

PERLINDUNGAN HUKUM BAGI PARA PIHAK DALAM AKTA NOTARIS YANG DIBUAT SECARA ELEKTRONIK

Satria Adi Nugraha

- Universitas Jember –

nugrahas327@gmail.com

ABSTRAK

Kemajuan teknologi informasi berdampak pada perkembangan hukum dan penerapannya, termasuk pada peran dan fungsi notaris dalam memberikan layanan secara elektronik, yang dikenal dengan istilah cyber notary. Konsep ini bertujuan untuk menyederhanakan dan mempermudah pelayanan bagi para pihak yang berkepentingan. Namun, di Indonesia belum terdapat kerangka hukum khusus yang mengatur mengenai cyber notary. Penelitian ini mengkaji perlindungan hukum terhadap keamanan data cyber notary berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini menggunakan metode penelitian hukum normatif atau doktrinal, dengan memanfaatkan bahan hukum primer dan sekunder. Pengumpulan bahan hukum dilakukan melalui studi dokumen atau studi kepustakaan. Analisis dilakukan secara deskriptif dengan menggunakan pendekatan perundang-undangan dan pendekatan konseptual. Penelitian ini menyimpulkan bahwa prosedur pelaksanaan cyber notary harus mengikuti ketentuan dalam pembuatan akta secara manual serta pengolahan Data Pribadi sebagaimana diatur dalam Pasal 16 hingga Pasal 18 Undang-Undang Perlindungan Data Pribadi. Perlindungan hukum terhadap keamanan data cyber notary akibat kelalaian notaris diatur dalam Pasal 46 dan Pasal 47, sedangkan perlindungan terhadap kejahatan siber diatur dalam Pasal 67 dan Pasal 68 Undang-Undang Perlindungan Data Pribadi.

Kata Kunci : Penyalahgunaan Keadaan, Notaris, Tanggung Jawab Notaris.

A. PENDAHULUAN

Perkembangan teknologi informasi yang demikian pesat telah membawa berbagai dampak yang sangat signifikan. Berbagai macam kemudahan ditawarkan oleh perkembangan telekomunikasi telah memungkinkan hubungan antar umat manusia dapat berlangsung secara cepat dan mudah tanpa memperhitungkan aspek ruang dan waktu. Di sisi lain, notaris sebagai pejabat umum yang bertugas melayani masyarakat diharapkan tidak ketinggalan dalam menyikapi perkembangan yang terjadi ini.

Cyber Notary merupakan konsep yang memanfaatkan kemajuan teknologi bagi para notaris untuk membuat akta autentik dalam dunia maya serta menjalankan tugasnya setiap hari. Misalnya: penandatanganan akta secara elektronik dan Rapat Umum Pemegang Saham secara telekonferensi. Hal ini bertujuan untuk mempermudah para pihak yang tinggalnya berjauhan, sehingga dengan adanya *cyber notary*, jarak tidak menjadi masalah lagi. Dengan adanya *cyber notary* dimaksudkan untuk memudahkan atau mempercepat pelaksanaan tugas dan kewenangan Notaris dalam membuat akta

otentik mengenai semua perbuatan atau perjanjian atau ketetapan yang diharuskan Undang-Undang atau apa yang dikehendaki para pihak yang berkepentingan untuk dinyatakan dalam akta autentik.

Tidak demikian dengan Pasal 16 ayat 1 huruf (m) UU Nomor 2 Tahun 2014 yang menyatakan bahwa: notaris harus hadir untuk membacakan dan menandatangani akta. Selain itu, akta yang dibuat tersebut masih memiliki tanda tanya apakah sudah memenuhi keotentikan akta yang telah diatur dalam Pasal 1868 Kitab Undang-Undang Hukum Perdata (KUH Perdata) atau tidak karena ketentuan dalam Pasal 1868 KUH Perdata merupakan syarat otentitas akta yang menyatakan bahwa suatu akta otentik adalah akta yang dibuat dalam bentuk yang ditentukan oleh undang-undang, dibuat oleh atau di hadapan pegawai-pegawai umum yang berkuasa untuk itu dan di tempat di mana akta dibuatnya.

Pengesahan akta notaris yang dibuat dengan cara *cyber notary* sebenarnya rawan untuk disalahgunakan oleh para pihak yang beritikad tidak baik. Apabila timbul suatu sengketa, para pihak dapat memungkiri proses pembacaan yang tidak dilakukan dengan benar-benar menghadap kepada notaris. *Cyber notary* dapat mengandung pengertian bahwa akta notaris yang dibuat dengan melalui alat elektronik atau notaris hanya mengesahkan suatu perjanjian yang pembacaan dan penandatanganan aktanya tidak dilakukan di hadapan notaris. Transaksi elektronik merupakan suatu perjanjian yang pembacaan dan penandatanganan aktanya tidak dilakukan di hadapan notaris. Hal tersebut akan mengakibatkan kerancuan apakah akta notaris tersebut telah memenuhi ketentuan sebagai akta autentik jika dikaitkan dengan Pasal 16 ayat 1 huruf (m) Undang-Undang Nomor 2 Tahun 2014 dan Pasal 1868 KUH Perdata.

Sebagaimana dalam *The United Nation Commision on International Trade Law* (UNCITRAL) yang telah lama merekomendasikan tentang perlunya pengakuan terhadap nilai hukum pada suatu informasi dan/atau dokumen elektronik. Sehubungan dengan itu, urgensi fungsi dan peran notaris secara elektronik mengemuka pada *International Congres XXIV* dari Latin Notaris Tahun 2004 yang kemudian kembali dibahas dalam *Working Group* untuk *Theme II (The Notary and Electronic Contracts)*. Dalam pembahasannya dianjurkan agar notaris membuka diri dengan mengakomodir semua perkembangan teknologi dengan tidak mengurangi ketentuan sebagaimana mestinya dengan menerima kemungkinan pembuatan akta autentik secara elektronik. Berdasarkan hal tersebut beberapa negara telah menerapkan *electronic notary* ataupun *cyber notary*

dalam sistem hukum nasionalnya, seperti Amerika dan Perancis. Berbeda halnya dengan Indonesia yang sampai saat ini masih belum sepenuhnya mengakomodir penerapan *electronic notary/cyber notary*.

Keberlakuan *cyber notary* dalam UUJN turut didukung dalam Pasal 1 angka 2 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur bahwa: “Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.”. Adanya UU ITE semakin menguatkan keberlakuan *cyber notary* di Indonesia. Sehingga tidak menutup kemungkinan Notaris dalam menjalankan jabatannya dapat dilakukan dengan jarak jauh dengan memanfaatkan kemajuan teknologi dewasa ini.

B. PERMASALAHAN

Berdasarkan uraian latar belakang di atas, maka dapat dirumuskan rumusan masalahnya antara lain sebagai berikut:

1. Bagaimana keabsahan hukum dari akta notaris yang dibuat secara elektronik menurut regulasi yang berlaku di Indonesia?
2. Apa saja tantangan dan kendala yang dihadapi dalam penerapan *cyber notary* di Indonesia?
3. Bagaimana mekanisme perlindungan hukum bagi para pihak yang terlibat dalam akta notaris elektronik dari aspek keamanan data dan kekuatan pembuktian?

C. PEMBAHASAN

1. Keabsahan Hukum dari Akta Notaris yang Dibuat Secara Elektronik

Pada Pasal 1 ayat 4 UU Nomor 11 Tahun 2008 tentang Informasi dan Tansaksi Elektronik (yang kemudian disebut UU ITE) menjelaskan bahwa akta elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan didengar melalui komputer atau sistem elektronik tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, atau simbol yang mempunyai makna dan dapat dipahami oleh orang yang mampu

memahaminya. Pada Pasal 5 ayat 1 UU ITE kemudian juga dijelaskan bahwa akta elektronik dapat digunakan sebagai alat bukti yang legal.

Berkenaan dengan wewenang lainnya yang dibebankan pada notaris adalah mensertifikasi transaksi yang menggunakan *cyber notary* sehingga hasil cetakan sertifikasi tersebut dapat dikelompokkan dalam akta elektronik. Suatu akta elektronik harus memiliki sejumlah unsur sebagaimana pada Pasal 1868 KUHperdata tentang keaslian dokumen. Tahap dalam pencetakan dokumen dengan cara konvensional, seperti:

- a. Para pihak/penghadap mendatangi kantor notaris kemudian menemui notaris dengan tujuan menyampaikan maksud dan tujuan mereka untuk selanjutnya dimasukkan pada akta notaris.
- b. Sesudahnya notaris mendengarkan maksud dan tujuan dari para pihak, notaris harus mengambil tindakan hukum atas apa yang dimaksudkan oleh para pihak sekaligus memberi definisi hukum terkait dokumen yang akan dibuat apakah telah sesuai dengan undang-undang atau tidak.
- c. Sesudahnya notaris mengetahui tindakan hukum yang dimaksudkan oleh para pihak, kemudian notaris membuat akta dengan bentuk serta cara yang sebagaimana dijelaskan pada Pasal 38 UUJN.

Wujud dan langkah-langkah pembuatan akta notaris dapat dikatakan sah apabila telah memenuhi ketentuan sebagaimana yang dijelaskan pada Pasal 38 UUJN. Adapun berkaitan dengan pembacaan akta yang dilakukan oleh notaris merupakan kewajiban dalam pembuatan akta autentik. Hal tersebut telah diatur pada Pasal 16 ayat 1 huruf (m) UUJN, sehingga apabila akta tersebut dibuat oleh notaris, maka harus dibacakan oleh notaris bukan oleh pihak ketiga seperti pegawai notaris (Dina, 2019 : 957). Adapun kegunaan pembacaan akta, antara lain:

- a. Disaat peresmian akta akan berakhir, masih terdapat peluang untuk notaris dapat memperbaiki kesalahan pada penulisan kata / kalimat yang sebelumnya tidak terlihat karena mungkin muncul kesalahan fatal atau yang memalukan;
- b. Para penghadap diberikan kesempatan mengajukan pertanyaan yang kurang jelas ataupun kurang dipahami dari isi akta yang dibacakan / ditulis;
- c. Notaris serta para penghadap memiliki kesempatan di sejumlah detik akhir sebelum akta tersebut telah ditandatangani oleh para penghadap, saksi, serta notaris untuk melakukan evaluasi tentang isi akta, mempertanyakan ataupun merubah isi akta (Fabela, 2023 : 676).

Apabila terjadi pelanggaran perihal tidak dibacakannya suatu akta, maka akta tersebut hanya memiliki kekuatan pembuktian setara dengan akta dibawah tangan atau akta tersebut telah kehilangan keotentisitasnya. Hal itu sudah diatur pada Pasal 16 ayat 9 UUJN berbunyi: *“Jika salah satu syarat sebagaimana dimaksud pada ayat 1 huruf (m) dan ayat 7 tidak dipenuhi, Akta yang bersangkutan hanya mempunyai kekuatan pembuktian sebagai akta di bawah tangan”*.

Dengan adanya Pasal 16 ayat 7 UUJN dapat menyebabkan sudut pandang yang berbeda dimana tidak adanya kewajiban bagi notaris untuk membacakan akta karena akta tersebut telah dibaca sendiri oleh para pihak. Akan tetapi kemudian diperjelas pada Pasal 16 ayat 8 UUJN bahwa: *“meskipun para pihak menginginkan aktanya dibaca sendiri, notaris tetap memiliki keharusan dalam membacakan kepala Akta, perbandingan, penjelasan pokok Akta secara jelas, singkat, dan penutup Akta.”*. Kemudian dapat disimpulkan bahwa notaris tetap wajib membacakan akta agar akta tersebut tetap menjadi akta autentik ataupun tak kehilangan keotentisitasnya karena tidak dibacakan oleh notaris. Adapun manfaat lain dari pembacaan akta oleh notaris yakni notaris memiliki waktu atau peluang untuk memperbaiki apabila adanya kesalahan yang sebelumnya tidak teramati. Pembacaan akta merupakan peluang akhir untuk seorang notaris guna memeriksa akta yang sudah dibuatnya. Akan tetapi, manfaat tersebut tak hanya itu saja, para penghadap mendapatkan peluang dalam mempertanyakan terkait sejumlah hal yang kurang jelas dalam isi akta serta pembacaan akta memberi peluang pada notaris serta para penghadap di detik-detik akhir, sebelum akta selesai disahkan melalui penandatanganan oleh para pihak, saksi serta notaris guna melaksanakan evaluasi dengan kata lain, revisi isi perjanjian hingga tak terjadi masalah kedepannya.

Berdasar teori kewenangan serta teori keabsahan pada segi kewenangan, notaris memiliki wewenang atribusi, dimana notaris diberi wewenang langsung oleh undang-undang guna membuat akta termasuk di dalamnya membacakan akta serta selama obyek perjanjian tersebut masih ada dalam wilayah kerja notaris, maka notaris tetap memiliki wewenang dalam membuat akta maupun pembacaan serta penandatanganan dengan memakai cyber notary serta akta tersebut tetap sah selama bentuk akta sesuai dengan ketentuan Pasal 38 UUJN dan Pasal 1868 KUHPerdara.

Pasal 1868 KUHPerdara mengatur bahwa akta autentik, termasuk akta notaris, harus dibuat sesuai dengan bentuk yang ditentukan oleh undang-undang dan di hadapan pejabat umum yang berwenang di lokasi di mana akta tersebut dibuat. Jika akta memenuhi bentuk

dan persyaratan tersebut serta dibuat oleh pejabat yang berwenang, maka akta tersebut dapat dianggap sebagai akta autentik. Namun, masalah muncul saat pembacaan dan penandatanganan akta dilakukan melalui *cyber notary*. Menurut Pasal 16 ayat 1 huruf (m) UUJN, pembacaan akta harus dilakukan di depan para pihak dan paling sedikit dihadiri oleh dua saksi, serta notaris harus hadir secara fisik dan menandatangani akta di hadapan para pihak dan saksi. Istilah "hadir secara fisik" berarti notaris harus hadir secara jasmani, dimana hal tersebut menjadi tidak terpenuhi apabila menggunakan metode *cyber notary*. Hal ini menciptakan konflik norma dalam UUJN, karena teknologi memungkinkan pertemuan jarak jauh dengan suara dan gambar yang nyata tetapi tidak memenuhi persyaratan hadir secara fisik yang diharuskan oleh undang-undang.

Sebagaimana telah disebutkan sebelumnya, notaris dapat menerbitkan sertifikat secara elektronik dengan jaminan kepastian hukum dari notaris kepada pihak terkait. Namun, hal ini bertentangan dengan Pasal 16 ayat 1 huruf (m) UUJN yang menyatakan bahwa "*pembacaan dan penandatanganan akta harus dilakukan di depan para pihak dan para saksi*". Ketentuan ini membatasi pekerjaan notaris, karena seharusnya dalam praktiknya notaris perlu memanfaatkan teknologi yang ada untuk membantu kinerjanya dan meningkatkan pelayanan kepada masyarakat. Intinya, diperlukan pembaruan UUJN, terutama dalam hal proses pembuatan akta secara umum dan khususnya dengan metode *cyber notary*. Selain itu, definisi sertifikasi menggunakan *cyber notary* atau pembuatan akta melalui *cyber notary* perlu dijelaskan lebih lanjut agar setara dengan pembuatan akta notaris secara manual. Tujuan dari perlunya pembaruan UUJN agar notaris dapat memanfaatkan kemajuan teknologi tanpa melanggar undang-undang yang mengatur pelaksanaan tugas mereka serta peraturan terkait lainnya.

Adapun dari tata cara pembuatan akta notaris dengan *cyber notary* memiliki tata cara yang sama dengan pembuatan akta notaris sebagaimana sebelumnya. Akan tetapi ada satu aspek yang berbeda dari keseluruhan tata cara adalah perihal menghadap, dimana sebelumnya menghadap dilakukan dengan cara tatap muka atau bertemu secara langsung akan tetapi menghadap dalam konteks *cyber notary* dilakukan dengan memanfaatkan teknologi seperti telekonferensi atau *video call*. Penggunaan telekonferensi atau *video call* dimaksudkan guna para pihak dapat menyatakan maksud dan tujuan kepada notaris. Para pihak wajib mengirimkan identitas mereka melalui media surat elektronik atau email kemudian notaris menyesuaikan identitas tersebut dengan para pihak yang ada pada telekonferensi tersebut. Kemudian, notaris membuat akta sesuai dengan yang sudah diatur

dalam perundang-undangan hingga selanjutnya akta tersebut dibacakan di depan para pihak melalui telekonferensi tersebut hingga akhirnya akta tersebut ditandatangani oleh para pihak, saksi serta notaris dengan menggunakan tanda tangan digital.

Mengenai tanda tangan digital, prosesnya melibatkan dua langkah utama. Pertama, pembuatan tanda tangan digital menggunakan sidik jari digital yang dihasilkan dari dokumen dan kunci pribadi. Kedua, pemastian tanda tangan digital dilakukan dengan memverifikasi tanda tangan tersebut terhadap dokumen asli dan kunci publik yang telah diberikan. Dengan cara ini, dapat dipastikan apakah tanda tangan digital tersebut benar-benar dibuat untuk dokumen yang sama menggunakan kunci pribadi tersebut (Rossalina, 2017 : 15).

2. Tantangan dan Kendala dalam Penerapan *Cyber Notary* di Indonesia

a. Kewenangan Notaris dalam Menggunakan *Cyber Notary* dalam Sistem SABH

Cyber notary berkaitan dengan sistem keamanan. Hubungan kewenangan notaris dalam menggunakan *cyber notary* dalam Sistem Administrasi Badan Hukum (SABH), seluruh notaris telah diminta untuk melakukan hal tersebut, tinggal mengikuti tahapan sistemnya saja. Seperti contoh, pemeriksaan keaslian dokumen yang dipersyaratkan, keaslian tanda tangan, dimana proses ini harus segera diverifikasi oleh notaris yang bersangkutan, karena jika tidak dilakukan maka proses dan tahapan selanjutnya tidak dapat dilakukan. Mengenai akta dan tanda tangan elektronik yang berkaitan dengan *cyber notary*, hal ini baru menjadi wacana di Indonesia, dan saat ini hanya sebatas pemindaian berita acara yang ditandatangani dan diunggah ke sistem seperti legalisasi elektronik, namun jika menyangkut tanda tangan elektronik masih belum terealisasi dan tidak ada

Legalisasi elektronik memiliki validasi yang kuat karena berasal dari sistem lembaga Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham) yang terhubung dengan notaris. Masyarakat umum juga bisa menggunakan sistem melalui jalur umum, karena jika melalui jalur notaris, notaris mempunyai ID khusus untuk mengaksesnya.

Seperti contoh, ketika klien ingin membuat PT, untuk pengesahan atau penerbitan akta, notaris mengikuti semua langkah sistem yang diperlukan, seperti KTP, NPWP dan fotokopi semuanya. Setelah semuanya telah memenuhi syarat, kemudian dikeluarkan surat keputusan menteri yang menyetujui pendirian PT, kemudian notaris mengesahkannya dengan cara dipindai (*scan*), kemudian notaris

menyatakan bahwa data yang diunggahnya adalah benar. Begitulah proses sertifikasinya, dan keterangan yang berbunyi: “Keputusan Menteri ini dicetak dari...” hal inilah yang memberikan rasa aman bagi notaris, bahwa ketika telah dicetak memang berdasarkan badan hukumnya. Sehingga keaslian sistem yang digunakan tercantum didalamnya. Temuan-temuan sebelumnya menunjukkan bahwa belum terdapat peraturan perundang-undangan yang secara khusus mengatur tentang *cyber notary*, dan untuk peraturan kedepannya perlu ditambahkan satu bab yang khusus mengatur tentang *cyber notary* dalam UUJN dan/atau dibuat Peraturan Pemerintah yang khusus mengatur tentang *cyber notary* (Chastra, 2021 : 17).

Mengenai kewenangan notaris dalam mengesahkan transaksi elektronik *cyber notary*, kewenangan yang dimaksud seperti kewenangan dari pusat, seperti kewenangan mengenai pembuatan surat keterangan (SK), dimana semua sudah dilaksanakan dalam sistem, hanya saja penandatanganan akta masih harus dipenuhi. Konsep *cyber notary* terkandung dalam Pasal 15 ayat 3 sebenarnya dapat diterapkan di Indonesia, dalam arti proses RUPS PT. Dalam RUPS tersebut, rapat dihadiri seluruh pihak. Notaris menyaksikan langsung pertemuan tersebut melalui telekomunikasi. Namun perlu ditegaskan lagi, hanya pada saat RUPS, bukan pada saat proses penandatanganan. Selanjutnya, setelah proses penandatanganan langsung kemudian data langsung di input, setelah di input kemudian data di pindai, setelah di pindai lalu membayar Penerimaan Negara Bukan Pajak (PNBP) kemudian proses terakhir adalah mengunggah semua data, setelah itu SK bisa segera diterbitkan. Dari sini terlihat kegunaannya *cyber notary* hanya terbatas pada sistem SABH saja. Apabila *cyber notary* berkaitan dengan penyimpanan, seperti menyimpan atau menyalin salinan berita acara akta secara elektronik (penyimpanan melalui komputer), semua tergantung pada notaris, akan menggunakan sistem penyimpanan seperti apa, ada notaris yang mau menggunakan sistem tersebut cadangan data, atau dengan sistem ketik ulang. Implementasi *cyber notary* merupakan langkah progresif untuk menyesuaikan hukum dengan kemajuan teknologi digital. Namun, keberhasilan implementasi tergantung pada seberapa baik ketentuan tersebut disusun dan diterapkan, serta sejauh mana mereka dapat memenuhi tujuan-tujuan yang diharapkan, seperti meningkatkan keamanan dan kepastian hukum dalam penggunaan dokumen elektronik, seorang notaris dapat memanfaatkan perkembangan teknologi atau yang disebut dengan *cyber notary* (Banjarani, 2023: 18).

b. Pengecekan Keaslian Tetap Secara Langsung (*Offline*)

Penerapan konsep *cyber notary* apabila mengacu pada UU PT yakni tentang pertemuan yang dilakukan melalui media telekonferensi dalam pembuatan berita acara. Mengacu pada Pasal 76 UU PT yakni “tempat pelaksanaan RUPS”. Sebagaimana dimaksud pada ayat 1 dan 2 harus berkedudukan di wilayah Indonesia. Namun apabila konsep *cyber notary* diterapkan di Indonesia mengacu pada pembuatan akta partai atau para pihak dengan menggunakan media elektronik atau telekonferensi. Sayangnya, ada beberapa hambatan dalam pelaksanaannya. Contohnya, para pihak tetap harus datang secara fisik, karena notaris menjamin keaslian sidik jari dan tanda tangan para pihak. Kendala lain yang dapat ditemui adalah bunyi isi akta yang dibuat, karena apabila tetap dilaksanakannya *cyber notary* maka bunyi adalah “tatap muka dengan saya melalui media *zoom*” sehingga kalimatnya menjadi tidak tepat (Merlyani, 2020 : 40).

c. Masih Membutuhkan Tanda Tangan Asli dan Sidik Jari

Sebagaimana diatur pada Pasal 44 ayat 1 UUDN, pasal ini mengatur tentang penandatanganan akta oleh para pihak, saksi, dan notaris secara langsung. Sedangkan apabila menerapkan konsep tersebut *cyber notary* semuanya serba elektronik dan para pihak, saksi dan notaris tidak bertemu secara langsung. Oleh karena itu, hal tersebut menjadi tidak dapat untuk dilakukan. Hal yang menjadi faktor penghambat adalah sifat asli tanda tangan, frasa tatap muka dan bukti sidik jari yang apabila di pengadilan tidak dapat dijadikan alat bukti.

Salah satu yang menjadi kesalahan adalah pembuatan akta notaris yang mana notaris lalai atas sidik jarinya, maka notaris akan ditegur Kemenkumham dan ditanyai dimana sidik jarinya hilang dan dicatat sebagai temuan. Terlebih lagi jika sidik jari tersebut hilang namun notaris mempunyai cadangan berupa hasil pindai sidik jari yang sudah jadi yang berasal dari sidik jari asli kemudian dicetak, kurang lebih seperti jatuhnya elektronik, tetap tidak dapat dilakukan dan tidak diperkenankan demikian sebagai temuan di Kemenkumham. Namun di sisi lain, faktor penghambat tersebut hanya berlaku pada tanda tangan dan sidik jari, sedangkan yang lain seperti KTP masih diperbolehkan. Ketentuan *cyber notary* tidak bersifat memaksa dalam arti bahwa mereka tidak memaksakan kepatuhan secara langsung kepada individu. Namun, mereka mengatur prosedur dan persyaratan yang harus dipenuhi untuk mendapatkan pengesahan atau notarisasi elektronik. Tujuan dari ketentuan ini adalah

untuk memberikan kerangka kerja yang jelas dan aman bagi penggunaan dokumen dan transaksi elektronik di dalam sistem hukum yang mengatur wilayah tersebut. Pengaturan mengenai sertifikasi transaksi elektronik oleh notaris (*cyber notary*) dalam peraturan perundang-undangan khususnya UUJN belum lengkap/tidak jelas karena belum diterbitkannya peraturan pelaksanaan terkait dengan hal tersebut (Syamsul, 2019 : 148).

d. Mengubah Unsur-Unsur Inti dalam Pembuatan Akta Notaris

Terdapat beberapa faktor penghambat dalam pembuatan konsep tersebut *cyber notary* tidak dapat diterapkan di Indonesia, salah satunya adalah penggunaan *cyber notary* yang lebih bersifat elektronik dapat mengubah unsur-unsur inti dalam pembuatan akta notaris sebagaimana termuat dalam Pasal 38 UUJN.

e. Notaris Sulit Mengenal Penghadap

Penggunaan konsep *cyber notary* juga telah meniadakan pertemuan fisik atau tatap muka sehingga menyulitkan notaris untuk mengenali penghadap dan dikhawatirkan identitas para pihak tidak dapat dibuktikan secara nyata.

Apabila digunakan *cyber notary* berkaitan dengan penggunaan media telekonferensi dalam menyelenggarakan RUPS dengan menggunakan akta relaas sebagaimana diatur dalam UU PT, maka penggunaannya dikecualikan dan sah untuk dilakukan, sebagaimana diatur dalam Pasal 77, yaitu: “Selain melalui RUPS sebagaimana dimaksud dalam Pasal 76, RUPS juga dapat dilakukan melalui telekonferensi, video konferensi, atau media elektronik lainnya yang memungkinkan seluruh peserta RUPS saling melihat dan mendengar secara langsung serta ikut serta dalam rapat”. Otoritas *cyber notary* umumnya digunakan dalam pelestarian bukti data elektronik (Shang, 2020 : 30).

Meski jarang terjadi, namun tidak menutup kemungkinan suatu saat bisa terjadi. Oleh karena itu, dapat disiasati penyimpanan salinan akta tersebut dengan cara memasukkannya ke *email*, lalu memasukkannya lagi ke email lain, sehingga nantinya jika ingin mengakses salinan akta tersebut, yang perlu dilakukan hanyalah cari melalui email dan tidak perlu melakukan apa pun lagi. *Cyber notary* dalam hal ini bukan berarti tidak adanya pertemuan antar para pihak atau pertemuan melalui telekonferensi, namun dalam hal ini para pihak tetap berhubungan langsung dengan notaris, hanya rancangan akta yang dapat dibaca dari komputer dan jika para pihak sepakat kemudian akta ditandatangani secara elektronik (Agung, 2022 : 8).

3. Mekanisme Perlindungan Hukum bagi Para Pihak dalam Akta Notaris Elektronik dari Aspek Keamanan Data dan Kekuatan Pembuktian

a. Perlindungan Hukum Keamanan Data *Cyber Notary* dari Tindakan *Cyber Crime*

Tantangan yang dihadapi dalam era masifnya perkembangan teknologi salah satunya adalah *cyber crime* atau kejahatan siber yang dapat mengganggu keamanan nasional dan dunia. Notaris mengemban tugas untuk secara aktif membantu mewujudkan kepastian hukum dan keamanan negara. *Cyber crime* merupakan kejahatan yang terjadi di dunia maya yang dilakukan tanpa memerlukan kontak langsung dengan korban dan dapat dilakukan dimana saja, dimana *cyber crime* ini pada umumnya dilakukan untuk membawa keuntungan finansial bagi pelaku. Contoh dari *cyber crime* terhadap data pribadi adalah *hacking* atau *cracker* (Abidin, 2017 : 511).

Cyber crime merupakan kejahatan dengan menggunakan jaringan dan komputer dalam bentuk *hacking*, penyebaran virus, *identity theft* atau pencurian data, *cyber harassment*, *skimming* dan lain-lain (Iftah, 2020 : 3). Pencurian data pribadi ini dapat dengan mudah dilakukan karena data yang kita miliki sekarang ini hampir seluruhnya tercatat secara *online*. Perbuatan mencuri data pribadi tersendiri merupakan bentuk perbuatan melawan hukum, meskipun belum ada peraturan tersendiri yang mengatur mengenai *cyber law*, namun dalam beberapa peraturan perundang-undangan, khususnya UU ITE mengatur bahwa “*setiap orang yang melanggar ketentuan dalam Pasal 26 dapat digugat atas kerugian yang ditimbulkan*”.

Dengan kemudahan yang diberikan oleh kemajuan teknologi dan informasi ini, kejahatan-kejahatan tersebut bisa dengan mudah dan efektif untuk dilakukan. Hal ini juga berpotensi pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Kemajuan teknologi informasi dan komunikasi membuat batas privasi makin tipis sehingga berbagai data-data pribadi semakin mudah untuk tersebar. Akibat meningkatnya isu mengenai perlindungan data pribadi menjadi hal yang serius karena penyebarannya dapat menimbulkan risiko kebocoran data pribadi seseorang. Data pribadi seperti NIK, nama, email, nomor telepon merupakan data yang sangat berharga karena bernilai jual tinggi saat ini.

Adapun wujud dari asas kemanfaatan yang diwujudkan berupa hal mengenai sertifikasi yang dilakukan menggunakan konsep *cyber notary* yang memudahkan

pelaksanaan jabatan oleh notaris. Hal ini juga merupakan perwujudan dari aspek efisiensi yang bersifat positif. Mengingat, dalam praktik yang berbasis digital dibutuhkan beberapa dokumen publik dalam bentuk elektronik termasuk dalam hal penandatanganan secara elektronik oleh notaris. Untuk mengenal para penghadap, notaris menggunakan identitas berupa KTP, SIM dan Paspor, dengan adanya konsep *cyber notary* maka media yang digunakan untuk mengenal penghadap adalah *Electronic Identity* (e-ID). e-ID merupakan sebuah bentuk dari penerapan konsep pemerintah yaitu *e-government* dalam hal pelayanan publik oleh pemerintah yang berarti pemanfaatan teknologi informasi oleh pemerintah dalam pemberian informasi dan pelayanan publik. Oleh karena identitas merupakan hal yang bersifat rahasia, sangat berbahaya bila data dapat diakses oleh semua pihak tanpa adanya hak akses apalagi pelaku *cyber crime* yang tidak bertanggung jawab, maka pemilik data yang sah harus memiliki perlindungan atas rekaman biometrik atas data pribadinya.

Dalam hal membahas aspek konsep *cyber notary*, yang mendapat perlindungan hukum dalam hal ini yaitu identitas pihak-pihak yang terlibat dalam praktik *cyber notary*. Sebelum membahas mengenai identitas elektronik atau e-ID terlebih dahulu perlu dibahas mengenai identitas yang digunakan sebagai pengenalan diri seseorang yang membedakannya dengan orang lain. Sedangkan e-ID adalah identitas atau pengenalan diri seseorang yang berbentuk atau menggunakan media elektronik yang memuat data-data perseorangan. Keperluan akan data pribadi pada era digital seperti sekarang ini sangat diperlukan dalam hal menghindari tindak kejahatan secara digital atau sering juga disebut dengan istilah kejahatan *cyber*, sedangkan gangguan digital yang lebih berbahaya yaitu peretasan (*hack*) perangkat komputer. Peretasan adalah kegiatan memodifikasi, masuk dengan paksaan atau menerobos ke dalam komputer dan jaringan komputer, dalam rangka mencari keuntungan bagi seseorang maupun kelompok. Peretasan perangkat komputer notaris yang memuat draf akta dapat menyebabkan hal sebagai berikut: penyalahgunaan informasi pribadi para pihak maupun objek perjanjian; kerahasiaan akta notaris dilanggar; manipulasi data yang merugikan para pihak dan notaris.

Pengaturan mengenai peretasan diatur dalam UU ITE. Peretasan didefinisikan sebagai tindakan kriminal di bidang kejahatan dunia maya. Pasal 30 UU ITE mengatur mengenai kualifikasi peretas yang dapat dijerat hukum pidana, berbunyi: “(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 UU ITE: “(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 juta 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 juta 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 juta rupiah).”

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 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 UU PDP berkaitan dengan 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).*”

b. Perlindungan Hukum Keamanan Data *Cyber Notary* Apabila Terjadi Kelalaian dari Pihak Notaris

Hak atas privasi sangat rentan untuk disalahgunakan, sehingga dapat merugikan masyarakat. Selain itu, pelanggaran data pribadi tidak hanya diakibatkan oleh kebocoran data pribadi, pelanggaran juga bisa terjadi dalam hal pemrosesan data pribadi yang tidak bertanggung jawab. Seperti pada saat data pribadi masyarakat digunakan untuk diperjualbelikan tanpa dasar yang jelas. Isu mengenai perlindungan data pribadi merupakan salah satu isu penting yang menjadi perhatian. Banyaknya penggunaan *digital platform* menjadi salah satu alasan mengapa perlindungan data pribadi menjadi penting untuk menjamin adanya keamanan data pribadi.

Tanggung jawab notaris terhadap keamanan akta digital ini dibatasi pada hilang atau kerusakan protokol yang disimpan secara elektronik oleh notaris serta menjaga kerahasiaan akta (Ni Ketut Supasti, 2019 : 3177). Terdapat beberapa kelemahan aturan undang-undang dalam hal menjamin kepastian juga perlindungan hukum bagi keamanan data pribadi para pihak dalam praktik *cyber notary*, peranan pihak yang menyimpan data pribadi sangat diperlukan guna mengurangi terjadinya kejahatan dalam dunia *cyber*. Notaris ialah salah satu pihak yang berperan dalam penyimpanan data pribadi, karena dalam akta yang dibuatnya ada kewajiban bagi para pihak untuk menyertakan data pribadi/identitasnya (Adinda, 2021 : 687).

Data pribadi inilah yang sering menjadi bahan untuk diperjualbelikan oleh oknum-oknum pelaku kejahatan *cyber* bahkan oleh oknum notaris yang tidak berintegritas dan tidak bertanggung jawab terhadap jabatan yang diembannya. Disisi lain, notaris memiliki kewajiban untuk merahasiakan akta berikut isinya sesuai dengan aturan yang diatur pada ketentuan UUJN. Adapun konsekuensi yang ditimbulkan akibat pelanggaran terhadap hal merahasiakan akta beserta isinya yaitu pada ketentuan Pasal 16 ayat 11 UUJN yang menyatakan bahwa seorang notaris yang melakukan

pelanggaran (tidak merahasiakan akta beserta isinya), akan mendapat sanksi/hukuman berupa peringatan yang dilakukan secara tertulis, pemberhentian secara dengan jangka waktu yang ditentukan yang bersifat sementara, dan yang terakhir pemberhentian secara hormat ataupun pemberhentian yang dilakukan dengan tidak hormat. Sebagaimana pengaturan yang tertuang pada ketentuan Pasal 16 ayat 12 UUJN yang menerangkan bahwa selain sanksi administrasi, adapun sanksi yang diatur oleh undang-undang yaitu berupa ganti rugi yang dilayangkan oleh penghadap kepada notaris akibat menderita kerugian.

Berbagai hal positif yang ditawarkan oleh kecanggihan teknologi tentu juga memiliki hal negatif, salah satunya yaitu gangguan digital berupa virus dalam komputer. Virus berdasarkan KBBI adalah program ilegal yang masuk ke dalam sistem komputer melalui jaringan hingga menyebar dan berpotensi merusak program dalam komputer. Gangguan digital yang disebabkan oleh virus, implikasinya terhadap perusakan berkas digital atau data yang terdapat dalam berkas tersebut, bahkan bisa saja hilang. Dalam hal belum adanya kebijakan penyimpanan minuta akta secara digital, maka hal ini akan berdampak terhadap draf akta yang telah dirancang. Peran notaris secara preventif yaitu memasang *anti-virus* pada seluruh perangkat yang digunakan merancang akta, serta lebih teliti dan membacakan akta sebelum penandatanganan akta yang merupakan kewajiban notaris sebagaimana diatur pada Pasal 16 huruf (m) UUJN.

Masalah keamanan dalam penyimpanan dokumen *cyber notary* sudah disiasati oleh *American Bar Association* (ABA), mereka menggunakan sistem kriptografi dan *Public Key Infrastructure* (PKI). Sistem ini dianggap aman dan dapat mengakomodir *cyber notary* karena pada sistem kriptografi memungkinkan dalam mengamankan pesan elektronik dan mengautentikasi identitas dari para pihak, terlebih lagi PKI memungkinkan menyediakan fasilitas tanda tangan dalam bentuk digital. Jadi, secara singkat *cyber notary* menurut ABA adalah konsep memanfaatkan perkembangan teknologi yang digunakan notaris dalam menjalankan tugas dan kewenangannya, seperti: digitalisasi dokumen, penandatanganan akta secara elektronik, pelaksanaan Rapat Umum Pemegang Saham (RUPS) secara telekonferensi, dan lainnya.

Dalam ketentuan Pasal 40 ayat 2 UU ITE memberikan penjelasan mengenai penyidikan dalam basis teknologi informasi dan dunia elektronik yang hanya dapat diterapkan dengan memperhatikan dengan lebih dalam pada hal melakukan

perlindungan terhadap kerahasiaan, privasi dan kelancaran dalam bidang keutuhan suatu data, pelayanan bidang publik berdasarkan pengaturan undang-undang yang berlaku saat ini. Sedangkan dalam ketentuan UU Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, di Pasal 1 angka 22 menjabarkan mengenai data pribadi merupakan data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Penyimpanan data pribadi wajib dilakukan oleh suatu negara, sedangkan penyelenggara instansi pelaksana juga mempunyai hak akses terhadap data pribadi penduduk.

Untuk menghindari penyalahgunaan wewenang di luar wilayah jabatan notaris, maka perlu pengaturan bahwa perangkat komputer yang digunakan oleh notaris yang menjalankan jabatannya perlu menginformasikan atau mendaftarkan *IP address*-nya di Kemenkumham. Selain itu, setiap akta elektronik yang dibuat perlu mencantumkan IP address dimaksud. Dengan demikian, pihak yang berwenang dapat melakukan pemeriksaan terkait praktik *cyber notary* yang dilakukan oleh seorang notaris terkait apakah sudah sesuai dengan wilayah jabatannya (Pangesti, 2020 : 15).

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 yang dimaksud pada pasal tersebut yaitu dalam hal kerahasiaan, integritas dan ketersediaan Data Pribadi, termasuk pelanggaran keamanan, baik yang di sengaja, yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang dikirim, disimpan, atau diproses. Semua ini dapat menimpa notaris dalam kewenangannya ketika membuat akta *cyber notary*. Notaris wajib bertanggung jawab

ketika terjadinya kegagalan dalam Perlindungan Data Pribadi sebagaimana disebutkan dalam Pasal 47 UU PDP.

D. KESIMPULAN

Dalam era digital saat ini, pemanfaatan teknologi dalam pembuatan akta notaris elektronik memiliki potensi besar untuk meningkatkan efisiensi dan aksesibilitas. Namun, perlindungan hukum bagi para pihak yang terlibat sangatlah penting. Regulasi yang ada harus mampu menjamin bahwa akta elektronik memiliki kekuatan hukum yang sama dengan akta konvensional, serta dilengkapi dengan mekanisme keamanan yang ketat untuk mencegah pemalsuan dan manipulasi data. Kesadaran masyarakat dan pendidikan mengenai teknologi notaris elektronik juga perlu ditingkatkan agar implementasinya dapat berjalan dengan baik.

Dukungan kerangka hukum yang kuat sangat diperlukan dalam penerapan akta notaris elektronik. Pemerintah dan otoritas terkait perlu menyusun regulasi yang komprehensif mengenai pembuatan dan penggunaan akta elektronik. Dengan kerjasama antara pemerintah, notaris, dan masyarakat, diharapkan akta notaris elektronik dapat memberikan manfaat optimal tanpa mengorbankan aspek keamanan dan keabsahan hukum, sehingga pengembangan teknologi ini dapat berjalan seiring dengan perlindungan hukum yang memadai.

E. DAFTAR PUSTAKA

- Adinda Ari Wijayanti, I Gusti Ketut Ariawan, *Upaya Perlindungan Terhadap Identitas Para Pihak dalam Praktik Cyber Notary*, Acta Comitas: Jurnal Hukum Kenotariatan, Vol. 06, No. 03, Desember, 2021.
- Aditya, Agung., Wulandari, Cahya., & Loso. (2022). *Cyber Notary: Between Notary Opportunities and Challenges in Facing the Era of Digital Disruption 4.0 Towards 5.0*. International Journal of Law Society Services, Vol.2, No.1 ,p. 8.
- Bahri, Syamsul., Yahanan, Annalisa., & Trisaka, Agus. (2019). *Kewenangan Notaris Dalam Mensertifikasi Transaksi Elektronik dalam Rangka Cyber Notary*. Repertorium: Jurnal Ilmiah Hukum Kenotariatan, Vol.8, No.2, pp, 142-157.
- Banjarani, Desia Rakhma., Adisti, Neisa Ang Rum., Nuriilah, Isma., & Primadianti, Helena. (2023). *Cyber Notary in Indonesia: Review During the Covid-19 Pandemic And The Urgency Of Post-Pandemi Covid-19 Legal Regulations*. Notariil Jurnal Kenotariatan, Vol.8, No.1, pp. 8-14.

- Chastra, DenyF. (2021). *Kepastian Hukum Cyber Notary Dalam Kaidah Pembuatan Akta Autentik Oleh Notaris Berdasarkan Undang-Undang Jabatan Notaris*. Indonesian Notary, Vol.3, No.2, p. 17.
- Dharmawan, Ni Ketut Supasti, Kasih, Desak Putu Dewi, Deris Setiawan, *Personal Data Protection And Liability Of Internet Service Provider: A Comparative Approach*, International Journal of Electrical and Computer Engineering, Vol.9, No.4, 2019.
- Dodo Zainal Abidin, *Kejahatan dalam Teknologi Informasi dan Komunikasi*. Jurnal Processor, Vol.10, No. 2, 2017.
- Fabela Rahma Moneteri, Budi Santoso. (2023). *Keabsahan Dan Kekuatan Pembuktian Akta Notaris: Perspektif Cyber Notary Di Indonesia*, Vol.16, No.2, 666-685
- Hartini, R. (2020). *Hukum Kepailitan*. Malang: UMMPress.
- Iftah, Putri Nurdiani, *Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime*, Jurnal Kriminologi Indonesia, Vol.16, No.2, 2020.
- Merlyani, Dwi., Yahanan, Annalisa., Trisaka, Agus. (2020). *Kewajiban Membacakan Akta Otentik oleh Notaris di Hadapan Hadirin dengan Konsep Cyber Notary*. Repertorium: Jurnal Ilmiah Hukum Notaris, Vol.9, No.1, pp. 36-47.
- Narbuko, Cholid, Achmadi Abu, *Metodologi Penelitian* (Jakarta: Sinar Grafika, 2015).
- Pangesti, Shinta., Darmawan, Grace I., & Limantara, Chintia P. (2020). *The Regulatory Concept of Cyber Notary in Indonesia*. Rechtsidee, Vol.7, pp, 1-18
- Regina Natalie Theixar, Ni Ketut Supasti Dharmawan, *Tanggung Jawab Notaris Dalam Menjaga Keamanan Digitalisasi Akta*, Acta Comitas: Jurnal Hukum Kenotariatan, Vol. 06, No. 1, Maret, 2021.
- Rossalina, Zainatun., Bakri, Moh., & Andrijani, Itta. (2017). *Keabsahan Akta Notaris yang Menggunakan Cyber notary sebagai Akta Otentik*. E-jurnal Pascasarjana Fakultas Hukum Universitas Brawijaya, p. 1-25.
- Shang, & Qiang. (2020). *Pelestarian Data Elektronik dan Penyimpanan Bukti dengan Blockchain*. Jurnal Ilmu dan Kedokteran Forensik, Vol,6, No.1, pp. 27-36.
- Teddy Lesmana, Eva Elis, Siti Hamimah, *Urgensi Undang-Undang Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia*, Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, Vol. 3, No. 2, 2022.