

Perlindungan Hukum terhadap para Penghadap dalam Penggunaan Identitas Digital pada Cyber Notary

Yessi Samahita¹, Yos Johan Utama²

¹⁻² Fakultas Hukum, Universitas Diponegoro Semarang, Indonesia

Email: samahitayessi0@gmail.com¹, yosjohanutama@yahoo.com²

*Penulis Korespondensi: samahitayessi0@gmail.com

Abstract. Digital transformation in notarial practice has encouraged the development of the cyber notary concept, including the use of digital identity in identifying and verifying appearers. However, such mechanisms raise legal issues concerning identity authenticity, the validity of electronic appearance, personal data security, and liability in cases of identity misuse or electronic system failure. This study aims to analyze legal protection for appearers in the use of digital identity within cyber notary practices and to formulate a legal protection framework capable of ensuring legal certainty. This research employs a normative legal method using statutory, conceptual, and analytical approaches. The findings indicate that the regulation of cyber notary in Indonesia has not yet comprehensively integrated notarial law, electronic transaction law, and personal data protection. The required legal protection consists of preventive measures through multi-layer authentication, the notary's precautionary principle, data security, and audit trails, as well as repressive protection through clear liability and legal remedy mechanisms. Regulatory reconstruction is therefore necessary to establish reliable digital identity verification standards and ensure the authenticity, security, and legal protection of appearers in electronic notarial services.

Keywords: *Appearers; Cyber Notary; Digital Identity; Legal Protection; Notary.*

Abstrak. Transformasi digital dalam praktik kenotariatan mendorong perkembangan konsep *cyber notary*, termasuk penggunaan identitas digital dalam proses pengenalan dan verifikasi para penghadap. Namun, mekanisme tersebut menimbulkan persoalan hukum mengenai autentisitas identitas, keabsahan proses menghadap, keamanan data pribadi, serta tanggung jawab ketika terjadi penyalahgunaan identitas atau kegagalan sistem elektronik. Penelitian ini bertujuan menganalisis perlindungan hukum terhadap para penghadap dalam penggunaan identitas digital pada *cyber notary* serta merumuskan konstruksi perlindungan yang memberikan kepastian hukum. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan analitis. Hasil penelitian menunjukkan bahwa pengaturan *cyber notary* di Indonesia belum mengintegrasikan secara komprehensif hukum kenotariatan, transaksi elektronik, dan perlindungan data pribadi. Perlindungan hukum yang diperlukan mencakup perlindungan preventif melalui autentikasi berlapis, prinsip kehati-hatian, keamanan data, dan *audit trail*, serta perlindungan represif melalui mekanisme pertanggungjawaban dan pemulihan kerugian. Rekonstruksi regulasi diperlukan agar identitas digital memiliki standar verifikasi yang jelas dan dapat menjamin autentisitas serta keamanan para penghadap.

Kata kunci: Cyber Notary; Identitas Digital; Notaris; Penghadap; Perlindungan Hukum.

1. LATAR BELAKANG

Transformasi digital telah memengaruhi hampir seluruh bentuk pelayanan hukum, termasuk praktik kenotariatan yang selama ini bertumpu pada pertemuan fisik, pemeriksaan identitas secara langsung, dan penandatanganan akta di hadapan notaris. Perkembangan konsep *cyber notary* membuka kemungkinan pemanfaatan teknologi elektronik dalam pelaksanaan sebagian fungsi kenotariatan, sehingga hubungan antara notaris dan para penghadap mulai bergeser dari mekanisme konvensional menuju mekanisme berbasis sistem elektronik. Perubahan tersebut menawarkan efisiensi, kecepatan pelayanan, dan kemudahan akses, tetapi pada saat yang sama menimbulkan persoalan mengenai kepastian hukum, autentisitas akta, serta perlindungan terhadap pihak yang terlibat dalam proses kenotariatan. Rihhadatul'aisy,

Mayana, dan Ramli (2026) menempatkan *cyber notary* sebagai bentuk pembaruan hukum yang memiliki urgensi sekaligus menghadapi tantangan implementasi, sedangkan Dewi dan Puspawati (2025) menunjukkan bahwa perkembangan paradigma *cyber notary* masih dibayangi problematika pengaturan dalam sistem hukum Indonesia.

Salah satu persoalan fundamental dalam penerapan *cyber notary* adalah cara memastikan identitas para penghadap ketika proses pengenalan tidak lagi sepenuhnya dilakukan melalui kehadiran fisik. Dalam praktik konvensional, identitas penghadap berkaitan langsung dengan kemampuan notaris memastikan bahwa orang yang menyatakan kehendak dalam suatu akta benar-benar merupakan subjek hukum yang identitasnya sesuai dengan dokumen yang diperlihatkan. Ketika mekanisme tersebut dialihkan ke lingkungan digital, identitas elektronik atau identitas digital menjadi instrumen penting untuk melakukan autentikasi dan verifikasi terhadap penghadap, namun sekaligus menghadirkan risiko pemalsuan identitas, penggunaan data tanpa hak, pengambilalihan akun, manipulasi informasi elektronik, dan kegagalan sistem verifikasi. Persoalan ini menjadi semakin relevan karena Najib (2023) menegaskan pentingnya keamanan data dalam penyelenggaraan *cyber notary* berdasarkan rezim perlindungan data pribadi, sementara Nugraha (2025) menempatkan perlindungan hukum para pihak sebagai persoalan utama dalam pembuatan akta notaris secara elektronik.

Penggunaan identitas digital tidak hanya berhubungan dengan aspek teknis autentikasi, tetapi juga menyangkut perlindungan terhadap hak-hak hukum para penghadap. Data identitas yang digunakan dalam proses kenotariatan dapat mencakup informasi personal yang memiliki nilai hukum dan harus dijamin kerahasiaan, keakuratan, keamanan, serta penggunaannya sesuai tujuan. Apabila identitas digital seseorang digunakan secara tidak sah atau diverifikasi secara tidak memadai, maka akibatnya tidak berhenti pada kebocoran data pribadi, tetapi dapat memengaruhi keabsahan pernyataan kehendak, kedudukan para pihak, kekuatan pembuktian akta, bahkan menimbulkan kerugian keperdataan. Karena itu, perlindungan para penghadap harus diletakkan bukan sekadar sebagai persoalan keamanan siber, melainkan sebagai bagian integral dari jaminan kepastian hukum dalam hubungan kenotariatan sebagaimana berkaitan dengan pembentukan akta elektronik yang dibahas oleh Eli dan Rasji (2025) serta kedudukan hukum akta *cyber notary* yang dikaji Faulina, Barkatullah, dan Gozali (2022).

Permasalahan tersebut menjadi lebih kompleks karena kerangka hukum kenotariatan Indonesia pada dasarnya masih dibangun melalui paradigma pembuatan akta yang mengutamakan kehadiran para pihak di hadapan notaris. Sementara itu, perkembangan teknologi menuntut pengakuan yang lebih jelas terhadap proses identifikasi, verifikasi

kehendak, penandatanganan, penyimpanan, dan pembuktian secara elektronik. Kinasih (2024) menunjukkan adanya persoalan kepastian hukum bagi notaris dalam penerapan *cyber notary* pada proses *verlijden* akta secara digital, sedangkan Iwaldo (2026) menyoroti kepastian hukum pembuatan akta autentik elektronik di Indonesia. Kondisi tersebut menunjukkan adanya ketegangan normatif antara kebutuhan modernisasi pelayanan kenotariatan dan konstruksi formal hukum kenotariatan, yang pada akhirnya juga menimbulkan ketidakjelasan mengenai standar perlindungan yang harus diberikan kepada penghadap dalam penggunaan identitas digital.

Aspek perlindungan hukum semakin penting karena kedudukan para penghadap berbeda dengan kedudukan notaris sebagai pejabat umum. Notaris dibebani kewajiban profesional dan prinsip kehati-hatian dalam memastikan kebenaran formal identitas dan kehendak pihak yang menghadap, sedangkan para penghadap pada dasarnya mempercayakan proses autentikasi dan dokumentasi perbuatan hukumnya kepada mekanisme kenotariatan. Pramudya, Wiratama, Kumalasari, dan Ali (2026) menggarisbawahi pentingnya prinsip kehati-hatian notaris sekaligus mengkritisi kesiapan regulasi kenotariatan dalam penerapan *cyber notary*. Di sisi lain, Wulandari, Hidayati, dan Ayu (2026) memusatkan perhatian pada perlindungan hukum terhadap notaris dalam pembuatan akta menggunakan *cyber notary*, sehingga muncul kebutuhan untuk menempatkan para penghadap sebagai subjek perlindungan yang berdiri sendiri, khususnya ketika kerugian timbul akibat kesalahan autentikasi identitas digital atau kelemahan sistem elektronik.

Ketidakjelasan regulasi juga dapat menyebabkan distribusi tanggung jawab hukum menjadi kabur ketika terjadi penyalahgunaan identitas digital dalam proses *cyber notary*. Persoalan mendasar yang kemudian muncul ialah siapa yang bertanggung jawab apabila seseorang berhasil menghadap secara elektronik menggunakan identitas pihak lain, apabila sistem verifikasi elektronik gagal mendeteksi ketidaksesuaian identitas, atau apabila data identitas penghadap bocor dan digunakan untuk melakukan perbuatan hukum tanpa persetujuannya. Rekonstruksi regulasi akta elektronik diperlukan agar terdapat batas yang jelas antara tanggung jawab notaris, penyelenggara sistem elektronik, penyedia identitas digital, dan para pihak yang melakukan perbuatan hukum. Riviyusnita dan Utomo (2026) menekankan perlunya rekonstruksi pengaturan akta elektronik notaris menuju kepastian hukum penyelenggaraan *cyber notary*, sedangkan Damayanti, Falah, Kumalasari, dan Ali (2026) menunjukkan pentingnya harmonisasi regulasi untuk menegaskan legitimasi akta *cyber notary* di Indonesia.

Kajian-kajian terdahulu telah membahas *cyber notary* dari perspektif kedudukan akta elektronik, kekuatan akta autentik elektronik, perlindungan data, kepastian hukum, prinsip kehati-hatian notaris, dan harmonisasi regulasi. Namun, berdasarkan fokus penelitian-penelitian tersebut, masih terdapat ruang kajian yang lebih spesifik mengenai perlindungan hukum terhadap para penghadap dalam penggunaan identitas digital sebagai tahapan awal yang menentukan validitas proses kenotariatan elektronik. Nugraha (2025) memang membahas perlindungan hukum para pihak dalam akta notaris elektronik dan Najib (2023) mengkaji keamanan data *cyber notary*, tetapi isu perlindungan penghadap terkait autentikasi identitas digital memerlukan analisis yang menghubungkan secara langsung norma kenotariatan, perlindungan data pribadi, keamanan sistem elektronik, serta konsekuensi hukum apabila proses identifikasi tersebut gagal. Dengan demikian, penelitian ini memiliki posisi yang berbeda karena tidak hanya mempertanyakan legalitas *cyber notary*, melainkan memusatkan analisis pada mekanisme hukum yang dapat menjamin bahwa orang yang menggunakan identitas digital sebagai penghadap adalah subjek hukum yang benar serta memperoleh perlindungan apabila identitasnya disalahgunakan.

Atas dasar persoalan tersebut, penelitian mengenai “Perlindungan Hukum terhadap Para Penghadap dalam Penggunaan Identitas Digital pada Cyber Notary” memiliki urgensi teoretis dan praktis. Secara teoretis, penelitian ini diperlukan untuk mengembangkan konstruksi perlindungan hukum dalam hukum kenotariatan digital dengan mengintegrasikan prinsip kepastian hukum, kehati-hatian notaris, autentikasi identitas, perlindungan data pribadi, dan keabsahan perbuatan hukum elektronik, sejalan dengan tuntutan pembaruan hukum *cyber notary* yang dikemukakan Rihhadatul'aisy et al. (2026) serta kebutuhan penguatan legitimasi regulasi sebagaimana dibahas Damayanti et al. (2026). Secara praktis, penelitian ini diharapkan dapat merumuskan bentuk perlindungan preventif melalui standar autentikasi dan verifikasi identitas digital serta perlindungan represif melalui kejelasan mekanisme pertanggungjawaban dan pemulihan apabila terjadi penyalahgunaan identitas. Dengan demikian, penelitian ini bertujuan menganalisis konstruksi perlindungan hukum bagi para penghadap dalam penggunaan identitas digital pada *cyber notary* serta merumuskan pengaturan yang mampu memberikan kepastian, keamanan, dan perlindungan hukum tanpa menghambat perkembangan digitalisasi pelayanan kenotariatan di Indonesia.

2. KAJIAN TEORITIS

Teori Perlindungan Hukum

Teori perlindungan hukum digunakan untuk menjelaskan bagaimana hukum memberikan jaminan terhadap hak dan kepentingan para penghadap dalam penggunaan identitas digital pada proses *cyber notary*. Perlindungan tersebut dapat diwujudkan dalam bentuk preventif melalui pengaturan mengenai verifikasi identitas, keamanan data pribadi, prinsip kehati-hatian notaris, serta pembatasan akses terhadap informasi pribadi, dan dalam bentuk represif melalui mekanisme pertanggungjawaban, penyelesaian sengketa, serta pemulihan kerugian apabila terjadi penyalahgunaan identitas. Dalam konteks kenotariatan elektronik, perlindungan hukum diperlukan karena penggunaan teknologi dapat menimbulkan risiko berupa pencurian identitas, manipulasi data, akses tanpa hak, maupun kegagalan autentikasi yang berpotensi merugikan para penghadap. Nugraha (2025) menegaskan pentingnya perlindungan hukum terhadap para pihak dalam pembuatan akta notaris secara elektronik, sedangkan Najib (2023) menunjukkan bahwa keamanan dan perlindungan data pribadi merupakan bagian penting dari perlindungan hukum dalam penyelenggaraan *cyber notary*.

Teori Kepastian Hukum

Teori kepastian hukum digunakan untuk menilai sejauh mana pengaturan *cyber notary* mampu memberikan kejelasan mengenai kedudukan identitas digital, proses menghadap secara elektronik, autentikasi para pihak, dan akibat hukum dari akta yang dibuat dengan menggunakan teknologi digital. Kepastian hukum mensyaratkan adanya norma yang jelas, konsisten, dapat diterapkan, dan mampu memberikan prediktabilitas terhadap hak serta kewajiban setiap pihak yang terlibat dalam suatu hubungan hukum. Dalam praktik *cyber notary*, persoalan muncul karena perkembangan teknologi belum sepenuhnya diikuti oleh pengaturan kenotariatan yang secara tegas mengatur prosedur pengenalan dan verifikasi penghadap secara digital. Iwaldo (2026) mengemukakan bahwa kepastian hukum masih menjadi persoalan utama dalam pembuatan akta autentik elektronik di Indonesia, sedangkan Kinasih (2024) menyoroti ketidakpastian dalam penerapan *cyber notary* pada proses *verlijden* akta secara digital. Oleh karena itu, teori kepastian hukum menjadi dasar untuk menguji apakah regulasi yang berlaku telah mampu menjamin identitas penghadap dan keabsahan tindakan notaris dalam lingkungan elektronik.

Konsep Cyber Notary dan Identitas Digital

Konsep *cyber notary* merupakan pengembangan fungsi kenotariatan melalui pemanfaatan teknologi informasi dalam sebagian atau seluruh tahapan pelayanan notaris, termasuk komunikasi dengan para pihak, verifikasi identitas, penandatanganan, pengelolaan dokumen, dan penyimpanan data elektronik. Dalam penelitian ini, identitas digital dipahami sebagai data atau kredensial elektronik yang digunakan untuk mengidentifikasi dan mengautentikasi seseorang dalam proses kenotariatan berbasis teknologi, sehingga keberadaannya harus mampu menghubungkan secara meyakinkan antara identitas hukum, orang yang menghadap, dan kehendak yang dinyatakannya. Rihhadatul'aisy, Mayana, dan Ramli (2026) menempatkan *cyber notary* sebagai bentuk pembaruan hukum yang penting tetapi masih menghadapi persoalan regulasi dan implementasi, sementara Riviyusnita dan Utomo (2026) menekankan perlunya rekonstruksi pengaturan akta elektronik untuk mencapai kepastian hukum. Sejalan dengan itu, Pramudya et al. (2026) menegaskan pentingnya prinsip kehati-hatian dalam pelaksanaan *cyber notary*, sehingga penggunaan identitas digital harus disertai mekanisme autentikasi yang andal agar modernisasi pelayanan notaris tidak mengurangi keamanan, autentisitas, dan perlindungan hukum terhadap para penghadap.

3. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan menempatkan hukum sebagai norma yang mengatur perlindungan para penghadap dalam penggunaan identitas digital pada penyelenggaraan *cyber notary*. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan analitis (*analytical approach*). Pendekatan perundang-undangan digunakan untuk menganalisis keterkaitan antara pengaturan jabatan notaris, transaksi dan sistem elektronik, tanda tangan elektronik, identitas digital, serta perlindungan data pribadi dalam konteks pelayanan kenotariatan berbasis elektronik. Pendekatan konseptual digunakan untuk mengkaji konsep perlindungan hukum, kepastian hukum, prinsip kehati-hatian notaris, autentikasi identitas, dan *cyber notary*, sedangkan pendekatan analitis digunakan untuk mengidentifikasi inkonsistensi, kekosongan, serta kebutuhan harmonisasi norma yang berkaitan dengan perlindungan penghadap dalam proses kenotariatan digital.

Bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan jabatan notaris, informasi dan transaksi elektronik, perlindungan data pribadi, penyelenggaraan sistem elektronik, serta ketentuan lain yang relevan dengan identitas digital

dan pembuatan akta notaris, sedangkan bahan hukum sekunder berupa artikel jurnal, hasil penelitian, buku, dan literatur ilmiah mengenai *cyber notary*, akta elektronik, keamanan data, dan perlindungan hukum para pihak. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dan penelusuran dokumen hukum, kemudian dianalisis secara kualitatif dengan teknik preskriptif-analitis melalui interpretasi dan sistematisasi norma hukum. Analisis tersebut diarahkan untuk menentukan bentuk perlindungan hukum preventif dan represif bagi para penghadap, menguraikan tanggung jawab hukum para pihak yang terlibat dalam penggunaan identitas digital, serta merumuskan konstruksi pengaturan *cyber notary* yang mampu menjamin kepastian hukum, keamanan data, dan autentisitas identitas penghadap.

4. HASIL DAN PEMBAHASAN

Kedudukan Hukum Identitas Digital Penghadap dalam Penyelenggaraan *Cyber Notary*

Transformasi digital dalam pelayanan kenotariatan memperlihatkan perubahan dari administrasi berbasis dokumen fisik menuju penggunaan sistem elektronik untuk menunjang pelayanan hukum. Perubahan tersebut tidak hanya menyangkut media pembuatan dokumen, tetapi juga menyentuh proses identifikasi, autentikasi, komunikasi, penandatanganan, dan penyimpanan dokumen para penghadap (Andriani et al., 2025; Adrianto & Sutrisno, 2026). Karena itu, persoalan utama *cyber notary* bukan semata-mata apakah teknologi dapat digunakan, tetapi apakah penggunaan teknologi tersebut mampu mempertahankan karakter autentik dan kepastian hukum dari tindakan notaris.

Konsep “menghadap” menjadi titik kritis dalam penggunaan identitas digital. Pasal 39 UU Jabatan Notaris mensyaratkan penghadap memenuhi kecakapan hukum serta dikenal oleh notaris atau diperkenalkan melalui mekanisme yang ditentukan undang-undang, dan pengenalan tersebut harus dinyatakan secara tegas dalam akta. Hutapea, Erliyani, dan Tornado (2023) menunjukkan bahwa perkembangan *cyber notary* menuntut penafsiran kembali terhadap konsep menghadap, sedangkan Kinasih (2024) mengaitkan persoalan tersebut dengan kepastian hukum dalam proses *verlijden* secara digital.

Dalam penelitian ini, identitas digital dipahami sebagai seperangkat data dan kredensial elektronik yang digunakan untuk membuktikan bahwa seseorang yang berinteraksi melalui sistem elektronik merupakan subjek hukum yang sebenarnya. Persoalannya, identitas yang sah secara administratif belum secara otomatis membuktikan bahwa pengguna identitas tersebut pada saat transaksi adalah pemilik identitas yang bersangkutan. Risiko *identity theft*, pemalsuan dokumen, penggunaan kredensial tanpa hak, hingga manipulasi komunikasi elektronik

menyebabkan verifikasi identitas menjadi unsur yang menentukan kualitas perlindungan penghadap (Faulina et al., 2022; Tubagus et al., 2023).

Konstruksi hukum tersebut menunjukkan adanya perbedaan antara validitas identitas dan autentikasi orang yang menggunakan identitas. Dalam proses konvensional, keduanya dapat diverifikasi melalui kehadiran fisik, pemeriksaan dokumen, komunikasi langsung, dan penilaian notaris terhadap penghadap. Dalam ruang digital, fungsi tersebut memerlukan mekanisme hukum dan teknologi yang mampu memberikan tingkat keyakinan yang setara agar autentisitas akta tidak semata bergantung pada kepemilikan akun atau dokumen elektronik (Iwaldo, 2026; Eli & Rasji, 2025).

Masalah ini semakin kompleks karena regulasi Indonesia telah mengenal kewenangan notaris terkait transaksi elektronik, tetapi belum membentuk prosedur *cyber notary* yang sepenuhnya terintegrasi. Penjelasan Pasal 15 ayat (3) UU Jabatan Notaris telah menjadi dasar diskursus mengenai kewenangan notaris mensertifikasi transaksi elektronik, sedangkan sejumlah persyaratan mengenai penghadapan, pembacaan, dan penandatanganan akta masih dibangun dalam paradigma konvensional. Kondisi tersebut menghasilkan kesenjangan antara perkembangan teknologi dengan konstruksi formal hukum kenotariatan (Rihhadatul'aisy et al., 2026; Dewi & Puspawati, 2025).

Tabel 1. Temuan Normatif Mengenai Penggunaan Identitas Digital dalam *Cyber Notary*.

Aspek yang Dianalisis	Konstruksi Hukum Saat Ini	Temuan Permasalahan	Implikasi bagi Penghadap
Identitas penghadap	Penghadap harus dikenal notaris atau diperkenalkan menurut mekanisme UUJN	Belum terdapat standar khusus pengenalan penghadap melalui identitas digital	Risiko ketidakpastian mengenai siapa yang sebenarnya menghadap
Kehadiran penghadap	Model UUJN bertumpu pada proses menghadap, pembacaan, dan penandatanganan	Kesetaraan hukum kehadiran virtual belum dirumuskan secara menyeluruh	Berpotensi menimbulkan sengketa terhadap proses pembentukan akta
Autentikasi digital	Teknologi memungkinkan sertifikat elektronik, biometrik, dan autentikasi elektronik	Belum ada standar khusus kenotariatan yang mengintegrasikan seluruh mekanisme tersebut	Tingkat keamanan dapat berbeda antarplatform
Dokumen elektronik	Rezim ITE mengakui informasi dan dokumen elektronik dalam batas yang ditentukan hukum	Hubungannya dengan formalitas akta notaris masih menjadi problem doktrinal	Timbul persoalan mengenai kekuatan pembuktian akta elektronik
Data identitas	Dilindungi melalui UU Pelindungan Data Pribadi	Proses verifikasi membutuhkan pengumpulan dan pemrosesan data pribadi	Penghadap menghadapi risiko kebocoran dan penyalahgunaan data
Tanggung jawab	Notaris memiliki kewajiban profesional dan kehati-hatian	Pembagian tanggung jawab dengan penyedia sistem belum terumuskan secara khusus	Pemulihan kerugian dapat menjadi kompleks apabila terjadi kegagalan sistem

Tabel tersebut memperlihatkan bahwa persoalan identitas digital berada pada persimpangan antara hukum kenotariatan, hukum transaksi elektronik, dan hukum perlindungan data pribadi. UU Nomor 2 Tahun 2014 sebagai perubahan UU Jabatan Notaris masih berlaku, sementara rezim ITE kini telah mengalami perubahan kedua melalui UU Nomor 1 Tahun 2024. Dengan demikian, pengembangan *cyber notary* harus dilakukan melalui harmonisasi, bukan sekadar penggunaan teknologi pada prosedur yang sebelumnya bersifat fisik.

Penggunaan *video conference*, misalnya, dapat membantu notaris melihat dan berkomunikasi dengan penghadap, tetapi tampilan audiovisual tidak dengan sendirinya menyelesaikan persoalan autentikasi. Cantiga (2025) memperlihatkan relevansi *video conference* terhadap diskursus keabsahan akta digital, sedangkan Sari dan Yanata (2026) menempatkan rekonstruksi regulasi *cyber notary* sebagai kebutuhan dalam menunjang transaksi pada ekonomi digital. Artinya, teknologi komunikasi harus dikombinasikan dengan autentikasi identitas yang dapat diaudit dan mempunyai dasar hukum.

Kesenjangan tersebut menunjukkan bahwa kepastian hukum tidak cukup dibangun dengan pengakuan abstrak terhadap *cyber notary*. Diperlukan rekonstruksi norma yang menjelaskan hubungan antara identitas digital, kehadiran elektronik, tanda tangan elektronik, verifikasi kehendak, dan tanggung jawab notaris agar seluruh tahapan dapat dinilai secara hukum. Hal ini sejalan dengan argumentasi Riviyusnita dan Utomo (2026) mengenai rekonstruksi pengaturan akta elektronik serta Damayanti et al. (2026) mengenai kebutuhan harmonisasi regulasi untuk menegaskan legitimasi *cyber notary*.

Berdasarkan temuan tersebut, identitas digital seharusnya tidak ditempatkan hanya sebagai pengganti kartu identitas fisik, tetapi sebagai sistem pembuktian identitas yang terdiri atas proses identifikasi, autentikasi, verifikasi, dan pencatatan jejak elektronik. Titik perlindungan hukumnya terletak pada kemampuan sistem memastikan keterhubungan antara identitas administratif, orang yang menghadap, kehendak hukum yang dinyatakan, serta tindakan penandatanganan. Tanpa standar tersebut, digitalisasi justru dapat memindahkan risiko dari persoalan pemalsuan dokumen fisik menuju penyalahgunaan identitas dan manipulasi autentikasi elektronik.

Konstruksi Perlindungan Hukum terhadap Para Penghadap dalam Penggunaan Identitas Digital pada *Cyber Notary*

Perlindungan terhadap penghadap harus mencakup perlindungan preventif dan represif. Perlindungan preventif diperlukan sebelum dan selama pembentukan akta untuk mencegah penyalahgunaan identitas, sedangkan perlindungan represif diperlukan ketika pelanggaran telah terjadi dan menimbulkan kerugian. Nugraha (2025) menempatkan perlindungan para

pihak sebagai bagian penting dari pembentukan akta notaris elektronik, sementara Najib (2023) menegaskan dimensi keamanan data berdasarkan hukum perlindungan data pribadi.

Perlindungan preventif pertama adalah penerapan prinsip kehati-hatian pada proses autentikasi. Verifikasi seharusnya tidak hanya didasarkan pada unggahan kartu identitas, tetapi dibangun melalui autentikasi berlapis yang secara kumulatif menghubungkan dokumen identitas, pemilik identitas, kredensial elektronik, dan kehendak hukum penghadap. Pendekatan tersebut selaras dengan penekanan Pramudya et al. (2026) terhadap prinsip kehati-hatian dalam *cyber notary* dan kajian Wulandari, Hidayati, dan Ayu (2026) mengenai perlindungan hukum dalam pelaksanaan jabatan notaris berbasis digital.

Verifikasi identitas juga harus tunduk pada prinsip perlindungan data pribadi karena proses tersebut membutuhkan pengumpulan dan penggunaan data milik penghadap. UU Nomor 27 Tahun 2022 mengatur hak subjek data, pemrosesan data pribadi, serta kewajiban pengendali dan prosesor data pribadi. Oleh sebab itu, digitalisasi kenotariatan tidak boleh menghasilkan praktik pengumpulan data yang berlebihan atau penyimpanan data tanpa sistem keamanan dan tujuan yang jelas (Marbun et al., 2025).

Perlindungan terhadap identitas tidak berhenti setelah akta ditandatangani. Data autentikasi, rekaman proses elektronik, minuta, dan dokumen pendukung harus dijaga dari perubahan, kehilangan, akses tanpa hak, serta kerusakan sistem dalam jangka panjang. Urgensi penyimpanan protokol elektronik telah dibahas oleh Surya et al. (2024), sedangkan Rahim dan Purba (2025) menunjukkan relevansi penyimpanan minuta secara elektronik sebagai salah satu mekanisme menghadapi risiko kerusakan dokumen.

Tabel 2. Model Perlindungan Hukum terhadap Penghadap dalam Penggunaan Identitas Digital.

Risiko Hukum	Perlindungan Preventif yang Direkomendasikan	Perlindungan Represif	Fokus Pertanggungjawaban
Penggunaan identitas orang lain	Verifikasi identitas berlapis, autentikasi biometrik/ <i>liveness</i> , pemeriksaan kredensial resmi	Pembatalan/pengujian tindakan hukum, investigasi digital, tuntutan terhadap pelaku	Pelaku penyalahgunaan dan pihak yang lalai
Pemalsuan wajah/suara atau <i>deepfake</i>	<i>Liveness detection</i> , autentikasi multifaktor, pemeriksaan langsung oleh notaris	Audit forensik atas rekaman dan <i>log</i> transaksi	Pelaku serta penyedia sistem apabila terdapat kelalaian
Pencurian kredensial elektronik	OTP/MFA, tanda tangan tersertifikasi, pengamanan perangkat	Pemblokiran kredensial dan penelusuran aktivitas	Pemilik/pengelola sistem sesuai sumber kesalahan
Kebocoran data pribadi	Enkripsi, pembatasan akses, minimisasi dan pembatasan tujuan pemrosesan	Pemberitahuan insiden, pemulihan data, ganti kerugian sesuai dasar hukum	Pengendali/prosesor data yang bertanggung jawab

Manipulasi dokumen	isi	<i>Hash, timestamp, jejak audit, pengendalian versi dokumen</i>	Pemeriksaan integritas dan pembuktian elektronik	Pengelola sistem dan pelaku manipulasi
Penyangkalan tanda tangan		Autentikasi kuat dan tanda tangan elektronik tersertifikasi	Verifikasi sertifikat dan rekonstruksi jejak transaksi	Penandatangan/pelaku atau penyedia layanan sesuai kesalahan
Hilang/rusaknya protokol elektronik		<i>Backup</i> , redundansi, kontrol akses dan mekanisme pemulihan	Restorasi serta audit insiden	Notaris dan penyelenggara penyimpanan sesuai kewenangan
Kegagalan verifikasi notaris		SOP verifikasi dan dokumentasi seluruh tahapan	Pertanggungjawaban profesional apabila terbukti terdapat kesalahan	Notaris berdasarkan tingkat kesalahan
Gangguan sistem elektronik		Standar keandalan, keamanan serta <i>business continuity plan</i>	Pemulihan sistem dan pertanggungjawaban penyelenggara	Penyelenggara sistem elektronik
Sengketa keabsahan proses menghadapi		Rekaman <i>audit trail</i> yang dapat diverifikasi dan standar normatif yang jelas	Pemeriksaan melalui mekanisme penyelesaian sengketa	Ditentukan berdasarkan sumber cacat proses

Model pada tabel tersebut menunjukkan bahwa teknologi biometrik, *liveness detection*, tanda tangan elektronik tersertifikasi, atau *audit trail* bukan dimaksudkan sebagai pengganti kewenangan notaris. Instrumen tersebut merupakan lapisan pembuktian tambahan untuk meningkatkan keyakinan notaris bahwa subjek yang berinteraksi secara elektronik benar merupakan penghadap yang bersangkutan. Hal tersebut penting karena perlindungan para pihak bergantung pada kombinasi antara validitas teknologi dan tanggung jawab profesional pejabat yang menjalankan proses kenotariatan (Nugraha, 2025; Pramudya et al., 2026).

Perlindungan represif diperlukan apabila mekanisme preventif gagal. Bentuknya dapat berupa pemulihan penguasaan identitas, koreksi atau penghapusan data sesuai dasar hukum, penelusuran jejak elektronik, tuntutan ganti kerugian, serta penerapan pertanggungjawaban administratif atau pidana apabila unsur masing-masing pelanggaran terpenuhi. Rezim PDP sendiri mencakup kewajiban pemrosesan, sanksi administratif, penyelesaian sengketa, larangan penggunaan data pribadi, dan ketentuan pidana.

Pembagian tanggung jawab juga harus dibuat secara proporsional. Notaris tidak seharusnya otomatis dibebani seluruh akibat yang timbul akibat serangan siber pada infrastruktur di luar kendalinya, tetapi tidak dapat pula dibebaskan ketika kerugian berasal dari kelalaian dalam melakukan verifikasi yang berada dalam ruang kewenangannya. Karena itu, rekonstruksi hukum perlu membedakan tanggung jawab notaris, penyelenggara sistem elektronik, penyelenggara sertifikasi elektronik, pengendali/prosesor data, dan pelaku penyalahgunaan identitas (Iwaldo, 2026; Riviyusnita & Utomo, 2026).

Perlindungan hukum juga harus mencakup hak penghadap untuk mengetahui bagaimana identitasnya digunakan. Penghadap harus memperoleh informasi yang memadai mengenai tujuan pemrosesan data, jenis data yang diproses, penggunaan pihak ketiga, durasi penyimpanan, serta risiko teknologi yang digunakan dalam proses kenotariatan. Model

demikian menjadikan persetujuan tidak sekadar formalitas, melainkan bagian dari kontrol subjek hukum atas identitas digitalnya (Najib, 2023; Marbun et al., 2025).

Dalam konteks yang lebih luas, kebutuhan memberikan perlindungan efektif kepada subjek hukum merupakan prinsip yang tidak terbatas pada bidang kenotariatan. Kajian Saputra et al. (2026) mengenai perlindungan pengungsi dalam hukum HAM internasional dan Hanafi et al. (2026) mengenai hukum Islam dalam perubahan sosial dapat digunakan **secara konseptual**, bukan sebagai sumber langsung *cyber notary*, untuk menunjukkan bahwa perubahan kondisi sosial menuntut hukum mempertahankan perlindungan terhadap subjek hukum ketika mekanisme normatif lama menghadapi realitas baru. Pada *cyber notary*, perubahan realitas tersebut adalah perpindahan proses identifikasi dan interaksi hukum ke ruang digital.

Pendekatan perlindungan yang berorientasi pada keadilan juga menuntut agar efisiensi digital tidak mengurangi posisi penghadap sebagai pemegang hak. Literatur mengenai keadilan sosial oleh Shifah et al. (2026) dan partisipasi dalam ruang demokrasi digital oleh Saputra, Asshofiah, dan Sholikhhi (2026) digunakan dalam penelitian ini sebagai penguat konseptual mengenai pentingnya akses, kontrol, dan perlindungan subjek dalam proses yang semakin terdigitalisasi. Dalam konteks kenotariatan, prinsip tersebut diterjemahkan menjadi hak atas keamanan identitas, transparansi pemrosesan, serta akses terhadap pemulihan ketika terjadi penyalahgunaan.

Demikian pula, kajian *Double Track* dan *Anti-SLAPP* oleh Saputra et al. (2026) memperlihatkan secara konseptual pentingnya desain perlindungan prosedural ketika terdapat risiko ketidakseimbangan kepentingan, sedangkan kajian kriminologis Saputra, Utari, dan Widyawati (2026) memberikan konteks lebih luas bahwa respons hukum tidak dapat hanya berorientasi pada akibat setelah pelanggaran terjadi. Kedua sumber tersebut bukan literatur langsung mengenai kenotariatan, tetapi dapat digunakan sebagai analogi untuk memperkuat pendekatan bahwa sistem *cyber notary* perlu mengutamakan pencegahan sekaligus menyediakan mekanisme pemulihan yang efektif.

Penyimpanan elektronik juga harus menjadi bagian dari arsitektur perlindungan karena pembuktian atas identitas dan kehendak penghadap dapat bergantung pada data historis transaksi. Jejak waktu, rekaman autentikasi, sertifikat elektronik, data perubahan dokumen, serta catatan akses dapat menjadi elemen penting ketika terjadi penyangkalan atau sengketa pada kemudian hari. Hal ini memperkuat urgensi pengembangan protokol elektronik sebagaimana dibahas Surya et al. (2024) dan Rahim dan Purba (2025).

Perlindungan penghadap membutuhkan harmonisasi antara UU Jabatan Notaris, rezim ITE, UU Pelindungan Data Pribadi, dan regulasi penyelenggaraan sistem elektronik. Kebutuhan harmonisasi tersebut sejalan dengan kajian Damayanti et al. (2026), sementara Rihhadatul'aisy et al. (2026) menempatkan pembaruan *cyber notary* sebagai kebutuhan yang disertai tantangan implementasi. Pembaruan tidak cukup dengan melegalkan media elektronik, tetapi harus membentuk prosedur yang menjamin identitas, kehendak, tanda tangan, integritas dokumen, keamanan data, dan pertanggungjawaban.

Dengan demikian, hasil penelitian menunjukkan bahwa konstruksi perlindungan hukum yang ideal adalah model multi-layer legal protection, yaitu perlindungan yang menggabungkan standar autentikasi digital, prinsip kehati-hatian notaris, tata kelola pelindungan data pribadi, keamanan sistem, penyimpanan jejak audit, dan mekanisme pertanggungjawaban. Pembaruan kekuatan akta autentik elektronik sebagaimana dibahas Eli dan Rasji (2025), perlindungan para pihak sebagaimana dikaji Nugraha (2025), serta rekonstruksi regulasi untuk mendukung ekonomi digital sebagaimana dikemukakan Sari dan Yanata (2026) mengarah pada kebutuhan yang sama: teknologi baru hanya dapat memperkuat fungsi kenotariatan apabila diikuti jaminan kepastian dan perlindungan hukum. Oleh karena itu, pengaturan *cyber notary* ke depan perlu menempatkan keandalan identitas digital penghadap sebagai salah satu syarat fundamental autentisitas proses, bukan sekadar sebagai persoalan administratif elektronik.

5. KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa perlindungan hukum terhadap para penghadap dalam penggunaan identitas digital pada *cyber notary* belum memperoleh konstruksi normatif yang sepenuhnya terpadu dalam sistem hukum Indonesia. Persoalan utama tidak hanya terletak pada pengakuan terhadap penggunaan teknologi elektronik, tetapi pada kepastian mengenai autentikasi identitas, keabsahan proses menghadap secara digital, perlindungan data pribadi, integritas dokumen, dan pembagian tanggung jawab apabila terjadi kegagalan verifikasi atau penyalahgunaan identitas. Perlindungan yang ideal harus dibangun melalui model *multi-layer legal protection* yang mengintegrasikan prinsip kehati-hatian notaris, autentikasi berlapis, tanda tangan elektronik yang dapat diverifikasi, keamanan sistem, pelindungan data pribadi, penyimpanan *audit trail*, serta mekanisme pertanggungjawaban dan pemulihan yang jelas. Oleh karena itu, identitas digital harus diposisikan sebagai elemen fundamental dalam menjamin autentisitas proses *cyber notary*, bukan sekadar pengganti administratif terhadap identitas fisik penghadap.

Pemerintah dan pembentuk undang-undang perlu melakukan harmonisasi dan rekonstruksi regulasi *cyber notary* dengan memperjelas standar penggunaan identitas digital dalam proses menghadap, pembacaan, persetujuan, dan penandatanganan akta secara elektronik. Pengaturan tersebut perlu menetapkan standar autentikasi berlapis, penggunaan tanda tangan elektronik yang andal, pencatatan *audit trail*, perlindungan dan pembatasan pemrosesan data pribadi, serta pembagian tanggung jawab yang proporsional antara notaris, penyelenggara sistem elektronik, penyelenggara sertifikasi elektronik, dan pihak lain yang terlibat. Organisasi profesi notaris juga perlu menyusun standar operasional dan pedoman kehati-hatian khusus untuk verifikasi identitas digital guna menciptakan praktik yang seragam. Dengan pengaturan yang lebih komprehensif, digitalisasi pelayanan kenotariatan dapat berkembang tanpa mengurangi kepastian hukum, keamanan, dan perlindungan terhadap para penghadap.

DAFTAR REFERENSI

- Adrianto, N., & Sutrisno, E. (2026). Kajian Hukum terhadap Notaris melalui Digitalisasi Layanan Hukum. *Jurnal Hukum Lex Generalis*, 7(4).
- 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*, 3(2), 2006-2014.
- Cantiqa, S. P. (2025). Keabsahan Akta Notaris Digital Melalui Video Conference Dalam Perspektif Hukum Teknologi Informasi. *Studia: Journal of Humanities and Education Studies*, 1(2), 151-158.
- Damayanti, N. E. W., Falah, M. K. H., Kumalasari, N., & Ali, M. (2026). Harmonisasi Regulasi dalam Menegaskan Legitimasi Akta Cyber Notary di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 4(4), 7481-7496.
- Dewi, N. P. K. R., & Puspawati, A. A. A. I. (2025). Analisis perkembangan paradigma cyber notary: Sintesis atas problematika pengaturan cyber notary di Indonesia. *Repertorium: Jurnal Ilmiah Hukum Kenotariatan*, 14(2), 1-14.
- Eli, G., & Rasji, R. (2025). Pembaharuan hukum terhadap kekuatan akta autentik elektronik. *Jurnal USM Law Review*, 8(2), 849-864.
- Faulina, J., Barkatullah, A. H., & Gozali, D. S. (2022). Kedudukan hukum akta notaris yang menerapkan konsep cyber notary di masa pandemi COVID-19 di Indonesia. *Notary Law Journal*, 1(3), 247-262.
- Hanafî, S., Saputra, D. R., Dewi, E. N., Adistia, A. N., Mahendra, Y. I., Akbar, Z. A., & Wijaya, A. (2026). Islamic law and social change: Contemporary applications of fiqh in Muslim societies. *Indonesian Journal of Sharia and Islamic Sciences*, 1(1), 19-27.
- Hutapea, C. W., Erliyani, R., & Tornado, A. S. (2023). Konsep Menghadap Notaris Dalam Pembuatan Akta Berdasarkan Perkembangan Cyber Notary. *Collegium Studiosum Journal*, 6(1), 132-145.

- Iwaldo, M. F. (2026). Kepastian Hukum Cyber Notary dalam Pembuatan Akta Autentik Elektronik di Indonesia. *Jurnal Kajian Hukum Dan Kebijakan Publik* | E-ISSN: 3031-8882, 4(1), 36-42.
- Kinasih, N. P. (2024). Kepastian hukum notaris menerapkan cyber notary dalam verlidjen akta notaris secara digital. *Acten Journal Law Review*, 1(3), 231-252.
- Marbun, D., Karimah, N., Pramono, P., Prayogo, R., & Ramadha, R. A. (2025). Perlindungan Data Pribadi dalam Implementasi E-Notary. *Jurnal Hukum Lex Generalis*, 6(12).
- Najib, A. (2023). Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi. *ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan*, 7(1), 43-59.
- Nugraha, S. A. (2025). Perlindungan Hukum Bagi Para Pihak Dalam Akta Notaris Yang Dibuat Secara Elektronik. *Argumentum: Jurnal Hukum*, 1(2), 27-44.
- Pramudya, M. I. B., Wiratama, A., Kumalasari, N., & Ali, M. (2026). Penerapan Cyber Notary dan Prinsip Kehati-hatian Notaris: Kritik Terhadap Kesiapan Regulasi Kenotariatan di Indonesia. *Legal Society: Jurnal PKM Fakultas Hukum*, 5(1), 23-35.
- Rahim, N. A., & Purba, H. (2025). Analisis Hukum Penyimpanan Minuta Akta secara Elektronik dalam Upaya Pencegahan Kerusakan Minuta Akta akibat Force Majeure. *Jurnal Hukum Lex Generalis*, 6(4).
- Rihhadatul'aisy, R. A., Mayana, R. F., & Ramli, T. S. (2026). Cyber Notary Sebagai Pembaharuan Hukum: Urgensi dan Tantangan dalam Implementasinya. *JURNAL USM LAW REVIEW*, 9(2), 909-933.
- Riviyusnita, R., & Utomo, S. (2026). Rekonstruksi Pengaturan Akta Elektronik Notaris Dalam Sistem Hukum Indonesia: Menuju Kepastian Hukum Penyelenggaraan Cyber Notary. *Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda*, 32(2).
- Saputra, D. R., Asshofiah, K., & Sholikhi, F. A. (2026). Youth Participation in Digital Democracy: A Narrative Analysis of Global Civic Engagement Reports. *Anthroposia: Journal of Social and Human Development*, 1(1), 28-36.
- Saputra, D. R., Hanafi, S., Dauda, S., Noya, M., & Ritonga, B. D. F. (2026). International human rights law: Protection of refugees in contemporary conflicts. *International Journal of Law and Political Authority*, 1(1), 01-09.
- Saputra, D. R., Mashyar, A., Wulandari, C., Dauda, S., & Mahendra, Y. I. (2026). Double Track and Anti-SLAPP: Indonesian Judicial Reasoning in Environmental Cases. *Walisongo Law Review (Walrev)*, 8(1), 114-130.
- Saputra, D. R., Utari, I. S., & Widyawati, A. (2026). Beyond Punishment: A Criminological Analysis of Social Determinants of Criminal Behavior in Contemporary Society. *International Journal of Applied Research and Innovation*, 1(3), 14-21.
- Sari, A. G., & Yanata, C. (2026). Rekonstruksi Regulasi Cyber Notary Guna Mendukung Ease of Doing Business (EODB) Di Era Ekonomi Digital Indonesia. *Ekasakti Legal Science Journal*, 3(2), 99-109.
- Shifah, L., Sugianto, S., Mutmainah, S., & Saputra, D. R. (2026). Islamic Economics and Social Justice: Zakat, Waqf, and Poverty Alleviation. *Indonesian Journal of Sharia and Islamic Sciences*, 1(1), 10-18.

- Surya, M. J. K., Maghfiroh, N., Pramesti, N., & Firnanda, A. (2024). Urgensi penyimpanan protokol notaris secara elektronik dalam kaitan cyber notary di Indonesia. *UNES Law Review*, 6(3), 8334-8346.
- Tubagus, D., Raffles, R., & Syamsir, S. (2023). Kekuatan Hukum Terhadap Akta Yang Dibuat Secara Elektronik (Cyber Notary) Dalam Prespektif Peraturan Perundang-Undangan. *Recital Review*, 5(1), 151-173.
- Wulandari, A. T., Hidayati, R., & Ayu, I. K. (2026). Perlindungan Hukum Terhadap Notaris Dalam Membuat Akta Menggunakan Cyber Notary Di Indonesia. *SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum*, 5(2), 91-101.