



## Kekuatan Pembuktian atau Fiksi Hukum? Rekonseptualisasi Kehadiran dalam Cyber Notary

Maftuha Kiswah<sup>1</sup>, Nuzulia Kumalasari<sup>2</sup>, Moch. Ali<sup>3</sup>

<sup>1,2,3</sup> Magister Kenotariatan, Fakultas Hukum, Universitas Jember  
[maftuhakiswah1@gmail.com](mailto:maftuhakiswah1@gmail.com)<sup>1</sup>, [nuzulia@unej.ac.id](mailto:nuzulia@unej.ac.id)<sup>2</sup>, [moh.ali@unej.ac.id](mailto:moh.ali@unej.ac.id)<sup>3</sup>

### Abstrak

Notaris berwenang membuat akta otentik berdasarkan tiga syarat kumulatif Pasal 1868 KUH Perdata, termasuk kehadiran fisik para pihak di hadapan notaris. Konsep cyber notary telah diakui dalam penjelasan Pasal 15 ayat (3) Undang-Undang Jabatan Notaris (UUJN) sejak 2014, namun peraturan pelaksanaannya belum pernah diterbitkan. Urgensi penelitian ini bertumpu pada ancaman empiris yang nyata: Tempo.co melaporkan kebocoran 337 juta data kependudukan pada Juli 2023, data yang menjadi basis verifikasi identitas penghadap oleh notaris, disusul serangan ransomware yang melumpuhkan Pusat Data Nasional pada Juni 2024, yang membuktikan bahwa infrastruktur digital penunjang kenotariatan sudah berada dalam risiko serius. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual, berlandaskan teori budaya hukum Lawrence M. Friedman serta teori hukum progresif Satjipto Rahardjo. Temuan menunjukkan bahwa regulasi yang berlaku menciptakan jebakan normatif: UUJN mendorong kewenangan notaris dalam transaksi elektronik, tetapi Pasal 5 ayat (4) huruf b UU ITE mengecualikan akta notaris dari pengakuan sebagai dokumen elektronik. Pergeseran ke kehadiran virtual merupakan pergeseran epistemik yang berpotensi mereduksi akta otentik menjadi fiksi hukum. Notaris pun menanggung beban baru sebagai pengendali data pribadi berdasarkan UU PDP. Artikel ini menyimpulkan bahwa harmonisasi UUJN, UU ITE, dan UU PDP merupakan prioritas mendesak, dan mengusulkan model rekonseptualisasi hybrid berbasis risiko: akta risiko tinggi wajib menggunakan kehadiran fisik, akta risiko sedang dapat dilakukan secara hybrid dengan syarat biometrik ketat, serta akta risiko rendah dapat sepenuhnya dilaksanakan secara virtual.

**Kata kunci:** Cyber Notary; Kekuatan Pembuktian; Budaya Hukum; Akta Otentik; Kehadiran Epistemik

### 1. Pendahuluan

Perkembangan teknologi informasi telah mendorong perubahan mendasar dalam praktik layanan hukum, termasuk dalam bidang kenotariatan yang selama ini identik dengan formalitas dan kehadiran fisik (Makarim, 2013). Di tengah arus digitalisasi tersebut, peran notaris justru diuji pada titik paling esensial, yaitu bagaimana hukum memaknai “kehadiran” dalam pembentukan akta otentik. Jabatan notaris dalam sistem hukum Indonesia memiliki fungsi sentral sebagai pejabat umum yang berwenang membuat akta otentik. Pasal 1 angka 7 UUJN menegaskan bahwa notaris adalah pejabat umum yang berwenang membuat akta otentik dan memiliki kewenangan lainnya sebagaimana dimaksud dalam undang-undang ini. Pasal 1868 KUHPerdata menetapkan tiga syarat kumulatif akta otentik, yakni akta dibuat dalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau di hadapan pejabat umum yang berwenang, dan dibuat di tempat di mana pejabat tersebut berwenang. Habib Adjie menguraikan bahwa kewenangan membuat akta otentik yang melekat pada jabatan notaris bersifat personal dan tidak dapat didelegasikan kepada pihak lain, karena akta yang dihasilkan merupakan refleksi langsung dari verifikasi yang notaris lakukan sendiri terhadap para penghadap (Adjie, 2013). Frasa “di hadapan” dalam ketentuan ini menjadi elemen yang paling krusial sekaligus paling kontroversial ketika hukum berhadapan dengan tuntutan digitalisasi.

Konsep *cyber notary* bukan gagasan yang lahir kemarin. Dewi dan Puspawati menjelaskan bahwa gagasan serupa, dengan istilah *electronic notary*, pertama kali dikemukakan oleh delegasi Prancis dalam *The Trade Electronics Data Interchange System (TEDIS) Legal Workshop* pada tahun 1989. Istilah *cyber notary* kemudian dipopulerkan oleh American Bar Association (ABA) Information Security Committee pada tahun 1994 sebagai respons terhadap kebutuhan akan kepastian dan perlindungan hukum dalam transaksi elektronik di ruang siber (Dewi & Puspawati, 2025). Di Indonesia, istilah *cyber notary* pertama kali muncul secara resmi dalam penjelasan Pasal 15 ayat (3) UUJN, yang menyebut “kewenangan mensertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*)” sebagai salah satu kewenangan lain yang dapat dimiliki notaris. Namun, lebih dari satu dekade telah berlalu sejak ketentuan itu dirumuskan, tetapi pengaturan pelaksanaannya belum pernah diterbitkan.

Di satu sisi, UU ITE mengakui keabsahan dokumen elektronik dan tanda tangan elektronik sebagai alat bukti yang sah. Di sisi lain, Pasal 5 ayat (4) huruf b UU ITE justru mengecualikan akta notaris dari pengakuan sebagai dokumen elektronik. Ghani dan Priyono menemukan bahwa ketidakselarasan antara UUJN dan UU ITE ini menciptakan vakum normatif yang menghambat implementasi *cyber notary* serta menimbulkan ketidakpastian hukum mengenai keabsahan akta yang dibuat melalui media elektronik (Ghani & Priyono, 2025).

Rachmawati dan Silviana, dalam penelitian empiris mereka yang melibatkan notaris di Kota Tangerang dan Subdit Notariat Kementerian Hukum dan HAM, menemukan bahwa akta notaris yang ditandatangani dengan tanda tangan elektronik dinyatakan tidak sah karena pembuatannya tidak sesuai dengan UUJN. Temuan tersebut secara konkret memperlihatkan bagaimana ketidaksesuaian prosedural dalam praktik digital dapat berdampak langsung pada status hukum suatu akta. Dalam konteks ini, penggunaan teknologi tidak serta-merta menjamin terpenuhinya syarat formil yang ditentukan oleh hukum positif. Konsekuensinya, akta tersebut terdegradasi dari akta otentik menjadi akta di bawah tangan sehingga kehilangan kekuatan pembuktian yang sempurna (Rachmawati & Silviana, 2025). Temuan ini menunjukkan bahwa persoalan *cyber notary* bukan semata soal kelengkapan regulasi, melainkan menyentuh inti kekuatan pembuktian yang selama ini menjadi *raison d'être* jabatan notaris.

Pertanyaannya kemudian bergeser: dari mana datangnya hambatan normatif yang membuat ketidakabsahan itu tak terhindarkan? Prakoso dan Sudarwanto mengidentifikasi bahwa hambatan utama *cyber notary* dalam tataran normatif terletak pada dua ketentuan UUJN: Pasal 16 ayat (1) huruf c yang mewajibkan pelekatan sidik jari penghadap pada minuta akta, dan Pasal 16 ayat (1) huruf m yang mewajibkan pembacaan akta di hadapan penghadap dengan kehadiran paling sedikit dua orang saksi dan penandatanganan saat itu juga. Kedua ketentuan ini secara tekstual menuntut kehadiran fisik dan belum ada peraturan yang secara legal mengatur pelekatan sidik jari secara digital (Prakoso & Sudarwanto, 2025). Loleh, Thalib, dan Towadi menambahkan dalam analisisnya bahwa tantangan ini tidak hanya berdimensi yuridis, melainkan juga menyentuh aspek infrastruktur teknologi yang belum merata serta rendahnya literasi digital di kalangan notaris dan masyarakat (Loleh et al., 2025).

Dimensi ancaman terhadap data pribadi memperkuat urgensi penelitian ini secara empiris. Tempo.co melaporkan bahwa pada Juli 2023 sekitar 337 juta data kependudukan dari Direktorat Jenderal Kependudukan dan Pencatatan Sipil bocor ke internet, termasuk nomor akta kelahiran dan akta pernikahan yang menjadi basis verifikasi identitas penghadap oleh notaris (Tempo.co, 2024). Pada Juni 2024, serangan *ransomware* kelompok “Brain Cipher” melumpuhkan Pusat Data Nasional Sementara dan menyebabkan data dari 210 instansi pemerintah tidak dapat dipulihkan (Tempo, 2024). Kedua peristiwa ini menunjukkan bahwa ancaman terhadap infrastruktur data yang menjadi tulang punggung layanan kenotariatan digital bukan sekadar skenario hipotetis, melainkan risiko nyata yang telah terjadi dan berulang kali.

Kajian-kajian sebelumnya oleh peneliti telah memberikan kontribusi penting dalam memetakan disharmoni regulasi serta hambatan teknis dalam *cyber notary*. Namun, terdapat dua aspek yang belum dikaji secara mendalam. Pertama, dimensi filosofis dari konsep “kehadiran” itu sendiri: apakah kehadiran virtual mampu memenuhi fungsi epistemik yang selama ini diemban oleh kehadiran fisik, ataukah ia sekadar fiksi hukum yang menyembunyikan hilangnya substansi? Kedua, posisi notaris sebagai pengendali data pribadi berdasarkan UU PDP dan implikasinya terhadap keabsahan akta secara formil. Wiyarta dan Silviana menegaskan bahwa notaris tidak hanya berperan sebagai pejabat yang mengesahkan dokumen, tetapi juga harus memastikan keamanan data dan integritas proses hukum secara menyeluruh (Wiyarta & Silviana, 2025).

Berdasarkan uraian di atas, artikel ini merumuskan dua permasalahan. Pertama, bagaimana disharmoni norma antara UUJN dan UU ITE memengaruhi kekuatan pembuktian akta otentik dalam konteks *cyber notary*, dan apakah kehadiran virtual dapat memenuhi fungsi epistemik kehadiran fisik atau sekadar menjadi fiksi hukum? Kedua, bagaimana model rekonseptualisasi kehadiran dalam *cyber notary* dapat dirumuskan agar mempertahankan kekuatan pembuktian akta, menempatkan kepatuhan terhadap perlindungan data pribadi sebagai syarat konstitutif—bukan sekadar kewajiban administratif—dan mengakomodasi budaya hukum masyarakat Indonesia secara bertahap?

## 2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif. Metode ini dipilih karena fokus kajian berangkat dari kekaburan norma dan konflik norma antara UUJN, UU ITE, dan UU PDP dalam konteks *cyber notary*. Penelitian hukum normatif menempatkan hukum sebagai sistem norma yang terdiri atas asas-asas, kaidah, dan doktrin yang termuat dalam peraturan perundang-undangan (Marzuki, 2017).

Penelitian ini menggunakan tiga pendekatan. Pertama, *statute approach* (pendekatan perundang-undangan), yakni menelaah KUHPerdara, UUJN, UU ITE, dan UU PDP untuk mengidentifikasi ketidakselarasan norma. Kedua, *conceptual approach* (pendekatan konseptual), yakni menganalisis konsep “kehadiran” dari perspektif epistemologi, ontologi, dan aksiologi hukum untuk menjawab apakah kehadiran virtual setara dengan kehadiran

fisik. Ketiga, pendekatan teoretis memanfaatkan teori budaya hukum Lawrence M. Friedman dan teori hukum progresif Satjipto Rahardjo untuk menganalisis kesiapan masyarakat serta arah pembaruan hukum (Marzuki, 2017). Bahan hukum dikumpulkan melalui studi dokumen dan dianalisis secara kualitatif dengan metode interpretasi yang sistematis dan teleologis.

### 3. Hasil dan Pembahasan

#### 3.1 Disharmoni Norma dan Implikasinya terhadap Kekuatan Pembuktian Akta Otentik

Kekuatan pembuktian akta otentik dalam sistem hukum perdata Indonesia bertumpu pada Pasal 1868 KUHPerduta yang menetapkan tiga syarat kumulatif: dibuat dalam bentuk yang ditentukan oleh undang-undang; dibuat oleh atau di hadapan pejabat umum yang berwenang; dan dibuat di tempat di mana pejabat itu berwenang. Ketiga syarat ini bersifat kumulatif. Tidak terpenuhinya salah satu syarat menyebabkan akta kehilangan otentisitas dan hanya berkuasa sebagai akta di bawah tangan (Subekti, 2008).

UUJN sebenarnya telah memberikan celah bagi *cyber notary* melalui Pasal 15 ayat (3) yang menyebutkan kewenangan untuk mensertifikasi transaksi elektronik dalam penjelasannya. Ghani dan Priyono menggarisbawahi bahwa celah ini bersifat implisit karena termuat dalam penjelasan pasal, bukan batang tubuh undang-undang, sehingga tidak memiliki daya ikat yang setara dengan norma utama (Ghani & Priyono, 2025). Dalam konteks tersebut, Edmon Makarim menegaskan bahwa notaris berperan sebagai pihak ketiga yang dipercaya dalam transaksi elektronik dan sertifikasi yang dilakukan notaris mencakup verifikasi identitas serta keaslian kehendak para pihak secara langsung (Makarim, 2013). Pasal 5 ayat (4) huruf b UU ITE justru mengecualikan akta notaris dari lingkup pengakuan sebagai dokumen elektronik, sehingga produk hukum yang dihasilkan notaris tidak memperoleh perlindungan sebagaimana dijamin dalam UU ITE. Dua aturan ini menciptakan apa yang dapat disebut sebagai “jebakan normatif”: di satu sisi, notaris didorong untuk berwenang dalam transaksi elektronik, tetapi di sisi lain, produk hukum yang dihasilkan tidak diakui sebagai dokumen elektronik. Ironisnya, Pasal 18 ayat (1) dari undang-undang yang sama justru menegaskan bahwa kontrak elektronik sah apabila memenuhi syarat Pasal 1320 KUH Perdata (Kiswah et al., 2025). Dengan kata lain, UU ITE mengakui perjanjian elektronik antara pelaku usaha dan konsumen, tetapi menolak mengakui produk hukum yang dibuat oleh pejabat negara yang secara khusus diberi kewenangan untuk itu oleh negara.

Rachmawati dan Silviana membedah dalam artikel hasil penelitiannya bahwa ketidakselarasan ini menghasilkan konsekuensi yuridis yang berat: akta notaris yang dibuat menggunakan tanda tangan elektronik tidak sah karena bertentangan dengan Pasal 16 ayat (1) huruf m yang mensyaratkan akta dibacakan di hadapan penghadap serta ditandatangani *saat itu juga* oleh penghadap, saksi, dan notaris (Rachmawati & Silviana, 2025). Dengan kata lain, ketentuan ini tidak hanya mengatur prosedur, tetapi juga menegaskan kesatuan waktu dan tempat dalam proses pembentukan akta. Frasa “ditandatangani saat itu juga” merupakan penegasan bahwa penandatanganan akta harus terjadi bersamaan dengan momen pembacaan di satu tempat yang sama. Tidak ada ruang untuk interpretasi bahwa penandatanganan dapat dilakukan secara elektronik di lokasi yang berbeda.

Ketentuan Pasal 16 ayat (1) huruf m UJN, yang dibaca bersama Pasal 16 ayat (1) huruf c yang mewajibkan pelekatan sidik jari penghadap pada minuta akta, semakin memperjelas bahwa UJN dibangun di atas paradigma kehadiran fisik sebagai syarat mutlak otentisitas. Prakoso dan Sudarwanto menegaskan bahwa frasa “menghadap” dalam UJN secara gramatikal bermakna pertemuan tatap muka langsung di satu tempat pada saat yang sama, bukan pertemuan yang dimediasi oleh teknologi (Prakoso & Sudarwanto, 2025). Islam, Kurniawan, dan Hirsanuddin menegaskan bahwa keabsahan akta notaris yang menggunakan *cyber notary* bergantung pada pemenuhan Pasal 16 ayat (1) huruf m UJN, dan akta yang tidak memenuhi syarat kehadiran fisik tersebut hanya memiliki kekuatan pembuktian sebagai akta di bawah tangan (Islam et al., 2023).

Subekti menerangkan bahwa akta otentik memiliki tiga lapis kekuatan pembuktian. Pertama, kekuatan pembuktian lahiriah (*uitwendige bewijskracht*), yakni akta yang membuktikan dirinya sendiri sebagai akta otentik tanpa pembuktian tambahan. Kedua, kekuatan pembuktian formal (*formele bewijskracht*), yakni apa yang dinyatakan dalam akta oleh pejabat dianggap benar terjadi. Ketiga, kekuatan pembuktian materiil (*materiele bewijskracht*), yakni isi akta dianggap terbukti terhadap siapa pun kecuali dapat dibuktikan sebaliknya (Subekti, 2008). Ketiga lapis kekuatan pembuktian ini hanya dapat melekat pada akta jika syarat-syarat UJN dan KUH Perdata terpenuhi secara kumulatif.

Konsekuensi degradasi akta otentik menjadi akta di bawah tangan sangat signifikan. Rachmawati dan Silviana menjelaskan bahwa akta di bawah tangan hanya memiliki kekuatan pembuktian formal apabila diakui oleh pihak yang menandatangani. Jika pihak tersebut menyangkal tanda tangannya, beban pembuktian beralih kepada pihak yang mengajukan akta tersebut. Akibatnya, untuk diajukan sebagai alat bukti di pengadilan, akta yang terdegradasi memerlukan alat bukti tambahan berupa saksi, persangkaan, atau sumpah (Rachmawati & Silviana, 2025). Ketidakpastian ini bukan hanya merugikan para pihak secara individual, tetapi juga melemahkan

kepercayaan publik terhadap sistem kenotariatan secara keseluruhan. Loleh, Thalib, dan Towadi mengingatkan bahwa ketidakpastian hukum ini dapat menghambat investasi dan memperlambat layanan hukum di era digital (Loleh et al., 2025).

### 3.2 Dimensi Filosofis Kehadiran: Pergeseran Epistemik dari Fisik ke Virtual

Untuk menjawab pertanyaan apakah *cyber notary* merupakan fiksi hukum atau perkembangan hukum yang sah, perlu dilakukan analisis terhadap konsep “kehadiran” dalam tiga dimensi filosofis: epistemologi, ontologi, dan aksiologi. Dewi dan Puspawati menjelaskan bahwa paradigma *cyber notary* yang berkembang di Indonesia cenderung memaknainya sebagai modernisasi pelaksanaan jabatan notaris, sementara paradigma asal (Amerika Serikat dan Prancis) menempatkannya sebagai instrumen untuk menghadirkan kepastian hukum dalam transaksi elektronik di *cyberspace*. Kedua paradigma ini memiliki implikasi yang berbeda terhadap konsep kehadiran (Dewi & Puspawati, 2025).

Dari perspektif ABA yang dikutip oleh Dewi dan Puspawati, *cyber notary* semula tidak dimaksudkan untuk menggantikan kehadiran fisik dalam pembuatan akta konvensional. Ia dirancang sebagai mekanisme untuk memberikan legitimasi hukum bagi transaksi yang *memang terjadi di ruang siber*, bukan untuk memindahkan pelaksanaan jabatan notaris konvensional ke dalam medium digital (Dewi & Puspawati, 2025). Kerancuan antara dua paradigma ini menjadi pangkal kebingungan dalam regulasi yang ada saat ini.

Karena itu, pertanyaan yang paling mendesak bukan sekadar “apakah *cyber notary* boleh dilakukan?” melainkan “apa yang sebenarnya dikerjakan oleh kehadiran fisik selama ini, dan bisakah teknologi menggantikan fungsi itu secara substantif?” Dari perspektif epistemologi, kehadiran fisik berfungsi sebagai mekanisme untuk memperoleh pengetahuan langsung (*first-hand knowledge*) bagi notaris. Notodisoerjo menjelaskan bahwa kehadiran di hadapan notaris memiliki fungsi ganda: secara formal sebagai syarat prosedural dan secara substansial memungkinkan notaris melakukan verifikasi identitas, menilai kecakapan hukum, serta menyaksikan kehendak bebas para penghadap (Notodisoerjo, 1993). Pengetahuan yang diperoleh notaris melalui kehadiran fisik bersifat total dan tidak termediasi: ia dapat membaca bahasa tubuh, mendeteksi tekanan atau paksaan, serta menilai kondisi mental penghadap secara langsung. Ghani dan Priyono menegaskan bahwa tanpa kehadiran fisik, notaris tidak dapat memverifikasi identitas secara langsung, termasuk keaslian tanda tangan dan sidik jari (Ghani & Priyono, 2025).

Dalam kehadiran virtual, karakter pengetahuan notaris berubah secara mendasar menjadi pengetahuan yang termediasi (*mediated knowledge*). Notaris mengamati para pihak melalui perangkat teknologi berupa kamera, mikrofon, dan layar monitor yang memiliki keterbatasan inheren. Rachmawati dan Silviana mengidentifikasi dalam penelitian mereka bahwa para notaris dan pejabat Kementerian Hukum dan HAM sepakat bahwa kehadiran virtual belum dapat memberikan jaminan verifikasi identitas yang setara dengan kehadiran fisik, terutama untuk keperluan penandatanganan akta dan pelekatan sidik jari (Rachmawati & Silviana, 2025). Wiyarta dan Silviana menambahkan bahwa meskipun teknologi biometrik dan otentikasi digital telah berkembang pesat, penerapannya dalam hukum Indonesia masih menghadapi hambatan regulasi dan pemahaman teknis di kalangan notaris (Wiyarta & Silviana, 2025).

Dari perspektif ontologi, kehadiran fisik bersifat presentasional: notaris dan penghadap hadir sebagai diri mereka sendiri dalam ruang dan waktu yang sama. Kehadiran virtual bersifat representasional: notaris berinteraksi bukan dengan penghadap itu sendiri, melainkan dengan citra digitalnya. Perbedaan ontologis ini tidak sepele. Dalam kehadiran virtual, selalu terdapat risiko bahwa representasi digital yang notaris saksikan berbeda dengan realitas penghadap yang sesungguhnya, baik karena teknologi *deepfake*, rekayasa latar belakang, atau karena orang yang tampil di layar bukan orang yang berhak. Dewi dan Puspawati menegaskan bahwa inilah yang membuat konsep “menghadap” dalam UUN sulit dipersamakan dengan pertemuan melalui video konferensi tanpa perubahan regulasi (Dewi & Puspawati, 2025).

Dari perspektif aksiologi, kehadiran fisik mengandung dimensi ritual dan kehormatan yang memberikan bobot psikologis-sosial pada perbuatan hukum. Prakoso dan Sudarwanto mengingatkan bahwa dalam tradisi hukum kenotariatan, menghadap notaris merupakan proses yang memiliki signifikansi seremonial yang menegaskan keseriusan dan mengikat perbuatan hukum (Prakoso & Sudarwanto, 2025). Loleh, Thalib, dan Towadi mencatat bahwa masyarakat Indonesia secara umum masih menempatkan kepercayaan terhadap otentisitas dokumen pada interaksi fisik secara langsung, dan kepercayaan terhadap dokumen elektronik perlu dibangun secara bertahap melalui edukasi serta pembuktian manfaat nyata (Loleh et al., 2025).

Dari ketiga dimensi analisis di atas, dapat disimpulkan bahwa kehadiran fisik bukan sekadar syarat formal-prosedural, melainkan mekanisme epistemik yang menjamin kualitas pengetahuan notaris, mekanisme ontologis yang memastikan keaslian identitas penghadap, serta mekanisme aksiologis yang memberikan bobot seremonial pada perbuatan hukum. Pergeseran ke kehadiran virtual merupakan pergeseran epistemik yang mengubah ketiga fungsi ini. Notodisoerjo sendiri telah menggariskan bahwa kepercayaan yang diberikan undang-undang kepada

akta otentik didasarkan pada asumsi bahwa notaris telah melihat, mendengar, dan menyaksikan sendiri apa yang dicantumkan dalam akta (Notodisoerjo, 1993). Jika asumsi ini tidak dapat dipenuhi melalui kehadiran virtual karena keterbatasan teknologi dan risiko manipulasi digital, maka akta yang dihasilkan memang dapat disebut sebagai “fiksi hukum”: mengaku otentik, tetapi tidak memiliki dasar epistemik yang memadai. Subekti menegaskan bahwa kekuatan pembuktian sempurna hanya dapat diberikan oleh undang-undang kepada akta yang dibuat oleh pejabat yang benar-benar menyaksikan peristiwa hukum yang tercatat (Subekti, 2008). Dalam kerangka hukum progresif Rahardjo, ketaatan pada syarat kehadiran fisik bukan sekadar formalisme—ia adalah penjaga substansi kebenaran yang dicatat oleh notaris. Melemahkannya tanpa kompensasi epistemik yang memadai berarti melemahkan kepercayaan publik yang menjadi fondasi sistem kenotariatan itu sendiri (Rahardjo, 2009).

### 3.3 Tantangan Keamanan dan Posisi Notaris sebagai Pengendali Data Pribadi

Implementasi *cyber notary* tidak hanya memunculkan persoalan tentang kekuatan pembuktian akta, tetapi juga menempatkan notaris dalam posisi hukum baru yang belum sepenuhnya diatur: sebagai pengendali data pribadi. Dalam kaitan tersebut, Najib mengkaji secara mendalam bahwa prosedur pelaksanaan *cyber notary* mengharuskan pengumpulan, pemrosesan, dan penyimpanan data pribadi para penghadap secara elektronik, yang berarti notaris tunduk pada ketentuan UU PDP (Najib, 2023). Dari sisi teknis, Munafan, Nuzulia, dan Ali menemukan bahwa penyimpanan protokol notaris secara digital, termasuk melalui sistem *blockchain*, membawa risiko peretasan, virus, dan kehilangan data yang tidak terdapat pada sistem konvensional (Munafan et al., 2025). Terlepas dari berbagai risiko tersebut, Anggita dan Nuzulia menegaskan bahwa tanggung jawab hukum notaris tetap melekat sepenuhnya pada akta yang dibuatnya, meskipun teknologi menjadi alat bantu dalam proses pembuatan akta, karena tanggung jawab tersebut tidak dapat dialihkan kepada sistem atau perangkat yang digunakan (Anggita & Kumala Sari, 2025).

UU PDP mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya. Dalam konteks *cyber notary*, data yang dikumpulkan notaris meliputi identitas diri, data biometrik, informasi keuangan, dan data hukum—seluruhnya merupakan data pribadi yang sensitif dan tidak jarang bersifat lintas platform. Najib menegaskan bahwa notaris dalam hal ini bertindak sebagai pengendali data pribadi (*personal data controller*) yang memiliki tanggung jawab penuh atas keamanan dan kerahasiaan data yang dikelola (Najib, 2023).

Pasal 27 UU PDP mewajibkan pengendali data pribadi untuk memproses data secara terbatas, spesifik, sah secara hukum, dan transparan. Pasal 16 sampai Pasal 18 UU PDP mengatur prosedur pemrosesan data pribadi secara rinci, termasuk syarat persetujuan subjek data dan tujuan pemrosesan yang sah. Dalam praktik *cyber notary*, notaris tidak hanya harus memenuhi syarat-syarat UUJN untuk keabsahan akta, tetapi juga harus memastikan bahwa seluruh proses pemrosesan data mematuhi ketentuan UU PDP. Kegagalan pada salah satu syarat ini tidak hanya memunculkan sanksi administratif dan pidana, tetapi juga berpotensi menggugurkan syarat formil pembuatan akta apabila data yang dikumpulkan tidak sah secara hukum (Najib, 2023).

Pasal 46 ayat (1) UU PDP mewajibkan pengendali data untuk menyampaikan pemberitahuan tertulis paling lambat 3 kali 24 jam kepada subjek data dan lembaga yang berwenang apabila terjadi kegagalan dalam perlindungan data pribadi, dan Pasal 47 UU PDP menegaskan tanggung jawab pengendali atas kegagalan tersebut. Dalam konteks kenotariatan, kegagalan perlindungan data ini dapat terjadi kapan saja, mulai dari peretasan sistem, kebocoran data identitas penghadap, hingga kerusakan atau kehilangan minuta akta digital.

Implikasi pidana dari kegagalan ini juga tidak ringan. Pasal 67 UU PDP mengancam dengan pidana penjara hingga 5 tahun bagi siapa pun yang dengan sengaja memperoleh, mengungkapkan, atau menggunakan data pribadi orang lain tanpa hak, dan Pasal 68 UU PDP mengancam dengan pidana penjara hingga 6 tahun bagi pelaku yang memalsukan data pribadi. Munafan, Nuzulia, dan Ali menemukan bahwa ancaman kejahatan siber terhadap data notaris, mulai dari *hacking*, *skimming*, hingga pencurian identitas, bukan ancaman hipotetis melainkan risiko nyata yang semakin berkembang seiring kecanggihan para pelaku kejahatan siber (Munafan et al., 2025).

Perlindungan terhadap kejahatan siber juga diatur dalam Pasal 30 UU ITE yang mengkriminalkan setiap akses ilegal terhadap sistem elektronik milik orang lain. Wiyarta dan Silviana menekankan bahwa notaris, sebagai pejabat publik yang mengelola data dan informasi sensitif, harus memastikan bahwa sistem teknologi yang digunakan dalam *cyber notary* memenuhi standar keamanan yang andal, termasuk penggunaan enkripsi data, tanda tangan digital yang tersertifikasi, serta sistem otentikasi berlapis (Wiyarta & Silviana, 2025).

Najib mengusulkan bahwa prosedur pelaksanaan *cyber notary* harus mengikuti ketentuan pembuatan akta secara manual dengan perbedaan hanya pada media “menghadap” yang dilakukan melalui video konferensi, dan setiap akta elektronik yang dibuat harus mencantumkan IP address perangkat notaris yang terdaftar di Kementerian Hukum dan HAM sebagai mekanisme pengawasan (Najib, 2023). Pendekatan ini memperlihatkan bahwa tanggung

jawab notaris dalam era *cyber notary* bersifat berlapis: tidak hanya bertanggung jawab atas otentisitas akta, tetapi juga atas keamanan infrastruktur digital yang digunakan.

### 3.4 Rekonseptualisasi Kehadiran: Teori Hukum Progresif dan Model Hybrid Berbasis Risiko

Persoalan *cyber notary* pada akhirnya adalah persoalan tentang bagaimana hukum merespons perubahan sosial yang dibawa oleh teknologi. Lawrence M. Friedman menganalisis efektivitas hukum melalui tiga komponen: struktur hukum (kelembagaan dan mekanisme penegakan), substansi hukum (norma-norma yang berlaku), dan budaya hukum. Dalam konteks *cyber notary*, ketiga komponen ini sama-sama bermasalah: substansi hukum bertentangan satu sama lain (UUJN vs. UU ITE), struktur kelembagaan pengawasan notaris digital belum terbentuk, dan budaya hukum masyarakat belum siap menerima otentisitas digital secara penuh. Friedman mendefinisikan budaya hukum (*legal culture*) sebagai sikap, nilai, dan opini masyarakat terkait hukum dan sistem hukum, serta menempatkannya sebagai kekuatan sosial yang menentukan bagaimana hukum digunakan, dihindari, atau disalahgunakan (Friedman, 1975).

Satjipto Rahardjo dalam teori hukum progresifnya menegaskan bahwa hukum dibuat untuk manusia, bukan manusia untuk hukum. Hukum harus terus berorientasi pada kebenaran dan keadilan, dan jika norma hukum yang ada tidak lagi mampu melayani kebutuhan manusia secara substantif, maka hukum harus berani melakukan terobosan (Rahardjo, 2009). Dalam konteks *cyber notary*, teori ini mengajarkan bahwa ketaatan buta pada paradigma kehadiran fisik, ketika teknologi telah menyediakan alternatif yang dapat menjamin substansi verifikasi, merupakan bentuk formalisme hukum yang kontraproduktif. Teori hukum progresif juga mengajarkan bahwa terobosan harus dilakukan dengan kehati-hatian, terutama ketika substansi yang ingin dilindungi—kekuatan pembuktian akta otentik—menyangkut kepentingan hukum masyarakat yang sangat vital.

Dewi dan Puspawati merumuskan sintesis yang tepat: perdebatan *cyber notary* di Indonesia selama ini stagnan karena mencampuradukkan dua konsep yang berbeda, yaitu *cyber notary* sebagai instrumen kepastian hukum dalam transaksi elektronik dan modernisasi jabatan notaris melalui teknologi. Pengaturan *cyber notary* hendaknya beranjak dari jenis transaksi elektronik yang memerlukan peran notaris, relevansi wilayah jabatan, instrumen hukum yang tepat, kekuatan pembuktian dan penyelesaian sengketa, serta keahlian khusus yang dibutuhkan oleh notaris (Dewi & Puspawati, 2025). Pendekatan ini menghindari dua kesalahan sekaligus: menolak *cyber notary* secara total atas nama asas tradisional dan menerima *cyber notary* secara penuh tanpa memperhatikan substansi kekuatan pembuktian.

Ghani dan Priyono menegaskan bahwa sinkronisasi antarperaturan perundang-undangan, penguatan infrastruktur teknologi, serta peningkatan kompetensi sumber daya manusia merupakan faktor penentu keberhasilan implementasi *cyber notary* di Indonesia (Ghani & Priyono, 2025). Pandangan ini selanjutnya dipertegas oleh Loleh, Thalib, dan Towadi yang mengidentifikasi langkah-langkah strategis yang diperlukan: penyusunan regulasi khusus, peningkatan kapasitas SDM notaris, penguatan infrastruktur teknologi, dan penguatan perlindungan data (Loleh et al., 2025). Dalam konteks yang sama, Prakoso dan Sudarwanto menambahkan bahwa pengaturan lebih lanjut melalui peraturan pemerintah atau peraturan menteri dapat menjadi solusi untuk menjembatani ketidaksinkronan hukum yang ada saat ini (Prakoso & Sudarwanto, 2025). Di sisi lain, Lubis et al. menyoroti bahwa negara-negara penganut sistem Civil Law menghadapi hambatan yang lebih besar dalam penerapan *cyber notary* dibandingkan dengan negara Common Law, karena dalam sistem Civil Law notaris adalah pejabat publik yang aktanya memperoleh kekuatan pembuktian sempurna secara *ex lege*—kekuatan ini bersumber dari fungsi verifikasi langsung yang ia emban, bukan dari formalitas administratif belaka. Inilah mengapa model hybrid berbasis risiko—bukan liberalisasi digital penuh—menjadi pilihan yang paling konsisten dengan tradisi hukum Civil Law yang dianut Indonesia (Lubis et al., 2022).

Berdasarkan analisis di atas, penulis mengusulkan model rekonseptualisasi hybrid berbasis risiko. Model ini tidak menolak *cyber notary* secara keseluruhan, tetapi membedakan mode kehadiran yang diperlukan berdasarkan tingkat risiko dan kompleksitas perbuatan hukum yang dituangkan dalam akta. Najib memberikan dukungan terhadap pendekatan gradual ini dengan menegaskan bahwa prosedur *cyber notary* pada prinsipnya dapat mengikuti ketentuan pembuatan akta secara manual selama substansi verifikasi terpenuhi (Najib, 2023).

Tabel 1. Model Rekonseptualisasi Hybrid Kehadiran dalam Cyber Notary

Kategori Akta	Tingkat Risiko	Mode Kehadiran	Syarat Tambahan
Peralihan hak tanah, wasiat, perjanjian kawin	Tinggi	Fisik wajib	Sidik jari pada minuta akta
Pendirian PT, fidusia, kredit perbankan	Sedang	Hybrid: fisik atau virtual dengan syarat	Biometrik tersertifikasi, TTE tersertifikasi, audit trail blockchain, IP address terdaftar

Legalisasi, salinan akta	waarmerking,	Rendah	Virtual penuh	Platform tersertifikasi, audit trail komprehensif
--------------------------	--------------	--------	---------------	---

Sumber: Konstruksi Penulis, 2026

Model hybrid ini dibangun berdasarkan tiga prinsip. Pertama, diferensiasi berdasarkan tingkat risiko akta. Tidak semua akta memerlukan tingkat verifikasi epistemik yang sama. Akta peralihan hak atas benda tidak bergerak, wasiat, dan perjanjian perkawinan memiliki konsekuensi hukum yang *irreversibel* dan bernilai sangat tinggi, sehingga jaminan epistemik berupa kehadiran fisik tetap diperlukan. Munafan, Kumalasari, dan Ali mendukung pendekatan yang berbeda-beda berdasarkan jenis perbuatan hukum ini, mengingat tingkat risiko kebocoran dan manipulasi data yang berbeda untuk setiap jenis akta (Munafan et al., 2025).

Kedua, penguatan standar keamanan digital sebagai kompensasi epistemik. Untuk akta kategori sedang yang diperbolehkan secara hybrid, diperlukan standar keamanan yang setara dengan jaminan yang selama ini diberikan oleh kehadiran fisik. Standar ini meliputi penggunaan tanda tangan elektronik yang tersertifikasi oleh lembaga yang diakui negara, verifikasi biometrik berlapis, pencatatan jejak audit (*audit trail*) yang tidak dapat dimanipulasi, serta pendaftaran alamat IP notaris. Wiyarta dan Silviana menekankan bahwa standar keamanan ini bukan hanya pelengkap teknis, melainkan syarat minimal agar pengetahuan yang diperoleh notaris melalui kehadiran virtual memiliki derajat keandalan yang layak untuk mendukung kekuatan pembuktian akta (Wiyarta & Silviana, 2025).

Ketiga, transformasi budaya hukum secara bertahap. Friedman menegaskan bahwa efektivitas hukum sangat bergantung pada kesesuaian antara norma hukum dan budaya hukum masyarakat tempat hukum diterapkan (Friedman, 1975). Sejalan dengan pandangan Friedman, Satjipto Rahardjo mengingatkan bahwa perubahan hukum yang tidak diiringi perubahan budaya akan menghasilkan kegagalan dalam implementasinya (Rahardjo, 2009). Bertolak dari pemikiran tersebut, implementasi model hybrid harus dilakukan secara bertahap: dimulai dari kategori akta risiko rendah dan wilayah dengan infrastruktur digital yang memadai, kemudian diperluas seiring dengan peningkatan kesiapan teknologi, kompetensi notaris, serta kepercayaan masyarakat. Dewi dan Puspawati merekomendasikan agar pengaturan *cyber notary* berfokus pada jenis transaksi elektronik yang memang memerlukan peran notaris, sehingga tidak terjadi kerancuan antara modernisasi pelaksanaan jabatan dan perlindungan hukum transaksi siber (Dewi & Puspawati, 2025). Dalam setiap tahap implementasi, kepatuhan terhadap UU PDP harus diperlakukan sebagai syarat konstitutif, bukan sekadar kewajiban administratif yang bersifat sampingan. Artinya, akta elektronik yang dibuat tanpa memenuhi standar perlindungan data pribadi berdasarkan UU PDP tidak hanya menimbulkan sanksi pidana bagi notaris, tetapi juga berpotensi melanggar syarat formil pembuatan akta apabila data yang menjadi dasar verifikasi identitas penghadap diperoleh atau diproses secara tidak sah.

#### 4. Kesimpulan

Artikel ini berangkat dari satu pertanyaan yang tampaknya teknis tetapi menyentuh hal yang sangat substansial: apakah hukum dapat mengakui kehadiran yang tidak benar-benar hadir? Jawaban atas pertanyaan ini ternyata tidak tunggal dan dua simpulan berikut mencoba menggambarkan kompleksitasnya.

Pertama, disharmoni norma antara UJN dan UU ITE menghasilkan “jebakan normatif” yang menempatkan *cyber notary* dalam posisi hukum yang tidak pasti. UJN mendorong kewenangan notaris dalam transaksi elektronik melalui penjelasan Pasal 15 ayat (3), tetapi UU ITE mengecualikan akta notaris dari pengakuan sebagai dokumen elektronik melalui Pasal 5 ayat (4) huruf b. Konsekuensinya, akta notaris yang dibuat melalui mekanisme *cyber notary* berpotensi terdegradasi dari akta otentik menjadi akta di bawah tangan, sehingga kehilangan tiga lapis kekuatan pembuktian yang sempurna.

Melangkah dari implikasi normatif tersebut, dari perspektif filosofis terlihat bahwa pergeseran dari kehadiran fisik ke virtual sesungguhnya merupakan pergeseran epistemik: pengetahuan langsung notaris berubah menjadi pengetahuan yang termediasi teknologi, hubungan presentasional menjadi representasional, dan bobot ritual hukum berkurang. Selama teknologi belum mampu menjamin substansi epistemik yang setara dengan kehadiran fisik untuk semua jenis akta, akta yang diklaim otentik tanpa pemenuhan syarat fisik berpotensi menjadi fiksi hukum yang kehilangan landasan.

Penilaian ini tidak bersifat mutlak; ia bergantung pada kategori akta, tingkat risiko perbuatan hukum yang dituangkan, serta seberapa andal teknologi verifikasi yang digunakan. Untuk kategori akta tertentu, teknologi yang tepat dan standar keamanan yang ketat dapat menjadi kompensasi epistemik yang sah.

Kedua, rekonseptualisasi kehadiran dalam *cyber notary* dapat dilakukan melalui model hybrid berbasis risiko yang membedakan mode kehadiran sesuai dengan kategori akta. Akta risiko tinggi tetap mensyaratkan kehadiran fisik karena konsekuensi hukumnya bersifat *irreversibel*. Akta risiko sedang dapat dilakukan secara hybrid dengan syarat keamanan digital yang ketat sebagai kompensasi epistemik. Akta risiko rendah dapat dilakukan sepenuhnya

secara virtual. Model ini sejalan dengan teori hukum progresif Rahardjo yang menuntut hukum berani berterobos untuk melayani kebutuhan manusia, sekaligus dengan teori budaya hukum Friedman yang menggariskan perlunya transformasi budaya yang bertahap dan terencana.

Sebagai rekomendasi, pembentuk undang-undang perlu segera mengambil tiga langkah. Pertama, merevisi Pasal 5 ayat (4) huruf b UU ITE dengan menambahkan pengecualian yang terukur: ketentuan tersebut tetap berlaku bagi akta notaris kategori risiko tinggi yang mensyaratkan kehadiran fisik, namun dikecualikan untuk akta notaris elektronik kategori risiko rendah dan sedang yang dibuat sesuai mekanisme, standar verifikasi identitas, serta standar keamanan yang ditetapkan dalam peraturan pemerintah. Kedua, menerbitkan peraturan pemerintah yang mengatur secara rinci mekanisme, standar keamanan, dan pengawasan *cyber notary* berdasarkan kategorisasi risiko akta. Ketiga, mengintegrasikan UU PDP secara eksplisit dalam kerangka hukum kenotariatan, sehingga tanggung jawab notaris sebagai pengendali data pribadi memiliki dasar dan batas yang jelas, dan kegagalan dalam perlindungan data memiliki konsekuensi hukum yang terukur tanpa serta-merta membatalkan keabsahan akta.

## Referensi

- Adjie, H. (2013). *Hukum notaris Indonesia: Tafsir tematik terhadap UU No. 30 Tahun 2004 tentang Jabatan Notaris*. PT Refika Aditama.
- Anggita, S. N., & Kumala Sari, N. (2025). Batasan tanggung jawab hukum notaris terhadap pembuatan akta autentik menggunakan artificial intelligence. *Acta Comitas: Jurnal Hukum Kenotariatan*, 10(3), 465–477. <https://doi.org/10.24843/AC.2025.v10.i03.pl>
- Dewi, N. P. K. R., & Puspawati, A. A. I. (2025). Analisis perkembangan paradigma cyber notary: Sintesis atas problematika pengaturan cyber notary di Indonesia. *Repertorium: Jurnal Ilmiah Hukum Kenotariatan*, 14(2). <https://doi.org/10.28946/rpt.v14i2.4905.5115>
- Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.
- Ghani, A. A., & Priyono, E. A. (2025). Analisis disharmonisasi regulasi dan tantangan implementasi cyber notary di Indonesia. *Jurnal Ilmu Hukum, Humaniora dan Politik*, 5(5). <https://doi.org/10.38035/jihhp.v5i5>
- Islam, A. Z., Kurniawan, & Hirsanuddin. (2023). Keabsahan akta notaris yang menggunakan cyber notary sebagai akta otentik. *UNES Law Review*, 6(2), 4524–4532. <https://doi.org/10.31933/unesrev.v6i2>
- Kiswah, M., Wibisono, W. F. R., Setyawan, F., & Adonara, F. F. (2025). Keabsahan perjanjian elektronik dan penyelesaian sengketa wanprestasi debitur pinjaman online. *Jurnal Magister Hukum PERSPEKTIF*, 16(2), 90–106.
- Loleh, R. R., Thalib, M. C., & Towadi, M. (2025). Legalitas digital di era global: Cyber notary sebagai pilar baru otentifikasi dokumen asing di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(3). <https://doi.org/10.61104/alz.v3i3.1732>
- Lubis, I., Murwadi, T., Siregar, M., Sukarja, D., Robert, H., D., & Ketaren, M. M. (2022). Comparison of civil law regarding the implementation of cyber notary in countries with common law and civil law traditions. *Jurnal IUS Kajian Hukum dan Keadilan*, 10(1), 1–11. <https://doi.org/10.29303/ius.v10i1.981>
- Makarim, E. (2013). *Notaris & transaksi elektronik: Kajian hukum tentang cybernotary atau electronic notary* (Ed. ke-2). Rajawali Pers.
- Marzuki, P. M. (2017). *Penelitian hukum*. Kencana.
- Munafan, R. A., Kumalasari, N., & Ali, M. (2025). Perlindungan hukum keamanan data cyber notary dalam penyimpanan protokol notaris di blockchain. *Global Research and Innovation Journal (GREAT)*, 1(2), 399–406.
- 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. <https://doi.org/10.23920/acta.v7i1.1680>
- Notodisoejo, R. S. (1993). *Hukum notariat di Indonesia: Suatu pengantar*. Raja Grafindo Persada.
- Prakoso, S. B. A., & Sudarwanto, A. S. (2025). Hambatan dan peluang notaris online (cyber notary) di Indonesia dalam memasuki cyber space. *Indonesian Journal of Social Sciences and Humanities*, 5(1), 71–75.
- Rachmawati, T. F., & Silviana, A. (2025). Tinjauan hukum keabsahan tanda tangan elektronik dalam akta notaris berdasarkan konsep cyber notary. *Inovasi: Jurnal Sosial Humaniora dan Pendidikan*, 4(2), 171–180. <https://doi.org/10.55606/inovasi.v4i2.4025>
- Rahardjo, S. (2009). *Hukum progresif: Sebuah sintesa hukum Indonesia*. Genta Publishing.
- Subekti, R. (2008). *Hukum pembuktian*. Pradnya Paramita.
- Tempo. (2024, 23 September). Gagal total negara melindungi data pribadi. *Koran Tempo, Editorial*. <https://koran.tempo.co/read/editorial/490002/pembobolan-data-pribadi-npwp>
- Tempo.co. (2024). Polemik data pribadi: 5 kasus kebocoran data di Indonesia selama 2023–2024. <https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924>
- Wiyarta, Z., & Silviana, A. (2025). Urgensi peran notaris dalam menjamin legalitas transaksi elektronik: Tinjauan hukum jabatan notaris. *Inovasi: Jurnal Sosial Humaniora dan Pendidikan*, 4(1), 389–404. <https://doi.org/10.55606/inovasi.v4i1.4223>
- Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek).
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.
- Undang-Undang Nomor 2 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 30 Tahun 2004 tentang Jabatan Notaris. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 3, Tambahan Lembaran Negara Republik Indonesia Nomor 5491.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.