JETISH: Journal of Education Technology Information Social Sciences and Health
E-ISSN: 2964-2507 P-ISSN: 2964-819X
Vol. 6 No. 1 Maret 2027

Upaya Hukum dalam Penyimpanan Dokumen Jangka Panjang Akta pada Akta Digital Notary

Faizma Zia Illaya[1] Dewi Septiana[2] Nenny Dwi Ariani[3] Mohammad Wendy Trijaya[4] Sayyidah Sekar Dewi Kulsum[5]
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Lampung, Kota Bandar Lampung, Provinsi Lampung, Indonesia[1,2,3,4,5]
Email: faizmaziaa@gmail.com[1] dewi.septian@fh.unila.ac.id[2] nenny.ariani@fh.unila.ac.id[3] mwtrijaya@gmail.com[4] sayyidah.sekar@fh.unila.ac.id[5]

Abstrak

Penyimpanan protokol notaris bersifat berkelanjutan lintas generasi pemegang jabatan, sedangkan media digital memiliki umur teknis yang terbatas. Kesenjangan tersebut melahirkan risiko yuridis berupa ketidakpastian kedudukan akta elektronik, hilangnya keautentikan dan integritas dokumen, ketidaktersediaan dokumen, serta pelanggaran kerahasiaan data pribadi. Artikel ini bertujuan menganalisis upaya hukum yang dapat ditempuh untuk menekan risiko tersebut dalam penyimpanan jangka panjang akta digital notary. Penelitian menggunakan metode hukum normatif-empiris dengan tipe deskriptif-analitis, pendekatan perundang-undangan dan konseptual, data sekunder yang dikumpulkan melalui studi kepustakaan dengan wawancara sebagai data pendukung, serta analisis kualitatif berlandaskan teori kepastian hukum, perlindungan hukum, dan pembuktian. Hasil analisis menunjukkan bahwa upaya hukum bersifat berlapis. Upaya preventif meliputi penegasan kedudukan jenis dokumen, verifikasi alih media, enkripsi, pengendalian akses, pencadangan multilokasi, preservasi tanda tangan elektronik, prosedur operasional baku, serah terima protokol, deteksi dini, dan kesiapsiagaan insiden. Upaya represif meliputi pengamanan bukti elektronik, pelaporan kegagalan pelindungan data dalam 3 x 24 jam, pemulihan dokumen, serta penegakan pertanggungjawaban administratif dan perdata. Keduanya perlu ditopang pembaruan regulasi, pembagian tanggung jawab, dan pengawasan kelembagaan. Selama belum ada pengaturan tegas, digitalisasi diposisikan sebagai sarana pendukung, bukan pengganti minuta akta asli.

Kata Kunci: Akta Digital Notaris, Upaya Hukum, Penyimpanan Jangka Panjang, Protokol Notaris, *Cyber Notary*

Abstract

Digital media have a limited technical lifespan. This gap gives rise to legal risks, including uncertainty regarding the status of electronic deeds, the loss of authenticity and document integrity, document unavailability, and breaches of personal data confidentiality. This article aims to analyze legal remedies that can be pursued to mitigate these risks in the long-term preservation of digital notary deeds. This research employs a normative-empirical legal methodology with a descriptive-analytical approach, utilizing statutory and conceptual frameworks. Secondary data were collected through literature studies and supplemented by interviews, followed by a qualitative analysis grounded in theories of legal certainty, legal protection, and evidence. The analysis reveals that legal remedies are multi-layered. Preventive measures include asserting the status of document types, media conversion verification, encryption, access control, multi-location backups, electronic signature preservation, standard operating procedures, protocol handovers, early detection, and incident preparedness. Repressive measures involve securing electronic evidence, reporting data protection failures within 3 x 24 hours, document recovery, and enforcing administrative and civil liabilities. Both approaches must be supported by regulatory updates, clear division of responsibilities, and institutional oversight. Pending explicit regulation, digitalization should function as a supporting mechanism rather than a replacement for the original deed minutes (minuta akta).

Keywords: *Digital Notary Deed, Legal Remedies, Long-Term Preservation, Notary Protocol, Cyber Notary*

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

PENDAHULUAN

Notaris merupakan pejabat umum yang diberi kewenangan oleh negara untuk membuat akta autentik mengenai perbuatan, perjanjian, dan ketetapan yang diharuskan oleh peraturan perundang-undangan atau dikehendaki oleh para pihak (Adjie, 2008). Kedudukan tersebut tidak semata-mata bersifat profesional, tetapi memiliki dimensi publik karena kewenangan notaris bersumber dari negara dan digunakan untuk melayani kepentingan masyarakat akan kepastian hukum (Borman, 2019). Akta yang dibuat notaris memiliki kekuatan pembuktian yang sempurna sebagaimana dimaksud dalam Pasal 1870 Kitab Undang-Undang Hukum Perdata (KUHPerdata), sepanjang akta tersebut dapat ditunjukkan keasliannya. Karena itu, persoalan penyimpanan akta tidak dapat dipandang sebagai urusan administratif belaka, melainkan sebagai bagian yang menentukan apakah kekuatan pembuktian tersebut dapat dipertahankan ketika akta dibutuhkan di kemudian hari. Undang-Undang Nomor 2 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 30 Tahun 2004 tentang Jabatan Notaris (UUJN) mewajibkan notaris membuat akta dalam bentuk minuta dan menyimpannya sebagai bagian dari protokol notaris. Protokol itu sendiri berstatus arsip negara yang harus dipelihara tanpa batas waktu tertentu, bahkan melampaui masa jabatan notaris yang bersangkutan melalui mekanisme penyerahan protokol kepada notaris lain. Dengan demikian, kewajiban penyimpanan dalam UUJN pada dasarnya bersifat berkelanjutan lintas generasi pemegang jabatan, sehingga secara praktis dapat dimaknai sebagai kewajiban penyimpanan permanen (Jagadhita & Bagiastra, 2025).

Pada saat yang sama, transformasi digital mendorong praktik kenotariatan untuk memanfaatkan teknologi informasi. Konsep cyber notary diperkenalkan sebagai bentuk adaptasi profesi notaris terhadap era digitalisasi (Makarim, 2013; Sya'roni, 2021), dan dalam praktik istilah akta digital notary digunakan untuk menyebut dua hal yang berbeda, yakni alih media akta konvensional ke dalam berkas digital dan penerapan cyber notary terbatas dalam proses pembuatan akta (Paramita, 2023). Penyimpanan digital menjanjikan efisiensi, kemudahan penelusuran, penghematan ruang, dan perlindungan dari kerusakan fisik. Akan tetapi, media digital tidak dirancang untuk bertahan puluhan tahun tanpa intervensi. Format berkas, perangkat lunak, sertifikat elektronik, dan algoritma kriptografi memiliki umur teknis yang jauh lebih pendek daripada kewajiban penyimpanan yang dibebankan hukum kepada notaris (Rizkianto dkk., 2022). Ketegangan antara kewajiban penyimpanan yang permanen dan umur teknis media digital yang terbatas menimbulkan serangkaian risiko yuridis. Kedudukan akta elektronik sebagai akta autentik belum memperoleh pengaturan yang tegas, keautentikan dan integritas dokumen dapat terancam oleh keusangan sertifikat elektronik maupun serangan siber, ketersediaan dokumen dapat terganggu oleh bencana atau kegagalan sistem, dan kerahasiaan data para penghadap dapat dilanggar melalui akses tanpa kewenangan. Risiko-risiko tersebut tidak hanya merugikan para pihak, tetapi juga dapat membebani notaris dengan tanggung jawab administratif, perdata, bahkan pidana.

Sejumlah penelitian terdahulu telah menyentuh persoalan ini dari berbagai sisi. Penelitian mengenai penyimpanan protokol notaris berbasis cloud computing menekankan manfaat pengurangan risiko fisik, tetapi sekaligus mengingatkan bahwa penyimpanan elektronik tidak serta-merta mengubah salinan digital menjadi minuta (Iriantoro & Hardiansyah, 2024; Solehudin & Djajaputra, 2023). Kajian lain membahas tanggung jawab notaris atas penyimpanan elektronik protokol (Ngadino, 2021), perlindungan data pribadi dalam layanan cyber notary (Najib, 2023), kepastian hukum penyimpanan dokumen notaris (Rizkianto dkk., 2022), urgensi pengaturan penyimpanan protokol sebagai arsip negara dengan sistem elektronik (Ghazala & Erni, 2022), serta kebutuhan regulasi bagi protokol yang telah berumur lebih dari dua puluh lima tahun (Jagadhita & Bagiastra, 2025). Kajian-kajian tersebut

umumnya bertumpu pada satu aspek, misalnya keabsahan akta, keamanan data, atau pengalihan protokol.

Research gap yang hendak diisi artikel ini terletak pada belum adanya telaah yang memadukan seluruh aspek tersebut menjadi satu rangkaian upaya hukum yang utuh dan berlapis untuk menekan risiko penyimpanan jangka panjang, yakni dari langkah pencegahan, penanganan setelah risiko terjadi, hingga pembaruan norma. Telaah yang ada cenderung berhenti pada identifikasi risiko atau pada rekomendasi teknis yang tidak dikaitkan dengan kewajiban hukum yang melekat pada notaris. Padahal, tindakan teknis seperti enkripsi, pencadangan, atau audit baru memiliki makna yuridis apabila dapat dipertanggungjawabkan sebagai pelaksanaan kewajiban jabatan dan dapat dibuktikan ketika terjadi sengketa. Perlu dijelaskan bahwa istilah upaya hukum dalam artikel ini tidak digunakan dalam pengertian hukum acara, yaitu perlawanan, banding, kasasi, atau peninjauan kembali. Istilah tersebut digunakan dalam arti luas, yaitu seluruh langkah berbasis norma hukum yang dapat ditempuh untuk mencegah, menangani, dan memulihkan akibat risiko yang timbul dari penyimpanan dokumen akta digital. Atas dasar itu, artikel ini bertujuan menganalisis upaya hukum yang dapat dilakukan untuk menekan risiko penyimpanan dokumen jangka panjang pada akta digital notary, baik yang bersifat preventif, represif, maupun yang berkaitan dengan pembaruan regulasi.

Penelitian Terdahulu yang Relevan

No	Penulis/ Tahun	Judul	Tujuan	Metode	Hasil	Kontribusi dan relevansi
1	Edmon Makarim (2020)	Keautentikan Dokumen Elektronik dalam Hukum Pembuktian Indonesia	Menganalisis kedudukan hukum, keautentikan, dan syarat formil/materiil dokumen serta tanda tangan elektronik dalam sistem pembuktian perdata.	Yuridis Normatif	Dokumen elektronik dapat bernilai otentik apabila memenuhi prinsip keutuhan (*integrity*), ketersediaan (*availability*), dan kerahasiaan (*confidentiality*) melalui penerapan infrastruktur kunci publik (PKI) yang tersertifikasi.	Memberikan landasan teoritis mengenai kriteria teknis-yuridis agar akta digital tidak kehilangan sifat keautentikannya saat disimpan dalam jangka panjang.
2	R.A. Emma Nurita (2012)	Cyber Notary: Pemikiran Awal Dalam Konsep Pembuktian Notaris di Indonesia	Menganalisis kesiapan regulasi (*UUJN*) dan implikasi hukum penerapan *cyber notary* terhadap tugas serta kewajiban notaris dalam pembuatan dan penyimpanan akta.	Yuridis Normatif	Praktik *cyber notary* masih mengalami hambatan yuridis karena UUJN masih mengagungkan asas *pada saat yang sama* (penandatanganan fisik secara langsung) dan penyimpanan minuta akta secara fisik.	Menjadi acuan dasar dalam mengidentifikasi kesenjangan hukum (*legal gap*) antara regulasi keanggotaan/keil muan notaris saat ini dengan kebutuhan digitalisasi protokol notaris.
3	Siti Yuniarti & Ahmad M. Ramli (2021)	Pelindungan Data Pribadi dan Keamanan Siber dalam Penyimpanan Dokumen Elektronik	Menelaah risiko kebocoran data dan tanggung jawab hukum penyedia sarana penyimpanan dokumen berbasis elektronik.	Yuridis Normatif dan Yuridis Empiris	Penyimpanan digital tanpa skema proteksi berlapis (enkripsi dan *multi-factor authentication*) berisiko memicu gugatan perdata atas perbuatan melawan hukum (PMH) akibat kegagalan	Relevan sebagai pisau analisis mengenai perlindungan data pribadi dan mitigasi risiko kejahatan siber pada akta digital jangka panjang.

					perlindungan data pribadi.	
4	Lucia B. W. & I Gusti Ngurah Parwata (2022)	Preservasi Digital dan Tantangan Daluarsa Teknis (*Technical Obsolescence*) pada Dokumen Hukum	Mengetahui kendala teknis-hukum dalam preservasi data digital jangka panjang akibat perkembangan format file dan perangkat keras.	Empiris	Media digital memiliki umur teknis terbatas (*format obsolescence*). Tanpa adanya prosedur alih media yang tersertifikasi, risiko hilangnya keutuhan (*integrity*) data sangat tinggi dalam jangka panjang.	Memberikan gambaran empiris mengenai risiko *obsolescence* media digital yang menjadi salah satu latar belakang ditempuhnya upaya hukum preventif.
5	Habib Adjie (2023)	Tanggung Jawab Notaris Terhadap Minuta Akta yang Mengalami Kerusakan dan Kehilangan dalam Era Digital	Menganalisis batas tanggung jawab notaris secara perdata dan administratif apabila terjadi kerusakan atau kerugian pada penyimpanan dokumen digital.	Yuridis Normatif	Notaris wajib menerapkan prinsip kehati-hatian (*duty of care*). Kegagalan melakukan *backup* atau enkripsi dapat dikategorikan sebagai kelalaian (*malpractice*) yang berujung pada gugatan ganti rugi.	Menjadi rujukan utama dalam memformulasikan bentukan upaya hukum represif dan penegakan pertanggungjawab an notaris jika terjadi insiden hilangnya data akta digital.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian hukum normatif-empiris dengan tipe deskriptif-analitis. Sifat deskriptif tampak pada upaya memaparkan secara sistematis ketentuan mengenai kewajiban penyimpanan akta dan protokol notaris, baik dalam bentuk konvensional maupun elektronik. Sifat analitis tampak pada penilaian kritis terhadap kecukupan norma tersebut dalam mengantisipasi risiko yuridis yang timbul dari penyimpanan jangka panjang (Muhammad, 2004). Meskipun demikian, bahan utama penelitian adalah data sekunder, sehingga karakter normatifnya dominan, sedangkan wawancara hanya berfungsi sebagai data pendukung untuk memperkaya pemahaman atas praktik. Pendekatan masalah yang digunakan adalah pendekatan perundang-undangan dan pendekatan konseptual (Marzuki, 2017). Pendekatan perundang-undangan dilakukan dengan menelaah KUHPerdata, UUJN, UU ITE sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024, Peraturan Pemerintah Nomor 71 Tahun 2019, Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, UU PDP, dan Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022. Pendekatan konseptual digunakan untuk mengkaji konsep akta autentik, cyber notary, tanda tangan elektronik, keautentikan, integritas, dan kerahasiaan dokumen, yang sebagian belum diatur tegas dalam peraturan yang berlaku. Sumber data terdiri atas bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa buku, jurnal, dan artikel ilmiah, serta bahan hukum tersier berupa kamus dan ensiklopedia untuk memastikan ketepatan istilah (Soekanto & Mamudji, 2001). Pengumpulan data dilakukan melalui studi kepustakaan dalam tiga tahap, yaitu inventarisasi, seleksi, dan sistematisasi bahan hukum. Pengolahan data dilakukan melalui identifikasi, seleksi, dan klasifikasi (Soekanto, 1986; Ali, 2009). Analisis dilakukan secara kualitatif dan bersifat preskriptif, yakni memberikan penilaian tentang apa yang seharusnya berlaku, bukan sekadar menggambarkan keadaan (Sunggono, 2021). Artikel ini memusatkan pembahasan pada rumusan masalah kedua penelitian, yakni upaya hukum untuk menekan risiko penyimpanan dokumen jangka panjang. Risiko yuridis yang menjadi dasar pembahasan dirangkum secara ringkas pada bagian awal pembahasan agar alur argumentasi tetap utuh.

HASIL PENELITIAN DAN PEMBAHASAN

Peta Risiko sebagai Dasar Perumusan Upaya Hukum

Upaya hukum hanya dapat dirumuskan secara tepat apabila risiko yang hendak ditekan telah dipetakan dengan jelas. Hasil penelitian menunjukkan empat kelompok risiko yuridis. Pertama, ketidakpastian hukum akibat belum adanya norma yang tegas menyamakan akta elektronik dengan akta autentik konvensional. UUJN tetap mensyaratkan pembacaan akta di hadapan penghadap dan saksi serta penyimpanan minuta (Pasal 16 ayat (1) huruf b dan m), sementara Pasal 15 ayat (3) UUJN tidak mengatur bentuk akta elektronik dan Pasal 5 ayat (4) UU ITE hanya menyerahkan penentuannya kepada undang-undang lain. Kedua, hilangnya keautentikan dan integritas dokumen, terutama karena sertifikat elektronik dan algoritma dapat menjadi usang. Ketiga, ketidaktersediaan dokumen akibat bencana, kegagalan sistem, kesalahan manusia, keusangan format, atau serangan siber seperti ransomware. Keempat, pelanggaran kerahasiaan yang melahirkan tanggung jawab berlapis bagi notaris menurut UUJN, KUHPerdata, dan UU PDP. Secara kritis, keempat risiko tersebut tidak berdiri sendiri. Ketidakpastian norma memperbesar dampak tiga risiko lainnya, sebab ketika status hukum suatu berkas digital tidak jelas, setiap gangguan teknis berubah menjadi sengketa tentang nilai pembuktian. Sebaliknya, gangguan teknis yang nyata memperlihatkan kelemahan norma yang abstrak. Dengan demikian, upaya hukum tidak cukup dirancang sebagai kumpulan tindakan teknis, melainkan harus disusun sebagai rangkaian tiga lapis yang saling mengunci: upaya preventif untuk mencegah risiko, upaya represif untuk menangani dan memulihkan akibat apabila risiko terjadi, serta pembaruan regulasi untuk menutup kekosongan norma yang menjadi akar persoalan.

Upaya Hukum Preventif: Mengubah Tindakan Teknis menjadi Pelaksanaan Kewajiban Jabatan

Dalam kerangka teori perlindungan hukum, upaya preventif bertujuan mencegah pelanggaran sebelum kerugian timbul. Titik tolak analisis adalah bahwa langkah preventif dalam penyimpanan akta digital bukan pilihan teknis yang bersifat sukarela, melainkan perwujudan kewajiban hukum yang sudah ada. Notaris wajib menyimpan minuta sebagai bagian dari protokol dan merahasiakan akta (Pasal 16 ayat (1) huruf b dan f UUJN), tetap bertanggung jawab atas akta meskipun protokol telah diserahkan (Pasal 65 UUJN), dan, apabila mengelola sistem elektronik sendiri, dapat dikualifikasikan sebagai penyelenggara sistem elektronik yang wajib menyelenggarakan sistem yang andal dan aman (Pasal 15 UU ITE) serta mampu menampilkan kembali dokumen secara utuh sesuai masa retensi (Pasal 16 ayat (1) UU ITE). Sebagai pengendali data pribadi, notaris juga terikat kewajiban pengamanan menurut Pasal 35 dan Pasal 39 UU PDP. Kelalaian menerapkan langkah pencegahan karenanya dapat dinilai sebagai pelanggaran kewajiban jabatan yang berujung pada sanksi administratif menurut Pasal 85 UUJN dan membuka tuntutan ganti rugi menurut Pasal 1365 dan Pasal 1366 KUHPerdata.

Langkah pertama yang bersifat fundamental adalah menegaskan kedudukan hukum setiap jenis dokumen. Hasil penelitian menunjukkan bahwa hasil pemindaian merupakan reproduksi, bukan minuta, dan Pasal 1888 KUHPerdata menegaskan bahwa kekuatan pembuktian suatu tulisan bergantung pada akta aslinya (Iriantoro & Hardiansyah, 2024). Oleh sebab itu, administrasi penyimpanan harus membedakan secara tegas tiga kategori, yaitu minuta akta asli, hasil alih media, dan salinan elektronik yang diberikan kepada pihak yang berhak. Penandaan status ini bukan formalitas. Ia mencegah anggapan keliru bahwa berkas digital setara dengan minuta, anggapan yang justru menjadi sumber risiko terbesar karena dapat menimbulkan rasa aman semu. Selama hukum positif belum menyamakan keduanya,

notaris tetap wajib memelihara minuta fisik, dan digitalisasi diposisikan sebagai salinan pengamanan serta sarana pencarian dan penelusuran. Langkah kedua adalah verifikasi dan dokumentasi proses alih media. Setiap pemindaian perlu dicatat secara sistematis, mencakup identitas dokumen, nomor akta, nomor repertorium, waktu pelaksanaan, identitas petugas, perangkat yang digunakan, dan hasil verifikasi kesesuaian dengan dokumen sumber (Budhijanto, 2023). Analisis kritisnya adalah bahwa catatan ini merupakan bukti proses. Dalam teori pembuktian, keandalan dokumen elektronik tidak ditentukan oleh keberadaan berkasnya, tetapi oleh kemampuan menunjukkan asal-usul dan keutuhannya. Tanpa catatan proses, hakim tidak memiliki dasar untuk menilai bahwa berkas digital benar-benar berasal dari minuta yang sah, sehingga nilai buktinya melemah justru ketika dibutuhkan.

Langkah ketiga adalah pengamanan teknis berlapis yang dikaitkan dengan kewajiban kerahasiaan. Enkripsi perlu diterapkan dengan pengelolaan kunci yang terpisah dari berkas, pengendalian akses harus berbasis tugas dan kewenangan disertai autentikasi berlapis, dan seluruh aktivitas pengguna harus tercatat dalam log. Apabila notaris memanfaatkan penyedia cloud, tanggung jawab notaris tidak berpindah kepada penyedia. Notaris tetap wajib menilai keandalan penyedia, termasuk lokasi penyimpanan, prosedur pencadangan dan pemulihan, pengelolaan akses administrator, kewajiban pemberitahuan insiden, serta mekanisme pengembalian data ketika layanan berakhir (Solehudin & Djajaputra, 2023; Najib, 2023). Di sinilah perjanjian dengan penyedia layanan berfungsi sebagai instrumen hukum preventif. Klausul tentang kerahasiaan, standar keamanan, dan pembagian tanggung jawab yang disusun sejak awal memperjelas siapa yang menanggung akibat apabila insiden terjadi, sehingga mengurangi ruang sengketa di kemudian hari. Standar ISO/IEC 27001 dapat dijadikan acuan tata kelola keamanan informasi, dan blockchain privat dapat dipertimbangkan untuk mencatat nilai hash atau jejak perubahan dokumen. Namun, keduanya harus diposisikan secara proporsional. ISO/IEC 27001 membantu menjaga kerahasiaan, keutuhan, dan ketersediaan data, tetapi tidak menjadikan dokumen sebagai akta autentik. Blockchain membuat perubahan sulit dilakukan tanpa terdeteksi, tetapi tidak membuktikan kebenaran isi pada saat pertama kali diunggah dan tidak membuktikan kewenangan pihak yang memasukkan data. Dengan kata lain, teknologi-teknologi ini memperkuat bukti pendukung dan keterlacakan, bukan menggantikan notaris, tanda tangan elektronik bersertifikat, ataupun persyaratan formal akta autentik. Pandangan yang menempatkan teknologi sebagai solusi tunggal berisiko menggeser tanggung jawab hukum dari manusia kepada sistem, padahal hukum kenotariatan menempatkan tanggung jawab itu pada notaris.

Langkah keempat berkaitan dengan ketersediaan jangka panjang, yang merupakan inti persoalan penyimpanan permanen. Data perlu dicadangkan pada lebih dari satu media dan lokasi, dan cadangan harus diuji pemulihannya secara berkala karena cadangan yang tidak pernah diuji tidak menjamin pemulihan berhasil. Notaris perlu menyusun rencana pemulihan bencana yang memuat penanggung jawab, urutan pemulihan, prosedur verifikasi pascapemulihan, dan mekanisme pemberian akses kepada penerima protokol. Untuk menghadapi keusangan teknologi, diperlukan pemeriksaan keterbacaan berkas secara periodik serta migrasi format yang menjaga keutuhan dokumen, metadata, dan jejak audit. Khusus untuk tanda tangan elektronik, notaris dapat memanfaatkan layanan preservasi tanda tangan dan penanda waktu elektronik sebagaimana dimungkinkan oleh Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022, dan merencanakan penguatan bukti sebelum sertifikat atau algoritma usang. Perlu dicatat secara kritis bahwa akibat hukum layanan preservasi tersebut terhadap kekuatan pembuktian akta notaris belum diatur. Karena itu, layanan ini baru dapat dipandang sebagai penguat bukti pendukung dan tidak dapat diandalkan sebagai pengganti minuta.

Langkah kelima adalah penataan administratif melalui prosedur operasional baku (SOP), pelatihan, dan serah terima protokol. SOP harus mengatur seluruh siklus dokumen, mulai dari pembuatan, penamaan, penyimpanan, pencadangan, pengaksesan, pemindahan, hingga pemusnahan, termasuk verifikasi identitas, tujuan, dan dasar kewenangan setiap permintaan akses. Pelatihan berkelanjutan bagi notaris dan staf diperlukan karena kesalahan manusia, seperti pengelolaan kata sandi yang lemah dan kerentanan terhadap phishing, kerap menjadi penyebab kebocoran dan kehilangan data. Adapun serah terima protokol digital harus lebih dari sekadar pemindahan folder atau kredensial. Penyerahan perlu disertai daftar dokumen, berita acara, hasil pemeriksaan integritas, nilai hash, format berkas, status sertifikat, metadata penting, dan catatan media penyimpanan, serta penonaktifan akses pihak lama setelah kewenangannya berakhir. Hal ini penting karena Pasal 65 UUJN membuat tanggung jawab notaris pembuat akta tetap melekat meskipun ia tidak lagi menguasai dokumen. Tanpa serah terima yang terverifikasi, terjadi ketimpangan: notaris lama bertanggung jawab atas dokumen yang tidak lagi dikendalikannya, sedangkan notaris penerima memegang dokumen yang keutuhannya belum tentu dapat ia pastikan (Kartika & Herman, 2026; Ma'ruf & Handoko, 2024).

Langkah keenam adalah deteksi dini dan kesiapsiagaan insiden. Deteksi dini dilakukan melalui pencatatan log, pemantauan pola akses yang tidak lazim, pemeriksaan integritas berkala dengan membandingkan nilai hash terhadap nilai awal, serta pengujian keterbacaan dan keberhasilan pencadangan. Pemeriksaan hash sangat penting karena dokumen yang diubah secara diam-diam tidak selalu tampak ketika dibuka. Kesiapsiagaan insiden berarti notaris menyiapkan rencana respons sebelum insiden terjadi, yang memuat penanggung jawab, jalur pelaporan, langkah awal pembatasan dampak seperti pencabutan kredensial, cara mengamankan log dan cadangan, serta daftar kontak pihak yang harus diberi tahu. Kesiapsiagaan ini bersinggungan langsung dengan tenggat hukum yang singkat. Kewajiban memberi tahu kegagalan pelindungan data dalam 3 x 24 jam menurut Pasal 46 UU PDP hanya dapat dipenuhi apabila prosedur, daftar kontak, dan format pemberitahuan telah tersedia sebelum insiden. Dengan demikian, kesiapsiagaan merupakan prasyarat kepatuhan, bukan pelengkap. Terakhir, seluruh langkah preventif harus didokumentasikan, yaitu catatan pelatihan, hasil audit, hasil uji pemulihan, tinjauan log, dan pembaruan SOP. Dokumentasi ini memiliki fungsi ganda. Bagi pengawas, ia memudahkan pemeriksaan oleh Majelis Pengawas. Bagi notaris, ia merupakan bukti bahwa ia telah bertindak dengan kehati-hatian. Dalam sengketa yang didasarkan pada Pasal 1365 atau Pasal 1366 KUHPerdata, unsur kesalahan dan kelalaian akan dinilai dari ada tidaknya langkah pencegahan yang wajar, sehingga dokumentasi yang tertib menjadi pembelaan yang paling kuat.

Upaya Hukum Represif: Menangani Insiden dan Menetapkan Pertanggungjawaban

Perlindungan preventif tidak pernah menghapus kemungkinan terjadinya insiden. Karena itu, teori perlindungan hukum menuntut adanya perlindungan represif, yakni upaya yang ditempuh setelah risiko terwujud untuk membatasi kerugian, memulihkan keadaan, dan menentukan pihak yang bertanggung jawab. Dalam konteks penyimpanan akta digital, upaya represif berjalan melalui tiga jalur yang saling berkaitan, yaitu penanganan insiden dan pengamanan bukti, pemenuhan kewajiban pelaporan, serta penegakan pertanggungjawaban. Jalur pertama adalah penanganan insiden dan pengamanan bukti elektronik. Segera setelah insiden diketahui, notaris perlu membatasi akses, mencabut kredensial yang disalahgunakan, dan mengamankan dokumen, log akses, metadata, nilai hash, berita acara, serta bukti komunikasi. Seluruh unsur tersebut harus diperlakukan sebagai satu kesatuan bukti. Apabila terdapat celah pencatatan, penggunaan akun bersama, atau pemindahan berkas tanpa

prosedur, keandalan dokumen dapat dipersoalkan. Dalam situasi demikian, konsep rantai penguasaan bukti menjadi penting. Setiap perpindahan dokumen, baik dari notaris kepada staf, media penyimpanan, penyedia cloud, maupun penerima protokol, harus dapat ditelusuri melalui cap waktu, pelaku, tujuan, media, dan hasil pemeriksaan integritas. Rantai ini membantu membuktikan bahwa dokumen tidak berubah sejak dibuat atau sejak pemeriksaan terakhir. Dari sudut pandang teori pembuktian, tindakan pascainsiden yang tertib justru menentukan apakah dokumen yang selamat masih dapat diterima sebagai alat bukti yang andal.

Jalur kedua adalah pelaporan dan pemulihan. Apabila insiden melibatkan data pribadi, notaris sebagai pengendali data wajib memberi tahu subjek data dan lembaga berwenang secara tertulis paling lambat 3 x 24 jam sejak kegagalan pelindungan diketahui (Pasal 46 ayat (1) UU PDP). Pada saat yang sama, notaris perlu memulihkan dokumen dari cadangan yang telah teruji, memverifikasi hasil pemulihan, dan mencatat seluruh langkah pemulihan agar perubahan sistem dapat ditelusuri. Dalam hal minuta fisik masih ada, perbandingan antara berkas hasil pemulihan dan minuta menjadi sarana verifikasi yang paling kuat. Hal ini menegaskan mengapa penghapusan minuta fisik setelah digitalisasi tidak dibenarkan, sebab minuta merupakan jangkar yang memungkinkan berkas digital diuji kebenarannya. Sebaliknya, apabila minuta hilang atau rusak, Pasal 1902 KUHPerdata menempatkan salinan sebagai permulaan bukti tertulis yang memerlukan alat bukti lain, dan penilaian akhirnya berada pada hakim. Salinan digital yang disertai catatan proses, nilai hash, dan log yang utuh dapat memperkuat posisi pembuktian tersebut, tetapi tidak mengembalikan kekuatan autentik minuta yang hilang.

Jalur ketiga adalah penegakan pertanggungjawaban, yang secara garis besar berlangsung dalam tiga ranah. Pada ranah administratif, pelanggaran kewajiban jabatan, seperti kewajiban menyimpan minuta, kewajiban merahasiakan akta, dan kewajiban penyerahan protokol, dapat dikenai sanksi menurut Pasal 85 UUJN melalui mekanisme pengawasan oleh Majelis Pengawas. Pada ranah perdata, pihak yang dirugikan dapat menuntut ganti rugi atas dasar perbuatan melawan hukum (Pasal 1365 KUHPerdata) atau kelalaian (Pasal 1366 KUHPerdata) apabila unsur kesalahan, kerugian, dan hubungan sebab akibat terpenuhi, dan subjek data pribadi dapat menggugat berdasarkan UU PDP (Pasal 12). Pada ranah pidana, UU PDP memuat larangan tertentu (Pasal 67) yang membuka kemungkinan pertanggungjawaban pidana, meskipun kajian ini tidak membahasnya secara mendalam. Hal yang patut dikritisi adalah bahwa penentuan pertanggungjawaban pada ranah perdata tidak bisa dilakukan secara mekanis. Kebocoran data tidak otomatis berarti notaris bersalah. Penilaian harus mempertimbangkan sumber insiden, bentuk pengendalian yang telah diterapkan, tingkat kepatuhan terhadap prosedur, peran notaris sebagai pengendali atau pihak yang dibantu penyedia layanan, serta hubungan langsung antara kelalaian dan kerugian (Najib, 2023). Jika penyalahgunaan terjadi karena kredensial tidak diamankan, akses tidak dibatasi, atau sertifikat tidak segera dicabut setelah diketahui berisiko, kelalaian itu menjadi dasar pertanggung jawaban pihak yang wajib mengamankan. Sebaliknya, jika insiden bersumber dari kelemahan penyedia layanan atau serangan pihak ketiga, pembagian tanggung jawab harus dianalisis berdasarkan perjanjian, kewajiban hukum, dan langkah pencegahan masing-masing pihak. Dengan demikian, tampak keterkaitan antara upaya preventif dan represif: notaris yang telah menjalankan dan mendokumentasikan langkah preventif berada pada posisi yang jauh lebih kuat ketika pertanggungjawabannya diperiksa, sedangkan notaris yang tidak memiliki catatan apa pun akan kesulitan membuktikan ketiadaan kelalaian.

Persoalan khusus muncul setelah jabatan notaris berakhir. Penyerahan protokol secara hukum, yang dibuktikan dengan berita acara menurut Pasal 63 UUJN, dapat berbeda dari

penyerahan secara teknis, karena akun, kunci, dan cadangan data masih mungkin dikuasai pihak lama atau penyedia layanan. Dalam kondisi ini, akta tetap dapat beredar atau digunakan tanpa kewenangan, sementara tanggung jawab menurut Pasal 65 UUJN tetap melekat pada notaris pembuat akta (Kartika & Herman, 2026). Upaya represif yang relevan mencakup pencabutan akses yang tidak lagi sah, verifikasi kewenangan penerima, serta pemeriksaan oleh Majelis Pengawas atas dugaan penyalahgunaan. Namun, efektivitasnya terbatas karena pengawasan saat ini masih bertumpu pada tindakan masing-masing notaris. Keterbatasan inilah yang mengarahkan pembahasan pada kebutuhan pergeseran ke model kelembagaan.

Pembaruan Regulasi dan Penguatan Pengawasan Kelembagaan

Upaya preventif dan represif di tingkat kantor notaris pada akhirnya dibatasi oleh kenyataan bahwa kerangka norma dasarnya belum jelas dan seragam. Dari sudut teori kepastian hukum, kondisi ini bermasalah, sebab notaris diminta memenuhi standar kehati-hatian tanpa kepastian tentang standar yang dimaksud. Boentoro dan Hartanto (2025) menganjurkan pembentukan dan pembaruan peraturan yang mempertimbangkan landasan politis, yuridis, dan filosofis. Anjuran itu sejalan dengan wacana di lingkungan Ikatan Notaris Indonesia mengenai pembuatan akta autentik secara hibrida melalui perubahan Pasal 1, Pasal 15, dan Pasal 16 UUJN. Pembaruan yang diperlukan setidaknya menyangkut lima hal. Pertama, norma perlu membedakan secara tegas tiga jenis dokumen, yaitu minuta yang sejak awal dibuat secara elektronik, dokumen hasil alih media dari minuta fisik, dan salinan elektronik, karena masing-masing memiliki proses pembentukan, kedudukan hukum, dan kekuatan pembuktian yang berbeda. Kedua, regulasi perlu menetapkan standar keamanan minimum yang wajib diterapkan notaris dan penyedia layanan teknologi informasi, mencakup pengendalian akses, enkripsi, autentikasi, pencatatan aktivitas, pencadangan di beberapa lokasi, pengujian pemulihan, audit berkala, dan kewajiban pelaporan insiden. Ketiga, perlu diatur pembagian tanggung jawab antara notaris, notaris penerima, lembaga pengawas, penyelenggara sertifikasi elektronik, dan penyedia layanan penyimpanan. Keempat, UUJN perlu dikaitkan dengan rezim sertifikasi elektronik, termasuk layanan preservasi tanda tangan elektronik, serta dengan ketentuan UU Kearsipan tentang arsip elektronik dan alih media. Kelima, perlu ditentukan pihak yang bertanggung jawab menjaga keterbacaan dan kemampuan verifikasi berkas digital pada protokol yang telah berumur dua puluh lima tahun atau lebih.

Poin kelima layak dibahas lebih jauh karena memperlihatkan celah yang nyata. Pasal 63 ayat (5) UUJN mengatur bahwa protokol yang berumur dua puluh lima tahun atau lebih pada saat penyerahan diserahkan oleh notaris penerima kepada Majelis Pengawas Daerah, dan Pasal 70 huruf e memberi kewenangan kepada Majelis Pengawas Daerah untuk menentukan tempat penyimpanannya. Apabila protokol itu berupa atau dilengkapi berkas digital, Majelis Pengawas Daerah akan menerima dokumen dengan sertifikat, format, dan algoritma yang telah berumur dua puluh lima tahun, padahal UUJN tidak menyebutkan siapa yang wajib memelihara keterbacaan dan keterverifikasiannya (Jagadhita & Bagiastra, 2025). Tanpa norma yang menetapkan penanggung jawab dan sumber daya, kewajiban penyimpanan permanen berpotensi menjadi kewajiban yang tidak dapat dipenuhi oleh siapa pun. Selain itu, Pasal 16 UU ITE mensyaratkan sistem elektronik mampu menampilkan kembali dokumen sesuai masa retensi, sementara UUJN tidak menetapkan batas akhir penyimpanan protokol, sehingga kewajiban tersebut harus dipenuhi tanpa kerangka waktu yang pasti. Ketidakselarasan ini merupakan contoh konkret disharmoni horizontal antara UUJN dan UU ITE yang perlu diselesaikan melalui pembaruan norma, bukan sekadar penafsiran.

Hasil wawancara dengan beberapa notaris di Bandar lampung pada Sabtu, 24 Oktober 2026 pukul 13.00 WIB menyatakan bahwa pengelolalaan protokol jangka panjang tidak dapat

bergantung pada kehati-hatian dan ketelitian masing-masing notaris, terutama bagi notaris dengan kantor bersekala kecil yang tidak selalu memiliki sumber daya untuk membangun infrastruktur keamanan yang memadai. Para narasumber memandang perlunya pergeseran dari model pertanggungjawaban personal ke model institusional yang didukung system digital terintegrasi, sebab beban kepatuhan yang sama bagi seluruh notaris tanpa dukungan kelembagaan berpotensi melahirkan kepatuhan yang bersifat formal. Karena itu, lembaga yang melibatkan Majelis Pengawas dan institusi pengelola protokol perlu diberi kewenangan untuk memantau status protokol, mengesahkan pengalihan hak akses, melakukan audit berkala, dan menindaklanjuti laporan dugaan penyalahgunaan (Kartika & Herman, 2026). Sistem terintegrasi yang mencatat siapa menguasai protokol, kapan akses dilakukan, dan tindakan apa yang dilakukan terhadap dokumen akan mengurangi kemungkinan penggunaan dokumen secara tersembunyi dan mempercepat identifikasi penyalahgunaan. Pembaruan regulasi juga harus tetap berpusat pada tujuan hukum kenotariatan, yaitu kepastian hukum, ketertiban, dan perlindungan para pihak. Pengaturan dokumen digital tidak boleh hanya menekankan efisiensi teknologi. Hal ini sejalan dengan temuan sejumlah penelitian bahwa digitalisasi harus berpegang pada prinsip keautentikan, legalitas, keamanan data, dan kepastian hukum (Ulandari, 2026; Herliyani dkk., 2025; Hasan dkk., 2026). Penerapan cyber notary yang berhasil memerlukan keterpaduan dasar hukum, standar teknis, SOP, peningkatan kompetensi, mekanisme pengawasan, dan prosedur pertanggungjawaban. SOP memberi pedoman operasional di tingkat kantor, pelatihan meningkatkan kemampuan pengguna, sedangkan regulasi memberi kepastian tentang kewenangan, status dokumen, dan pembagian tanggung jawab.

Sintesis: Ketahanan Hukum Penyimpanan Akta Digital

Apabila ketiga lapis upaya tersebut dipandang sebagai satu kesatuan, tampak bahwa upaya hukum dalam penyimpanan akta digital bertumpu pada satu gagasan inti, yaitu menjaga agar dokumen tetap dapat membuktikan dirinya sendiri sepanjang waktu. Upaya preventif menjaga kemampuan itu pada saat ini, upaya represif memulihkannya ketika terancam, dan pembaruan regulasi menjamin bahwa kemampuan tersebut memiliki landasan hukum yang pasti di masa depan. Selama landasan itu belum tersedia, sikap yang paling dapat dipertanggungjawabkan adalah menempatkan penyimpanan elektronik sebagai instrumen mitigasi dan pendukung, dengan minuta fisik sebagai dokumen utama. Sikap ini tidak menolak digitalisasi. Sikap ini justru menyiapkan tata kelola agar apabila kelak hukum memberi kekuatan pembuktian yang lebih luas kepada akta elektronik, notaris telah memiliki rekam jejak pengelolaan yang dapat diverifikasi.

KESIMPULAN

Penyimpanan dokumen jangka panjang pada akta digital notary menghadapi risiko yuridis berupa ketidakpastian kedudukan akta elektronik, hilangnya keautentikan dan integritas dokumen, ketidaktersediaan dokumen, serta pelanggaran kerahasiaan data pribadi. Risiko-risiko ini saling memperkuat dan bersumber dari ketegangan antara kewajiban penyimpanan permanen menurut UUJN dan umur teknis media digital, serta dari belum adanya norma yang tegas menyamakan akta elektronik dengan akta autentik konvensional. Upaya hukum untuk menekan risiko tersebut bersifat berlapis. Upaya preventif meliputi penegasan kedudukan tiga jenis dokumen, verifikasi dan dokumentasi alih media, enkripsi dan pengendalian akses, pencadangan multilokasi disertai pengujian pemulihan, preservasi tanda tangan dan migrasi format, SOP, pelatihan, serah terima protokol yang terverifikasi, deteksi dini, serta kesiapsiagaan insiden. Langkah-langkah tersebut merupakan perwujudan kewajiban

jabatan notaris menurut UUJN, UU ITE, dan UU PDP, sehingga bukan pilihan teknis semata. Upaya represif mencakup pengamanan bukti elektronik dengan rantai penguasaan, pembatasan akses, pelaporan kegagalan pelindungan data dalam 3 x 24 jam, pemulihan dokumen, serta penegakan pertanggungjawaban administratif dan perdata sesuai penyebab dan tingkat kesalahan. Kedua upaya itu perlu ditopang pembaruan regulasi yang membedakan jenis dokumen, menetapkan standar keamanan minimum, membagi tanggung jawab, menyelaraskan UUJN dengan rezim sertifikasi elektronik dan kearsipan, serta menentukan penanggung jawab keterbacaan protokol berumur dua puluh lima tahun atau lebih. Selama belum ada pengaturan yang tegas, hasil digitalisasi tidak dapat menggantikan minuta akta asli, dan penyimpanan elektronik perlu diposisikan sebagai sarana pendukung pengamanan, pengelolaan, pencarian, dan penelusuran dokumen.

Kebaruan (novelty) penelitian ini terletak pada pengembangan kerangka perlindungan hukum berlapis terhadap penyimpanan jangka panjang dokumen kenotariatan dalam ekosistem digital dengan mengintegrasikan dimensi keautentikan akta, keberlanjutan preservasi elektronik, keamanan informasi, dan pertanggungjawaban hukum notaris. Berbeda dari kajian cyber notary yang umumnya berfokus pada keabsahan akta elektronik, kewenangan notaris dalam pemanfaatan teknologi informasi, atau aspek keamanan sistem digital secara terpisah, penelitian ini menempatkan kesenjangan antara kewajiban penyimpanan protokol notaris lintas generasi dan keterbatasan teknis media penyimpanan digital sebagai persoalan hukum utama. Kontribusi konseptual penelitian diwujudkan melalui integrasi upaya preventif dan represif yang mencakup verifikasi alih media, preservasi tanda tangan elektronik, enkripsi, pencadangan multilokasi, pengendalian akses, pengamanan bukti elektronik, pemulihan dokumen, serta mekanisme pertanggungjawaban administratif dan perdata. Selain itu, penelitian ini menegaskan pentingnya pembedaan antara digitalisasi dokumen sebagai sarana preservasi dan pengakuan dokumen digital sebagai akta autentik, sehingga pemanfaatan teknologi tidak secara otomatis mengubah kedudukan hukum minuta akta asli. Dengan demikian, penelitian ini menawarkan kerangka perlindungan hukum dan tata kelola preservasi digital notaris yang menghubungkan kepastian hukum, integritas dokumen, kerahasiaan data, dan keberlanjutan penyimpanan protokol sebagai dasar pengembangan regulasi cyber notary di Indonesia.

DAFTAR PUSTAKA

Abady, A. R. P., & Rahayu, M. I. F. (2023). Penyuluhan hukum pembuatan akta oleh notaris berdasarkan Undang-Undang Nomor 2 Tahun 2014 tentang Jabatan Notaris. Journal on Education, 5(2).

Adjie, H. (2008). Hukum notaris Indonesia: Tafsir tematik terhadap UU No. 30 Tahun 2004 tentang Jabatan Notaris. Bandung: Refika Aditama.

Ali, Z. (2009). Metode penelitian hukum. Jakarta: Sinar Grafika.

Anggriani, S., Firdaus, R. S., & Suherlan, W. A. S. (2023). Analisis penyimpanan protokol notaris secara elektronik. Notaire, 6(3).

Boentoro, R., & Hartanto, S. (2025). Penerapan cyber notary dalam penyimpanan minuta akta notaris sebagai bagian dari protokol notaris. Notary Journal, 5(1).

Borman, M. S. (2019). Kedudukan notaris sebagai pejabat umum dalam perspektif Undang-Undang Jabatan Notaris. Jurnal Hukum dan Kenotariatan, 3(1).

Budhijanto, D. (2023). Hukum pelindungan data pribadi di Indonesia: Cyberlaw & cybersecurity. Bandung: Refika Aditama.

Ghazala, M., & Erni, D. (2022). Urgensi pengaturan penyimpanan protokol notaris sebagai arsip negara dengan sistem elektronik di Indonesia. Kertha Semaya: Journal Ilmu Hukum, 10(3).

Hasan, N., Nawi, S., Khalid, H., & Abbas, I. (2026). The essence of a notary's responsibility in the preparation of cyber-notary–based authentic deeds. Journal of Cultural Analysis and Social Change, 11(1).

Herliyani, E., Sutrisno, E., & Astawa, I. G. P. (2025). Digitalization of notary services towards legal certainty for the parties in making deeds. Veredas do Direito, 22(6).

Iriantoro, A., & Hardiansyah, B. S. (2024). Electronic storage of notary protocols based on a cloud computing system in the cyber notary concept. Jurnal Hukum Prasada, 11(2).

Jagadhita, I. D. M. A., & Bagiastra, I. N. (2025). Urgensi regulasi penyimpanan protokol notaris pasca 25 tahun dalam rangka reformasi hukum kenotariatan di Indonesia. Acta Comitas: Jurnal Hukum Kenotariatan, 10(2).

Kartika, & Herman. (2026). Legal accountability for the misuse of post-death notarial deeds in the digital notarial administration system. Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi, 3(3).

Ma'ruf, M. A., & Handoko, W. (2024). Tanggung jawab notaris terhadap peralihan protokol notaris yang diserahkan kepadanya. Notarius, 16(3).

Maharani, Y. Z. Z., Khoidin, & Tektona, R. I. (2024). Tanggung jawab notaris terhadap pembuatan akta otentik melalui sistem elektronik. Aktivisme: Jurnal Ilmu Pendidikan, Politik dan Sosial Indonesia, 2(1).

Makarim, E. (2013). Notaris dan transaksi elektronik: Kajian hukum tentang cybernotary di Indonesia. Jakarta: RajaGrafindo Persada.

Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Jakarta: Kencana.

Mertokusumo, S. (2020). Mengenal hukum: Suatu pengantar (Cet. ke-2). Yogyakarta: Cahaya Atma Pustaka.

Muhammad, A. (2004). Hukum dan penelitian hukum. Bandung: Citra Aditya Bakti.

Najib, A. (2023). Perlindungan hukum keamanan data cyber notary berdasarkan Undang-Undang Pelindungan Data Pribadi. Acta Diurnal, 7(1).

Ngadino. (2021). Tanggung jawab notaris terhadap penyimpanan elektronik protokol notaris. Jurnal Pembaruan Hukum, 8(1).

Nurita. (2012). Cyber notary: Pemahaman awal dalam konsep pemikiran. Bandung: Refika Aditama.

Paramita, S. (2023). Legalization of cyber notary-based notary deeds as authentic deeds. Authentica, 6(1).

Rizkianto, K., Rahayu, K., & Mukhidin. (2022). Cyber notary: Kepastian hukum penyimpanan dokumen notaris. Diktum, 10(2).

Rosadi, S. D. (2023). Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022). Jakarta: Sinar Grafika.

Soekanto, S. (1986). Pengantar penelitian hukum. Jakarta: UI Press.

Soekanto, S., & Mamudji, S. (2001). Penelitian hukum normatif: Suatu tinjauan singkat. Jakarta: RajaGrafindo Persada.

Solehudin, D., & Djajaputra, G. (2023). Penyimpanan protokol notaris pada cloud storage dalam konsep cyber notary. Jurnal Sosial dan Teknologi, 3(1).

Sona, M. N. (2023). Penerapan cyber notary di Indonesia dan kedudukan hukum akta notaris yang berbasis cyber notary. Officium Notarium, 2(3).

Sunggono, B. (2021). Metodologi penelitian hukum (Cet. ke-14). Jakarta: RajaGrafindo Persada.

Sya'roni, M. (2021). Transformasi digital dalam praktik kenotariatan di Indonesia. Semarang: UNDIP Press.

Ulandari, A. (2026). Transformasi digital dalam kenotariatan: Validitas akta elektronik dan tanggung jawab notaris di era e-government. Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora, 3(1).