



Bentuk Tanggung Jawab Hukum Notaris terhadap Kelalaian Kebocoran Data Akta Elektronik di Sistem Cyber

Ni Kadek Melati Anggun Yulian¹, Ni Gusti Agung Ayu Mas Tri Wulandari²

¹Universitas Pendidikan Nasional, E-mail: melatianggunyulian@gmail.com

²Universitas Pendidikan Nasional, E-mail: mastriwulandari@undiknas.ac.id

Info Artikel

Masuk: 11 September 2025
Diterima: 31 Desember 2025
Terbit: 31 Desember 2025

Keywords:

Legal protection; Cyber Notary;
Personal Data

Abstract

This normative legal research to analyze the form of legal responsibility incumbent upon a Notary for negligence resulting in the breach of electronic deed data within the cyber system. Legal protection for the aggrieved parties is established by the Law on Notary Position (UUJN) and the Law on Personal Data Protection (UU PDP). The Notary is professionally obligated to maintain the confidentiality of the deed. A breach of this duty may incur administrative sanctions and civil sanctions in the form of compensation liability, as stipulated in Article 16 paragraphs (11) and (12) of the UUJN. As a Data Controller (Pengendali Data Pribadi), the Notary bears full responsibility for any failure in Personal Data Protection (PDP) (Article 47 UU PDP). Upon such a failure, the Notary must provide written notification to the Data Subject and the Institution within a maximum of 3×24 hours, detailing the disclosed data, the time of disclosure, and the remedial measures undertaken (Article 46 UU PDP). The Form of Legal Responsibility encompasses both civil and criminal liabilities. The Notary, as the electronic system operator, is generally required to be accountable for data breaches arising from negligence. Under the UU PDP, the Notary must secure Personal Data by implementing effective technical and operational measures (Article 35 UU PDP). Furthermore, the UU PDP prescribes stringent criminal sanctions: any individual who intentionally and unlawfully obtains, discloses, or uses unauthorized Personal Data faces a penalty of imprisonment for up to 5 years and/or a maximum fine of Rp5 Billion.

Abstrak

Penelitian hukum normatif ini bertujuan menganalisis bentuk tanggung jawab hukum Notaris terhadap kelalaian kebocoran data akta elektronik dalam sistem siber. Perlindungan Hukum bagi pihak yang dirugikan bersumber dari Undang-Undang Jabatan Notaris (UUJN) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Notaris wajib merahasiakan akta. Pelanggaran kerahasiaan dapat memicu sanksi administratif (peringatan, pemberhentian) sesuai Pasal 16 ayat (11) UUJN, dan sanksi perdata berupa ganti rugi (Pasal 16 ayat (12) UUJN). Sebagai Pengendali Data Pribadi, Notaris wajib memikul tanggung jawab penuh atas kegagalan Perlindungan Data Pribadi (PDP) (Pasal 47 UU PDP). Jika terjadi kegagalan, Notaris harus memberi

Kata kunci:

Perlindungan hukum; Notaris
Siber, Data Pribadi

Corresponding Author:

Ni Kadek Melati Anggun Yulian,
E-mail:
melatianggunyulian@gmail.com

DOI:

10.24843/JMHU.2025.v14.i04.
p07

pemberitahuan tertulis kepada Subjek Data Pribadi dan Lembaga paling lambat 3×24 jam, yang memuat detail data yang terungkap dan upaya pemulihan (Pasal 46 UU PDP). Bentuk Tanggung Jawab Hukum Notaris mencakup aspek perdata dan pidana. Notaris sebagai penyelenggara sistem elektronik wajib bertanggung jawab atas kelalaiannya terhadap kebocoran data. Dalam kerangka UU PDP, Notaris bertanggung jawab mengamankan Data Pribadi melalui langkah-langkah teknis dan operasional yang efektif (Pasal 35 UU PDP). Notaris juga wajib mengumumkan kegagalan proteksi data kepada publik (Pasal 46 UU PDP). Selain itu, UU PDP mengatur sanksi pidana tegas: setiap orang yang dengan sengaja memperoleh, mengungkapkan, atau menggunakan data pribadi bukan miliknya secara melawan hukum, diancam pidana penjara paling lama 5 tahun dan/atau denda hingga Rp5 Miliar.

1. Pendahuluan

Pemanfaatan teknologi oleh seorang notaris dalam melakukan pekerjaannya seperti *e-notary*, ada pula yang memilih istilah *cyber notary*, di Indonesia sendiri konsep yang seringkali dikemukakan menggunakan istilah *cyber notary*.¹ Di era yang secanggih sekarang, layanan *cyber notary* diharapkan dapat memberikan kemudahan bagi notaris dalam menjalankan setiap tugas-tuganya.²

Kemajuan perkembangan teknologi mengharuskan masyarakat untuk dapat dengan cepat beradaptasi dengan hal baru. Untuk menyesuaikan perkembangan yang semakin pesat itu, hukum positif juga harus bisa mengimbangi perkembangan yang terjadi saat ini. Namun, di balik kemajuan tersebut, muncul tantangan baru berupa ancaman kejahatan siber (*cybercrime*). Kejahatan siber (*cybercrime*) terjadi di berbagai bidang termasuk bidang kenotariatan. Selama ini pelayanan notaris pada masyarakat masih bersifat konvensional, akan tetapi seiring dengan perkembangan teknologi informasi yang memaksa setiap lini kehidupan bertransformasi dari cara kerja konvensional ke sistem elektronik, pelayanan notaris juga sedang bergeser mengarah ke pelayanan berbasis elektronik yaitu seperti *cyber notary*.³

Konsep mengenai *cyber notary* termuat didalam ketentuan Undang-Undang Nomor 2 tahun 2014 tentang perubahan UU Nomor 30 Tahun 2004 tentang Jabatan Notaris (yang selanjutnya disingkat UUJN). Dalam Undang-Undang tersebut menjelaskan bahwa

¹ Pramudyo, Eri, Ranti Fauza Mayana, dan Tasya Safiranita Ramli. "Tinjauan Yuridis Penerapan Cyber Notary Berdasarkan Perspektif UU ITE dan UUJN." *Jurnal Indonesia Sosial Sains* 2, No. 8 (2021): 1239-1258.

² Theixar, Regina Natalie, dan Ni Ketut Supasti Dharmawan. "Tanggung Jawab Notaris Dalam Menjaga Keamanan Digitalisasi Akta." *Acta Comitas: Jurnal Hukum Kenotariatan* 6, No. 1 (2021): 1-15.

³ Irawan, Ade, M. Ryan Bakry, dan Frengki Hardian. "Eksistensi Aspek Teknologi Dalam Pembuatan Akta Autentik Secara Elektronik Pada Pengaturan Jabatan Notaris Di Era Industri 5.0." *COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat* 2, No. 8 (2022): 1501-1521.

kewenangan notaris juga terkait sertifikasi transaksi yang dilakukan secara elektronik (*Cyber Notary*).⁴

Menjaga keamanan dan kerahasiaan data akta sudah seharusnya dilakukan oleh Notaris selaku pengemban kewajiban untuk merahasiakan segala sesuatu mengenai akta yang dibuatnya. Hal ini menimbulkan pertanyaan mengenai sejauh mana tanggung jawab hukum seorang notaris jika terjadi kebocoran data akta melalui sistem elektronik yang digunakannya. Kewajiban untuk merahasiakan segala sesuatu yang tertulis di dalam akta maupun segaka keterangan yang diperoleh notaris dari para pihak bukan hanya untuk melindungi kepentingan para pihak, melainkan juga untuk kepentingan notaris dimana ia harus menjaga kepercayaan masyarakat terhadap jabatan notaris.⁵ Dalam perspektif hukum perdata dan hukum bisnis, kebocoran data bisa berdampak pada kerugian material, pembatalan perjanjian, atau bahkan gugatan wanprestasi. Berdasarkan analisis penulis, dilihat dalam Pasal 15 Ayat 3 UUJN dijelaskan bahwa notaris memiliki kewenangan dalam membuat akta secara digital, namun ketentuan lebih lanjut dan spesifik seperti proses pelaksanaan, batasan tanggung jawab, dan sanksi yang akan diberikan kepada notaris apabila ada kelalaian kebocoran data masih belum diatur secara tegas sehingga menimbulkan kekaburuan norma dalam penerapannya, baik dalam UUJN, kode etik notaris, ataupun Peraturan Pemerintah lainnya.

Sedangkan, jika dilihat dalam Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (yang selanjutnya disingkat UU ITE) memang telah dijelaskan bahwa apabila ada kebocoran data, maka penyelenggara sistem elektronik yaitu dalam hal ini adalah notaris wajib bertanggung jawab atas kelalaianya. Namun dalam aturan ini juga belum diatur secara gamblang jenis tanggung jawab atau sanksi seperti apa yang harus dikenakan atas kelalaianya dalam menjalankan kewenangan. Jika dilihat dari Peraturan Pemerintah Nomor 71 Tahun 2019 khususnya pada Pasal 58, telah dijelaskan bahwa tanggung jawab ada pada penyelenggara sertifikasi yaitu notaris apabila terjadi kebocoran data baik yang disengaja ataupun lalai sekalipun. Namun masih sama seperti dua aturan sebelumnya, dalam aturan ini masih belum diatur secara jelas seperti apa tanggung jawab yang harus dilakukan notaris atas kelalaianya. Oleh karena itu, penting untuk meninjau aspek tanggung jawab notaris dari sisi perundangan yang berlaku, seperti UUJN, Undang-Undang Perlindungan Data Pribadi, serta ketentuan hukum perikatan dalam Kitab Undang-Undang Hukum Perdata (selanjutnya disebut KUHPPerdata).

Notaris yang dimintakan pertanggung jawaban harus dipastikan apakah notaris tersebut dengan sengaja melakukan perbuatan yang merugikan pihak lain atau karena lalai dalam menjalankan tanggung jawabnya. Kelalaian menurut hukum pidana diartikan sebagai tindakan yang kurang melakukan tindakan pencegahan atau kurang

⁴ Chastra, Deny Fernaldi. "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris." *Indonesian Notary* 3, No.2 (2021): 248-267

⁵ Mipon, Intan Permata, dan Mohamad Fajri Mekka Putra. "Penyelenggaraan Pelindungan Data Pribadi oleh Notaris berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *Jurnal Hukum & Pembangunan* 53, No.3 (2023): 479 - 492

berhati-hati.⁶ Menurut hukum perdata, kelalaian merupakan suatu tindakan yang dilakukan seseorang yang menyebabkan kerugian pada orang lain dan mengharuskan orang tersebut untuk mempertanggung jawabkan perbuatannya atau mengganti kerugian pihak yang dirugikan. Timbulnya kerugian menjadi salah satu unsur akibat hukum yang muncul dari kelalaian notaris tersebut, selain itu kesalahan dari notaris tersebut juga menjadi unsur selanjutnya dalam kelalaian yang perlu dipertanggung jawabkan.⁷

Mengacu pada permasalahan ketidakjelasan pengaturan mengenai tanggung jawab notaris atas kelalaiannya menyebabkan kebocoran data akta elektronik sebagaimana termaktub pada Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka penulis tertarik mengkaji bentuk tanggung jawab notaris terhadap kelalaian kebocoran data elektronik, baik dari sisi preventif maupun represif, serta memberikan analisis hukum terhadap perlindungan bagi para pihak yang dirugikan ke dalam proposal penelitian tesis ini.

Jurnal ilmiah ini mengangkat 2 (dua) permasalahan yang akan menjadi pokok pembahasan yakni: 1) Bagaimana perlindungan hukum bagi pihak yang dirugikan akibat kelalaian notaris dalam hal kebocoran data akta elektronik di sistem *cyber*? 2) Bagaimana bentuk tanggung jawab hukum seorang notaris terhadap kelalaian kebocoran data akta elektronik melalui sistem *cyber*? Jurnal ilmiah ini memiliki tujuan penelitian yakni untuk mengetahui dan menganalisis mengenai “Bentuk Tanggung Jawab Hukum Notaris Terhadap Kelalaian Kebocoran Data Akta Elektronik Di Sistem Cyber”

Penelitian ini menggunakan *state of art* sebagai pembanding dengan memperlihatkan penelitian sebelumnya yang membahas penelitian serupa, sehingga penelitian ini memiliki suatu kebaharuan hukum dalam pembahasannya. Adapun *state of art* yang digunakan adalah: 1) Mislaini dan Habib Adjie pada jurnal Unes Law Review pada Volume 6, Nomor 2, Desember 2023 dengan judul “Tanggung Jawab Notaris dalam Pengamanan Data Pribadi dalam Perjanjian Notariil Pada Era Digital”⁸, 2) Katarina Arinda Sisca pada jurnal Ilmiah Hukum Kenotariatan Repertorium pada Volume 1, Nomor 1, April 2024 dengan judul “Penegakan Hukum Notaris Yang Menggunakan Data Pribadi Orang Lain Dalam Akta: Perspektif Perlindungan Data”.⁹ Perbedaan dengan jurnal ilmiah ini adalah penelitian ini mengangkat permasalahan yakni mengenai perlindungan hukum bagi pihak yang dirugikan akibat kelalaian notaris dalam hal kebocoran data akta elektronik di sistem *cyber* dan bentuk tanggung jawab hukum seorang notaris terhadap kelalaian kebocoran data akta elektronik melalui

⁶ Leba, Nikanort. “Pertanggungjawaban Hukum Kelalaian Pengemudi Perusahaan Dalam Kecelakaan Lalu Lintas Yang Mengakibatkan Kematian.” *Lex Administratum* 11, No.1 (2023): 1-11

⁷ Siregar, Maria Magdalena, Aarce Tehupeiry, dan L. Elly AM Pandiangan. “Analisis Hukum Kelalaian Pembuatan Akta Wasiat Oleh Notaris.” *Jurnal Hukum To-Ra: Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, No.1 (2023): 185-201.

⁸ Mislaini dan Habib Adjie. “Tanggung Jawab Notaris dalam Pengamanan Data Pribadi dalam Perjanjian Notariil Pada Era Digital”. *Unes Law Review* 6, No. 2 (2023): 7481-7490.

⁹ Sisca, Katarina Arinda. “Penegakan Hukum Notaris Yang Menggunakan Data Pribadi Orang Lain Dalam Akta: Perspektif Perlindungan Data.” *Repertorium: Jurnal Ilmiah Hukum Kenotariatan* 13, No.1 (2024): 95-103.

sistem *cyber*, sehingga jurnal ilmiah ini memiliki nilai kebaharuan dalam dunia penelitian hukum dan tidak memiliki unsur plagiat dalam pembuatannya.

2. Metode Penelitian

Kajian ini mengaplikasikan metode secara normatif. Menurut Soerjono Soekanto, penelitian normatif merupakan penelitian yang mengkaji asas-asas hukum, sejarah hukum, sistematik hukum, dan juga perbandingan hukum.¹⁰ Kajian normatif atau secara umum juga dikenal sebagai kajian yuridis normatif dipahami sebagai suatu penelitian yang berkaitan terkait pada asas-asas, terkait juga pada sistematika, terkait pada sejarah, serta berkaitan juga pada taraf sinkronisasi hukum serta perbandingan yang berkaitan dengan hukum. Isu hukum pada penelitian ini adalah mengkaji dan menganalisa prinsip dan asas-asas hukum mengenai tanggung jawab hukum seorang notaris. Dalam UUJN sudah diatur apa saja tanggung jawab seorang notaris dalam menjalankan tugasnya, namun penelitian ini akan berfokus pada tanggung jawab pejabat notaris dalam bidang perdata yang lalai dalam membuat akta autentik sehingga terjadi kebocoran data akta elektronik dalam sistem *cyber*.

3. Hasil dan Pembahasan

3.1 Perlindungan Hukum Bagi Pihak Yang Dirugikan Akibat Kelalaian Notaris Dalam Hal Kebocoran Data Akta Elektronik Di Sistem *Cyber*

Hak privasi warga negara Indonesia berada pada posisi yang rentan terhadap potensi eksploitasi yang dapat mengakibatkan kerugian substantif bagi masyarakat. Pelanggaran terhadap hak fundamental ini tidak hanya diakibatkan oleh insiden kebocoran data (*data breach*), melainkan juga berakar pada praktik pemrosesan data pribadi yang tidak akuntabel dan tidak bertanggung jawab. Fenomena ini terwujud secara nyata dalam penggunaan data individu untuk aktivitas komersial atau perdagangan tanpa adanya landasan hukum yang sah atau persetujuan eksplisit dari subjek data. Dengan demikian, isu perlindungan data pribadi telah bertransformasi menjadi prioritas krusial yang memerlukan attensi serius, khususnya mengingat peningkatan adopsi platform digital yang massif, oleh karena itu penjaminan keamanan data pribadi merupakan imperatif mendesak guna memelihara integritas hak-hak individu dan menjaga stabilitas digital publik.¹¹

¹⁰ Laksana, Anak Agung Ngurah Mahendra Wahyu, dan Kadek Julia Mahadewi. "Legitimasi Hukum yang Tak Terbantahkan: Kekuatan Pembuktian Akta Dibawah Tangan yang Telah Disahkan oleh Notaris." *Jurnal Kewarganegaraan* 7, No.1 (2023): 466-471.

¹¹ Dharmawan, Ni Ketut Supasti, Desak Putu Dewi Kasih, dan Deris Stiawan. "Personal Data Protection and Liability of Internet Service Provider: A Comparative Approach." *International Journal of Electrical and Computer Engineering (IJECE)* 9, No.4 (2019): 3175-3184.

Tanggung jawab Notaris dalam menjamin keamanan akta digital secara spesifik mencakup kerugian akibat hilangnya atau rusaknya protokol yang tersimpan secara elektronik, sekaligus kewajiban menjaga kerahasiaan akta tersebut. Meskipun demikian, regulasi undang-undang yang ada disinyalir masih mengandung kelemahan struktural yang berimplikasi pada belum terjaminnya kepastian dan perlindungan hukum yang komprehensif, khususnya terkait keamanan data pribadi para pihak dalam implementasi *cyber notary*. Mengingat sifat akta Notaris yang mewajibkan penyertaan data pribadi/identitas para penghadap, peranan pihak yang menyimpan data dalam hal ini Notaris sebagai pemegang protokol menjadi esensial guna meminimalisasi risiko kejahatan di dunia siber.¹²

Data pribadi yang tersimpan merupakan aset yang rentan dieksplorasi, sering kali menjadi komoditas perdagangan ilegal oleh pelaku kejahatan siber, bahkan melibatkan oknum Notaris yang mengabaikan integritas dan tanggung jawab jabatan mereka. Meskipun demikian, Notaris memiliki kewajiban mutlak untuk merahasiakan akta beserta seluruh isinya sesuai dengan ketentuan yang termaktub dalam UUJN. Pelanggaran terhadap kewajiban kerahasiaan ini dapat memicu konsekuensi hukum yang tegas, sebagaimana diatur dalam Pasal 16 ayat (11) UUJN, berupa sanksi administrasi seperti peringatan tertulis, pemberhentian sementara dengan batas waktu, hingga pemberhentian secara hormat atau tidak hormat. Lebih lanjut, selain sanksi administrasi tersebut, Pasal 16 ayat (12) UUJN juga menggariskan adanya sanksi perdata berupa kewajiban ganti rugi yang dapat diajukan oleh pihak penghadap kepada Notaris atas kerugian yang diderita akibat pelanggaran tersebut.¹³

Kecanggihan teknologi komputasi, di samping menawarkan aspek positif, juga menghadirkan risiko negatif berupa gangguan digital, utamanya dalam bentuk virus komputer, yang didefinisikan sebagai program ilegal yang menyusup dan menyebar melalui jaringan dengan potensi merusak sistem. Implikasi dari gangguan digital ini adalah kerusakan, bahkan hilangnya, berkas digital atau data yang terkandung di dalamnya. Apabila belum terdapat kebijakan resmi mengenai penyimpanan minuta akta secara digital, serangan virus secara langsung akan berdampak buruk pada draf akta yang telah dirancang. Notaris memiliki peran preventif krusial, yaitu dengan menginstal perangkat lunak anti-virus pada seluruh perangkat kerja yang digunakan untuk merancang akta, serta menjalankan kewajiban ketelitian dengan membacakan isi akta secara saksama sebelum penandatanganan, sesuai mandat yang tercantum dalam Pasal 16 huruf (m) UUJN.¹⁴

Guna menyiapi isu keamanan dalam penyimpanan dokumen *cyber notary*, *American Bar Association* (ABA) telah mengadopsi solusi teknis melalui penerapan sistem kriptografi dan *Public Key Infrastructure* (PKI). Sistem ini dianggap memiliki kapabilitas untuk mengamankan pesan elektronik dan mengautentikasi identitas para pihak melalui kriptografi, sementara PKI secara spesifik memfasilitasi penggunaan tanda tangan digital. Secara esensial, *cyber notary* menurut ABA dimaknai sebagai suatu konsep pemanfaatan kemajuan teknologi oleh Notaris dalam menjalankan kewenangan jabatannya, meliputi digitalisasi dokumen, penandatanganan akta secara elektronik,

¹² *Ibid.*, h. 2175

¹³ *Ibid.*, h. 2176

¹⁴ Theixar, Regina Natalie, dan Ni Ketut Supasti Dharmawan. *Op.cit.*

serta pelaksanaan prosedur seperti Rapat Umum Pemegang Saham (RUPS) melalui telekonferensi. Sejalan dengan itu, peraturan di Indonesia mewajibkan perlindungan data, di mana Pasal 40 ayat (2) UU ITE menekankan bahwa penyidikan berbasis teknologi informasi harus menjamin perlindungan kerahasiaan, privasi, dan keutuhan data, serta kelancaran pelayanan publik. Lebih lanjut, data pribadi didefinisikan dalam Pasal 1 angka (22) Undang-undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (selanjutnya disebut UU Administrasi Kependudukan) sebagai data perseorangan tertentu yang wajib disimpan, dirawat, dijaga kebenaran, dan dilindungi kerahasiaannya oleh negara, meskipun penyelenggara instansi pelaksana juga diberikan hak akses terhadap data kependudukan tersebut.¹⁵

Upaya mitigasi risiko penyalahgunaan wewenang di luar batas wilayah jabatan Notaris, dipandang perlu adanya regulasi yang mewajibkan perangkat komputasi yang digunakan oleh Notaris untuk menginformasikan atau mendaftarkan *IP address*-nya kepada Kementerian Hukum dan Hak Asasi Manusia. Selain itu, setiap akta elektronik yang diterbitkan hendaknya mencantumkan *IP address* tersebut sebagai metadata. Implementasi mekanisme ini akan memfasilitasi pihak yang berwenang untuk melaksanakan pemeriksaan dan audit secara efektif terkait praktik *cyber notary* yang dijalankan oleh Notaris, sehingga dapat diverifikasi apakah tindakan yang dilakukan telah sesuai dengan batasan yurisdiksi atau wilayah jabatan yang telah ditetapkan.¹⁶

Mengacu pada permasalahan ketidakjelasan pengaturan mengenai tanggung jawab notaris atas kelalaianya menyebabkan kebocoran data akta elektronik, maka penulis tertarik mengkaji perlindungan hukum notaris terhadap kelalaian kebocoran data elektronik. Berdasarkan teori perlindungan hukum menurut wahyu sasongko dari Universitas Lampung menjelaskan bahwa perlindungan hukum itu terdiri dari perlindungan hukum preventif dan perlindungan hukum represif, yang keseluruhannya bermuara pada perlindungan hukum terhadap warga masyarakatnya karena itu perlindungan hukum tersebut akan melahirkan pengakuan dan perlindungan hak asasi manusia dalam wujudnya sebagai makhluk individu dan makhluk social dalam wadah negara kesatuan yang menjunjung tinggi semangat kekeluargaan demi mencapai kesejahteraan bersama.¹⁷ Permasalahan perlindungan hukum ini dapat dikaji menggunakan teori penafsiran hukum sistematis.

Berdasarkan teori Penafsiran hukum dikenal salah satunya yakni Penafsiran hukum sistematis (*systematische interpretative*). Teori Penafsiran hukum Sistematis adalah metode penafsiran yang melihat suatu ketentuan hukum tidak berdiri sendiri, melainkan

¹⁵ Wijayanti, Adinda Ari, dan I. Gusti Ketut Ariawan. "Upaya Perlindungan Terhadap Identitas Para Pihak Dalam Praktik Cyber Notary." *Acta Comitas: Jurnal Hukum Kenotariatan* 6, No.03 (2021): 679-695.

¹⁶ Najib, Ainun. "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi." *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 7, No. 1 (2023): 43-59.

¹⁷ Imanullah, Mochammad Najib. "Perlindungan hukum preventif dan represif bagi pengguna uang elektronik dalam melakukan transaksi tol nontunai." *Jurnal Privat Law* 9, No. 1 (2021): 218-226.

sebagai bagian yang terintegrasi dari keseluruhan sistem perundang-undangan.¹⁸ Undang-Undang yang dapat menyelesaikan permasalahan tersebut yakni adalah UU ITE dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut sebagai UU PDP).

Perlindungan hukum bagi Notaris selaku pengendali data pribadi ketika terjadi kelalaian dari pihak Notaris dalam *cyber notary* diatur dalam Pasal 46 UU PDP yang menyebutkan: "(1) Dalam hal terjadi kegagalan Perlindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada: a. Subyek Data Pribadi dan b. Lembaga. (2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat: a. Data Pribadi yang terungkap; b. Kapan dan bagaimana Data Pribadi terungkap; c. Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi. (3) Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Perlindungan Data Pribadi."

Kegagalan Perlindungan Data Pribadi (PDP) didefinisikan secara komprehensif mencakup kompromi terhadap aspek kerahasiaan, integritas, dan ketersediaan Data Pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak, yang berujung pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang sedang dikirim, disimpan, atau diproses. Seluruh bentuk kegagalan perlindungan ini berpotensi menimpa Notaris saat menjalankan kewenangan dalam pembuatan akta *cyber notary*. Oleh karena itu, Notaris wajib memikul tanggung jawab penuh atas terjadinya kegagalan dalam Perlindungan Data Pribadi, sesuai dengan ketentuan yang termaktub dalam Pasal 47 UU PDP.

3.2 Bentuk Tanggung Jawab Hukum Seorang Notaris Terhadap Kelalaian Kebocoran Data Akta Elektronik Melalui Sistem Cyber

Diskursus mengenai perlindungan informasi, istilah informasi personal dan data individu menjadi rujukan utama, seiring dengan meningkatnya urgensi untuk memastikan keamanan data pribadi di Indonesia. Sebagai respons terhadap kebutuhan ini, institusi legislatif, yakni Dewan Perwakilan Rakyat Republik Indonesia (DPR RI), telah merampungkan pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) menjadi peraturan yang mengikat. Pengesahan ini disepakati dalam Rapat Paripurna pada hari Selasa, 20 September 2022, dan kini secara resmi diundangkan sebagai Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Penetapan Undang-Undang ini menandai langkah signifikan dan progresif dalam mengatasi tantangan regulasi sebelumnya, di mana perlindungan data pribadi masih tersebar dan tidak terkonsolidasi dalam berbagai regulasi sektoral.¹⁹

Kejahatan siber (*cyber crime*) mencakup serangkaian aktivitas kriminal yang dilakukan melalui sistem dan jaringan komputer, seperti peretasan (*hacking*), penyebaran *malware*

¹⁸ Safaat, Ahmad M.S., *Penemuan Hukum Dan Berbagai Metode Interpretasi Atau Penafsiran Hukum*, Jakarta: Pusat Pengkajian Kebijakan Hukum dan Hak Asasi Manusia (PPKHHAM), 2015, h. 73

¹⁹ Indarta, Yose. *Cyber Law: Dimensi Hukum dalam Era Digital*. Jakarta: Pustaka Galeri Mandiri, 2025. h. 90

(termasuk virus), pencurian identitas (*identity theft*), eksfiltrasi data, pelecehan digital (*cyber harassment*), hingga *skimming*. Kemudahan akses saat ini, di mana hampir seluruh data pribadi individu telah tersimpan secara daring, menjadikan praktik pencurian data sebagai ancaman yang kian mudah direalisasikan. Secara substansial, tindakan ilegal mengambil data pribadi ini merupakan perbuatan yang dikategorikan melawan hukum. Meskipun kerangka hukum siber (*cyber law*) yang berdiri sendiri masih dalam pengembangan, beberapa regulasi, khususnya UU ITE telah memberikan landasan hukum. UU ITE secara eksplisit menyatakan bahwa setiap pelanggar ketentuan Pasal 26 dapat menghadapi tuntutan ganti rugi atas kerugian yang ditimbulkan oleh perbuatannya.

Kemajuan pesat di bidang teknologi dan informasi telah memberikan kemudahan, namun secara bersamaan, juga memfasilitasi pelaksanaan berbagai tindak kejahatan siber secara lebih efektif dan efisien. Situasi ini menciptakan kerentanan signifikan, khususnya dalam sektor pengelolaan data dan informasi, yang menuntut adanya perlindungan data pribadi yang kuat. Perkembangan teknologi informasi dan komunikasi (TIK) secara inheren telah mengikis batas-batas privasi, membuat penyebaran berbagai data-data pribadi menjadi semakin tak terhindarkan. Akibatnya, isu perlindungan data pribadi kini menjadi perhatian yang sangat serius, mengingat potensi risiko kebocoran data yang ditimbulkan oleh penyebarannya. Jenis data sensitif seperti Nomor Induk Kependudukan (NIK), nama lengkap, alamat email, hingga nomor telepon seluler, saat ini dianggap sangat berharga karena memiliki nilai jual tinggi di pasar gelap.

Konsep Notaris Siber (*Cyber Notary*) menunjukkan implementasi nyata dari prinsip kemanfaatan dan efisiensi dalam menjalankan profesi Notaris. Sistem ini memfasilitasi sertifikasi digital, yang secara signifikan menyederhanakan praktik kenotariatan. Adopsi praktik digital ini menuntut dokumen-dokumen publik tersedia dalam format elektronik, termasuk perlunya tanda tangan elektronik oleh Notaris. Secara konvensional, Notaris mengandalkan dokumen fisik seperti KTP, SIM, atau Paspor untuk verifikasi identitas para pihak yang hadir (penghadap). Namun, dengan adanya konsep Notaris Siber, media pengenalannya beralih menggunakan Identitas Elektronik (*Electronic Identity* atau e-ID). e-ID ini merupakan perwujudan dari pemerintahan elektronik (*e-government*) yang bertujuan meningkatkan layanan publik melalui pemanfaatan teknologi informasi. Mengingat sifat identitas yang rahasia dan sangat sensitif, terdapat risiko besar data tersebut diakses oleh pihak yang tidak berhak, terutama oleh pelaku kejahatan siber yang tidak bertanggung jawab. Oleh karena itu, perlindungan rekaman biometrik yang terkait dengan data pribadi menjadi keharusan fundamental bagi pemilik data yang sah.²⁰

Perlindungan hukum secara spesifik ditujukan kepada identitas pihak-pihak yang terlibat dalam proses kenotariatan digital. Sebelum mendalami konsep Identitas Elektronik (e-ID), penting untuk memahami bahwa identitas pada dasarnya adalah ciri khas yang digunakan untuk membedakan seseorang dengan individu lainnya. Sementara itu, e-ID diartikan sebagai pengenal diri yang diwujudkan atau dimediasi

²⁰ Rebeka, Sintya. "Perkembangan Peran Notaris Di Era Digital: Analisis Peluang Dan Tantangan Pasca UU No. 1 Tahun 2024." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 12, No.6 (2025): 2673-2684.

oleh teknologi elektronik, yang umumnya menyimpan data-data pribadi dalam format kartu pintar (*smart card*). Kebutuhan akan data pribadi di era digital saat ini menjadi krusial, terutama untuk menangkal kejahatan siber yang semakin marak. Di antara berbagai gangguan digital, peretasan (*hacking*) terhadap perangkat komputer merupakan ancaman yang paling berbahaya. Peretasan didefinisikan sebagai upaya modifikasi, akses paksa, atau penerobosan ke dalam sistem atau jaringan komputer yang dilakukan untuk kepentingan pribadi atau kelompok tertentu. Jika perangkat komputer Notaris yang menyimpan draf akta berhasil diretas, dampak buruk yang dapat terjadi meliputi:

1. Penyalahgunaan informasi pribadi para pihak atau objek perjanjian.
2. Pelanggaran terhadap kerahasiaan akta notaris.
3. Manipulasi data yang dapat merugikan Notaris dan pihak-pihak yang terkait.²¹

Berdasarkan Hans Kelsen (Teori Hukum Murni) yang menyatakan bahwa tanggung jawab hukum berkaitan erat dengan kewajiban hukum. Seseorang bertanggung jawab secara hukum atas suatu perbuatan jika ia dapat dikenakan sanksi apabila perbuatannya bertentangan dengan norma hukum, tidak terkecuali seorang yang berprofesi sebagai notaris.²²

Regulasi terkait tindakan peretasan, yang dikategorikan sebagai kejahatan siber (*cyber crime*), termuat dalam UU ITE. Dalam konteks hukum, peretasan merujuk pada Akses Ilegal ke sistem elektronik. Pasal 30 UU ITE mengatur kualifikasi perbuatan yang dapat dipidana, yang secara esensial mencakup:

“(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.” Ancaman terhadap pelanggaran di atas dimuat dalam Pasal 46 UUITE: “(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus raja rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus raja rupiah). (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus raja rupiah).”

²¹ Mislaini, Mislaini, dan Habib Adjie. “Tanggung Jawab Notaris dalam Pengamanan Data Pribadi dalam Perjanjian Notariil Pada Era Digital.” *UNES Law Review* 6, No.2 (2023): 7481-7490.

²² Fazriah, Dina. “Tanggung Jawab Atas Terjadinya Wanprestasi Yang Dilakukan Oleh Debitur Pada Saat Pelaksanaan Perjanjian.” *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 1, No. 2 (2023): 1-25.

Kerangka UU PDP, seorang Notaris diakui sebagai Pengendali Data Pribadi karena memiliki kewenangan untuk menetapkan secara langsung tujuan dari pemrosesan data pribadi yang diintegrasikan dalam akta otentik. Mengacu pada peran krusial ini, Notaris bertanggung jawab penuh untuk mengamankan informasi pribadi saat menyusun dan melaksanakan perjanjian notaris, sebagaimana diamanatkan oleh Pasal 35 UU PDP. Pasal tersebut menegaskan bahwa Pengendali Data Pribadi memiliki kewajiban untuk menjaga serta memastikan keamanan Data Pribadi yang diprosesnya melalui dua tindakan utama. Pertama, Notaris harus melakukan penyusunan dan implementasi langkah-langkah teknis dan operasional yang efektif guna melindungi Data Pribadi dari segala bentuk pemrosesan yang bertentangan dengan ketentuan peraturan perundang-undangan. Kedua, Notaris wajib menetapkan tingkatan keamanan Data Pribadi dengan mempertimbangkan secara cermat sifat dan potensi risiko yang melekat pada Data Pribadi yang harus dilindungi selama proses pemrosesan tersebut berlangsung.²³

Pengendali Data, dalam konteks ini adalah Notaris, bertanggung jawab untuk memperkuat dan menjaga keamanan Data Pribadi. Apabila Notaris selaku Pengendali Data gagal menjamin atau melindungi Data Pribadi, atau jika terjadi insiden kebocoran atau kegagalan proteksi Data Pribadi, maka kewajiban Pengendali Data adalah mengumumkan kepada publik mengenai kejadian kegagalan tersebut, sesuai dengan ketentuan Pasal 46 UU PDP yang menentukan bahwa: (1) "Dalam hal terjadi kegagalan Perlindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3×24 (tiga kali dua puluh empat) jam kepada: Subjek Data Pribadi; dan Lembaga." (2) "Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat: Data Pribadi yang terungkap; Kapan dan bagaimana Data Pribadi terungkap; dan Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pegendali Data Pribadi." (3)" Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Perlindungan Data Pribadi."

UU PDP yang telah disahkan oleh Pemerintah, diharapkan dapat meminimalisir munculnya pelanggaran atau penyalahgunaan data pribadi warga negara Indonesia dengan adanya sanksi yang telah diatur dalam Pasal 67 yang menyatakan "(1) Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data diri pribadi sebagaimana dimaksud dalam Pasal 65 Ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan atau pidana denda paling banyak Rp. 5.000.000.000.00 (Lima Miliar rupiah).(2) Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 Ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan atau pidana denda paling banyak Rp. 4.000.000.000.00 (Empat Miliar rupiah). (3) Setiap orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 Ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan atau pidana denda paling banyak Rp. 5.000.000.000.00 (Lima Miliar rupiah)." Selanjutnya disebutkan pula pada Pasal 68 UUPDP berkaitan dengan

²³ Susanti, Sari, and Sari Sari. "Integrasi Konsep Pelindungan Data Pribadi Pengguna Jasa Notaris Berdasarkan Undang Undang Pelindungan Data Pribadi dan Jabatan Notaris." *Innovative: Journal Of Social Science Research* 4, No.6 (2024): 688-705.

Data Pribadi palsu yaitu: "Setiap orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau pidana denda paling banyak Rp. 6.000.000.000.00 (Enam Miliar rupiah)."

4. Kesimpulan

Perlindungan hukum bagi pihak yang dirugikan akibat kelalaian Notaris dalam hal kebocoran data akta elektronik di sistem siber. Perlindungan ini bersumber dari beberapa regulasi, di antaranya adalah Undang-Undang Jabatan Notaris (UUJN) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Berdasarkan UUJN, Notaris wajib merahasiakan akta, dan pelanggaran kewajiban kerahasiaan ini dapat menimbulkan sanksi administratif (seperti peringatan tertulis hingga pemberhentian) sesuai Pasal 16 ayat (11) UUJN, serta sanksi perdata berupa kewajiban ganti rugi terhadap pihak yang dirugikan sesuai Pasal 16 ayat (12) UUJN. Selanjutnya, sebagai Pengendali Data Pribadi, Notaris wajib memikul tanggung jawab penuh atas kegagalan Perlindungan Data Pribadi (PDP) sesuai Pasal 47 UU PDP. Jika terjadi kegagalan PDP, Notaris wajib menyampaikan pemberitahuan tertulis kepada Subjek Data Pribadi dan Lembaga paling lambat 3×24 jam, yang isinya minimal memuat data yang terungkap, waktu terungkap, serta upaya penanganan dan pemulihan.

Bentuk tanggung jawab hukum seorang Notaris terhadap kelalaian kebocoran data akta elektronik melalui sistem siber. Tanggung jawab Notaris ini mencakup aspek perdata dan pidana. Secara umum, Notaris sebagai penyelenggara sistem elektronik wajib bertanggung jawab atas kelalaianya terhadap kebocoran data, meskipun jenis tanggung jawab dan sanksinya belum diatur secara gamblang di aturan sebelumnya. Dalam kerangka UU PDP, Notaris bertanggung jawab untuk melakukan penyusunan dan implementasi langkah-langkah teknis dan operasional yang efektif, serta menetapkan tingkatan keamanan Data Pribadi. Apabila Notaris gagal dalam melindungi Data Pribadi, ia wajib mengumumkan kegagalan proteksi Data Pribadi kepada publik, sesuai dengan Pasal 46 UU PDP. Selain itu, UU PDP juga mengatur sanksi pidana yang tegas, di mana setiap orang yang dengan sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya dapat dipidana dengan penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 Miliar. Sanksi pidana yang lebih berat juga dikenakan bagi pembuat atau pemalsu Data Pribadi dengan maksud menguntungkan diri sendiri atau orang lain.

Daftar Pustaka

- Chastra, Deny Fernaldi. "Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris." *Indonesian Notary* 3, No.2 (2021): 248-267
- Dharmawan, Ni Ketut Supasti, Desak Putu Dewi Kasih, dan Deris Stiawan. "Personal Data Protection and Liability of Internet Service Provider: A Comparative Approach." *International Journal of Electrical and Computer Engineering (IJECE)* 9, No.4 (2019): 3175-3184.

- Fazriah, Dina. "Tanggung Jawab Atas Terjadinya Wanprestasi Yang Dilakukan Oleh Debitur Pada Saat Pelaksanaan Perjanjian." *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 1, No. 2 (2023): 1-25.
- Imanullah, Mohammad Najib. "Perlindungan hukum preventif dan represif bagi pengguna uang elektronik dalam melakukan transaksi tol nontunai." *Jurnal Privat Law* 9, No. 1 (2021): 218-226.
- Indarta, Yose. *Cyber Law: Dimensi Hukum dalam Era Digital*. Jakarta: Pustaka Galeri Mandiri, 2025.
- Irawan, Ade, M. Ryan Bakry, dan Frengki Hardian. "Eksistensi Aspek Teknologi Dalam Pembuatan Akta Autentik Secara Elektronik Pada Pengaturan Jabatan Notaris Di Era Industri 5.0." *COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat* 2, No. 8 (2022): 1501-1521.
- Laksana, Anak Agung Ngurah Mahendra Wahyu, dan Kadek Julia Mahadewi. "Legitimasi Hukum yang Tak Terbantahkan: Kekuatan Pembuktian Akta Dibawah Tangan yang Telah Disahkan oleh Notaris." *Jurnal Kewarganegaraan* 7, No.1 (2023): 466-471.
- Leba, Nikanort. "Pertanggungjawaban Hukum Kelalaian Pengemudi Perusahaan Dalam Kecelakaan Lalu Lintas Yang Mengakibatkan Kematian." *Lex Administratum* 11, No.1 (2023): 1-11
- Mipon, Intan Permata, dan Mohamad Fajri Mekka Putra. "Penyelenggaraan Pelindungan Data Pribadi oleh Notaris berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *Jurnal Hukum & Pembangunan* 53, No.3 (2023): 479 - 492
- Mislaini dan Habib Adjie. "Tanggung Jawab Notaris dalam Pengamanan Data Pribadi dalam Perjanjian Notariil Pada Era Digital". *Unes Law Review* 6, No. 2 (2023): 7481-7490.
- Mislaini, Mislaini, dan Habib Adjie. "Tanggung Jawab Notaris dalam Pengamanan Data Pribadi dalam Perjanjian Notariil Pada Era Digital." *UNES Law Review* 6, No.2 (2023): 7481-7490.
- Najib, Ainun. "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi." *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan* 7, No. 1 (2023): 43-59.
- Pramudy, Eri, Ranti Fauza Mayana, dan Tasya Safiranita Ramli. "Tinjauan Yuridis Penerapan Cyber Notary Berdasarkan Perspektif UU ITE dan UUJN." *Jurnal Indonesia Sosial Sains* 2, No. 8 (2021): 1239-1258.
- Rebeka, Sintya. "Perkembangan Peran Notaris Di Era Digital: Analisis Peluang Dan Tantangan Pasca UU No. 1 Tahun 2024." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 12, No.6 (2025): 2673-2684.
- Safaat, Ahmad M.S., *Penemuan Hukum Dan Berbagai Metode Interpretasi Atau Penafsiran Hukum*, Jakarta: Pusat Pengkajian Kebijakan Hukum dan Hak Asasi Manusia (PPKHHAM), 2015.
- Siregar, Maria Magdalena, Aarce Tehupeitory, dan L. Elly AM Pandiangan. "Analisis Hukum Kelalaian Pembuatan Akta Wasiat Oleh Notaris." *Jurnal Hukum To-Ra: Hukum Untuk Mengatur dan Melindungi Masyarakat* 9, No.1 (2023): 185-201.
- Sisca, Katarina Arinda. "Penegakan Hukum Notaris Yang Menggunakan Data Pribadi Orang Lain Dalam Akta: Perspektif Perlindungan Data." *Repertorium: Jurnal Ilmiah Hukum Kenotariatan* 13, No.1 (2024): 95-103.

- Susanti, Sari, and Sari Sari. "Integrasi Konsep Pelindungan Data Pribadi Pengguna Jasa Notaris Berdasarkan Undang Undang Pelindungan Data Pribadi dan Jabatan Notaris." *Innovative: Journal Of Social Science Research* 4, No.6 (2024): 688-705.
- Theixar, Regina Natalie, dan Ni Ketut Supasti Dharmawan. "Tanggung Jawab Notaris Dalam Menjaga Keamanan Digitalisasi Akta." *Acta Comitas: Jurnal Hukum Kenotariatan* 6, No. 1 (2021): 1-15.
- Wijayanti, Adinda Ari, dan I. Gusti Ketut Ariawan. "Upaya Perlindungan Terhadap Identitas Para Pihak Dalam Praktik Cyber Notary." *Acta Comitas: Jurnal Hukum Kenotariatan* 6, No.03 (2021): 679-695.

Peraturan Perundang-undangan

Kitab Undang-Undang Hukum Perdata

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124 Dan Tambahan Lembaran Negara Republik Indonesia Nomor 4674)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 Dan Tambahan Lembaran Negara Republik Indonesia Nomor 4843)

Undang-Undang Nomor 2 Tahun 2014 Tentang Perubahan Uu Nomor 30 Tahun 2004 Tentang Jabatan Notaris (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 3 Dan 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 Dan Tambahan Lembaran Negara Republik Indonesia Nomor 6820)