https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Vol. 01, No. 02, 2025, Hal. 399-406

PERLINDUNGAN HUKUM KEAMANAN DATA CYBER NOTARY DALAM PENYIMPANAN PROTOKOL NOTARIS DI BLOCKCHAIN

Rico Aldy Munafan[1], Nuzulia Kumalasari[2], Moh Ali[3]
Fakultas Hukum, Universitas Jember, Jember
E-mail: *ricoaldymunafan@gmail.com[1], nuzuliakumalasari@unej.ac.id[2], mohali@unej.ac.id[3]

ABSTRAK

Penerapannya blockchain masih banyak kendala dan permasalahan yang terlebih dahulu diselesaikan salah satunya ialah tidak adanya dasar hukum yang jelas, dimana sampai saat ini belum ada undang-undang dan aturan yang mengatur secara khusus terkait penyimpanan protokol notaris pada dunia digital. Dengan demikian penulis tertarik untuk membahasnya dalam karya ilmiah berikut ini, dengan memfokuskan mengenai apa saja resiko penerapan blockchain dalam penyimpanan protokol notaris dan bagaimana perlindungan hukum keamanan data cyber notary dalam penyimpanan protokol notaris di blockchain. dengan tujuan untuk mengetahui penerapan dan perlindungan hukum keamanan data cyber notary dalam penyimpanan protokol notaris di blockchain. Dengan menggunakan metode penelitianhukum normatif, yang menggunakan data sekunder yang berbentuk hukum tertulis, pendekatan dalam penelitian ini memakai pendekatan perbandingan dan pendekatan perundang-undangan. Hasil penelitian ini menunjukkan bahwa, Peratama, penerapan cyber notary dalam penyimpanan protokol notaris di blockchain memberikan beberapa risiko yang pertama biaya pengoprasian dan perawatan yang tinggi, rentan dengan ancaman virus dan serangan cyber yang dapat mengancam kapan saja, sehingga memberikan risiko kehilangan data pribadi dari para pihak. Kedua, perlindungan hukum terhadap keamanan data cyber notary dalam penyimpanan protokol notary di blockchain sampai sekarang belum ada aturan yang secara detail memberikan perlindungan dan secara eksplisit mengatur terkait cyber notary, namun terkait perlindungan data dan ancama peretasan dapat mengacu pada peraturan pasal 30 Undang-Undang Informasi dan Teknologi Elektronik mengenai kejahatan cyber dan dalam Undang-Undang Perlindungan Data Pribadi pada pasal 67.

Kata Kunci **Cyber Notary, Blockchain, Protokol Notaris**

ABSTRACT

The application of blockchain still has many obstacles and problems that must first be resolved, one of which is the absence of a clear legal basis, where until now there have been no laws and regulations that specifically regulate the storage of notary protocols in the digital world. Thus the author is interested in discussing it in the following scientific work, focusing on what are the risks of applying blockchain in storing notary protocols and how the legal protection of cyber notary data security in storing notary protocols on the blockchain. with the aim of knowing the application and legal protection of cyber notary data security in storing notary protocols on the blockchain. By using normative legal research methods, which use secondary data in the form of written law, the approach in this study uses a comparative approach and a statutory approach. The results of this study indicate that, First, the application of cyber notary in storing notary protocols on the blockchain provides several risks, the first is high operating and maintenance costs, vulnerable to virus threats and cyber attacks that can threaten at any time, thus providing a risk of losing personal data from the parties. Second, legal protection of cyber notary data security in storing the notary protocol on the blockchain until now there has been no regulation that provides detailed protection and explicitly regulates cyber notary, but related to data protection and hacking threats can refer to the regulations in article 30 of the Electronic Information and Technology Law regarding cyber crime and in the Personal Data Protection Law in article 67.

Keywords ***Cyber Notary, Blockchain, Notary Protocol***

1. PENDAHULUAN

Perkembangan zaman saat ini di era industri 4.0 teknologi informasi dan komunikasi tidak terlepas dari perkembangan AI atau artificial intelligance yang biasanya dikenal kecerdasan buatan. Kecerdasan buatan merupakan perangkat lunak atau sebuah teknologi komputer yang mempunyai kecerdasan setara dengan kemampuan manusia, selain itu AI juga dapat melakukan pekerjaan sebaik dan seperti layaknya manusia biasa, semua itu disebabkan AI bekerja dengan mempelajari data-data yang dialisis dan diterimanya. Akhir-akhir ini teknologi melakukan perkembangan jaringan dengan kemampuan pengamanan yang jadi keunggulannya. Teknologi jaringan tersebut dikenal dengan nama blockchain, teknologi ini pertama kali diperkanalkan dalam teknologi bitcoin pada tahun 2008, blockchain bisa memberikan jaminan keamanan yang cukup tinggi bagi data yang disimpan pada jaringan teknologinya, dimana keamanan jaringan blockchain melibatkan beberapa pihak sebagai pemberi akses. Dalam teknologi blockchain juga mempunyai keunggulan lainnya yaitu riwayat transaksi yang ada didalamnya tidak dapat dihapus maupun diubah tanpa adanya perubahan secara keseluruhan dari isi blockchain, sehingga menghindari adanya manipulasi data.

Perkembangan teknologi telah menyebabkan peningkatan minat pada segala kegiatan digital seperti halnya blockchain, dimana mendorong transformasi pada berbagai bidang, tidak menutup kemungkinan teknologi informasi digunakan pada bidang hukum, termasuk pada profesi notaris dalam menjalankan segala kewenangannya, terkusus dalam pembuatan dokumen-dokumen penting seperti akta autentik. Banyak peluang yang menjanjikan untuk notaris dalam menggunakan teknologi yang dimotori oleh Kemen ATR/BPN atau Kementerian Agraria dan Tata Ruang/Badan Pertanahan Nasional yang mengeluarkan aturan baru terkait Dokumen Elektronik yaitu dalam peraturan Menteri ATR/BPN nomor 1 tahun 2021, maka dengan aturan tersebut dapat dijadikan dasar pemberlakuan dokumen dan sertifikat elektronik, sehingga ada peluang untuk menerapkan digitalisai secara terbuka.

Selain itu dalam UUJN pasal 15 juga memberikan kewenangan lainnya pada notaris, sehingga dapat dimaknai notaris bisa memberikan pelayanan hukum secara digital dengan memanfaatkan teknologi informasi termasuk juga menggunakan teknologi blockchain dalam menyimpan protokol notaris. Akan tetapi belum ada keterangan secara rinci yang menjelaskan bentuk konkret kewenangan tersebut. Selain itu, masih banyak pasal dalam UUJN yang tumpang tindih dimana dalam pembuatan akta autentik harus menghadap secara langsung, dan juga notaris dalam jabatannya masih terbatas dengan wilayah kerjanya sehingga hal ini bertentangan dengan cara kerja cyber notary itu sendiri diman tidak terbatas oleh ruang dan waktu. Tidak jelasnya peraturan mengenai cuber notary menyebabkan kebingungan dan kegelisahan notaris bila menjalankan kewenangannya secara digital termasuk bila menggunakan blockchain dalam penyimpanan protokolnya. Pelayanan hukum cyber notary membutuhkan payung hukum atau landasan hukum yang jelas agar bisa digunakan sebagai dasar seorang notaris menjalankan kewenangannya dalam memberikan layanan hukum kepada masyarakat, dengan adanya landasan hukum juga dapat melindungi hak-hak dari para pihak maupun notaris itu sendiri, termasuk hak perlundungan dan keamanan data.

Berdasarkan penelitian Daniyah Fadhilah Hasyan, dengan judul "Pemanfaatan Kecerdasan Buatan dan Blockchain dalam Pembuatan Akta Notaris di Indonesia" yang diterbitkan pada jurnal Notarius, Volume 17 Nomor 1 tahun 2024. dimana hasil penelitiannya menyatakan bahwa blockchain atau teknologi berbasis kecerdasan buatan mempuyai peluang untuk dapat di terapkan dalam profesi notaris dalam pekerjaanya

untuk meningkatkan efisiensi saat melakukan pelayanan hukum pada masyarakat, karena teknologi tersebut melahirkan produck smart contract yang memungkinkan dalam pembuatan rancangan kontrak dan analisis putusan hukumnya. Dengan menggunakan blockchain kontrak yang sudah dibuat bisa disimpan dengan aman serta tidak mudah melakukan perubahan sehingga dapat mencegah tindakan manipulasi dan penipuan terkait data.

Selanjutnya pada penelitian Tiara Karlina, dengan judul "Penerapan Teknologi Blockchain dalam Penyimpanan Protokol Notaris" yang diterbitkan pada Badamai: Law Journal, Volume 9 Issue 1 tahun 2024. Hasil penelitiannya menyatakan bahwa implementasi penyimpanan protokol notaris secara digital dalam blockchain sangat penting, karena dengan diterapkannya penyimpanan protokol secara digital dalam blockchain notaris dapat melakukan pekerjaanya dalam menyimpan dokumen-dokumen penting atau minuta akta dengan lebih aman, efektif, dan efesien. Kemudian berdasarkan penelitian Ceavin Rufus De Prayer Purba, dengan judul "Implementasi Teknologi Blockchain pada Real Estate Transaction" yang diterbitkan Makalah II4031 Kriptografi dan Koding, Semester II Tahun 2023/2024. Hasil penelitian tersebut menunjukkan bahwa implementasi teknologi blockchain dalam transaksi real estate mempunyai banyak manfaat diantaranya ialah dapat mengurangi risiko penipuan, meningkatkan transparansi, mempercepat proses transaksi, efesien serta mendorong inovasi

Perbedaan penelitian yang akan dilakukan dengan penelitian terdahulu tersebut ialah, penulis disini ingin menekankan pentingnya perlindungan hukum terkait arsip data yang disimpan secara digital atau dalam hal ini dikenal dengan teknologi blockchain, memang berdasrkan penelitian terdahulu implementasi dan penerapan teknologi khususnya dibidang cyber notary banyak memberikan kemudahan dalam pekerjaan notaris apalagi terkait penyimpanan protokol notaris menggunakan blockchain.

Tetapi disisi lain penulis menyoroti dalam penerapannya blockchain masih banyak kendala dan permasalahan yang terlebih dahulu diselesaikan salah satunya ialah tidak adanya dasar hukum yang jelas, dimana sampai saat ini belum ada undang-undang dan aturan yang mengatur secara khusus terkait penyimpanan protokol notaris pada dunia digital, yang berikutnya terkait potensi peretasan dan pencurian data oleh serangan siber yang dapat mengancam keamanan data sewaktu-waktu, risiko tekena Virus, sehingga perlu adanya perlindungan tambahan pada sistem blockchain, kemudian dengan menggunakan teknologi blockchain maka perlu juga memperhatikan terkait perawatan agar tetap menjaga sistem dapat digunakan secara lancar. Dengan demikian penulis tertarik untuk membahasnya dalam karya ilmiah berikut ini, dengan memfokuskan mengenai apa saja resiko penerapan blockchain dalam penyimpanan protokol notaris dan bagaimana Perlindungan Hukum Keamanan Data Cyber Notary Dalam Penyimpanan Protokol Notaris Di Blockchain. dengan tujuan untuk mengetahui penerapan dan perlindungan hukum Keamanan Data Cyber Notary Dalam Penyimpanan Protokol Notaris Di Blockchain.

2. METODE PENELITIAN

Metode penelitian ini menggunakan jenis penelitian hukum normatif, yakni penelitian yang menggunakan data sekunder yang berbentuk hukum tertulis. Pendekatan dalam penelitian ini memakai pendekatan perbandingan (comparative approach) yaitu membandingkan peraturan perundang-undangan dengan peraturan yang lain, kemudian pendekatan perundang-undangan (statute approach) yakni menelaah semua aturan yang mempunyai kaitan dengan permasalahan yang diangkat penulis. Penelitian ini bersifat

deskriptif analisis yakni menghubungkan teori, praktik dengan peraturan perundang-undangan serta juga dikaitkan dengan permasalahan pada jurnal ini. Sumber data penelitian ini ialah data sekunder yang di dapat dari peraturan perundang-undangan yang berhubungan dengan Cyber Notary serta telaah pada penelitian terdahulu.

3. HASIL DAN PEMBAHASAN

3. 1 Risiko Penyimpanan Protokol Notaris Di Blockchain

Penyimpanan protokol notaris menggunakan teknologi blockchain selain memberikan dampak pofitif agar lebih mudah, efektif dan efesien, teknologi blockchain juga memberikan dampak negatif yang memiliki beberapa resiko bila benar-benar diterapkan dalam penyimpanan protokol notaris, salah satu resikonya ialah rentan terhadap serangan dan berbagai ancaman keamanan seperti virus dan peretasan. Dimana teknologi yang berbasis digital akan terus menghadapi resiko keamanan siber yang selalu berkembang dan dinamis, artinya para oknum peretas akan terus mencari celah baru guna mengeksploitasi sitem teknologi tersebut. Walaupun teknologi blockchain sering di anggap sebagi sistem yang sangat aman untuk arsip atau penyimpanan serta pengelolaan protokol notaris, bukan berarti sistem blockchain seluruhnya kebal terhadap serangan dan ancaman peretasan.

Dimasa yang akan datang serangan cyber bisa saja terjadi, mengingat para peretas terus mengembangkan skil dan teknik-teknik baru serta teknologi yang digunakan terus di upgrade lebih canggih agar dapat menembus sekat-sekat keamanan yang terdapat pada suatu sistem. Serangan juga bisa dilancarkan melalui perangkat pengguna, jadi meskipun dalam sistem blockchain memberikan keamanan tingkat tinggi melalui enkripsi serta mekanisme konsensus yang ketat perlu terus pembaruan dan memperkuat sistem keamanan dalam blockchain, guna untuk mencegah dan menghadapi serangan cyber dimasa yang akan datang.

Terdapat resiko lainnya dalam penerapan teknologi blockchain yaitu terkait dengan biaya transaksi dan pemeliharan jaringan blockchain yang relatif cukup tinggi. Pemeliharaan jaringan juga perlu sumber daya teknis yang bukan sedikit mulai dari tenaga ahli yang dapat mengoprasikan dan mengelola sistem dengan baik. Biaya transaksi dalam jaringan blockchain bisa meningkat secara signifikan dan sangat fluktuatif ketika jaringan mengalami kepadatan yang tinggi, dimana dapat menambah beban biaya bagi pihak pengguna yang sering melakukan transaksi.

Resiko yang perlu dan penting untuk dipertimbangkan bila menerapkan teknologi blockchain ialah keamanan data para pihak yang terkait dengan transaksi pada notaris, berdasarkan peraturan pada Undang-Undang Jabatan Notaris tidak disebutkan secara eksplisit bahwa kewajiban notaris salah satunya ialah memberikan perlindungan hukum terkait data-data para pihak yang telah menghadap kepadanya. Akan tetapi dalam pasal 16 ayat (1) huruf a Undang-Undang Jabatan Notaris dinyatakan bahwa notaris wajib menjaga kepentingan para pihak yang berhubungan dengan perbuatan hukum, artinya dalam pasal tersebut walaupun tidak disebutkan secara langsung mengenai perlindungan data para pihak, notaris mempunyai tanggung jawab untuk menjaga dan melindungi kepentingan hukum dari para pihak yang terlibat, karena perlindungan data merupakan bagian dari menjaga kepentingan, dengan data yang terlindungi dan aman maka kepentingan para pihak juga akan terjaga. Jadi meskipun tidak diterangkan secara langsung dalam UUJN untuk melindungi data, kewajiban menjaga kepentingan para pihak juga termasuk juga menjaga dan melindungi data para pihak yang menghadap kepada Notaris.

Selain beberapa resiko diatas, dengan diterapkannya blockchain juga menjadi tantangan baru bagi notaris karena tidak punya besik atau latar belakang teknis, apalagi teknologi blockchain yang cukup rumit dan adanya kebutuhan khusus untuk menerapkan serta mengelola operasional sehari-hari. Pengelolaan dan penerapan blockchain membutuhkan pemahaman yang mendalam terkait konsep-konsep teknis, seperti verifikasi dan menyimpan transaksi, pemeliharaan jaringan dan pengamanan data blockchain, selain itu juga ddibutuhkan keahlian praktis dalam mengelola infrastruktur teknis yang mendorong penggunaaan blockchain, seperti mengatur koneksi internet, mamantau, mengontrol sistem dan keamanan. Dengan demikian hal tersebut juga beresiko adanya kesalahan dalam menjalankan dan perawatan sistem blockchain, yang nantinya bisa jadi menyebabkan kelalaian administratif dan kerugian data yang berpotensi merugikan pihak yang terlibat.

3. 2 Perlindungan Hukum Keamanan Data Cyber Notary Dalam Penyimpanan Protokol Notaris Di Blockchain

Penerapan teknologi blockchain sebagai penyimpan protokol notaris dapat menyebabkan beberapa dampak negatif seperti virus dan peretasan, untuk mencegah itu semua maka perlu adanya perlindungan baik secara sistem maupun hukum. Virus merupakan program ilegal yang masuk kedalam sistem komputer lewat jaringan, virus dapat menyebar keseluruh sistem yang ada didalam perangkat komputer, sehingga berpotensi dapat merusak program pada komputer tersebut. Gangguan digital yang diakibatkan oleh virus bisa mengakibatkan kerusakan data dan fatalnya bisa menyebabkan data tersebut hilang. Dengan demikian maka perlu peran notaris untuk memasang anti virus pada seluruh komputer atau prangkat yang digunakan.

Menurut pasal 40 ayat (2) Undang-Undang ITE menyatakan bahwa teknologi informasi atau berbasis digital hanya bisa diterapkan bila mempunyai sistem atau telah menerapkan serta memperhatikan terkait perlindungan data, baik menjaga privasi data, keutuhan data, kelancaran dan pelayanan publik yang sesuai dengan aturan Undang-Undang. Sedangkan menurut pasal 1 angka (22) Undang-Undang Nomor 24 Tahun 2013 mengenai Administrasi Kependudukan menyatakan bahwa data pribadi adalah data perseorangan tertentu yang di simpan, dirawat, dijaga kebenaran dan dilindungi privasinya.

Dalam melindungi data para pihak dan menghindari penyalahgunaan wewenang diluar wilayah jabatan Notaris, maka butuh aturan yang mewajibkan notaris menginformasikan dan mendaftarkan IP address perangkat komputer yang dipakai notaris dalam melakukan pekerjaanya pada Kementrian Hukum dan Hak Asasi Manusia. Selain hal tersebut, setiap akta elektronik yang dibuat notaris perlu mensertakan IP address notaris tersebut, guna untuk pemeriksaan oleh pihak yang berwenang dalam memeriksa apakah praktik cyber notary yang dilakukan oleh seorang notaris sudah sesuai dengan ketentuan yang berlaku.

Perlindungan hukum selain terhadap para pihak juga penting diberikan kepada notaris selaku pemegang dan yang menjalankan teknologi blockchain atau pemegang data pribadi para pihak, jika terjadi kesalahan atau kelalaian yang dilakukan notaris dalam cyber notary dalam pasal 46 ayat 1 UUPDP menyatakan bahwa jika terjadi kegagalan dalam melindungi data pribadi, pengendali data pribadi wajib menyampaikan pemberitahuan secara tertulis paling telat 3 × 24 jam kepada subyek data pribadi tersebut dan juga kepada lembaga yang terkait, kemudian dalam ayat 2 dijelaskan bahwa pemberitahuan secara tertulis yang dimaksud ayat 1 mininal memuat terkait data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data tersebut. Pada ayat 3

menyatakan bahwa pengendali data pribadi dalam hal ini notaris wajib memberitahukan kepada masyarakat terkait kegagalan perlindungan data pribadi.

Kegagalan perlindungan data pribadi yang dimaksud pada pasal 46 tersebut ialah terkait kerahasiaan data, integritas dan ketersediaan data tersebut, termasuk adanya pelanggaran keamanan baik yang tidak disengaja maupun yang disengaja, dimana peretasan tersebut bertujuan untuk merusak, mencuri dan menghilangkan, merubah, menyebarkan maupun akses layanan yang tidak sah. Kejadian tersebut dapat kapan saja menimpa notaris dalam jabatannya dalam membuat akta dan menyimpan protokol notaris secara digital atau elektronik. Dengan demikian notaris wajib bertanggung jawab ketika terjadinya kebocoran sistem dan kegagalan dalam melindungi data pribadi dari para pihak yang terlibat transaksi dengan notaris, sebagaimana diterangkan dalam pasal 47 UUPDP.

Resiko yang perlu adanya perlindungan sistem dan hukum selain serangan virus ialah tindak kejahatan cyber crime atau peretasan, cyber crime adalah kejahatan dengan melalui jaringan komputer dalam bentuk hacking, skimming, pencurian data dan cyber harassment. Dengan penerapan cyber notary apalagi penyimpanan protokol notaris dalam sistem blockchain maka sangat perlu adanya perlindungan baik secara sistem maupun hukum itu sendiri, salah satunya ialah untuk mencegah adanya serangan cyber atau peretasan guna melindungi data-data dari para pihak, dimana notaris sebagai pejabat umum berwebang dan bertanggung jawab untuk membantu mewujudkan kepastian hukum. Pencurian atau peretasan dapat dengan mudah dilakukan karena semua data baik data pribadi para pihak, minuta akta dan dokumen-dokumen penting lainnya bila diterapkan sistem blockchain akan disimpan secara digital, walaupun blockchain mempunyai keunggulan sebagai sistem yang paling tinggi tingkat keamanannya tetapi bukan tidak mungkin bisa di bobol, mengingat para hacking semakin hari semakin berkembang keterampilannya.

Pembuatan akta dan penyimpanan minuta akta dengan teknologi blockchain atau secara digital dapat mempermudah pekerjaan notaris, sehingga lebih efektif dan efisien, jika cyber notary di terapkan maka butuh beberapa dokumen elektronik dalam prosesi pelayanan hukum pada masyarakat salah satunya ialah dengan adanya tanda tangan secara digital, e-ID atau Identitas secara digital pula, secara hukum identitas merupakah data pribadi yang bersifat privat atau rahasia, sangat beresiko bila data sampai di retas dan disalahgunakan oleh orang lain yang tidak bertanggung jawab, untuk itu pemilik data berhak atas perlindungan data pribadinya. Jika terdapat peretasan dalam sistem blockchain makan dampak yang diakibatkan ialah hipanya data yang dicuri oleh hacking, sehingga rawan penyalahgunaan informasi pribadi para pihak atau terhadap objek perjanjian, kerahasiaan akta notaris yang dilanggar, serta manipulasi data yang dapat merugikan pihak-pihak yang terkait.

Terkait peretasan diatur dalam ketentuan pasal 30 Undang-Undang Informasi dan Teknologi Elektronik yang mengkualifikasikan tindak kejahatan cyber yang dapat dikenai hukuman pidana yaitu yang pertama, setiap orang dengan sengaja dan tanpa hak mengakses sistem elektronik milik orang lain dengan cara apapun. Kedua, setiap orang dengan sengaja dan tanpa hak mengakses sistem elektronik milik orang lain dengan cara apapun, yang bertujuan mendapat informasi elektronik atau dokumen elektronik. Ketiga, setiap orang dengan sengaja dan tanpa hak mengakses sistem elektronik milik orang lain dengan cara apapun yang membobol sistem pengaman. Dimana dalam pasal 45 UUITE perbuatan di atas dapat diancam hukuman pidana penjara paling lama 8 tahun dan denda paling banyak Rp. 800.000.000 (delapan ratus juta rupiah).

Dalam Undang-Undang Perlindungan Data Pribadi pada pasal 67 ayat 1 mengatakan bahawa setiap orang yang dengan sengaja serta melawan hukum untuk mendapat dan memperoleh data pribadi milik orang lain dengan tujuan keuntungan bagi dirinya sendiri maupun orang lain yang bisa menyebabkan kerugian bagi pemilik data diri pribadi tersebut dapat dikenai hukuman pidana penjara paling lama 5 tahun atau diekani pidana denda paling banyak Rp. 5.000.000.000.00 (Lima Miliar rupiah). Kemudian dalam ayat 2 menyatakan bahwa setiap orang yang dengan sengaja telah melawan hukum membocorkan dan menyebar data pribadi milik orang lain dapat dikenai pidana penjara paling lama 4 tahun atau dikenai pidana denda paling banyak Rp. 4.000.000.000.00 (Empat Miliar rupiah). Kemudian dalam ayat 3 menyatakan bahwa setiap orang yang dengan sengaja telah melawan hukum memakai data pribadi milik orang lain dapat dikenai pidana penjara paling lama 5 tahun atau dikenai pidana denda paling banyak Rp. 5.000.000.000.00 (Lima Miliar rupiah). Kemudian dalam pasal 68 Undang-Undang Perlindungan Data Pribadi menyatakan bahwa setiap orang yang dengan sengaja membuat data pribadi palsu atau telah memalsukan dat pribadi dengan tujuan untuk menguntungkan dirinya sendiri maupun orang lain yang bisa menyebabkan kerugian bagi pihak lain dapat dikenai ancaman pidana penjara paling lama 6 tahun atau pidana denda paling banyak Rp. 6.000.000.000.00 (Enam Miliar rupiah).

4. KESIMPULAN

Dalam penerapan cyber notary dalam penyimpanan protokol notaris di blockchain memberikan beberapa risiko yang pertama terkait tingginya biaya oprasional dan perawatannya dalam mengoprasikan teknologi blockchain agar tetap berjalan lancar. Yang kedua terkait serangan virus yang kapan saja bisa terjadi dan dapat merusak sistem dan data yang berada pada prangkat yang digunakan notaris dalam menjalankan pekerjaanya memberikan pelayanan hukum kepada masyarakat. kemudian yang ketiga dan yang paling ditakutkan ialah adanya serangan cyber atau peretasan data yang dilakukan oleh hacking yang mencari keuntungan bagi kepentingannya, dimana dapat dengan mudah membobol sitem blockchen meskipun diyakini mempunyai sitem keamanan yang tinggi, tapi mengingat para hacking juga terus mengembangkan sitem dan kemampuannya, sehingga rawan terhadap data yang disimpan secara digital. Disisi lain notaris juga mempunyai tantangan baru dalam transisi dari sistem penyimpanan secara konvesional ke sistem elektronik menggunakan teknologi blockchain.

Perlindungan hukum terhadap keamanan data cyber notary dalam penyimpanan protokol notary di blockchain sampai sekarang belum ada aturan yang secara detail memberikan perlindungan dan secara eksplisit mengatur terkait cyber notary, namun terkait perlindungan data dan ancama peretasan dapat mengacu pada peraturan pasal 30 Undang-Undang Informasi dan Teknologi Elektronik mengenai kejahatan cyber dan dalam Undang-Undang Perlindungan Data Pribadi pada pasal 67. Tetapi masih perlu adanya kepastian hukum baru yang secara jelas mengatur terkait cyber notary dan penyimpanan protokol notaris secara digital di blockchain, diawali dengan adanya kewenangan dan tanggung jawab notaris dalam cyber notary, adanya perlindungan dari Direktorat Tindak Pidana Siber secara khusus, adanya pengawasan dan sanksi secara langsung maupun tidak langsung.

5. 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, hal, 686.

Ainun Najib, Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi, Acta Diurnal Jurnal Ilmu Hukum Kenotariatan, Vol. 7, No. 1, 2023, hal. 44.

Ceavin Rufus De Prayer Purba, Implementasi Teknologi Blockchain pada Real Estate Transaction, Makalah II4031 Kriptografi dan Koding, Semester II Tahun 2024.

CSA. Teddy Lesmana, Eva Elis, Siti Hamimah, "Urgensi Undang-Undang Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Mayarakat Indonesia", Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, Vol. 3, No. 2, 2022, hlm. 2.

Daniyah Fadhilah Hasyan, Pemanfaatan Kecerdasan Buatan dan Blockchain dalam Pembuatan Akta Notaris di Indonesia, Jurnal Notarius, Vol. 17, No. 1, 2024, hal. 435.

Iftah Putri Nurdiani, Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime, Jurnal Kriminologi Indonesia, Vol.16, No.2, 2020, hlm. 3.

Imam Teguh Islamy, Sisca Threecya Agatha, Rezky Ameron, Berry Humaidi Fuad, Evan Evan, Nur Aini Rakhmawati, "Pentingnya Memahami Penerapan Privasi Di Era Teknologi Informasi", Jurnal Teknologi Informasi dan Pendidikan.Vol. 11 No. 2. 2018, hlm. 23.

M. Syamsudin, Operasionalisasi Penelitian Hukum (Jakarta: PT. Raja Grafindo Persada, 2007), h. 57.

Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

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, hal. 6.

Shinta Pangesti, Darmawan, Grace I, Cynthia P Limantara, Konsep Pengaturan Cyber Notary Di Indonesia, Jurnal Rechtsidee, Vol. 7, Desember, 2020, hal. 15.

Tiara Karlina, Penerapan Teknologi Blockchain dalam Penyimpanan Protokol Notaris, Badamai: Law Journal, Vol. 9, Issue 1, 2024, hal. 131.

Victor Amrizal, Qurrotul Aini, Kecerdasan Buatan (Jakarta: Halaman Moeka, 2013), hal. 56.

Zibin Zheng, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, 2017, hal. 120.