

Keabsahan Persetujuan para Pihak dalam Akta Notaris yang Menggunakan Biometric Verification Ditinjau dari Hukum Perjanjian dan Perlindungan Data Pribadi

Tangkas Ihza Pratama Aji¹, Ery Agus Priyono²

¹⁻² Fakultas Hukum, Universitas Diponegoro Semarang, Indonesia

*Penulis Korespondensi: tangkasihzapratama@gmail.com

Abstract. Digital transformation in notarial practice has encouraged the use of biometric verification as a means of strengthening the identification of parties involved in the execution of notarial deeds. However, successful biometric verification raises legal questions regarding whether identity authentication can be equated with valid consent under contract law and how the biometric data of appearing parties should be protected. This study aims to analyze the validity of parties' consent in notarial deeds using biometric verification from the perspectives of contract law and personal data protection. It employs normative legal research using statutory and conceptual approaches by examining contract law, notarial law, electronic transactions, and personal data protection. The findings indicate that biometric verification merely serves as a supporting instrument for identity authentication and cannot automatically establish the existence of valid agreement as required under Article 1320 of the Indonesian Civil Code. Biometric data also requires heightened protection because it constitutes specific personal data. This study proposes a dual consent model that distinguishes consent to the substance of a legal transaction from consent to biometric data processing, thereby strengthening legal certainty, data protection, and the evidentiary integrity of notarial transactions.

Keywords: Biometric Verification; Consent; Contract Law; Notarial Deed; Personal Data Protection.

Abstrak. Transformasi digital dalam bidang kenotariatan mendorong penggunaan *biometric verification* sebagai sarana untuk memperkuat identifikasi para pihak dalam pembuatan akta notaris. Namun, keberhasilan verifikasi biometrik menimbulkan persoalan mengenai apakah autentikasi identitas dapat dipersamakan dengan persetujuan yang sah menurut hukum perjanjian serta bagaimana perlindungan terhadap data biometrik para penghadap. Penelitian ini bertujuan menganalisis keabsahan persetujuan para pihak dalam akta notaris yang menggunakan *biometric verification* berdasarkan hukum perjanjian dan rezim perlindungan data pribadi. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual melalui analisis terhadap hukum perjanjian, jabatan notaris, transaksi elektronik, serta perlindungan data pribadi. Hasil penelitian menunjukkan bahwa *biometric verification* hanya berfungsi sebagai instrumen pendukung autentikasi identitas dan tidak dapat secara otomatis membuktikan adanya kesepakatan sebagaimana disyaratkan dalam Pasal 1320 KUHPerdata. Data biometrik juga memerlukan perlindungan khusus karena termasuk data pribadi yang bersifat spesifik. Penelitian ini menawarkan model *dual consent* yang memisahkan persetujuan terhadap substansi perbuatan hukum dari persetujuan pemrosesan data biometrik untuk memperkuat kepastian hukum dan perlindungan para pihak.

Kata kunci: Akta Notaris; Persetujuan; Perjanjian Hukum; Perlindungan Data Pribadi; Verifikasi Biometrik.

1. LATAR BELAKANG

Transformasi digital telah mengubah cara subjek hukum mengidentifikasi diri, menyatakan kehendak, dan memberikan persetujuan dalam berbagai transaksi keperdataan. Perkembangan tanda tangan elektronik, sertifikasi elektronik, serta konsep *cyber notary* menunjukkan bahwa pembuktian identitas dan kehendak para pihak semakin bergeser dari mekanisme konvensional menuju mekanisme berbasis teknologi (Dewi et al., 2024; Hairunnisa, 2025; Rihhadatul'aisy et al., 2026). Dalam bidang kenotariatan, perkembangan tersebut memunculkan diskursus mengenai legalitas akta elektronik, penggunaan tanda tangan

elektronik, dan kepastian hukum *cyber notary* yang sampai saat ini masih menghadapi persoalan harmonisasi dengan karakter formal akta autentik (Irawati, 2024; Affan, 2025; Iwaldo, 2026). Salah satu perkembangan yang belum memperoleh perhatian memadai ialah penggunaan *biometric verification* berupa sidik jari, pengenalan wajah, iris, suara, atau karakteristik biologis lainnya sebagai sarana untuk memverifikasi identitas sekaligus mendukung proses pemberian persetujuan para pihak dalam pembuatan akta notaris.

Secara keperdataan, penggunaan *biometric verification* tidak dapat serta-merta dipersamakan dengan adanya persetujuan yang sah dalam suatu perjanjian. Pasal 1320 Kitab Undang-Undang Hukum Perdata menempatkan kesepakatan para pihak sebagai salah satu syarat sah perjanjian, sehingga persoalan utamanya bukan hanya apakah seseorang berhasil diidentifikasi secara teknis, tetapi apakah identitas yang terverifikasi tersebut benar-benar diikuti oleh pernyataan kehendak yang bebas, sadar, dan ditujukan untuk menimbulkan akibat hukum. Kajian mengenai tanda tangan elektronik telah banyak diarahkan pada validitas alat autentikasi dan pembuktian kehendak dalam transaksi elektronik, baik dalam perjanjian umum maupun transaksi perbankan (Fardela, 2024; Mugiyo, 2026; Fadhilah, 2024). Namun, autentikasi biometrik menghadirkan persoalan yang berbeda karena keberhasilan sistem mengenali karakteristik biologis seseorang belum dengan sendirinya membuktikan adanya *meeting of minds* sebagaimana dipersyaratkan dalam hukum perjanjian.

Persoalan tersebut menjadi lebih kompleks ketika *biometric verification* digunakan dalam konteks akta notaris yang secara hukum memiliki karakter formal dan kekuatan pembuktian khusus. Literatur mengenai tanda tangan elektronik pada akta notaris menunjukkan adanya perdebatan mengenai hubungan antara teknologi autentikasi dengan persyaratan formal pembuatan akta autentik, khususnya terkait kehadiran, pembacaan, penandatanganan, dan identifikasi para penghadap (Khairuddin, 2023; Marbun et al., 2026). Demikian pula, kajian mengenai *cyber notary* menempatkan kepastian hukum sebagai persoalan sentral karena digitalisasi fungsi notaris harus tetap mempertahankan autentisitas akta dan tanggung jawab personal notaris sebagai pejabat umum (Affan, 2025; Iwaldo, 2026; Rihhadatul'aisy et al., 2026). Dengan demikian, penggunaan biometrik tidak hanya menimbulkan pertanyaan apakah identitas seseorang telah terverifikasi, tetapi juga apakah proses tersebut dapat memenuhi atau mendukung unsur kesepakatan dan formalitas autentik yang menjadi dasar keabsahan akta.

Di sisi lain, data biometrik bukan sekadar instrumen teknis, melainkan bagian dari data pribadi yang memiliki tingkat sensitivitas tinggi karena melekat secara permanen pada karakteristik individu. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data

Pribadi menempatkan data biometrik sebagai data pribadi yang bersifat spesifik, sehingga pemrosesannya harus memenuhi dasar pemrosesan, tujuan yang sah, prinsip transparansi, keamanan, dan akuntabilitas. Permasalahan perlindungan data dalam praktik kenotariatan sebenarnya telah muncul dalam konteks penggunaan sistem elektronik yang mengharuskan notaris atau PPAT mengakses serta memproses data tertentu, sebagaimana terlihat dalam kajian mengenai kerahasiaan data wajib pajak dalam proses validasi melalui E-PHTB Notaris/PPAT (Supriyanti, 2023). Perkembangan sertifikat elektronik, penggunaan QR Code dalam dokumen pertanahan, dan digitalisasi dokumen hak atas tanah juga menunjukkan bahwa integrasi teknologi ke dalam pelayanan hukum selalu membawa konsekuensi terhadap autentisitas, keamanan, dan perlindungan informasi personal (Hadi, 2022; Oktaviani, 2023).

Dari perspektif perlindungan data pribadi, masalah yang lebih mendasar muncul karena konsep “persetujuan” dalam rezim perlindungan data tidak identik dengan “kesepakatan” dalam hukum perjanjian. Seseorang dapat memberikan persetujuan terhadap pemrosesan data biometriknya untuk tujuan verifikasi identitas, tetapi persetujuan tersebut belum tentu sekaligus merupakan persetujuan untuk terikat pada seluruh isi perjanjian yang dituangkan dalam akta notaris. Sebaliknya, seseorang mungkin telah menyatakan kehendaknya untuk membuat suatu perjanjian, tetapi pemrosesan data biometriknya tetap harus memiliki dasar hukum dan memenuhi prinsip perlindungan data pribadi secara tersendiri. Kajian mengenai transaksi elektronik, benda virtual, sertifikasi elektronik, dan *financial technology* memperlihatkan semakin kuatnya kebutuhan untuk membedakan aspek autentikasi teknologi dari konsekuensi hukum substantif yang lahir dari suatu transaksi (Rindasiwi, 2022; Hairunnisa, 2025; Yanti, 2025), sehingga penyamaan antara autentikasi biometrik dan persetujuan hukum berpotensi menimbulkan kekeliruan konseptual.

Risiko tersebut semakin penting apabila sistem biometrik mengalami kesalahan identifikasi, penyalahgunaan data, manipulasi identitas, atau digunakan tanpa informasi yang memadai kepada pemilik data. Dalam praktik transaksi yang berkaitan dengan aset bernilai tinggi, termasuk pertanahan, persoalan pemalsuan identitas dan penipuan dapat menimbulkan akibat hukum serius bagi para pihak serta pejabat yang terlibat, sehingga kebutuhan terhadap mekanisme verifikasi yang kuat harus tetap diimbangi dengan kontrol terhadap validitas kehendak dan tanggung jawab hukum (Rudi Margono, 2026). Teknologi memang dapat memperkuat proses identifikasi, tetapi ketergantungan berlebihan terhadap hasil verifikasi otomatis justru berpotensi menggeser fungsi notaris dari penilai langsung terhadap identitas dan kehendak penghadap menjadi sekadar pengguna hasil sistem elektronik. Dalam kerangka perlindungan hukum yang lebih luas, orientasi terhadap perlindungan hak individu tetap

penting ketika teknologi atau sistem kelembagaan digunakan untuk menentukan posisi hukum seseorang, meskipun kajian pada bidang lain memiliki objek perlindungan yang berbeda (Saputra et al., 2026).

Kajian terdahulu menunjukkan bahwa penelitian kenotariatan digital masih dominan membahas tanda tangan elektronik, legalitas akta elektronik, dan konsep *cyber notary*. Marbun et al. (2026), Fardela (2024), serta Khairuddin (2023) berfokus pada keabsahan tanda tangan elektronik dalam hubungannya dengan akta notaris, sedangkan Irawati (2024), Affan (2025), Iwaldo (2026), dan Rihhadatul'aisy et al. (2026) menempatkan legalitas serta kepastian hukum akta autentik elektronik dan *cyber notary* sebagai pusat kajian. Literatur lain berkembang pada pembuktian tanda tangan elektronik dalam perjanjian kredit, transaksi elektronik, sertifikasi elektronik, dan administrasi pertanahan digital (Mugiyanto, 2026; Dewi et al., 2024; Hadi, 2022; Oktaviani, 2023). Akan tetapi, masih terdapat celah konseptual mengenai hubungan antara tiga persoalan yang berbeda tetapi saling berkaitan, yakni validitas identifikasi biometrik, eksistensi kesepakatan sebagai syarat sah perjanjian, dan legalitas pemrosesan data biometrik sebagai data pribadi spesifik dalam proses pembuatan akta notaris.

Berdasarkan kesenjangan tersebut, penelitian mengenai keabsahan persetujuan para pihak dalam akta notaris yang menggunakan *biometric verification* memiliki urgensi teoritis sekaligus praktis. Secara teoritis, penelitian ini diperlukan untuk menentukan batas konseptual antara verifikasi identitas, persetujuan pemrosesan data pribadi, dan kesepakatan sebagai pernyataan kehendak dalam hukum perjanjian, sehingga penggunaan teknologi tidak mengaburkan unsur subjektif yang menentukan sah atau tidaknya suatu perbuatan hukum. Secara praktis, hasil penelitian diharapkan dapat memberikan parameter bagi notaris mengenai kedudukan *biometric verification*, kewajiban memperoleh dan membuktikan persetujuan, batas pemrosesan data biometrik, serta konsekuensi hukum apabila terjadi cacat kehendak atau pelanggaran perlindungan data pribadi. Oleh karena itu, penelitian ini diarahkan untuk menganalisis keabsahan persetujuan para pihak yang diverifikasi melalui teknologi biometrik dalam pembuatan akta notaris berdasarkan hukum perjanjian serta membangun konstruksi perlindungan hukum terhadap data biometrik para penghadap berdasarkan rezim perlindungan data pribadi.

2. KAJIAN TEORITIS

Kajian pertama bertumpu pada teori hukum perjanjian, khususnya mengenai kesepakatan sebagai salah satu syarat sah perjanjian sebagaimana tercermin dalam Pasal 1320 KUHPerdara. Kesepakatan tidak hanya menunjukkan adanya tindakan formal para pihak, tetapi juga

mencerminkan kehendak yang bebas, sadar, dan tidak mengandung cacat kehendak. Dalam konteks transaksi digital, tanda tangan elektronik dan instrumen autentikasi dapat berfungsi sebagai sarana pembuktian identitas dan tindakan hukum, tetapi tidak serta-merta menggantikan unsur kehendak sebagai dasar terbentuknya persetujuan (Dewi et al., 2024; Fardela, 2024; Mugiyanto, 2026). Oleh karena itu, *biometric verification* secara teoretis harus ditempatkan sebagai instrumen autentikasi yang mendukung pembuktian identitas, sedangkan keabsahan persetujuan tetap ditentukan oleh terpenuhinya unsur kehendak para pihak dalam hubungan kontraktual.

Kajian kedua menggunakan teori akta autentik dan kepastian hukum dalam praktik kenotariatan. Akta notaris memperoleh kekuatan autentiknya karena dibuat oleh atau di hadapan pejabat yang berwenang serta memenuhi bentuk dan prosedur yang ditentukan oleh peraturan perundang-undangan. Perkembangan *cyber notary*, akta elektronik, dan tanda tangan elektronik menunjukkan adanya kebutuhan untuk menyesuaikan praktik kenotariatan dengan teknologi tanpa mengurangi unsur kehadiran, identifikasi, pembacaan, penandatanganan, dan tanggung jawab notaris dalam memastikan kehendak penghadap (Khairuddin, 2023; Irawati, 2024; Affan, 2025; Iwaldo, 2026). Dalam perspektif ini, penggunaan biometrik harus dipahami sebagai sarana tambahan yang memperkuat identifikasi dan integritas proses, bukan sebagai pengganti fungsi yuridis notaris dalam membentuk dan memastikan keautentikan akta.

Kajian ketiga menggunakan teori perlindungan data pribadi yang menempatkan data biometrik sebagai informasi yang membutuhkan perlindungan khusus karena melekat secara langsung pada karakteristik biologis seseorang. Pemrosesan data semacam ini harus didasarkan pada tujuan yang jelas, pembatasan penggunaan, keamanan, transparansi, dan akuntabilitas, sehingga persetujuan terhadap penggunaan data biometrik tidak dapat disamakan dengan persetujuan terhadap isi perjanjian. Persoalan kerahasiaan dan keamanan data dalam sistem elektronik yang digunakan oleh notaris/PPAT telah menunjukkan pentingnya perlindungan terhadap informasi pribadi dalam proses pelayanan hukum digital (Supriyanti, 2023; Hairunnisa, 2025). Dengan demikian, perlindungan hukum terhadap penggunaan *biometric verification* perlu dibangun melalui pemisahan antara persetujuan kontraktual dan persetujuan pemrosesan data, sehingga hak keperdataan dan hak atas perlindungan data para penghadap dapat terlindungi secara seimbang.

3. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian hukum normatif dengan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menganalisis ketentuan hukum yang berkaitan dengan syarat sah perjanjian, kedudukan dan kewenangan notaris, penggunaan sistem elektronik, serta perlindungan data pribadi, terutama Kitab Undang-Undang Hukum Perdata, Undang-Undang tentang Jabatan Notaris, Undang-Undang tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pendekatan konseptual digunakan untuk mengkaji konsep persetujuan, kesepakatan, autentikasi identitas, *biometric verification*, kehendak para pihak, akta autentik, serta perlindungan data biometrik. Kedua pendekatan tersebut digunakan untuk menentukan apakah keberhasilan verifikasi biometrik dapat diposisikan sebagai bukti adanya persetujuan yang sah atau hanya berfungsi sebagai instrumen verifikasi identitas dalam proses pembuatan akta notaris.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan hukum perjanjian, jabatan notaris, transaksi elektronik, dan perlindungan data pribadi, sedangkan bahan hukum sekunder berupa buku, artikel jurnal, tesis, disertasi, serta hasil penelitian yang membahas tanda tangan elektronik, *cyber notary*, sertifikasi elektronik, dan digitalisasi pelayanan hukum. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan teknik inventarisasi, klasifikasi, dan sistematisasi berdasarkan isu hukum yang diteliti. Seluruh bahan hukum dianalisis secara kualitatif menggunakan metode preskriptif-analitis dengan menafsirkan hubungan antara norma hukum perjanjian dan perlindungan data pribadi, kemudian menarik argumentasi hukum mengenai keabsahan persetujuan para pihak, kedudukan *biometric verification* dalam pembuatan akta notaris, serta bentuk perlindungan hukum yang seharusnya diberikan terhadap data biometrik para penghadap.

4. HASIL DAN PEMBAHASAN

Keabsahan Persetujuan Para Pihak dalam Akta Notaris yang Menggunakan *Biometric Verification*

Keabsahan persetujuan dalam akta notaris harus dibedakan secara tegas dari keberhasilan verifikasi identitas secara teknologi. *Biometric verification* pada dasarnya membuktikan kecocokan karakteristik biologis seseorang dengan data referensi, sedangkan kesepakatan dalam Pasal 1320 KUHPerdata berkaitan dengan adanya kehendak para pihak untuk

mengikatkan diri. Oleh karena itu, keberhasilan pemindaian sidik jari atau wajah tidak dengan sendirinya membuktikan adanya persetujuan terhadap substansi perjanjian. Perbedaan antara autentikasi dan kehendak hukum tersebut menjadi penting sebagaimana perdebatan mengenai tanda tangan elektronik dalam akta notaris (Marbun et al., 2026; Fardela, 2024; Khairuddin, 2023).

Kesepakatan merupakan syarat subjektif yang harus lahir secara bebas dan tidak mengalami cacat kehendak. Persetujuan yang sah bukan hanya persoalan siapa yang melakukan tindakan, melainkan apakah pihak tersebut memahami dan menghendaki akibat hukum yang timbul. Sistem biometrik dapat meningkatkan keyakinan mengenai identitas, tetapi tidak mampu secara mandiri mengidentifikasi adanya kekhilafan, paksaan, ataupun penipuan. Perkembangan tanda tangan digital menunjukkan bahwa teknologi autentikasi tetap harus ditempatkan dalam konstruksi hukum perikatan yang lebih luas (Dewi et al., 2024; Fadhilah, 2024; Mugiyanto, 2026).

Kondisi tersebut menjadi lebih kompleks pada akta notaris karena autentisitas akta bergantung pula pada terpenuhinya bentuk dan prosedur yang ditentukan undang-undang. Digitalisasi tidak dapat menghilangkan fungsi notaris dalam memastikan identitas, kapasitas, kehendak, dan pemahaman penghadap. Penelitian mengenai *cyber notary* menunjukkan bahwa persoalan utamanya terletak pada kepastian mengenai kesesuaian teknologi dengan ketentuan formal akta autentik (Affan, 2025; Iwaldo, 2026; Rihhadatul'aisy et al., 2026). Irawati (2024) juga menempatkan legalitas akta elektronik sebagai persoalan yang harus dibaca bersama ketentuan khusus mengenai jabatan notaris.

Berdasarkan konstruksi tersebut, *biometric verification* lebih tepat ditempatkan sebagai instrumen pendukung identifikasi daripada sebagai pengganti persetujuan. Sidik jari, pengenalan wajah, iris, atau bentuk biometrik lainnya dapat memperkuat proses identifikasi dan menyediakan jejak autentikasi. Akan tetapi, persetujuan tetap harus ditunjukkan melalui pernyataan kehendak yang dapat dikaitkan dengan isi akta. Pola yang sama terlihat pada penggunaan teknologi dalam sertifikat elektronik dan dokumen pertanahan, ketika sistem digital berfungsi memperkuat autentisitas tetapi tetap membutuhkan dasar hukum mengenai konsekuensi dokumennya (Hadi, 2022; Oktaviani, 2023).

Tabel 1. Parameter Keabsahan Persetujuan dalam Penggunaan *Biometric Verification*.

Aspek yang Dinilai	Fungsi <i>Biometric Verification</i>	Persyaratan Hukum	Implikasi terhadap Akta
Identitas penghadap	Mencocokkan karakteristik biologis dengan identitas terdaftar	Identitas harus dapat dipastikan secara sah	Memperkuat proses identifikasi
Kehendak para pihak	Tidak secara langsung membuktikan kehendak	Harus terdapat kesepakatan yang bebas	Biometrik tidak menggantikan persetujuan
Pemahaman isi akta	Tidak dapat memastikan pemahaman	Notaris harus memastikan penghadap memahami substansi	Pembacaan dan penjelasan tetap diperlukan
Cacat kehendak	Tidak mendeteksi kekhilafan, paksaan, atau penipuan	Kehendak harus bebas dari cacat	Verifikasi biologis tidak menyembuhkan cacat kehendak
Penandatanganan	Dapat menjadi unsur autentikasi tambahan	Harus mengikuti bentuk yang ditentukan hukum	Tidak otomatis menggantikan tanda tangan
Pembuktian	Menghasilkan jejak autentikasi digital	Integritas dan keterlacakan harus terjamin	Dapat menjadi bukti pendukung
Kehadiran penghadap	Dapat mendukung verifikasi jarak jauh	Tetap bergantung pada pengaturan mengenai kehadiran	Tidak otomatis menyamakan kehadiran virtual dan fisik
Persetujuan pemrosesan data	Membuktikan penggunaan identitas biologis	Harus dibedakan dari persetujuan terhadap isi perjanjian	Memerlukan dasar pemrosesan tersendiri

Sumber: Analisis penulis berdasarkan hukum perjanjian dan literatur kenotariatan digital (Marbun et al., 2026; Affan, 2025; Iwaldo, 2026; Rihhadatul'aisy et al., 2026).

Tabel tersebut menunjukkan adanya tiga lapisan hukum yang tidak boleh disamakan, yaitu identifikasi, autentikasi, dan persetujuan. Identifikasi menjawab pertanyaan tentang siapa penghadap, autentikasi memastikan bahwa identitas tersebut digunakan oleh orang yang benar, sedangkan persetujuan menjawab apakah orang tersebut menghendaki perbuatan hukum. Sistem hukum sertifikasi elektronik juga menempatkan keandalan identitas dan autentikasi sebagai unsur penting dalam transaksi elektronik (Hairunnisa, 2025). Karena itu, pencocokan biometrik seharusnya diperlakukan sebagai bagian dari *authentication architecture*, bukan sebagai satu-satunya indikator kesepakatan.

Pembuktian menjadi aspek penting apabila persetujuan kemudian dipersengketakan. Data biometrik dapat membantu menunjukkan bahwa tindakan tertentu dilakukan oleh identitas tertentu, tetapi kekuatan pembuktiannya tetap perlu dinilai bersama isi akta dan proses pembuatannya. Dalam sengketa perdata, alat bukti tidak hanya dinilai dari keberadaannya tetapi juga dari keterkaitan, autentisitas, dan kemampuannya membuktikan fakta hukum yang dipersoalkan (Zakky et al., 2026). Pengalaman sengketa jual beli tanah juga menunjukkan pentingnya bentuk dan kualitas alat bukti dalam menentukan perlindungan hak keperdataan para pihak (Trinanda & Ramadhan, 2026).

Formalitas tetap mempunyai fungsi substantif dalam menciptakan kepastian hukum. Hal tersebut terlihat pula pada jaminan fidusia, ketika kepatuhan terhadap prosedur pendaftaran berpengaruh terhadap legitimasi tindakan hukum berikutnya (Tanuwijaya, 2026). Dalam kenotariatan, prosedur formal tidak semata bersifat administratif karena berfungsi mempertahankan kualitas pembuktian akta autentik. Pengawasan terhadap kepatuhan administratif notaris juga menjadi bagian dari mekanisme mempertahankan standar profesi sebagaimana dikaji Aulia et al. (2026).

Penggunaan biometrik dengan demikian tidak seharusnya menghasilkan anggapan bahwa teknologi telah menggantikan seluruh proses pembentukan kehendak. Perkembangan *financial technology* memperlihatkan bahwa efektivitas digitalisasi harus tetap disertai kejelasan regulasi, tata kelola, dan perlindungan pihak yang bertransaksi (Yanti, 2025; Saputra & Noya, 2026). Hal serupa berlaku terhadap transaksi atas benda virtual yang menunjukkan perubahan bentuk objek dan media transaksi tidak menghapus kebutuhan akan kepastian terhadap hubungan hukum para pihak (Rindasiwi, 2022). Prinsip tersebut relevan pula dalam menentukan posisi biometrik dalam akta notaris.

Dalam praktik, ancaman manipulasi identitas juga harus diperhitungkan. Penggunaan biometrik memang dapat mengurangi sebagian risiko pemalsuan identitas, tetapi teknologi tersebut tidak sepenuhnya menghilangkan kemungkinan penyalahgunaan data, pemalsuan dokumen pendukung, atau rekayasa sistem autentikasi. Permasalahan pemalsuan dan penipuan dalam transaksi pertanahan memperlihatkan bahwa kualitas pemeriksaan identitas tetap menentukan keamanan suatu perbuatan hukum (Rudi Margono, 2026). Dengan demikian, *biometric verification* seharusnya memperkuat prinsip kehati-hatian notaris, bukan menggantikannya.

Dari perspektif doktrinal, perkembangan ini juga merupakan bagian dari perubahan hukum akibat transformasi sosial dan teknologi. Kajian dalam berbagai bidang menunjukkan bahwa hukum terus menghadapi kebutuhan untuk menyesuaikan instrumen tradisional dengan perubahan struktur sosial, teknologi, dan pola hubungan antarindividu (Hanafi et al., 2026; Saputra et al., 2026a). Bahkan pada bidang yang berbeda, perlindungan hak dan kepastian prosedural tetap menjadi unsur penting ketika negara atau institusi menggunakan instrumen baru untuk menentukan posisi hukum seseorang (Saputra et al., 2026b; Hidayat et al., 2026). Dalam konteks kenotariatan, perubahan tersebut harus dilakukan tanpa mengurangi unsur kehendak sebagai inti dari hukum perjanjian.

Berdasarkan analisis tersebut, persetujuan dalam akta notaris yang menggunakan *biometric verification* dapat dinilai sah apabila biometrik hanya digunakan sebagai sarana verifikasi tambahan dan persetujuan tetap memenuhi syarat hukum perjanjian serta prosedur pembuatan akta. Keabsahan tidak boleh dibangun semata-mata berdasarkan *biometric match*. Notaris tetap harus memastikan bahwa pihak yang teridentifikasi benar-benar memahami, menyetujui, dan secara sadar menghendaki isi perbuatan hukum. Pendekatan ini sekaligus menjaga keseimbangan antara modernisasi pelayanan kenotariatan dan karakter formal akta autentik.

Perlindungan Data Biometrik Para Pihak dan Tanggung Jawab Notaris dalam Penggunaan *Biometric Verification*

Penggunaan *biometric verification* menimbulkan persoalan kedua yang berbeda dari keabsahan perjanjian, yaitu perlindungan terhadap data biometrik para penghadap. Data tersebut mempunyai karakter yang berbeda dari data identitas biasa karena melekat pada ciri fisik atau biologis seseorang. Kebocoran kata sandi dapat diatasi dengan mengganti kata sandi, sedangkan karakter biometrik pada dasarnya tidak mudah diganti. Oleh karena itu, tingkat kehati-hatian dalam pengumpulan dan penyimpanannya harus lebih tinggi.

Persoalan kerahasiaan data sebenarnya telah muncul dalam praktik notaris dan PPAT yang terhubung dengan sistem elektronik pemerintahan. Supriyanti (2023) membahas perlindungan kerahasiaan data wajib pajak dalam proses validasi melalui E-PHTB Notaris/PPAT, yang menunjukkan bahwa digitalisasi fungsi notarial selalu membawa persoalan akses dan pengamanan informasi. Permasalahan serupa menjadi lebih serius ketika objek pemrosesan merupakan sidik jari, wajah, atau karakter biologis lainnya. Digitalisasi sertifikat tanah dan penggunaan QR Code juga memperlihatkan perlunya memastikan integritas dan keamanan informasi dalam dokumen elektronik (Hadi, 2022; Oktaviani, 2023).

Persetujuan terhadap pemrosesan biometrik harus dipisahkan dari persetujuan untuk membuat perjanjian. Pihak yang menyetujui isi akta belum tentu secara otomatis memberikan persetujuan bagi penyimpanan data biometriknya untuk tujuan lain. Sebaliknya, persetujuan penggunaan sidik jari untuk verifikasi identitas tidak dapat dipandang sebagai persetujuan terhadap seluruh klausula perjanjian. Pemisahan ini penting agar persetujuan tidak berubah menjadi klausula umum yang memberikan kewenangan pemrosesan data tanpa batas.

Tabel 2. Matriks Risiko dan Perlindungan Data Biometrik dalam Pembuatan Akta Notaris.

Tahap Pemrosesan	Risiko Utama	Prinsip Perlindungan	Tindakan yang Diperlukan
Pengumpulan	Data dikumpulkan tanpa pengetahuan penghadap	Transparansi dan dasar pemrosesan	Informasi yang jelas sebelum pengambilan biometrik
Verifikasi	<i>False acceptance</i> atau <i>false rejection</i>	Akurasi	Verifikasi tambahan terhadap dokumen identitas
Penyimpanan	Kebocoran atau akses tidak sah	Keamanan	Enkripsi, kontrol akses, dan pembatasan pengguna
Penggunaan	Pemakaian untuk tujuan berbeda	Pembatasan tujuan	Penggunaan hanya sesuai tujuan yang diinformasikan
Pengiriman	Intersepsi atau penyalahgunaan pihak ketiga	Kerahasiaan	Saluran transfer yang aman
Retensi	Penyimpanan terlalu lama	Pembatasan penyimpanan	Penentuan jangka waktu retensi
Penghapusan	Data tetap tersimpan setelah tujuan selesai	Akuntabilitas	Mekanisme penghapusan yang dapat diverifikasi
Insiden keamanan	Pencurian identitas dan kerugian pihak	Pertanggungjawaban	Respons insiden dan pemberitahuan sesuai ketentuan
Sengketa	Kesulitan membuktikan persetujuan pemrosesan	Keterlacakan	Audit trail dan dokumentasi persetujuan

Sumber: Analisis penulis berdasarkan prinsip perlindungan data dan perkembangan transaksi elektronik

(Supriyanti, 2023; Hairunnisa, 2025; Saputra & Noya, 2026; Romadon et al., 2026).

Tabel tersebut menunjukkan bahwa keamanan data harus diperhatikan sejak pengumpulan sampai penghapusan. Perlindungan tidak cukup dilakukan hanya dengan memperoleh persetujuan pada awal proses. Pengendali data harus dapat menunjukkan tujuan, keamanan, pembatasan akses, dan periode penyimpanan yang dapat dipertanggungjawabkan. Perkembangan diskursus mengenai hak digital warga negara juga memperkuat perlunya kontrol terhadap penggunaan teknologi yang memproses informasi personal (Romadon et al., 2026).

Notaris juga harus memahami bahwa penggunaan penyedia sistem biometrik pihak ketiga dapat menciptakan rantai pemrosesan yang lebih kompleks. Data dapat berpindah dari perangkat notaris menuju penyedia teknologi, pusat data, atau layanan verifikasi identitas lainnya. Dalam kondisi tersebut, keamanan tidak hanya ditentukan oleh kantor notaris tetapi juga oleh tata kelola penyedia teknologi. Permasalahan tata kelola digital serupa dapat ditemukan dalam kajian regulasi fintech dan transaksi elektronik yang menempatkan kepastian aturan serta distribusi tanggung jawab sebagai unsur penting (Saputra & Noya, 2026; Naftali & Lie, 2026).

Tanggung jawab notaris perlu dibedakan berdasarkan sumber pelanggarannya. Kesalahan dalam memastikan identitas dan kehendak para pihak dapat berkaitan dengan tanggung jawab profesi dan akibat terhadap kekuatan akta. Kebocoran atau penyalahgunaan biometrik dapat

menimbulkan dimensi perlindungan data dan tanggung jawab keperdataan. Pada saat yang sama, pelanggaran administratif dalam menjalankan jabatan tetap dapat menjadi objek mekanisme pengawasan profesi (Aulia et al., 2026).

Dalam hubungan keperdataan, kerugian akibat penyalahgunaan data dapat membuka ruang tuntutan apabila terdapat kesalahan, pelanggaran kewajiban, dan hubungan kausal dengan kerugian. Perlindungan konsumen dalam transaksi digital menunjukkan bahwa pelanggaran kewajiban pelaku sistem dapat menghasilkan konsekuensi terhadap hak pihak yang dirugikan (Naftali & Lie, 2026). Perspektif pembuktian juga penting karena penggugat harus mampu menunjukkan hubungan antara tindakan pemrosesan, kesalahan, dan kerugian yang dialaminya (Zakky et al., 2026). Dengan demikian, dokumentasi proses biometrik memiliki fungsi preventif sekaligus pembuktian.

Risiko penyalahgunaan data juga berkaitan dengan keamanan ruang digital yang lebih luas. Perkembangan *cyber sovereignty* menunjukkan bahwa pengelolaan data dan infrastruktur digital semakin menjadi persoalan hukum yang melampaui batas hubungan kontraktual semata (Anwar & Azmi, 2026). Di sisi lain, perkembangan norma hak asasi menunjukkan bahwa perlindungan hak individu terus berkembang mengikuti perubahan bentuk ancaman dan teknologi (Pramudita & Fadhlulloh, 2026). Kedua pendekatan tersebut mendukung argumentasi bahwa efisiensi digital tidak boleh mengurangi kontrol individu terhadap informasi yang melekat pada dirinya.

Perlindungan biometrik juga harus dikaitkan dengan kemungkinan diskriminasi atau kesalahan algoritmik. Kesalahan identifikasi dapat menyebabkan seseorang gagal melakukan transaksi, ditolak sistem, atau bahkan diposisikan sebagai pihak yang berbeda. Dalam kerangka yang lebih luas, perkembangan hukum menunjukkan pentingnya mempertimbangkan dampak sosial ketika suatu sistem menentukan atau membatasi hak seseorang (Saputra et al., 2026c). Analisis kriminologis terhadap perilaku dan sistem sosial juga menunjukkan bahwa respons hukum seharusnya tidak hanya berorientasi pada akibat akhir, tetapi memperhatikan faktor yang membentuk risiko terjadinya pelanggaran (Saputra et al., 2026d).

Penggunaan teknologi baru seharusnya tetap mempertahankan keseimbangan antara kepastian dan perlindungan hak. Prinsip serupa terlihat dalam sengketa investasi, ketika kepastian bagi satu kepentingan harus diseimbangkan dengan kewenangan dan kepentingan hukum lainnya (Rumambi & Lie, 2026). Pada isu lingkungan, kebutuhan menyeimbangkan kepentingan juga terlihat dalam pendekatan perlindungan antargenerasi dan pengembangan argumentasi hak baru (Hidayat et al., 2026). Meskipun kedua kajian tersebut tidak secara langsung membahas kenotariatan, keduanya memperlihatkan pola penting bahwa pembaruan

hukum harus mempertimbangkan keseimbangan kepentingan, bukan hanya efisiensi institusional.

Hal serupa dapat dilihat pada pembentukan kebijakan yang bersinggungan dengan keluarga dan hukum pidana. Perluasan instrumen hukum tanpa batas yang jelas dapat menimbulkan persoalan proporsionalitas dan hubungan antara kepentingan negara serta ruang privat individu (Maula, 2026). Dalam penggunaan biometrik, prinsip tersebut berarti bahwa tujuan peningkatan keamanan transaksi tidak boleh menjadi dasar bagi pengumpulan data tanpa batas. Pembatasan tujuan merupakan bagian penting dari perlindungan terhadap otonomi individu.

Kajian mengenai perlindungan pengungsi dan perkembangan standar hak asasi memang berada di luar objek kenotariatan, tetapi memberikan perspektif mengenai pentingnya perlindungan hukum ketika individu berada dalam posisi yang rentan terhadap sistem institusional (Saputra et al., 2026e; Pramudita & Fadhlulloh, 2026). Demikian pula, kajian mengenai partisipasi masyarakat dalam ruang demokrasi digital menunjukkan bahwa teknologi memperluas interaksi sekaligus menciptakan tuntutan baru terhadap jaminan hak digital (Saputra et al., 2026c). Konteks tersebut mendukung perlunya pendekatan berbasis hak dalam pemrosesan biometrik.

Perubahan paradigma hukum juga dapat dilihat dari cara pengadilan mengembangkan alasan hukum dalam menghadapi kepentingan yang saling bertentangan. Kajian mengenai *Double Track* dan *Anti-SLAPP* memperlihatkan pentingnya konstruksi penalaran hukum dalam memberikan perlindungan efektif ketika instrumen hukum konvensional berhadapan dengan masalah baru (Saputra et al., 2026b). Dalam konteks biometrik, kebutuhan serupa muncul karena norma hukum perjanjian, kenotariatan, dan perlindungan data harus ditafsirkan secara sistematis. Ketiganya tidak dapat diterapkan secara terpisah.

Penggunaan *biometric verification* pada akhirnya dapat diterima sebagai instrumen modernisasi kenotariatan sepanjang tidak mengurangi prinsip kehati-hatian, kerahasiaan, dan akuntabilitas. Sistem biometrik harus ditempatkan sebagai alat pendukung yang membantu notaris memastikan identitas, bukan sebagai mekanisme otomatis yang mengambil alih penilaian hukum terhadap kehendak penghadap. Sertifikasi elektronik, tanda tangan digital, dan *cyber notary* menunjukkan bahwa inovasi hukum digital memerlukan pengaturan teknis sekaligus kepastian mengenai akibat hukumnya (Hairunnisa, 2025; Marbun et al., 2026; Rihhadatul'aisy et al., 2026). Oleh karena itu, perlindungan data dan keabsahan persetujuan harus dibangun dalam satu sistem yang saling melengkapi.

Hasil penelitian ini menunjukkan perlunya model dual consent dalam penggunaan *biometric verification* pada pembuatan akta notaris. Persetujuan pertama merupakan kesepakatan keperdataan terhadap substansi perbuatan hukum, sedangkan persetujuan kedua berkaitan dengan pemrosesan data biometrik apabila persetujuan digunakan sebagai dasar pemrosesan. Pemisahan tersebut mencegah anggapan bahwa keberhasilan autentikasi sekaligus membuktikan kehendak kontraktual dan persetujuan pengolahan data. Model ini dapat memberikan kepastian yang lebih baik bagi notaris maupun penghadap dalam perkembangan sistem kenotariatan digital.

Dengan demikian, konstruksi hukum yang ideal tidak menempatkan biometrik sebagai pengganti tanda tangan, kehadiran, atau pernyataan kehendak tanpa dasar hukum yang tegas. *Biometric verification* seharusnya berfungsi sebagai lapisan tambahan dalam sistem identifikasi, didukung *audit trail*, keamanan data, mekanisme persetujuan yang terpisah, serta verifikasi langsung oleh notaris. Pendekatan tersebut selaras dengan kebutuhan kepastian hukum dalam digitalisasi transaksi sekaligus menjaga perlindungan hak para pihak. Konstruksi ini menjadi titik pembeda penelitian ini dari kajian terdahulu yang lebih dominan membahas tanda tangan elektronik dan legalitas *cyber notary*.

5. KESIMPULAN DAN SARAN

Penggunaan *biometric verification* dalam pembuatan akta notaris pada prinsipnya dapat digunakan sebagai instrumen pendukung untuk memperkuat verifikasi identitas para penghadap, tetapi keberhasilan autentikasi biometrik tidak dapat secara otomatis dipersamakan dengan adanya persetujuan yang sah menurut hukum perjanjian. Keabsahan persetujuan tetap harus memenuhi unsur kesepakatan sebagaimana dimaksud dalam Pasal 1320 KUHP, yaitu adanya kehendak yang bebas, sadar, dan tidak mengandung cacat kehendak, serta tetap memperhatikan formalitas pembuatan akta autentik berdasarkan ketentuan jabatan notaris. Pada saat yang sama, data biometrik merupakan data pribadi yang bersifat spesifik sehingga pemrosesannya harus dilakukan berdasarkan tujuan yang sah, transparansi, keamanan, pembatasan penggunaan, serta akuntabilitas sesuai prinsip perlindungan data pribadi. Oleh karena itu, penelitian ini menegaskan perlunya pemisahan antara persetujuan terhadap substansi perbuatan hukum dan persetujuan terhadap pemrosesan data biometrik melalui konsep *dual consent*, sehingga *biometric verification* tidak menggantikan fungsi notaris dalam memastikan identitas, kapasitas, pemahaman, dan kehendak para pihak, melainkan menjadi lapisan autentikasi tambahan yang memperkuat kepastian hukum dan perlindungan para penghadap.

Pembentuk peraturan perundang-undangan perlu menyusun pengaturan yang lebih spesifik mengenai penggunaan *biometric verification* dalam praktik kenotariatan, terutama mengenai kedudukan hukum hasil verifikasi biometrik, standar teknologi yang dapat digunakan, tata cara memperoleh persetujuan, penyimpanan dan penghapusan data, penggunaan penyedia sistem pihak ketiga, serta mekanisme pertanggungjawaban apabila terjadi kesalahan autentikasi atau kebocoran data. Organisasi profesi dan lembaga pengawas notaris juga perlu menyusun pedoman teknis yang menegaskan bahwa verifikasi biometrik hanya merupakan sarana pendukung identifikasi dan tidak menggantikan kewajiban notaris untuk memastikan kehendak serta pemahaman para penghadap secara langsung. Dalam praktiknya, notaris sebaiknya menerapkan prinsip *dual consent*, *data minimization*, pembatasan tujuan, pengamanan teknis, serta *audit trail* yang dapat diverifikasi sehingga penggunaan teknologi biometrik dapat meningkatkan keamanan transaksi tanpa mengurangi autentisitas akta maupun hak perlindungan data pribadi para pihak.

DAFTAR REFERENSI

- Affan, M. (2025). Urgensi Kepastian Hukum Terhadap Keabsahan Akta Notaris Dengan Penggunaan Cyber Notary. *Dinamika*, 31(1), 11887-11914.
- Anwar, M., & Azmi, A. (2026). Cyber Sovereignty and International Law: Legal Challenges in the Digital Age. *Iustitia: Journal of Legal Theory, Politics, and International Relations*, 1(1), 47-56.
- Aulia, N., Nurikah, N., & Rayhan, A. R. A. (2026). Prosedur Pengawasan oleh Majelis Pengawas Daerah terhadap Pelanggaran Administratif Berdasarkan Undang-Undang Jabatan Notaris di Kabupaten Serang. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 416-424.
- Dewi, D. C., Amelia, D., Pratama, F. R., Shidiq, F., Ferdansyah, F., & Anugrah, D. (2024). Tanda tangan elektronik sebagai solusi hukum perikatan dalam era digital di Indonesia. *Letterlijk*, 1(2), 217-230.
- Fadhilah, A. (2024). *Implikasi penggunaan tanda tangan digital pada Pondok Pesantren Sabilurrosyad dan Pondok Pesantren Hidayatul Muhtadi'ien As' adiyah Perspektif Hukum Positif* (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim).
- Fardela, B. (2024). *Keabsahan Tanda Tangan Elektronik Pada Pembuatan Akta Notaris Dalam Perspektif Hukum Positif Di Indonesia* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
- Hadi, N. I. (2022). *Kepastian Hukum Sertipikat Hak Atas Tanah Elektronik Dalam Hukum Pertanahan di Indonesia* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
- Hairunnisa, H. (2025). *Analisis Komparasi Sistem Hukum di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura* (Doctoral dissertation, IAIN PAREPARE).

- 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.
- Hidayat, E. F., Kurniawan, B., & Zaini, A. (2026). Constitutional Ecocentrism: Reinvigorating Intergenerational Justice Rooted in Pancasila Through the Recognition of Nature's Rights. *Mimbar Keadilan*, 19(2), 244-258.
- Irawati, F. (2024). *Legalitas Akta Elektronik Dalam Konsep Cyber Notary di Indonesia* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
- 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.
- Khairuddin, M. (2023). *Keabsahan Tanda Tangan Notaris dan Para Pihak Secara Elektronik Pada Akta Notaris* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
- Marbun, D., Lestari, E. A., Dewi, P. S., & Harlia, T. (2026). Keabsahan Hukum Tanda Tangan Elektronik pada Akta Notaris. *Jurnal Hukum Lex Generalis*, 7(4).
- Maula, A. S. (2026). Persinggungan Hukum Pidana dan Perlindungan serta Keharmonisan Keluarga dalam Kriminalisasi Perilaku menurut KUHP Baru. *Journal of Legal, Political, and Humanistic Inquiry*, 1(3), 352-363.
- Mugiyanto, M. (2026). *Analisis Yuridis Keabsahan dan Kekuatan Pembuktian Tanda Tangan Elektronik dalam Perjanjian Kredit Perbankan di Indonesia* (Doctoral dissertation, Hukum).
- Naftali, K. E., & Lie, G. (2026). Legal Protection for Consumers in E-Commerce Transactions Resulting from Breaches of Contract by Businesses: A Study of the Shopee and Tokopedia Platforms. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 208-217.
- OKTAVIANI, O. (2023). *Analisis Hukum Implementasi QR (Quick Response) Code pada Sertifikat Tanah Elektronik= Legal Analysis of QR (Quick Response) Code Implementation On Electronic Land Certificates* (Doctoral dissertation, UNIVERSITAS HASANUDDIN).
- Pramudita, S. A. E., & Fadhlulloh, Q. H. (2026). The Evolution of International Human Rights Norms: A Doctrinal Study of United Nations Legal Instruments. *Iustitia: Journal of Legal Theory, Politics, and International Relations*, 1(1), 11-23.
- 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.
- Rindasiwi, B. P. (2022). *Evaluasi Regulasi Permainan Interaktif Elektronik Di Indonesia (Studi Terhadap Transaksi Elektronik Atas Benda Virtual)* (Doctoral dissertation, Universitas Islam Riau).
- Romadon, B., Ihsan, I., & Muslim, M. (2026). State Responsibility in Protecting Citizens' Digital Rights under Indonesian Constitutional Law. *Iustitia: Journal of Legal Theory, Politics, and International Relations*, 1(2), 88-102.
- Rudi Margono, S. H. (2026). *Menyusun Dakwaan Mafia Tanah: Teknik Penggabungan Pasal Pemalsuan, Penipuan, dan Tindak Pidana Korupsi*. PROFESOR RUDI MARGONO.

- Rumambi, M. G., & Lie, G. (2026). Antara Kedaulatan Negara dan Kepastian Investor: Analisis Kritis Arbitrase Internasional dalam Sengketa Investasi Asing. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 306-317.
- Saputra, D. R., & Noya, M. (2026). Legal Certainty in Fintech Regulation: A Normative Study of Peer-to-Peer Lending Governance in Indonesia. *Lex Recta: Journal of Law and Normative Justice*, 1(1), 40-49.
- Saputra, D. R., Asshofiah, K., & Sholikh, 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.
- Supriyanti, N. M. (2023). *Perlindungan Hukum Atas Kerahasiaan Data Wajib Pajak Dalam Proses Validasi Melalui E-PHTBNotaris/PPAT* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).
- Tanuwijaya, M. C. (2026). Pendaftaran Jaminan Fidusia sebagai Syarat Eksekusi yang Sah: Analisis Hukum Positif Indonesia. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 318-327.
- Trinanda, M. E., & Ramadhan, M. V. (2026). Pembuktian Jual Beli Tanah di Bawah Tangan dalam Sengketa Perdata: Analisis Putusan PN Nabire No. 30/Pdt. G/2020/PN Nabire. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 20-29.
- Yanti, M. (2025). *Analisis soal financial technology (fintech) perbankan syariah pada PT. Bank Sumut Cabang Syariah Padangsidimpuan* (Doctoral dissertation, UIN Syekh Ali Hasan Ahmad Addary Padangsidimpuan).
- Zakky, M. S., Asshidiqi, A., & Simarmata, A. S. H. (2026). Legal analysis of issues of evidence and testimony in civil disputes in court. *Journal of Legal, Political, and Humanistic Inquiry*, 1(4), 218-226.