



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 2 (2026) pp: 11409-11422

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Ancaman Penggunaan *Deepfake* pada Kehadiran Penghadap dalam Layanan Kenotariatan

Hairul Anwar¹, Lena Hanifah²

¹Magister Hukum, Fakultas Hukum, Universitas Lambung Mangkurat

²Fakultas Hukum, Universitas Lambung Mangkurat

¹hairulanwar2610@gmail.com, ²lhaniifah@ulm.ac.id

Abstrak

Perkembangan teknologi kecerdasan buatan, khususnya *deepfake*, menghadirkan tantangan baru terhadap implementasi cyber notary di Indonesia. Penelitian ini bertujuan menganalisis ancaman manipulasi identitas digital terhadap keotentikan akta, bentuk pertanggungjawaban hukum notaris, kelemahan regulasi deteksi fraud biometrik, serta kontradiksi yuridis antara Undang-Undang Jabatan Notaris dan rezim hukum transaksi elektronik. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Bahan hukum dianalisis secara preskriptif melalui penelaahan terhadap KUHPdata, Undang-Undang Jabatan Notaris, Undang-Undang Informasi dan Transaksi Elektronik, serta regulasi dan praktik cyber notary di beberapa negara. Hasil penelitian menunjukkan bahwa teknologi *deepfake* mendekonstruksi asas *verschijnen* dan mengaburkan pemenuhan unsur “di hadapan” notaris sebagaimana dipersyaratkan Pasal 1868 KUHPdata dan Pasal 16 ayat (1) huruf m UUJN. Manipulasi identitas visual dan auditori berpotensi menimbulkan cacat kehendak berupa penipuan, sehingga akta kehilangan kekuatan pembuktian lahiriah, formal, dan materiil. Pertanggungjawaban notaris didasarkan pada prinsip *liability based on fault* dan hanya dapat dibebankan apabila terdapat kesengajaan atau kelalaian dalam memenuhi prinsip kehati-hatian. Penelitian ini juga menemukan adanya kekosongan pengaturan mengenai *liveness detection*, teknologi anti-spoofing, integrasi data kependudukan, serta batas pertanggungjawaban notaris. Oleh karena itu, diperlukan harmonisasi UUJN dan UU ITE melalui rekonstruksi regulasi cyber notary berbasis *Functional Equivalence Theory*. Rekonstruksi tersebut mencakup redefinisi frasa “menghadap” agar mencakup kehadiran virtual yang andal, penerapan autentikasi biometrik berlapis, penggunaan sertifikat elektronik tersertifikasi, pembangunan infrastruktur kenotariatan digital nasional, serta penetapan kegagalan deteksi manipulasi identitas tingkat lanjut sebagai risiko siber sistemik yang tidak otomatis membebani notaris guna menjamin kepastian hukum, perlindungan data pribadi, dan kepercayaan publik dalam transaksi elektronik nasional.

Kata kunci: Cyber Notary; Deepfake; Akta Autentik; Pertanggungjawaban Notaris; Verifikasi Identitas Digital.

1. Latar Belakang

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) telah memengaruhi berbagai sektor industri kreatif, termasuk industri musik. Teknologi tersebut memungkinkan pengguna untuk menghasilkan maupun mengolah karya musik melalui berbagai fitur, seperti perubahan aransemen, modifikasi karakter suara, hingga penciptaan versi baru dari lagu yang telah ada sebelumnya. Seiring dengan meningkatnya penggunaan *platform* digital, hasil adaptasi lagu berbasis kecerdasan buatan semakin mudah diproduksi, didistribusikan, dan diakses oleh masyarakat luas.

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam berbagai bidang, termasuk profesi notaris. Di era digital yang serba cepat, mekanisme kerja notaris yang masih mengandalkan pertemuan langsung dan dokumen fisik mulai dipandang kurang efektif dan efisien. Kondisi tersebut semakin mengemuka sejak pandemi COVID-19 yang membatasi interaksi tatap muka dan mendorong transformasi layanan berbasis digital.

Dalam bidang hukum, kecerdasan buatan (*Artificial Intelligence/AI*) memiliki potensi untuk meningkatkan akurasi dan efisiensi melalui kemampuannya mengenali permasalahan, merumuskan solusi secara cepat, serta menstrukturisasi pengetahuan secara digital. Pemanfaatan sistem AI dapat menjadi instrumen penting bagi notaris dalam menerapkan prinsip kehati-hatian, antara lain melalui identifikasi potensi kecurangan dengan algoritma pengenalan, penyusunan draf akta secara sistematis, serta pengurangan kesalahan dalam peninjauan hukum.

Transformasi menuju era industri 4.0 dan dampak berkelanjutan pascapandemi mendorong urgensi penerapan layanan kenotariatan berbasis digital (*cyber notary*). Konsep ini memungkinkan notaris melaksanakan tugasnya melalui media elektronik, mulai dari pembuatan, pengesahan, hingga penyimpanan dokumen secara digital dengan dukungan tanda tangan elektronik, sertifikat elektronik, dan pertemuan virtual. Penerapan *cyber notary* menawarkan efisiensi waktu dan biaya, perluasan akses layanan, serta peningkatan keamanan terhadap risiko pemalsuan dokumen.

Namun demikian, implementasi *cyber notary* di Indonesia masih menghadapi hambatan regulasi. Pasal 16 ayat (1) huruf m Undang-Undang Jabatan Notaris mewajibkan pembacaan dan penandatanganan akta dilakukan secara fisik di hadapan notaris, sedangkan Pasal 5 ayat (4) huruf b Undang-Undang Informasi dan Transaksi Elektronik secara eksplisit mengecualikan akta notariil dari dokumen elektronik yang memiliki kekuatan pembuktian penuh. Disharmoni norma tersebut menimbulkan ketidakpastian hukum bagi notaris yang berupaya mengadopsi teknologi digital tanpa mengabaikan kewajiban prosedural konvensional.

Sebagai pejabat umum, notaris memiliki kewenangan untuk membuat akta autentik yang berkedudukan sebagai alat bukti tertulis dengan kekuatan pembuktian sempurna. Kehadiran fisik para penghadap sebagaimana diatur dalam Undang-Undang Jabatan Notaris bukan sekadar formalitas administratif, melainkan mekanisme yuridis untuk memastikan kebenaran formil, kapasitas hukum, kebebasan kehendak, serta kesesuaian identitas para pihak. Integritas akta autentik sangat bergantung pada kemampuan notaris dalam memverifikasi secara langsung persesuaian kehendak para penghadap guna mencegah terjadinya cacat hukum.

Di sisi lain, peningkatan transaksi digital menuntut layanan notaris yang lebih cepat, mudah dijangkau, aman, dan tetap memiliki kepastian hukum. Tantangan utama dalam implementasi *cyber notary* tidak hanya berkaitan dengan aspek regulasi dan perlindungan data, tetapi juga ancaman penyalahgunaan teknologi AI, khususnya *deepfake*. Teknologi ini memungkinkan manipulasi identitas visual dan auditori secara real-time sehingga seseorang yang hadir dalam proses notarisasi virtual berpotensi hanyalah representasi digital hasil rekayasa.

Ancaman *deepfake* menjadi persoalan serius karena dapat mengaburkan kepastian hukum mengenai subjek hukum yang menghadap serta mengganggu pemenuhan asas kesepakatan sebagai syarat sah perjanjian. Fenomena *hyperreality* yang dihasilkan melalui rekayasa identitas digital berpotensi menghilangkan keotentikan proses, integritas dokumen, serta validitas kehendak para pihak. Apabila identitas dan kehadiran penghadap tidak dapat diverifikasi secara akurat, maka keabsahan formal maupun kekuatan pembuktian akta autentik dapat dipertanyakan.

Dalam konteks tersebut, penerapan prinsip kehati-hatian tidak lagi terbatas pada pemeriksaan dokumen dan verifikasi identitas secara konvensional, tetapi juga mencakup kemampuan notaris dalam mengenali risiko manipulasi digital. Kewaspadaan digital menjadi bagian integral dari pelaksanaan jabatan notaris untuk memastikan bahwa proses notarisasi tetap memenuhi unsur keautentikan, kepastian hukum, dan perlindungan terhadap para pihak. Dengan demikian, penguatan kompetensi digital serta dukungan sistem verifikasi berbasis teknologi menjadi kebutuhan yang tidak dapat diabaikan.

Selain itu, ketiadaan pengaturan khusus mengenai standar verifikasi identitas digital dan penggunaan teknologi AI dalam layanan kenotariatan berpotensi menimbulkan kekosongan hukum. Kondisi ini menempatkan notaris pada posisi yang rentan terhadap risiko sengketa maupun pertanggungjawaban hukum akibat penyalahgunaan teknologi. Oleh karena itu, diperlukan penguatan kerangka regulasi yang mampu mengakomodasi perkembangan teknologi tanpa mengesampingkan prinsip-prinsip dasar kenotariatan. Analisis terhadap risiko manipulasi AI dalam layanan *cyber notary* menjadi penting untuk menjaga validitas, keabsahan formal, serta kekuatan pembuktian lahiriah, formal, dan materiil akta autentik di era digital.

2. Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif yang berfokus pada pengkajian norma hukum positif, asas hukum, dan doktrin hukum yang berkaitan dengan perlindungan hak cipta terhadap praktik adaptasi lagu berbasis kecerdasan buatan. Penelitian hukum normatif digunakan karena objek kajian penelitian ini menitikberatkan pada pengaturan hukum terhadap praktik adaptasi lagu berbasis kecerdasan buatan dalam perspektif Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang berkaitan dengan hak cipta, khususnya Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, serta peraturan lain yang relevan dengan penggunaan karya musik pada *platform* digital. Sementara itu, pendekatan konseptual dilakukan melalui kajian terhadap pendapat para ahli, doktrin hukum, dan konsep-konsep yang berkaitan dengan hak cipta, hak moral, hak ekonomi, pengadaptasian, pengaransemenan, serta pemanfaatan kecerdasan buatan dalam industri musik.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer berupa peraturan perundang-undangan yang berkaitan dengan objek penelitian. Bahan hukum sekunder terdiri atas buku, jurnal ilmiah, hasil penelitian, dan pendapat para ahli yang membahas hak cipta dan perkembangan kecerdasan buatan. Adapun bahan hukum tersier berupa kamus hukum dan bahan penunjang lainnya. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (*library research*) dengan menelusuri, menginventarisasi, dan mempelajari berbagai bahan hukum yang relevan. Selanjutnya, seluruh bahan hukum dianalisis secara kualitatif dengan menggunakan metode penafsiran gramatikal dan sistematis untuk memperoleh argumentasi hukum mengenai pengaturan hak cipta terhadap praktik adaptasi lagu berbasis kecerdasan buatan.

Hasil analisis kemudian disusun secara deskriptif-analitis, sehingga diperoleh kesimpulan mengenai pengaturan hukum terhadap praktik adaptasi lagu berbasis kecerdasan buatan dalam perspektif hak cipta di Indonesia.

3. Hasil dan Diskusi

3.1 Manipulasi Identitas Visual dan Auditori dalam Skema *Cyber Notary*

Transformasi digital dalam layanan kenotariatan telah menggeser paradigma kehadiran dari pertemuan fisik menuju interaksi virtual. Pasal 16 ayat (1) huruf m Undang-Undang Nomor 2 Tahun 2014 tentang Jabatan Notaris (UUJN) mewajibkan notaris membacakan akta di hadapan penghadap dengan disaksikan paling sedikit dua orang saksi. Konsep *verschijnen* secara historis dimaknai sebagai kehadiran fisik secara langsung. Namun, perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/AI*), khususnya *deepfake*, menghadirkan ancaman baru terhadap autentisitas akta karena mampu merekayasa wajah dan suara seseorang dengan tingkat kemiripan yang sangat tinggi.

Manipulasi visual dan auditori melalui *deepfake* tidak hanya menimbulkan distorsi informasi, tetapi juga mengancam keaslian materiil akta. Ketika kehadiran fisik digantikan oleh kehadiran virtual, notaris berada pada posisi rentan karena kemampuan indrawi manusia tidak lagi memadai untuk membedakan subjek hukum yang sebenarnya dengan simulasi digital yang dihasilkan oleh algoritma *Generative Adversarial Networks* (GANs). Kondisi ini berpotensi mengganggu pelaksanaan kewajiban notaris untuk bertindak saksama sebagaimana diatur dalam Pasal 16 ayat (1) huruf a UUJN.

Transformasi digital dalam layanan kenotariatan pada hakikatnya tidak hanya mengubah media komunikasi antara notaris dan penghadap, tetapi juga menggeser paradigma pembuktian dari verifikasi berbasis kehadiran fisik menuju verifikasi berbasis teknologi. Pergeseran tersebut menuntut adanya penyesuaian terhadap konsep autentisitas yang selama ini dibangun atas interaksi langsung antara notaris dan para pihak. Tanpa mekanisme autentikasi digital yang memadai, pemanfaatan teknologi justru berpotensi mengurangi tingkat kepercayaan masyarakat terhadap akta autentik sebagai alat bukti yang memiliki kekuatan pembuktian sempurna.

Perkembangan teknologi kecerdasan buatan berlangsung jauh lebih cepat dibandingkan pembentukan regulasi. Ketidakseimbangan tersebut menciptakan kesenjangan antara norma hukum dan realitas praktik kenotariatan digital. Akibatnya, notaris dihadapkan pada situasi dilematis, yaitu tuntutan untuk beradaptasi dengan perkembangan teknologi sekaligus kewajiban untuk tetap mematuhi ketentuan hukum positif yang masih berorientasi pada kehadiran fisik. Oleh karena itu, tantangan utama dalam implementasi *cyber notary* tidak terletak pada penggunaan teknologi itu sendiri, melainkan pada kemampuan sistem hukum untuk menjaga keseimbangan antara inovasi digital dan prinsip-prinsip fundamental kenotariatan, khususnya kepastian hukum, kehati-hatian, dan perlindungan terhadap keotentikan akta.

Problem yuridis muncul ketika notaris melakukan identifikasi subjek hukum melalui media telekonferensi. Apabila notaris dikelabui oleh representasi visual hasil *deepfake*, maka identifikasi dalam kepala akta dan

komparasi menjadi cacat. Kondisi tersebut berimplikasi pada pelanggaran asas kecermatan yang melekat pada jabatan notaris dan berpotensi menimbulkan kelalaian dalam pelaksanaan kewajiban untuk bertindak saksama serta mengutamakan kepentingan para pihak sebagaimana diatur dalam Pasal 16 ayat (1) huruf a UUJN. Dalam konteks ini, manipulasi identitas digital tidak hanya mengancam keabsahan formal akta, tetapi juga meruntuhkan kepastian hukum karena tindakan hukum yang dituangkan dalam akta berpotensi dilakukan oleh subjek hukum yang tidak sah.

3.1.1. Dekonstruksi Asas *Verschijnen* di Era Digital

Secara teoretis, kehadiran fisik bertujuan agar notaris dapat memastikan secara langsung identitas, kapasitas hukum, dan kehendak bebas para pihak. Keaslian akta autentik tidak hanya ditentukan oleh bentuk formalnya, tetapi juga oleh proses pembentukannya di hadapan pejabat umum yang berwenang.

Dalam skema *cyber notary*, transmisi data video elektronik menciptakan kaburnya batas antara realitas dan simulasi. Penggunaan *deepfake* yang menampilkan representasi digital di layar pada hakikatnya menegasikan unsur kehadiran fisik (*verschijnen*) sebagaimana dipersyaratkan Pasal 1868 KUHPdata dan UUJN. Akibatnya, akta yang dihasilkan berpotensi mengalami cacat formil dan kehilangan sifat autentisitasnya.

Manipulasi identitas digital juga berdampak pada aspek materiil perjanjian. Pemalsuan identitas melalui *deepfake* dapat dikualifikasikan sebagai tipu muslihat (*bedrog*) sebagaimana diatur dalam Pasal 1321 *juncto* Pasal 1328 KUHPdata. Konsekuensinya, kesepakatan para pihak menjadi cacat sehingga perjanjian dapat dibatalkan karena tidak terpenuhinya syarat sah perjanjian sebagaimana dimaksud dalam Pasal 1320 KUHPdata.

Manipulasi identitas dalam skema *cyber notary* umumnya dilakukan melalui tiga mekanisme, yaitu:

- a. Rekayasa Visual dan Auditori, berupa peniruan wajah dan suara secara presisi selama proses notarisasi virtual.
- b. Fenomena *Hyperreality*, yaitu kaburnya batas antara fakta dan simulasi sehingga representasi digital tampak lebih nyata daripada subjek hukum yang sebenarnya.
- c. Manipulasi Kehadiran Virtual, yaitu penggunaan identitas hasil rekayasa untuk mengelabui notaris seolah-olah pihak yang sah hadir dan memberikan persetujuan.

Fenomena tersebut menunjukkan bahwa kehadiran virtual belum sepenuhnya dapat menggantikan kehadiran fisik dalam menjamin keamanan dan kepastian hukum. Oleh karena itu, diperlukan penguatan standar keamanan teknologi dan pembaruan regulasi *cyber notary* untuk menjamin perlindungan hukum preventif.

3.1.2. Ancaman *Deepfake* terhadap Kebenaran Materiil dan *Duty of Care* Notaris

Dalam hukum pembuktian, notaris dituntut untuk menjamin kebenaran materiil dari identitas dan kehendak para pihak. Intervensi teknologi *deepfake* mengaburkan batas antara kehendak dan pernyataan, sehingga identifikasi subjek hukum melalui media telekonferensi berpotensi mengalami cacat.

Kondisi ini menimbulkan dilema terhadap pelaksanaan *duty of care* notaris sebagaimana diatur dalam Pasal 16 ayat (1) huruf a UUJN. Kewajiban bertindak saksama tidak lagi cukup dilakukan melalui verifikasi konvensional karena manipulasi digital tingkat tinggi sulit dideteksi secara visual. Ketika identitas penghadap dimanipulasi, kebenaran materiil akta menjadi diragukan dan akta berpotensi kehilangan kekuatan pembuktiannya.

Perkembangan regulasi melalui Undang-Undang Nomor 1 Tahun 2024 yang menekankan penggunaan sertifikat elektronik turut memunculkan tumpang tindih antara verifikasi indrawi oleh notaris dan verifikasi sistematis oleh Penyelenggara Sertifikat Elektronik (PSrE). Ketiadaan infrastruktur keamanan biometrik, deteksi *liveness*, dan integrasi data kependudukan menyebabkan proses verifikasi virtual masih menyisakan celah hukum.

Apabila akta lahir dari proses identifikasi yang dimanipulasi oleh *deepfake*, maka syarat kesepakatan sebagaimana diatur dalam Pasal 1320 KUHPdata tidak terpenuhi. Manipulasi identitas tersebut dapat dikategorikan sebagai penipuan berdasarkan Pasal 1328 KUHPdata sehingga mengakibatkan akta kehilangan sifat autentisitasnya dan berpotensi batal demi hukum.

Permasalahan ini semakin kompleks karena pengaturan *cyber notary* di Indonesia masih bersifat ambivalen. Penjelasan Pasal 15 ayat (3) UUJN membuka ruang sertifikasi transaksi elektronik, sementara Pasal 16 ayat (1) huruf m UUJN dan Pasal 5 ayat (4) huruf b Undang-Undang Informasi dan Transaksi Elektronik tetap menegaskan pentingnya kehadiran fisik dan mengecualikan akta notariil dari dokumen elektronik. Kondisi tersebut menempatkan notaris pada risiko tanggung jawab profesional yang semakin besar.

3.1.3. Hakikat Kepastian Hukum dan Otentisitas Akta dalam Ranah Kenotariatan

Kepastian hukum menuntut agar hukum diterapkan secara jelas, konsisten, dan dapat diprediksi. Dalam ranah kenotariatan, kepastian hukum diwujudkan melalui akta autentik yang memiliki kekuatan pembuktian lahiriah, formal, dan materiil.

Keabsahan akta autentik sangat bergantung pada kepastian identitas para penghadap. Namun, UUJN belum mengatur secara rinci standar teknis verifikasi identitas, sehingga notaris pada umumnya hanya memeriksa dokumen identitas berdasarkan aspek lahiriahnya. Apabila dokumen tersebut merupakan hasil pemalsuan atau pencurian identitas yang tidak terdeteksi, maka akta yang dihasilkan mengandung cacat subjektif.

Dalam konteks *cyber notary*, risiko ketidakpastian identitas semakin meningkat akibat potensi manipulasi data biometrik dan akun digital. Tanpa protokol verifikasi yang setara dengan pertemuan fisik, penggunaan media elektronik membuka peluang terjadinya peniruan identitas yang mengancam keabsahan akta.

Pada praktiknya, notaris sering berada pada posisi yang dilematis. Di satu sisi, notaris bukan aparat penegak hukum yang memiliki kewenangan melakukan pemeriksaan forensik terhadap dokumen identitas. Namun, di sisi lain, notaris tetap memikul tanggung jawab atas kebenaran formil akta yang dibuatnya.

Oleh karena itu, diperlukan sinkronisasi antara sistem administrasi kependudukan dengan mekanisme verifikasi kenotariatan melalui integrasi data kependudukan, autentikasi biometrik, dan standar keamanan digital yang memadai. Kepastian hukum hanya dapat diwujudkan apabila notaris memiliki instrumen hukum dan teknis yang jelas untuk memverifikasi identitas para pihak. Tanpa dukungan tersebut, akta autentik yang seharusnya menjadi alat bukti terkuat justru berpotensi menjadi sumber ketidakpastian hukum baru.

3.2 Konsep Dasar *Hyperreality* dalam Dimensi Kenotariatan

Perkembangan teknologi informasi telah membawa hukum perdata Indonesia pada transformasi ontologis yang tidak hanya mengubah media pencatatan dari kertas ke digital, tetapi juga memengaruhi pemaknaan terhadap keautentikan akta. Dalam konteks ini, akta autentik yang selama ini dipahami sebagai manifestasi kebenaran formal dan materiil berhadapan dengan fenomena digitalisasi yang menciptakan ruang antara realitas dan simulasi.

Jean Baudrillard dalam *Simulacra and Simulation* menjelaskan bahwa *hyperreality* merupakan kondisi ketika simulasi menjadi lebih nyata daripada realitas itu sendiri. Dalam ranah kenotariatan, akta fisik pada mulanya merupakan representasi langsung dari kesepakatan para pihak yang terjadi di hadapan pejabat umum. Namun, transformasi menuju *cyber notary* menggeser paradigma tersebut karena akta digital tidak lagi sekadar merepresentasikan peristiwa hukum, melainkan menjadi realitas hukum itu sendiri dalam bentuk data dan kode biner.

Peralihan dari *paper-based reality* menuju *data-based hyperreality* mengubah mekanisme verifikasi dalam praktik kenotariatan. Notaris tidak lagi memeriksa tanda tangan basah dan kehadiran fisik para pihak, melainkan memverifikasi identitas digital melalui tanda tangan elektronik, sertifikat elektronik, dan sistem kriptografi. Akibatnya, keautentikan akta tidak lagi bertumpu pada interaksi langsung antara notaris dan penghadap, tetapi pada integritas sistem teknologi yang digunakan.

Meskipun demikian, Pasal 1868 KUHPerdata dan Pasal 16 ayat (1) huruf m Undang-Undang Jabatan Notaris tetap mensyaratkan bahwa akta autentik harus dibuat di hadapan pejabat umum yang berwenang. Secara doktrinal, frasa "di hadapan" dimaknai sebagai kehadiran fisik dalam ruang dan waktu yang sama. Kehadiran fisik tersebut merupakan sarana bagi notaris untuk memastikan identitas, kecakapan, dan kehendak bebas para pihak.

Konsep *virtual presence* yang berkembang dalam skema *cyber notary* menghadirkan tantangan terhadap konstruksi hukum tersebut. Meskipun para pihak dapat saling melihat dan mendengar melalui media elektronik, kehadiran virtual pada hakikatnya merupakan representasi audio-visual yang belum sepenuhnya diakui sebagai substitusi kehadiran fisik oleh hukum positif Indonesia. Kondisi ini menimbulkan ketegangan antara kebutuhan digitalisasi layanan hukum dan prinsip kehati-hatian dalam jabatan notaris.

Ancaman terbesar dalam dimensi *hyperreality* adalah munculnya teknologi *deepfake* sebagai bentuk *simulakratur murni*. Melalui manipulasi wajah dan suara berbasis kecerdasan buatan, identitas digital dapat terlepas sepenuhnya dari subjek hukum yang sebenarnya. Dalam situasi demikian, notaris berpotensi memberikan legitimasi hukum terhadap simulasi digital yang tidak memiliki keterkaitan dengan realitas biologis maupun kehendak asli para pihak.

Penggunaan *deepfake* dalam proses kenotariatan mengancam kebenaran materiil akta, karena notaris kehilangan kemampuan untuk memastikan bahwa pihak yang hadir benar-benar merupakan subjek hukum yang berwenang. Akibatnya, fungsi notaris sebagai pejabat umum yang menjamin kebenaran identitas, kapasitas hukum, dan kehendak para pihak mengalami dekonstruksi.

Risiko tersebut semakin kompleks karena transformasi identitas menjadi data (*datification*) menghilangkan berbagai unsur non-verbal yang selama ini menjadi indikator penting dalam pembentukan kesepakatan, seperti ekspresi wajah, intonasi suara, dan gestur tubuh. Oleh karena itu, ancaman *hyperreality* tidak hanya bersifat teknis, tetapi juga bersifat eksistensial terhadap fungsi notaris sebagai penjamin kebenaran materiil.

Di tengah perkembangan teknologi, notaris tetap memiliki kewajiban moral dan hukum untuk memastikan bahwa kehendak yang dituangkan dalam akta benar-benar berasal dari para pihak. Teknologi harus diposisikan sebagai sarana pendukung, bukan pengganti otoritas notaris sebagai pejabat umum. Oleh karena itu, diperlukan rekonstruksi regulasi yang mampu mengakomodasi digitalisasi tanpa menghilangkan prinsip dasar kenotariatan, khususnya kepastian hukum, keautentikan, dan prinsip kehati-hatian.

3.2.1. Ancaman Deepfake sebagai Simulakratur Murni

Teknologi *deepfake* merupakan manifestasi nyata dari konsep *simulakratur murni* yang dikemukakan Jean Baudrillard, yaitu kondisi ketika citra digital tidak lagi merepresentasikan realitas, melainkan berdiri sebagai entitas mandiri yang terputus dari subjek aslinya.

Dalam konteks kenotariatan, fenomena ini menciptakan paradoks karena identitas visual dan auditori yang ditampilkan melalui media elektronik dapat diterima sebagai kebenaran, padahal tidak memiliki hubungan dengan subjek hukum yang sesungguhnya. Akibatnya, notaris berisiko berhadapan dengan simulasi digital yang secara visual tampak autentik, tetapi secara hukum tidak memiliki legitimasi.

Penggunaan *deepfake* mengancam pemenuhan unsur "di hadapan" sebagaimana diatur dalam Pasal 1868 KUHPerdara dan Pasal 16 ayat (1) huruf m UUDN. Jika identitas yang hadir hanyalah simulasi digital, maka prosedur formal pembuatan akta tidak terpenuhi secara substantif sehingga akta berpotensi kehilangan sifat autentisitasnya.

Selain merusak kekuatan pembuktian formal, *deepfake* juga mengganggu kekuatan pembuktian materiil karena kehendak yang dituangkan dalam akta tidak berasal dari subjek hukum yang sebenarnya. Oleh karena itu, perkembangan teknologi simulasi menuntut pembaruan mekanisme autentikasi digital dan peningkatan standar verifikasi identitas dalam praktik *cyber notary*.

3.2.2. Transformasi Bentuk Hukum dari Paper-Based Menuju Data-Based

Digitalisasi layanan hukum telah menggeser paradigma akta autentik dari bentuk fisik berbasis kertas menuju bentuk elektronik berbasis data. Dalam sistem konvensional, kekuatan pembuktian akta bertumpu pada keberadaan fisik dokumen, tanda tangan basah, dan kehadiran langsung para pihak.

Dalam ekosistem digital, fungsi tersebut digantikan oleh sertifikat elektronik, infrastruktur kunci publik, dan mekanisme verifikasi berbasis sistem. Pergeseran ini menciptakan bentuk keautentikan baru yang bersandar pada validasi teknologi.

Namun, hukum positif Indonesia masih mempertahankan konsep kehadiran fisik sebagai syarat utama pembentukan akta autentik. Akibatnya, terjadi ketidaksinkronan antara perkembangan teknologi dan pengaturan normatif yang menimbulkan ketidakpastian hukum dalam implementasi *cyber notary*.

Oleh karena itu, diperlukan rekonstruksi terhadap konsep akta autentik yang tidak lagi berfokus pada media fisik, melainkan pada proses autentikasi yang mampu menjamin identitas, kehendak, dan integritas para pihak. Dengan demikian, digitalisasi kenotariatan dapat berjalan seiring dengan perlindungan terhadap kepastian hukum dan keautentikan akta.

3.3 Cacat Prosedural dan Kekuatan Pembuktian Akta Akibat Manipulasi *Deepfake*

Eksistensi akta autentik dalam sistem hukum perdata Indonesia bertumpu pada ketentuan Pasal 1868 Kitab Undang-Undang Hukum Perdata (KUHPperdata), yang mensyaratkan bahwa akta harus dibuat dalam bentuk yang ditentukan oleh undang-undang serta dibuat oleh atau di hadapan pejabat umum yang berwenang. Kewenangan notaris bersifat atributif, sehingga pelaksanaan jabatannya hanya sah sepanjang seluruh formalitas yang ditentukan dalam Undang-Undang Jabatan Notaris (UUJN) dipenuhi secara sempurna.

Salah satu formalitas esensial adalah kewajiban pembacaan dan penandatanganan akta sebagaimana diatur dalam Pasal 16 ayat (1) huruf m UUJN. Kewajiban ini bukan sekadar prosedur administratif, melainkan instrumen untuk memastikan bahwa isi akta telah dipahami dan disetujui secara sadar oleh para pihak. Oleh karena itu, frasa "di hadapan" secara doktrinal dimaknai sebagai kehadiran fisik para penghadap di hadapan notaris.

Penggunaan teknologi *deepfake* dalam skema *cyber notary* berpotensi meruntuhkan makna kehadiran tersebut. Meskipun teknologi komunikasi memungkinkan interaksi audio-visual secara real-time, manipulasi identitas melalui rekayasa wajah dan suara menghilangkan kemampuan notaris untuk melakukan verifikasi langsung terhadap identitas, kecakapan, dan kebebasan kehendak para pihak. Akibatnya, syarat formal pembuatan akta tidak lagi terpenuhi secara materiil.

3.3.1. Kecacatan Syarat Subjektif Sahnya Perjanjian (*Wilsgebreken*)

Dalam hukum perdata, kesepakatan menempati posisi sentral sebagai syarat subjektif sahnya perjanjian sebagaimana diatur dalam Pasal 1320 ayat (1) KUHPperdata. Kesepakatan merupakan manifestasi kehendak bebas para pihak untuk menimbulkan akibat hukum tertentu.

Asas kebebasan berkontrak (*partij autonomie*) memberikan ruang bagi setiap individu untuk menentukan nasib hukumnya sendiri, sepanjang tidak bertentangan dengan undang-undang, ketertiban umum, dan kesusilaan. Oleh karena itu, hukum memberikan perlindungan terhadap kehendak yang dinyatakan secara bebas sekaligus membuka kemungkinan pembatalan apabila kesepakatan lahir dari cacat kehendak (*wilsgebreken*).

Dalam doktrin hukum perdata, cacat kehendak meliputi kekhilafan (*dwaling*), paksaan (*dwang*), dan penipuan (*bedrog*). Kekhilafan sebagaimana diatur dalam Pasal 1322 KUHPperdata hanya relevan apabila menyangkut hakikat objek atau identitas subjek yang menjadi dasar utama perjanjian. Paksaan menurut Pasal 1324 KUHPperdata harus menimbulkan ketakutan yang nyata dan bersifat melawan hukum. Sementara itu, penipuan sebagaimana diatur dalam Pasal 1328 KUHPperdata mensyaratkan adanya tipu muslihat yang secara aktif mendorong pihak lain untuk melakukan perbuatan hukum yang sebenarnya tidak dikehendaki.

Dalam konteks *deepfake*, manipulasi identitas digital memenuhi karakteristik *bedrog* karena menciptakan representasi palsu yang mengelabui notaris maupun pihak lain mengenai identitas subjek hukum yang sebenarnya. Akibatnya, kesepakatan yang lahir tidak lagi mencerminkan kehendak autentik para pihak sehingga mengandung cacat subjektif dan berpotensi dibatalkan.

3.3.2. Distorsi Identitas Digital Melalui Teknologi *Deepfake*

Pasal 1868 KUHPdata mensyaratkan bahwa akta autentik dibuat oleh atau di hadapan pejabat umum yang berwenang. Frasa "di hadapan" secara normatif mengandung makna adanya kesatuan ruang dan waktu antara notaris dan para penghadap agar notaris dapat menjalankan fungsi konstatir secara langsung, yaitu melihat, mendengar, dan meyakini identitas serta kehendak para pihak.

Perkembangan teknologi *deepfake* menghadirkan tantangan serius terhadap konstruksi tersebut. Melalui manipulasi wajah dan suara secara real-time, teknologi ini menciptakan ilusi kehadiran yang sulit dibedakan dari realitas. Distorsi identitas digital tersebut meruntuhkan fungsi penginderaan notaris dan mengaburkan kepastian mengenai subjek hukum yang sebenarnya.

Konsekuensinya, syarat formal "di hadapan" sebagaimana dimaksud dalam Pasal 1868 KUHPdata tidak terpenuhi secara substansial. Kondisi ini semakin kompleks karena terdapat ketidaksinkronan norma antara Pasal 15 ayat (3) UUJN yang membuka ruang pemanfaatan teknologi informasi dengan Pasal 16 ayat (1) huruf m UUJN yang tetap mensyaratkan kehadiran fisik para pihak.

Ketiadaan regulasi yang secara khusus mengatur mekanisme verifikasi identitas digital dan mitigasi risiko *deepfake* menciptakan kekosongan hukum (*rechtsvacuum*) dalam implementasi *cyber notary*. Akibatnya, notaris dihadapkan pada risiko hukum yang tinggi tanpa didukung instrumen autentikasi yang memadai.

Apabila manipulasi identitas terbukti terjadi, akta yang dihasilkan kehilangan sifat autentisitasnya karena tidak memenuhi syarat formal pembentukan akta autentik. Berdasarkan Pasal 1869 KUHPdata, akta yang tidak dibuat sesuai ketentuan undang-undang tidak lagi memiliki kekuatan sebagai akta autentik dan hanya dapat diperlakukan sebagai akta di bawah tangan sepanjang ditandatangani oleh para pihak.

Namun, apabila penggunaan *deepfake* menyebabkan tidak terpenuhinya unsur kehadiran, identitas, dan kehendak yang sah dari para pihak, maka akta tersebut tidak hanya kehilangan kekuatan pembuktian formal dan materiil, tetapi juga tidak dapat dipertahankan sebagai alat bukti yang memiliki nilai pembuktian sempurna.

Manipulasi identitas melalui *deepfake* mengakibatkan runtuhnya kekuatan pembuktian lahiriah, formal, dan materiil akta. Hakim tidak lagi terikat pada kebenaran yang tercantum dalam akta, melainkan bebas menilai kekuatan pembuktiannya berdasarkan alat bukti lain yang diajukan di persidangan. Dengan demikian, penggunaan *deepfake* dalam layanan kenotariatan digital tidak hanya menimbulkan cacat prosedural, tetapi juga mengancam fungsi akta autentik sebagai instrumen utama dalam mewujudkan kepastian hukum.

3.4 Bentuk Pertanggung jawaban Hukum Notaris dalam Menjaga Keotentikan Akta dari Ancaman *Deepfake*

Pertanggungjawaban hukum notaris dalam menghadapi ancaman manipulasi identitas berbasis *Deepfake* harus ditempatkan dalam kerangka jabatan notaris sebagai pejabat umum yang menjalankan sebagian fungsi negara di bidang pembuktian perdata. Sebagai pejabat umum, notaris tidak memikul tanggung jawab mutlak (*strict liability*), melainkan pertanggungjawaban yang didasarkan pada adanya kesalahan (*liability based on fault*). Oleh karena itu, keberhasilan pelaku memanfaatkan teknologi *Deepfake* untuk memalsukan identitas penghadap tidak serta-merta menjadikan notaris bertanggung jawab secara hukum. Pertanggungjawaban baru dapat dibebankan apabila terbukti bahwa notaris melakukan kesengajaan (*dolus*) atau kelalaian (*culpa*) dalam menjalankan kewajiban jabatannya.

Parameter utama untuk menilai ada atau tidaknya kesalahan notaris merujuk pada kewajiban bertindak jujur, mandiri, tidak berpihak, dan saksama sebagaimana diatur dalam Pasal 16 ayat (1) huruf a Undang-Undang Jabatan Notaris. Prinsip kehati-hatian tersebut mengharuskan notaris melakukan verifikasi identitas secara optimal sesuai standar profesional yang berlaku. Dalam konteks ancaman *Deepfake*, ukuran kelalaian tidak dapat didasarkan pada kemampuan notaris mendeteksi manipulasi digital tingkat lanjut secara mandiri, melainkan pada ada atau tidaknya upaya yang patut dan wajar (*reasonable measures*) untuk memastikan keaslian identitas para penghadap.

Apabila notaris tetap melaksanakan pembuatan akta meskipun terdapat indikasi kuat mengenai ketidaksesuaian identitas, kejanggalan perilaku penghadap, inkonsistensi data kependudukan, atau tanda-tanda manipulasi visual dan audio, maka notaris dapat dinilai telah melanggar prinsip kehati-hatian. Sebaliknya, apabila notaris telah

melaksanakan seluruh prosedur verifikasi yang tersedia sesuai ketentuan peraturan perundang-undangan dan standar profesi, maka kerugian yang timbul akibat penggunaan *Deepfake* seharusnya dibebankan kepada pelaku pemalsuan, bukan kepada notaris.

Secara yuridis, bentuk pertanggungjawaban notaris dapat diklasifikasikan ke dalam tiga ranah, yaitu pertanggungjawaban administratif, perdata, dan pidana.

Pertama, pertanggungjawaban administratif timbul apabila notaris terbukti melanggar kewajiban jabatan sebagaimana diatur dalam Undang-Undang Jabatan Notaris dan Kode Etik Notaris. Pelanggaran terhadap kewajiban untuk bertindak saksama, memverifikasi identitas penghadap, atau memastikan terpenuhinya syarat formal pembuatan akta dapat dikenakan sanksi administratif berupa teguran lisan, teguran tertulis, pemberhentian sementara, hingga pemberhentian dengan tidak hormat. Penjatuhan sanksi administratif dilakukan melalui mekanisme pengawasan oleh Majelis Pengawas Notaris sesuai dengan tingkat pelanggaran yang dilakukan.

Kedua, pertanggungjawaban perdata lahir apabila kelalaian notaris mengakibatkan kerugian bagi para pihak. Berdasarkan Pasal 1365 KUHPerdata, notaris dapat dimintai ganti kerugian apabila terpenuhi unsur-unsur perbuatan melawan hukum, yaitu adanya perbuatan melawan hukum, adanya kesalahan, timbulnya kerugian, dan adanya hubungan kausal antara kesalahan notaris dengan kerugian yang dialami pihak lain. Dalam konteks *Deepfake*, tuntutan ganti rugi hanya dapat diajukan apabila dapat dibuktikan bahwa notaris mengabaikan kewajiban verifikasi identitas yang semestinya dilakukan sehingga memungkinkan terjadinya pemalsuan identitas.

Ketiga, pertanggungjawaban pidana hanya dapat dikenakan apabila notaris terbukti secara sengaja turut serta, membantu, atau mengetahui adanya manipulasi identitas digital dalam proses pembuatan akta. Penerapan sanksi pidana terhadap notaris tidak dapat didasarkan semata-mata pada kegagalan mendeteksi teknologi *Deepfake* yang canggih, melainkan harus dibuktikan adanya unsur kesengajaan, penyalahgunaan wewenang, atau persekongkolan dengan pelaku pemalsuan. Dengan demikian, pemidanaan terhadap notaris tetap harus berpedoman pada asas tiada pidana tanpa kesalahan (*geen straf zonder schuld*).

Rekonstruksi pertanggungjawaban hukum notaris dalam menghadapi ancaman *Deepfake* harus dibangun secara proporsional dengan memperhatikan keseimbangan antara perlindungan hukum bagi masyarakat dan perlindungan terhadap notaris sebagai pejabat umum. Negara tidak dapat membebankan seluruh risiko kegagalan otentikasi digital kepada notaris tanpa disertai penyediaan infrastruktur hukum dan teknologi yang memadai. Oleh karena itu, diperlukan regulasi yang mengatur standar verifikasi identitas digital, kewajiban penggunaan teknologi anti-spoofing, integrasi sistem dengan basis data kependudukan nasional, serta penyusunan standar operasional prosedur *Cyber Notary* yang jelas dan terukur.

Dengan adanya parameter verifikasi yang baku, batas antara risiko teknologi dan kelalaian notaris dapat ditentukan secara objektif. Kejelasan norma tersebut tidak hanya memberikan perlindungan hukum bagi notaris dalam menjalankan jabatannya, tetapi juga menjamin terpeliharanya kepercayaan publik terhadap akta otentik sebagai instrumen pembuktian yang memiliki kepastian, keadilan, dan kemanfaatan hukum.

3.5 Celah Hukum (*Legal Loopholes*) dan Kelemahan Regulasi Standardisasi Deteksi Fraud Biometrik Visual

Penempatan kewajiban verifikasi identitas pada notaris dalam ekosistem kenotariatan digital saat ini menghadapi persoalan mendasar berupa adanya celah hukum (*legal loopholes*) akibat ketiadaan regulasi teknis yang mengatur standardisasi sistem deteksi fraud biometrik visual. Meskipun Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik telah mewajibkan penyelenggara sistem elektronik untuk menjamin keamanan, keandalan, dan integritas sistem, pengaturan tersebut masih bersifat umum (*lex generalis*) dan belum secara spesifik mengatur standar teknologi anti-spoofing untuk mencegah manipulasi identitas berbasis kecerdasan buatan seperti *Deepfake*.

Ketiadaan parameter teknis tersebut menciptakan kontradiksi normatif yang serius. Di satu sisi, Pasal 39 ayat (1) dan Pasal 40 ayat (1) Undang-Undang Jabatan Notaris mewajibkan notaris mengenal penghadap dan memastikan seluruh prosedur pembacaan serta penandatanganan akta dilakukan sesuai ketentuan formal. Di sisi lain, negara belum menyediakan infrastruktur verifikasi digital yang terstandarisasi dan terintegrasi untuk mendukung

pelaksanaan kewajiban tersebut dalam ruang siber. Akibatnya, notaris dibebani tanggung jawab hukum yang tinggi tanpa disertai instrumen teknologi yang memadai untuk mendeteksi pemalsuan identitas berbasis biometrik.

Kesenjangan antara kewajiban normatif dan keterbatasan instrumen verifikasi tersebut menimbulkan ketidakpastian hukum mengenai batas pertanggungjawaban notaris. Kewajiban bertindak amanah, jujur, saksama, mandiri, tidak berpihak, dan menjaga kepentingan para pihak sebagaimana diatur dalam Pasal 16 ayat (1) huruf a UUJN tidak dapat ditafsirkan secara ekstensif hingga mewajibkan notaris memiliki kompetensi forensik digital untuk mengidentifikasi manipulasi *Deepfake* tingkat lanjut. Sebagaimana dikemukakan oleh Habib Adjie, tanggung jawab notaris pada dasarnya dibatasi pada aspek formal dan prosedural dalam pelaksanaan jabatan. Oleh karena itu, apabila notaris telah melaksanakan seluruh kewajiban verifikasi sesuai standar yang ditentukan peraturan perundang-undangan, maka kegagalan mendeteksi manipulasi digital yang berada di luar kemampuan manusia pada umumnya tidak dapat secara otomatis dikualifikasikan sebagai bentuk kelalaian jabatan.

Permasalahan menjadi semakin kompleks karena hingga saat ini belum terdapat regulasi yang mewajibkan integrasi sistem verifikasi identitas notaris dengan basis data biometrik nasional yang dikelola oleh Direktorat Kependudukan dan Pencatatan Sipil. Padahal, Pasal 58 ayat (4) Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan menegaskan bahwa data kependudukan dapat dimanfaatkan untuk pelayanan publik, pembangunan, alokasi anggaran, pembangunan demokrasi, serta penegakan hukum dan pencegahan kriminal. Ketidadaan integrasi tersebut menyebabkan proses verifikasi identitas dalam layanan kenotariatan digital masih bergantung pada dokumen dan tampilan visual yang rentan dimanipulasi.

3.5.1 Relevansi Teori *Self-Determination* Informasi terhadap Praktik *Liveness Detection*

Implementasi teknologi *Liveness Detection* dalam praktik *Cyber Notary* harus ditempatkan dalam kerangka perlindungan data pribadi dan penghormatan terhadap hak privasi individu. Pemanfaatan teknologi ini melibatkan pemrosesan data biometrik berupa citra wajah, pola suara, dan karakteristik fisiologis lainnya yang tergolong sebagai data pribadi bersifat spesifik dan sensitif.

Dalam perspektif Teori *Self-Determination* Informasi, setiap individu memiliki hak untuk menentukan kapan, bagaimana, dan sejauh mana informasi mengenai dirinya dikumpulkan, diproses, dan didistribusikan kepada pihak lain. Oleh karena itu, penggunaan teknologi *Liveness Detection* tidak dapat semata-mata dipandang sebagai instrumen keamanan digital, melainkan juga harus menjamin adanya persetujuan yang sah, transparansi pemrosesan data, pembatasan tujuan penggunaan, dan perlindungan terhadap risiko penyalahgunaan data biometrik.

Dalam konteks kenotariatan, penerapan prinsip *self-determination* informasi menjadi penting agar upaya notaris dalam mewujudkan kepastian hukum melalui verifikasi identitas tidak justru mengorbankan hak privasi para penghadap. Dengan demikian, pengembangan sistem verifikasi biometrik harus dilengkapi dengan mekanisme perlindungan data yang sejalan dengan prinsip kehati-hatian dan keadilan preventif.

3.5.2 Kekosongan Aturan Teknis (*Liveness Detection* dan *Anti-Spoofing*)

Ketidadaan standar teknis mengenai *Liveness Detection* dan *Anti-Spoofing* menimbulkan kekosongan hukum (*rechtsvacuum*) yang berdampak langsung terhadap kepastian hukum dalam pembentukan akta otentik secara elektronik. Tanpa adanya ambang batas teknis yang ditetapkan negara, validitas proses verifikasi identitas menjadi bergantung pada kebijakan masing-masing penyelenggara sistem elektronik yang memiliki tingkat keamanan berbeda-beda.

Kerentanan tersebut membuka peluang terjadinya manipulasi identitas melalui teknologi *Deepfake*, *Face Spoofing*, maupun *Presentation Attack* yang dapat mengakibatkan terjadinya cacat kehendak berupa penipuan (*bedrog*) sebagaimana diatur dalam Pasal 1328 KUHPdata. Dalam kondisi demikian, kesepakatan para pihak menjadi tercemar karena notaris tidak berhadapan dengan subjek hukum yang sebenarnya.

Lebih lanjut, kegagalan verifikasi identitas akibat manipulasi *Deepfake* juga berimplikasi terhadap tidak terpenuhinya syarat formal pembuatan akta otentik sebagaimana diatur dalam Pasal 1868 KUHPdata dan Pasal 16 ayat (1) huruf m UUJN. Ketidakterpenuhinya unsur "dibuat oleh atau di hadapan pejabat umum yang berwenang" menyebabkan akta kehilangan sifat otentiknya.

Konsekuensi yuridis atas pelanggaran formal tersebut ditegaskan dalam Pasal 1869 KUHPerdara, yang menyatakan bahwa akta yang dibuat oleh pejabat yang tidak berwenang atau mengandung cacat bentuk tidak mempunyai kekuatan sebagai akta otentik, melainkan hanya mempunyai kekuatan pembuktian sebagai akta di bawah tangan sepanjang ditandatangani oleh para pihak.

Namun demikian, dalam konteks manipulasi *Deepfake*, degradasi menjadi akta di bawah tangan tidak selalu dapat dipertahankan. Pemalsuan identitas yang menyebabkan ketidakpastian mengenai pihak yang sebenarnya memberikan persetujuan mengakibatkan hilangnya keaslian tanda tangan, identitas, dan kehendak para pihak. Dengan demikian, akta tersebut tidak hanya kehilangan otentisitasnya, tetapi juga kehilangan dasar validitas sebagai akta di bawah tangan karena unsur persetujuan yang sah tidak pernah terbentuk.

Akibatnya, akta yang lahir dari proses verifikasi identitas yang terkontaminasi *Deepfake* harus dipandang batal demi hukum (*nietig van rechtswege*), karena cacat tersebut menyentuh aspek fundamental pembentukan perjanjian dan otentisitas akta sejak awal. Akta demikian dianggap tidak pernah ada, tidak memiliki kekuatan pembuktian yang mengikat bagi hakim, dan seluruh akibat hukum yang ditimbulkannya menjadi gugur secara otomatis.

3.5.3 Kerentanan Penggunaan Platform Pihak Ketiga

Penggunaan platform komunikasi digital komersial pihak ketiga dalam praktik *Cyber Notary* menimbulkan risiko hukum yang signifikan karena sebagian besar platform tersebut tidak dirancang untuk memenuhi kebutuhan pembuktian hukum dan verifikasi identitas tingkat tinggi.

Secara teknis, platform komunikasi umum umumnya belum dilengkapi dengan fitur biometrik canggih seperti *Passive Liveness Detection*, *Active Liveness Detection*, maupun *Presentation Attack Detection* yang mampu mengidentifikasi manipulasi visual secara real-time. Selain itu, sebagian besar platform juga tidak menyediakan audit trail forensik, pencatatan metadata, dan mekanisme pembuktian digital yang memenuhi standar pembuktian elektronik.

Kondisi tersebut menyebabkan notaris berpotensi gagal memenuhi kewajiban untuk mengenal penghadap sebagaimana diatur dalam Pasal 39 ayat (1) UUN. Kegagalan verifikasi identitas yang bersumber dari keterbatasan sistem pihak ketiga pada akhirnya dapat berimplikasi pada hilangnya keotentikan akta.

Oleh karena itu, diperlukan pembangunan infrastruktur kenotariatan digital yang terstandarisasi oleh negara (*state-standardized infrastructure*) dan terintegrasi dengan basis data kependudukan nasional. Integrasi dengan sistem Direktorat Jenderal Kependudukan dan Pencatatan Sipil yang dilengkapi teknologi anti-spoofing akan memberikan kepastian hukum yang lebih kuat bagi notaris dalam menjalankan kewajiban verifikasi identitas.

Dalam hal notaris telah menggunakan sistem resmi yang tersertifikasi negara dan melaksanakan seluruh prosedur verifikasi sesuai standar operasional yang berlaku, maka kegagalan sistem dalam mendeteksi manipulasi *Deepfake* tingkat lanjut patut dikualifikasikan sebagai risiko siber yang berada di luar kendali notaris (*cyber force majeure*). Dengan demikian, tanggung jawab hukum atas kegagalan sistem tidak dibebankan kepada notaris secara pribadi, melainkan kepada penyelenggara sistem elektronik sesuai prinsip pembagian tanggung jawab dalam penyelenggaraan sistem elektronik.

Sebaliknya, apabila notaris tetap menggunakan platform digital yang tidak memenuhi standar keamanan dan verifikasi biometrik yang memadai, maka notaris dapat dianggap tidak memenuhi prinsip kehati-hatian dalam menjalankan jabatan. Dalam keadaan demikian, notaris berpotensi dimintai pertanggungjawaban administratif maupun perdata apabila terbukti terdapat hubungan kausal antara kelalaiannya dengan kerugian yang dialami para pihak.

3.6 Kontradiksi Yuridis antara Kewajiban Absolut UUN dan Realitas Ruang Digital

Eksistensi notaris dalam sistem hukum Indonesia menempati posisi sentral sebagai pejabat umum yang diberikan kewenangan atribusi oleh negara untuk membuat akta autentik. Berdasarkan Pasal 1868 Kitab Undang-Undang Hukum Perdata (KUHPerdara), akta autentik merupakan akta yang dibuat dalam bentuk yang ditentukan undang-undang, oleh atau di hadapan pejabat umum yang berwenang, serta dibuat dalam wilayah kewenangannya.

Ketentuan tersebut menegaskan bahwa autentisitas akta tidak hanya ditentukan oleh substansi perbuatan hukum, tetapi juga oleh terpenuhinya syarat formil yang melekat pada proses pembuatannya.

Dalam menjalankan kewenangannya, notaris terikat pada prinsip *tabellionis officium fideliter exercebo* yang menghendaki pelaksanaan jabatan secara saksama, mandiri, tidak berpihak, dan berlandaskan prinsip kehati-hatian. Prinsip tersebut tercermin dalam kewajiban notaris untuk memastikan identitas, kecakapan hukum, serta kehendak bebas para pihak sebelum menuangkannya ke dalam akta autentik. Oleh karena itu, kehadiran fisik para penghadap selama proses pembacaan dan penandatanganan akta dipandang sebagai instrumen untuk menjamin kepastian hukum dan mencegah terjadinya sengketa di kemudian hari.

Namun, perkembangan teknologi informasi telah melahirkan ruang siber (*cyberspace*) yang mengubah pola interaksi hukum masyarakat. Transaksi elektronik, identitas digital, dan komunikasi berbasis telekonferensi telah mendorong lahirnya konsep *Cyber Notary* yang menawarkan redefinisi kehadiran dari dimensi fisik menjadi kehadiran virtual. Konsep ini menimbulkan kontradiksi dengan Pasal 16 ayat (1) huruf m Undang-Undang Nomor 2 Tahun 2014 tentang Jabatan Notaris yang mewajibkan pembacaan dan penandatanganan akta dilakukan secara langsung di hadapan notaris.

Ketegangan normatif tersebut semakin diperkuat oleh Putusan Mahkamah Konstitusi Nomor 22/PUU-XVII/2019 yang menegaskan bahwa unsur "menghadap" harus dimaknai sebagai kehadiran fisik secara nyata. Di sisi lain, Pasal 5 ayat (4) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 mengecualikan akta notaris dari kategori dokumen elektronik yang memiliki kekuatan hukum. Kondisi ini menunjukkan adanya disharmonisasi antara UUNJ dan UU ITE yang menimbulkan kekosongan hukum (*rechtsvacuum*) dalam implementasi *Cyber Notary* di Indonesia.

3.6.1. Karakteristik Ruang Digital dan Urgensi *Cyber Notary* di Indonesia

Perkembangan teknologi digital telah mengubah identitas, dokumen, dan hubungan hukum menjadi representasi data elektronik yang dapat dipertukarkan secara cepat tanpa batas teritorial. Dematerialisasi tersebut menggeser paradigma eksistensi subjek hukum dari entitas yang terikat ruang fisik menjadi entitas digital yang beroperasi dalam ruang siber yang bersifat nirbatas (*borderless*).

Transformasi tersebut turut mengubah mekanisme verifikasi identitas. Identitas yang semula dibuktikan melalui dokumen fisik kini direpresentasikan melalui sertifikat elektronik dan tanda tangan elektronik yang didukung infrastruktur kunci publik (*Public Key Infrastructure*). Melalui teknologi tersebut, integritas data, autentikasi identitas, dan prinsip nirsangkal (*non-repudiation*) dapat diwujudkan dalam transaksi elektronik.

Karakteristik ruang digital tersebut berbenturan dengan sistem kenotariatan Indonesia yang masih berorientasi pada kehadiran fisik. Padahal, meningkatnya transaksi elektronik menuntut kehadiran notaris sebagai pihak ketiga tepercaya (*trusted third party*) yang mampu menjamin kepastian hukum dalam ruang siber. Oleh karena itu, pelembagaan *Cyber Notary* menjadi kebutuhan mendesak untuk menjembatani kepastian hukum konvensional dengan perkembangan teknologi digital.

3.6.2. Analisis Komparatif Implementasi *Cyber Notary* di Negara-Negara *Civil Law* (atau *Common Law*)

Transformasi layanan kenotariatan di berbagai negara umumnya didasarkan pada *Functional Equivalence Theory* yang diperkenalkan oleh UNCITRAL. Teori ini menegaskan bahwa dokumen elektronik dapat memperoleh pengakuan hukum yang setara dengan dokumen fisik sepanjang mampu memenuhi fungsi hukum yang sama, khususnya dalam aspek autentikasi, integritas, dan pembuktian.

Prancis menjadi salah satu negara yang mengadopsi pendekatan progresif melalui *Acte Authentique Électronique* (AAE), yang memberikan kekuatan pembuktian sempurna (*force probante*) dan kekuatan eksekutorial (*force exécutoire*) terhadap akta elektronik. Sementara itu, Jerman melalui *Gesetz zur Umsetzung der Digitalisierungsrichtlinie* (DiRUG) menerapkan *Online-Beurkundung* secara terbatas, khususnya dalam pendirian perseroan terbatas (*GmbH*).

Dalam mitigasi risiko siber, Jerman menerapkan standar keamanan yang ketat melalui penggunaan *electronic identity* (eID) berbasis *Near Field Communication* (NFC), teknologi *liveness detection*, serta penyimpanan dokumen dalam *Elektronisches Urkundenarchiv*. Berbeda dengan negara-negara tersebut, implementasi *Cyber Notary* di Indonesia masih terkendala antinomi antara Penjelasan Pasal 15 ayat (3) UUJN dan Pasal 5 ayat (4) UU ITE, serta rigiditas penafsiran frasa "menghadap" sebagai kehadiran fisik.

3.6.3 Rekonstruksi Harmonisasi Regulasi *Cyber Notary* dalam Menghadapi Ancaman Deepfake

Pembentukan rezim *Cyber Notary* di Indonesia memerlukan harmonisasi antara UUJN dan UU ITE melalui rekonstruksi regulasi yang komprehensif. Langkah awal yang perlu dilakukan adalah redefinisi frasa "menghadap" agar tidak lagi dimaknai secara eksklusif sebagai kehadiran fisik, melainkan mencakup kehadiran virtual yang memiliki tingkat keandalan setara berdasarkan pendekatan *Functional Equivalence Theory*.

Pengakuan terhadap kehadiran virtual harus diimbangi dengan penerapan standar keamanan siber yang ketat. Revisi UUJN perlu mengatur penggunaan verifikasi biometrik berlapis (*multi-factor biometric authentication*), integrasi dengan data kependudukan nasional, penggunaan sertifikat elektronik tersertifikasi, teknologi *liveness detection*, serta sistem anti-spoofing sesuai standar ISO/IEC 30107.

Selain itu, negara perlu membangun infrastruktur digital kenotariatan nasional yang terintegrasi melalui kerja sama antara Kementerian Hukum, Kementerian Komunikasi dan Digital, Badan Siber dan Sandi Negara, serta Direktorat Jenderal Kependudukan dan Pencatatan Sipil. Pengaturan tersebut juga harus memberikan kepastian mengenai batas pertanggungjawaban notaris terhadap kegagalan deteksi manipulasi identitas berbasis *deepfake*. Sepanjang notaris telah melaksanakan prosedur verifikasi sesuai standar yang ditetapkan, kegagalan deteksi akibat manipulasi teknologi tingkat tinggi sepatutnya dikualifikasikan sebagai risiko siber sistemik (*force majeure digital*), sehingga tanggung jawab hukum dapat dialihkan kepada penyelenggara sistem elektronik yang lalai memenuhi standar keamanan.

4. Kesimpulan

Perkembangan teknologi kecerdasan buatan, khususnya teknologi *deepfake*, telah menghadirkan tantangan mendasar terhadap implementasi *cyber notary* di Indonesia. Manipulasi identitas visual dan auditori melalui rekayasa wajah serta suara mampu mendekonstruksi asas *verschijnen* yang selama ini dimaknai sebagai kehadiran fisik para penghadap di hadapan notaris. Fenomena *hyperreality* menyebabkan batas antara realitas dan simulasi menjadi kabur, sehingga notaris tidak lagi dapat mengandalkan kemampuan indrawi semata untuk memastikan identitas, kecakapan hukum, dan kehendak bebas para pihak. Kondisi tersebut berimplikasi pada meningkatnya risiko terjadinya cacat kehendak (*wilsgebreken*), khususnya penipuan (*bedrog*), yang mengakibatkan tidak terpenuhinya syarat subjektif sahnyanya perjanjian sebagaimana diatur dalam Pasal 1320 juncto Pasal 1328 KUHPerdata. Penggunaan identitas digital hasil manipulasi *deepfake* dalam proses pembuatan akta juga berpotensi menimbulkan cacat prosedural yang meruntuhkan kekuatan pembuktian akta autentik. Distorsi identitas digital menyebabkan unsur "dibuat oleh atau di hadapan pejabat umum yang berwenang" sebagaimana diatur dalam Pasal 1868 KUHPerdata dan Pasal 16 ayat (1) huruf m UUJN tidak terpenuhi secara substantif. Akibatnya, akta kehilangan kekuatan pembuktian lahiriah, formal, dan materiil, bahkan dalam kondisi tertentu dapat dinyatakan batal demi hukum (*nietig van rechtswege*) karena tidak pernah terbentuk kesepakatan yang sah sejak awal. Dengan demikian, ancaman *deepfake* tidak hanya menimbulkan persoalan teknis dalam verifikasi identitas, tetapi juga mengancam eksistensi akta autentik sebagai instrumen utama kepastian hukum dalam sistem pembuktian perdata Indonesia. Pertanggungjawaban hukum notaris dalam menghadapi ancaman *deepfake* harus didasarkan pada prinsip tanggung jawab karena kesalahan (*liability based on fault*) dan bukan tanggung jawab mutlak (*strict liability*). Notaris hanya dapat dimintai pertanggungjawaban administratif, perdata, maupun pidana apabila terbukti melakukan kesengajaan atau kelalaian dalam memenuhi kewajiban untuk bertindak jujur, mandiri, tidak berpihak, dan saksama sebagaimana diatur dalam Pasal 16 ayat (1) huruf a UUJN. Namun demikian, pengaturan hukum positif saat ini masih menyisakan celah hukum berupa ketiadaan standar teknis verifikasi identitas digital, *liveness detection*, teknologi anti-spoofing, serta integrasi dengan basis data kependudukan nasional. Kondisi tersebut menimbulkan ketidakpastian mengenai batas pertanggungjawaban notaris sekaligus menempatkan notaris pada posisi yang rentan terhadap risiko hukum akibat kegagalan deteksi manipulasi identitas berbasis kecerdasan buatan. Di sisi lain, implementasi *cyber notary* di Indonesia masih menghadapi kontradiksi yuridis antara kebutuhan digitalisasi layanan hukum dengan rigiditas pengaturan dalam UUJN dan UU ITE. Kewajiban kehadiran fisik sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf m UUJN dan pengecualian akta notaris dari dokumen elektronik berdasarkan Pasal 5 ayat (4) UU ITE menunjukkan adanya disharmonisasi regulasi yang

menghambat pelebagaan *cyber notary*. Oleh karena itu, diperlukan rekonstruksi hukum melalui harmonisasi antara UUJN dan UU ITE dengan mengadopsi pendekatan *Functional Equivalence Theory*, redefinisi frasa “menghadap” agar mencakup kehadiran virtual yang andal, standarisasi verifikasi biometrik berlapis, penerapan teknologi *liveness detection* dan *anti-spoofing*, serta pembangunan infrastruktur kenotariatan digital nasional yang terintegrasi. Selain itu, perlu ditetapkan batas pertanggungjawaban notaris secara tegas sehingga kegagalan deteksi manipulasi identitas yang terjadi meskipun notaris telah melaksanakan seluruh prosedur verifikasi sesuai standar dapat dikualifikasikan sebagai risiko siber sistemik (*digital force majeure*).

Referensi

1. Adjie, Habib. 2008. Hukum Kenotariatan Indonesia: Penjelasan Tematis Jabatan Notaris Berdasarkan UUJN. Bandung: Refika Aditama.
2. Adjie, Habib. 2009. Sanksi Perdata Dan Administrasi Terhadap Notaris Sebagai Pejabat Publik. Bandung: Refika Aditama.
3. Baudrillard, Jean. 1994. Simulacra and Simulation. New York: University of Michigan Press.
4. Budiono, Herlien. 2013. Kumpulan Tulisan Hukum Kenotariatan. Bandung: PT Citra Aditya Bakti.
5. Hadjon, Philipus M. 1987. Perlindungan Hukum Bagi Rakyat Indonesia. Surabaya: Bina Ilmu.
6. HS., Salim. 2019. Peraturan Jabatan Notaris. Jakarta: Sinar Grafika.
7. Kie, Tan Thong. Studi Notariat.
8. Makarim, Edmon. Notaris dan Transaksi Elektronik: Kajian Hukum tentang Cybernotary atau Electronic Notary di Indonesia. Jakarta.
9. Marzuki, Peter Mahmud. 2008. Pengantar Ilmu Hukum. Jakarta: Kencana.
10. Mertokusumo, Sudikno. 2007. Mengenal Hukum: Suatu Pengantar. Yogyakarta: Liberty.
11. Repi, Viktor Vekky Ronald, dkk. 2024. *Artificial intelligence*. Sidoarjo: Penamuda Media.
12. Saputra, A. D. 2025. Praktik Kenotariatan Notaris dan AI. CV Rey Media Grafika.
13. Subekti. Hukum Perjanjian.
14. Sutarno. 2010. Tanggung Jawab Profesi Notaris.
15. Tim Penulis IKANO UNPAD. 2023. Cyber Notary Dan Tantangan Notaris Di Era Digital. Bandung: PT Refika Aditama.
16. Tim Penyusun PDAT. 2024. Bahaya *Deepfake* AI Dan Bagaimana Dampak Negatif Di Berbagai Negara. Jakarta: TEMPO Publishing.
17. Westin, Alan. 1967. Privacy and Freedom. New York Atheneum.
18. Wesna, Putu Ayu Sriasih. 2022. Hukum Cyber Notary. Malang PT Literasi Nusantara Abadi Group.