penyusunan kode etik baru yang sesuai dengan praktik digital.

B. Peran dan Tanggung Jawab Notaris dalam Perlindungan Data Pribadi dalam Praktik Cyber Notary

Seiring dengan lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), notaris memiliki kewajiban hukum yang semakin berat dalam menjaga kerahasiaan data pribadi klien yang diproses secara elektronik. Pasal 1 angka 1 UU PDP memberikan definisi: “Data Pribadi adalah setiap data tentang seseorang yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.”

Jika dikaitkan dengan praktik kenotariatan, hampir seluruh akta yang dibuat notaris berisi data pribadi klien, mulai dari identitas, data keuangan, hingga dokumen hukum perusahaan. Data tersebut bahkan bisa termasuk kategori data spesifik sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b UU PDP yang mencakup data keuangan pribadi. Dengan demikian, notaris tidak hanya berperan sebagai pembuat akta, tetapi juga sebagai pengendali (data controller) dan pemroses (data processor) data pribadi dalam lingkup profesinya.

Hal ini juga sejalan dengan Pasal 16 ayat (1) huruf f UUJN, yang mewajibkan notaris untuk merahasiakan segala sesuatu mengenai akta yang dibuatnya dan segala keterangan yang diperoleh guna pembuatan akta sesuai sumpah jabatan. Artinya, kewajiban kerahasiaan yang sebelumnya bersifat etik-profesional kini diperkuat dengan rezim hukum perlindungan data pribadi yang memiliki sanksi administratif maupun pidana. Dalam rezim UU PDP, subjek hukum yang memproses data terbagi menjadi pengendali data pribadi dan prosesor data pribadi. Pasal 1 angka 4 dan 5 UU PDP menjelaskan: Pengendali Data Pribadi adalah pihak yang menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Prosesor Data Pribadi adalah pihak yang memproses data pribadi atas nama pengendali data pribadi.

Posisi notaris dapat dikategorikan sebagai pengendali data pribadi, karena notaris menentukan tujuan pengumpulan dan penggunaan data dalam pembuatan akta autentik. Dengan demikian, notaris memiliki tanggung jawab langsung terhadap keamanan, kerahasiaan, dan akuntabilitas pemrosesan data klien. Hal ini diperkuat dalam Pasal 20 ayat (1) UU PDP yang mewajibkan pengendali data pribadi untuk melaksanakan pemrosesan data sesuai prinsip: Keabsahan dasar pemrosesan, pembatasan tujuan, keterbukaan, akurasi, pembatasan penyimpanan, integritas dan kerahasiaan, serta akuntabilitas.

Dalam konteks cyber notary, tanggung jawab ini berarti notaris harus memastikan bahwa setiap akta elektronik yang dibuat, disimpan, maupun ditransmisikan telah melalui mekanisme keamanan informasi yang memenuhi standar enkripsi, autentikasi, dan audit. UU ITE memberikan dasar hukum penggunaan tanda tangan elektronik dalam akta digital. Pasal 11 ayat (1) UU ITE menyatakan: "Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah." Lebih lanjut, Pasal 12 ayat (1) UU ITE menegaskan bahwa tanda tangan elektronik memiliki kekuatan pembuktian yang sama dengan tanda tangan konvensional sepanjang memenuhi persyaratan tertentu, antara lain: Terkait hanya dengan penanda tangan, data pembuatan tanda tangan elektronik hanya berada dalam kuasa penanda tangan, segala perubahan terhadap tanda tangan elektronik dapat diketahui, dan segala perubahan terhadap informasi elektronik terkait dapat diketahui.

Dalam praktik cyber notary, penerapan tanda tangan elektronik yang bersertifikat (certificate-based digital signature) menjadi syarat mutlak agar akta elektronik diakui sah secara hukum. Selain itu, sesuai Pasal 15 ayat (1) UU ITE, penyelenggara sistem elektronik (dalam hal ini bisa termasuk sistem cyber notary) wajib menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab, serta harus mampu menjamin ketersediaan, keutuhan, kerahasiaan, dan keteraksesan data pribadi. Dengan demikian, notaris sebagai pengguna sistem harus memastikan bahwa sistem manajemen keamanan informasi (information security management system) yang digunakan memenuhi standar nasional maupun internasional, misalnya ISO/IEC 27001.

Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Jabatan Notaris (UUJN), dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah menyediakan kerangka normatif, masih terdapat disharmoni hukum yang cukup signifikan. Ketidaksinkronan ini menimbulkan keraguan dalam praktik, terutama ketika notaris dituntut untuk beradaptasi dengan kebutuhan digitalisasi melalui konsep cyber notary. Pertama, UUJN memang menekankan pentingnya kerahasiaan akta sebagai bagian dari kewajiban profesi notaris. Namun, regulasi tersebut belum mengatur secara detail mekanisme perlindungan data dalam bentuk elektronik. Padahal, digitalisasi akta menuntut adanya standar teknis dan prosedural mengenai bagaimana data elektronik disimpan, diamankan, serta dijaga kerahasiaannya.

Kedua, UU PDP menempatkan notaris dalam posisi sebagai pengendali data pribadi (data controller), yang berarti notaris memikul tanggung jawab penuh atas pengelolaan data sensitif

klien. Namun, undang-undang ini tidak memberikan pengaturan secara spesifik mengenai kedudukan notaris sebagai pejabat umum yang memiliki fungsi otentikasi. Hal ini menimbulkan celah interpretasi, apakah notaris diperlakukan sama dengan badan hukum atau korporasi biasa, ataukah memiliki perlakuan khusus sebagai pejabat publik. Ketiga, UU ITE memang telah mengakui keberlakuan tanda tangan elektronik sebagai sah dan memiliki kekuatan hukum yang mengikat. Akan tetapi, undang-undang tersebut tidak secara langsung menjawab persoalan mendasar: apakah akta elektronik yang dibuat dan ditandatangani secara digital dapat dianggap memenuhi syarat akta otentik sebagaimana dimaksud dalam Pasal 1868 Kitab Undang-Undang Hukum Perdata (KUHPerdata). Pasal tersebut secara eksplisit menyatakan bahwa akta otentik harus dibuat oleh atau di hadapan pejabat umum yang berwenang, dalam bentuk yang ditentukan oleh undang-undang. Pertanyaan ini menegaskan bahwa tanpa penyesuaian regulasi, akta elektronik masih berpotensi dianggap tidak memenuhi standar formal sebagai akta otentik.

Risiko pelanggaran data pribadi dalam praktik cyber notary merupakan isu yang tidak bisa diabaikan. Seiring dengan meningkatnya digitalisasi layanan kenotariatan, ancaman terhadap keamanan informasi menjadi semakin kompleks dan beragam. Notaris, sebagai pihak yang memegang data sensitif klien, berhadapan langsung dengan potensi kebocoran maupun penyalahgunaan informasi apabila tidak ada sistem perlindungan yang memadai. Salah satu risiko yang paling menonjol adalah kebocoran data pribadi akibat peretasan sistem (hacking). Serangan siber yang menargetkan server atau sistem penyimpanan data notaris dapat mengakibatkan informasi penting—seperti identitas, dokumen hukum, hingga informasi keuangan—jatuh ke tangan pihak yang tidak berwenang. Hal ini tidak hanya merugikan klien, tetapi juga mencoreng kepercayaan publik terhadap profesi notaris.

Selain itu, risiko penyalahgunaan akses oleh pihak internal juga perlu diwaspadai. Pegawai atau pihak lain yang diberi wewenang mengelola sistem dapat menyalahgunakan akses tersebut untuk kepentingan pribadi atau bahkan menjual data kepada pihak ketiga. Faktor human error maupun moral hazard inilah yang menjadikan pengawasan internal sangat krusial. Keterlibatan pihak ketiga dalam praktik cyber notary, seperti penggunaan platform penyimpanan cloud, juga menghadirkan tantangan tersendiri. Jika platform tersebut tidak memenuhi standar keamanan yang ditetapkan oleh regulasi, maka data pribadi klien berpotensi terekspos kepada risiko kebocoran maupun eksploitasi. Dengan demikian, pemilihan penyedia layanan teknologi harus dilakukan secara hati-hati dengan memperhatikan prinsip akuntabilitas dan kepatuhan terhadap standar perlindungan data.

Di sisi lain, terdapat risiko over-compliance, yakni ketika penerapan standar perlindungan data dilakukan terlalu ketat sehingga justru menghambat akses masyarakat terhadap layanan kenotariatan. Prosedur yang rumit dan tidak ramah pengguna dapat menurunkan efektivitas layanan serta mengurangi kepercayaan masyarakat terhadap sistem digital. Terakhir, potensi konflik kepentingan (conflict of interest) juga tidak boleh diabaikan. Risiko ini muncul ketika data pribadi yang dikumpulkan dalam rangka pembuatan akta digunakan untuk tujuan lain di luar kepentingan hukum, misalnya kepentingan komersial atau pemasaran. Praktik semacam ini jelas bertentangan dengan prinsip perlindungan data pribadi sebagaimana diatur dalam UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menekankan pembatasan tujuan (purpose limitation) dalam setiap proses pengolahan data. Agar praktik cyber notary dapat berjalan sejalan dengan prinsip perlindungan data pribadi, diperlukan sejumlah rekomendasi normatif yang bersifat konkret dan aplikatif. Tanpa adanya kerangka regulasi yang jelas, risiko pelanggaran data pribadi maupun ketidakpastian hukum akan terus menghantui penerapan sistem ini.

Pertama, perlu dibentuk regulatory sandbox oleh Kementerian Hukum dan HAM bersama dengan Kementerian Komunikasi dan Informatika. Regulatory sandbox ini berfungsi sebagai ruang uji coba terbatas untuk model layanan cyber notary dengan pengawasan yang

ketat. Melalui mekanisme ini, pemerintah dapat mengidentifikasi kelemahan teknis maupun celah hukum sebelum sistem diterapkan secara nasional, sehingga risiko dapat diminimalkan sejak awal.

Kedua, penerapan standar keamanan nasional mutlak diperlukan. Seluruh notaris yang menggunakan sistem digital harus diwajibkan untuk menerapkan standar sertifikasi keamanan informasi, misalnya ISO 27001 atau standar sejenis yang diakui secara internasional. Standar ini menjadi jaminan bahwa pengelolaan data pribadi dilakukan sesuai dengan prinsip keamanan, integritas, dan kerahasiaan.

Ketiga, Ikatan Notaris Indonesia (INI) perlu merumuskan kode etik digital kenotariatan yang relevan dengan perkembangan teknologi. Kode etik ini setidaknya harus mengatur larangan penggunaan platform pihak ketiga yang tidak memenuhi standar keamanan, kewajiban menerapkan prinsip data minimization, serta mempertegas tanggung jawab moral dan hukum notaris dalam menjaga kerahasiaan data klien di ruang siber.

Keempat, mekanisme pengawasan lintas otoritas juga sangat penting untuk menjamin akuntabilitas. Pengawasan tidak bisa hanya dilakukan oleh Kementerian Hukum dan HAM, tetapi juga perlu melibatkan Otoritas Jasa Keuangan dan Otoritas Perlindungan Data. Dengan adanya mekanisme pengawasan bersama, praktik cyber notary dapat diawasi dari berbagai aspek: legalitas, keamanan data, hingga potensi konflik kepentingan.

Kelima, perlu disusun pedoman perlindungan data pribadi khusus profesi notaris. Pedoman ini bersifat teknis dan wajib, mengatur tata cara pengumpulan, penyimpanan, dan penghapusan data pribadi, sekaligus mewajibkan adanya mekanisme pemberitahuan kebocoran data (data breach notification) apabila terjadi insiden. Dengan adanya pedoman ini, tanggung jawab notaris menjadi lebih jelas sekaligus memberikan perlindungan nyata bagi masyarakat sebagai pengguna jasa kenotariatan digital.

Secara etis, peran notaris sebagai pejabat umum yang dipercaya publik menuntut integritas lebih tinggi dibanding profesi hukum lainnya. Notaris tidak hanya berfungsi sebagai pengesah dokumen, tetapi juga simbol kepercayaan publik terhadap negara. Jika notaris gagal menjaga kerahasiaan data pribadi, maka tidak hanya klien yang dirugikan, tetapi juga legitimasi negara dalam menjamin kepastian hukum. Dari perspektif filsafat hukum, hal ini menyangkut perlindungan hak privasi yang merupakan bagian dari hak asasi manusia. Pasal 28G ayat (1) UUD 1945 menegaskan: “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.” Dengan demikian, cyber notary bukan hanya isu teknis administratif, tetapi juga menyangkut tanggung jawab konstitusional negara dalam melindungi hak privasi warga negara

KESIMPULAN

Harmonisasi regulasi antara Undang-Undang Jabatan Notaris (UUJN), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam mendukung implementasi cyber notary di Indonesia, yaitu: Implementasi cyber notary di Indonesia masih menghadapi berbagai kendala, seperti ketidakharmonisan aturan, ketidakjelasan status akta elektronik, dan risiko pelanggaran data pribadi. Perbedaan antara KUH Perdata, UU Jabatan Notaris, dan UU ITE membuat penerapan akta digital belum sejalan. Selain itu, keterbatasan aturan dalam UUJN menyulitkan notaris beradaptasi dengan era digital, sementara UU Perlindungan Data Pribadi menambah tanggung jawab baru tanpa mekanisme yang jelas bagi Notaris.Implementasi cyber notary di Indonesia

menghadapi tantangan serius berupa disharmoni regulasi, keraguan status hukum akta elektronik, serta risiko pelanggaran data pribadi. Disharmoni regulasi terlihat dari kontradiksi antara KUHPerdata, UUJN, dan UU ITE, di mana akta otentik masih mensyaratkan kehadiran fisik para pihak, sementara dokumen elektronik dan tanda tangan digital telah diakui sah dalam sistem hukum Indonesia. Selain itu, keterbatasan pengaturan dalam UUJN membuat notaris kesulitan untuk beradaptasi dengan kebutuhan digitalisasi, sementara UU PDP memberi tanggung jawab tambahan dalam hal perlindungan data pribadi, tanpa memberikan mekanisme spesifik yang sesuai dengan karakter pejabat umum.

REFERENSI

Alamanda, M. D., & Anindita, S. L. (2025). *Tantangan dan prospek cyber notary di Indonesia*. Syntax Literate: Jurnal Ilmiah Indonesia. https://doi.org/10.36418/SYNTAX-LITERATE.V10I5.58183

Andriani, M., Padiya, A., & Ulfah, M. (2025). *Transformasi digital dalam praktik kenotariatan: Analisis yuridis terhadap penerapan cyber notary di Indonesia*. Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory. https://doi.org/10.62976/IJIJEL.V3I2.1202

Arifin, D. (2025). Perlindungan data pribadi dalam transformasi digital layanan kenotariatan di Indonesia. *Jurnal Hukum & Informatika, 10*(1), 45–62.

Asriannor, Zikri, M. A., Gazali, M. I., & Nugraha, R. D. (2025). *Tantangan dan peluang profesi notaris di era digital*. Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory. https://doi.org/10.62976/IJIJEL.V3I2.1205

Bayumurti, K., Perdana, N., & Tjandra, R. S. (2025). *Penerapan konsep cyber notary dalam praktek hukum di Indonesia*. Jurnal Hukum Lex Generalis. https://doi.org/10.56370/JHLG.V6I4.896

Choirunnisa, L., Oktaviana, T. H. C., Ridlo, A. A., & Rohmah, E. I. (2023). Peran Sistem Pemerintah Berbasis Elektronik (SPBE) dalam meningkatkan aksesibilitas pelayanan publik di Indonesia. *Sosio Yustisia: Jurnal Hukum dan Perubahan Sosial, 3*(1), 71–95.

Eli, G., & Rasji. (2025). *Pembaharuan hukum terhadap kekuatan akta autentik elektronik*. Jurnal USM Law Review.

Ferryanto, J., Tan, W., & Sudirman, L. (2024). Potensi dan tantangan hukum digitalisasi layanan kenotariatan: Analisis komparatif Indonesia dan Amerika Serikat. *Jurnal MEDIASAS Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah*. https://doi.org/10.58824/MEDIASAS.V7I2.135

Jasmine, A., Djaja, B., & Sudirman, M. (2024). Tanggung jawab notaris dalam perlindungan data pribadi klien berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. *Jurnal Ilmu Hukum, Humaniora dan Politik*. https://doi.org/10.38035/JIHHP.V5I1.3204

Junaidi, F. (2025). Tanggung jawab notaris dalam perlindungan data pribadi sesuai UU PDP. *Jurnal Hukum dan Teknologi, 18*(1), 101–117.

Lubis, I., Lubis, D. I. S., & Lubis, A. H. (2025). Rekonstruksi hukum cyber notary law untuk menjaga kepercayaan, integritas dan keadilan dalam sistem hukum. *Notaire*. https://doi.org/10.20473/NTR.V8I1.64253

Mahyuddin, D. L., & Saleh, M. M. (2025). Diskrepansi regulasi: Tinjauan atas perbedaan persyaratan pengangkatan notaris dengan notaris pengganti dalam praktik notarial Indonesia. *Jurnal Pendidikan Indonesia*. https://doi.org/10.59141/JAPENDI.V6I5.7749

Mayana, R. F., & Santika, T. (2021). Legalitas tanda tangan elektronik: Posibilitas dan tantangan notary digitalization di Indonesia. *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan dan Ke-PPAT-an*. https://doi.org/10.23920/ACTA.V4I2.517

Meranggi, I. N. T. W. R., & Lukman, J. P. (2024). Transformasi digital layanan pemasyarakatan di Kantor Wilayah Kementerian Hukum dan HAM (Kemenkumham) Bali. *Deleted Journal*. https://doi.org/10.61292/SHKR.139

Nugroho, S. (2023). Cyber notary dan tantangan keabsahan akta elektronik di civil law system Indonesia. *Jurnal Hukum Bisnis, 15*(3), 78–94.

Prasetyo, B. A. (2021). *Kenotariatan digital dan perlindungan hukum*. Gadjah Mada University Press.

Rizkia, N. D., Fardiansyah, H., Sekolah, D., Ilmu, T., Dharma, H., & Andigha. (2022). Peran notaris dalam transformasi digital dalam rangka kesejahteraan masyarakat Indonesia. *Jurnal Hukum Sasana*. https://doi.org/10.31599/SASANA.V8I2.1097

Rizkianti, W., Hutabarat, S. M. D., Nugroho, A. A., Firdaus, M., & Latri, A. A. (2025). Cyber notary di Indonesia: Tantangan, peluang dan kebutuhan rekonstruksi hukum. *Notaire*. https://doi.org/10.20473/NTR.V8I1.67806

Rukmana, R., Savitri, N. D., & Padha, Y. A. (2021). Peran notaris dalam transaksi perdagangan berbasis elektronik. https://doi.org/10.23887/JKH.V7I1.32324

Sitaresmi, A., & Ristawati, R. (2025). Perlindungan data pribadi post-mortem oleh notaris melalui penyimpanan protokol notaris: Prospek dan tantangannya. *Halu Oleo Law Review*. https://doi.org/10.33561/HOLREV.V9I1.125

Wirawan, V. (2020). *Penerapan e-government dalam menyongsong era Revolusi Industri 4.0 kontemporer di Indonesia*. https://doi.org/10.18196/JPHK.1101