

BARCODING DIGITAL SIGNATURE AUTHENCITY SEBAGAI ALAT BUKTI PERKARA PIDANA

Agus BudiantoFakultas Hukum Universitas Pelita Harapan | agus.budianto@uph.edu**Shinta Pangesti**Fakultas Hukum Universitas Pelita Harapan | shinta.pangesti@uph.edu**Debora Pasaribu**Fakultas Hukum Universitas Pelita Harapan | debora.pasaribu@uph.edu**Stephanie Faustina**Program Pascasarjana Magister Kenotariatan UPH | stephanie.faustina123@yahoo.co.id

ARTICLE INFO

Article history:*Received*

30 November 2020

Revised

26 Januari 2021

Accepted

18 Mei 2021

Kata-kata Kunci:

Siber Notaris, Tanda tangan Digital, Keabsahan Tanda tangan Digital.

Keywords:

Cyber Notary, Digital Signature; Authenticity of Digital Signatures

Abstrak

Bisnis dan setiap layanan publik, dalam kondisi yang penuh ketidakpastian karena pandemi Covid-19, termasuk didalamnya konsep penggunaan cyber notary bagi pejabat pembuat akta otentik. Penelitian ini adalah penelitian hukum normatif, dengan menggunakan data primer dan data sekunder. Perolehan data primer melalui focus group discussion, interview secara langsung atau melalui seminar online, dengan teknik non-random purposive sampling. Cyber notary diselenggarakan untuk membuktikan dokumen pendukung dari suatu akta yang wajib dilengkapi dengan tanda tangan elektronik yang terdaftar. Suatu digital signature telah memenuhi unsur secara yuridis, yaitu seseorang yang membutuhkan tanda tangan digitalnya dianggap mengakui apa yang dituliskannya secara keseluruhan dalam dokumen elektronik yang bersangkutan. Oleh karenanya mendesak bagi Kemenkumham untuk segera membuat peraturan tentang digital signature dalam akta otentik notaris, mengingat sah secara hukum sebagai alat bukti surat sebagaimana disebutkan dalam Pasal 184 ayat (1) UU No. 8 Tahun 1981 tentang Kitab Hukum Acara Pidana.

Abstract

Business and every public service, in conditions full of uncertainty due to the Covid-19 pandemic, includes the concept of using a cyber notary for authentic deed officials. This research is normative legal research, using secondary data and primary data. The primary data is obtained through focus group discussions (FGD), interviews, and online seminars using a non-random purposive sampling technique. A cyber notary is held to prove the supporting documents of a deed completed with a registered electronic signature. Digital signature has been fulfilled by law, which means a person who needs a digital signature is considered to admit what has been written in the electronic document. Therefore, it is urgent for the Ministry of Law and Human Rights to immediately provide regulations regarding the digital signatures on the notary's authentic deed, considering becomes legally valid as a piece of evidence as stated in Article 184 paragraph (1) of Law No. 8 the Year 1981 concerning the Criminal Procedure Law.

PENDAHULUAN

Teknologi informasi berbasis daring (*online*) merupakan hal yang tidak asing lagi dan menjadi *trend* di seluruh dunia, tentunya hal ini memberikan dampak yang sangat besar bagi kehidupan manusia. Teknologi berbasis *online* tidak hanya memberikan berbagai kemudahan, tetapi juga membuat berbagai hal menjadi efisien. Masuknya pengaruh teknologi ini menyebabkan perkembangan dan perubahan pola pikir masyarakat di berbagai bidang tidak dapat dihindari. Perubahan yang paling terasa dapat dilihat dari munculnya berbagai perusahaan *startup*, menjamurnya *online shop*¹, perubahan dalam pola kehidupan masyarakat sehari-hari, perubahan di dalam birokrasi pemerintah, hingga perubahan dalam bidang hukum. Munculnya perusahaan-perusahaan *startup* di Indonesia membawa dampak yang signifikan dalam bidang bisnis perdagangan dan jasa. *Startup* sendiri didefinisikan sebagai suatu peluang bisnis baru yang memiliki potensi dengan memanfaatkan teknologi². Bisnis ini didirikan oleh orang perorangan atau perusahaan dalam kondisi yang penuh ketidakpastian³, dengan mencoba berbagai macam metode agar suatu produk atau jasa yang ditawarkan dapat diterima oleh masyarakat.

Berkaitan dengan bisnis yang sukses dalam keadaan yang tidak pasti tersebut, Indonesia mengalami keadaan yang tidak pasti, ketika di awal tahun 2020, seluruh dunia dilanda pandemi Novel Coronavirus 2019 (nCoV-2019) yang secara resmi dinamai sebagai *Corona Virus Disease 2019* (Covid-19) oleh WHO dan *severe acute respiratory syndrome coronavirus 2* (SARS-CoV-2) oleh ICTV, termasuk genus β , memiliki envelope, berbentuk bundar atau oval dan sering pleomorfik, dengan diameter antara 60-140 nm. Virus ini dapat ditemukan dalam sel epitelial pernafasan setelah 96 jam dengan kultur *in vitro*, dan membutuhkan waktu sekitar 6 hari untuk dapat diisolasi dan dilakukan kultur *cell line* Vero E6 dan Huh-7. Saat ini, sumber utama infeksi adalah para pasien Covid-19. Pembawa (*carrier*) yang *asimptomatik* juga berpotensi menjadi sumber infeksi. Virus ini umumnya ditularkan melalui kontak langsung dan percikan (*droplet*) dan penularan lewat udara mungkin terjadi pada orang yang lama terpapar konsentrasi udara tinggi pada ruang tertutup.⁴

Pandemi Covid-19 telah memberi pengaruh efek domino tidak hanya di Indonesia tetapi juga di hampir seluruh belahan bumi yang berjumlah 188 negara dengan positif Covid-19 mencapai 59.481.313 kasus dan korban meninggal sebanyak 1.404.542 jiwa di seluruh dunia⁵. Kasus Covid-19 di Indonesia, hingga saat ini, terkonfirmasi sebanyak 511.836 kasus, dengan jumlah meninggal dunia

¹ Afifatur Rohimah, 'Era Digitalisasi Media Pemasaran Online dalam Gugurnya Pasar Ritel Konvensional' (2018) 6 (2) KANAL (Jurnal Ilmu Komunikasi) 91, 92.

² Hendry E. Ramdhan, *Startup Lessons* (Penebar Plus 2016) 52.

³ Yudha Yudhanto, *Information Technology Business Start-Up* (Elex Media Komputindo 2019) 2.

⁴ Komisi Kesehatan Nasional RRC, *Guidance for Corona Virus Disease 2019: Prevention, Control, Diagnosis and Management* (Forum Academia NTT ed, People's Medical Publishing House 2019) 3-4.

⁵ WHO, 'WHO Coronavirus Disease (COVID 19) Dashboard' (world Health Organization) <https://covid19.who.int/?gclid=EAIaIQobChMI9p7lvKOf7QIVDyUrCh0jqAPTEAAYASAAEgI8OPD_BwE> diakses pada tanggal 26 November 2020.

sebanyak 16.225 jiwa⁶. Dengan memperhatikan pernyataan resmi World Health Organization (WHO) yang menyatakan Covid-19 sebagai pandemi global, pernyataan resmi Presiden Republik Indonesia yang menyatakan penyebaran Covid-19 sebagai Bencana Nasional (Bencana Non-Alam), berdasarkan Keputusan Presiden No. 12 Tahun 2020 tentang Penetapan Bencana Non-Alam Penyebaran Covid-19 Sebagai Bencana Nasional dan Keputusan Kepala Badan Nasional Penanggulangan Bencana (BNPB) No. 13A Tahun 2020 tentang Perpanjangan Status Keadaan Tertentu Darurat Bencana Wabah Penyakit Akibat Virus Corona di Indonesia.

Kemudian, diikuti dengan Keputusan Menteri Kesehatan (Kepmenkes) No. HK.01.07/Menkes/239/2020 tentang Penetapan Pembatasan Sosial Berskala Besar (PSBB) di Wilayah Provinsi DKI Jakarta Dalam Rangka Percepatan Penanganan Covid-19, Pemerintah mengeluarkan pernyataan PSBB sesuai dengan Pasal 59 Undang-Undang (UU) No. 6 Tahun 2018 tentang Keekarantinaan Kesehatan, sebagai upaya pencegahan pandemi global. PSBB adalah pembatasan kegiatan tertentu penduduk dalam suatu wilayah yang diduga terinfeksi Covid-19 sedemikian rupa untuk mencegah kemungkinan penyebaran Covid-19. Selain DKI Jakarta yang telah dua kali menerapkan PSBB, juga diikuti dengan daerah-daerah lain, sebagai penyangga DKI (bodetabek) berdasarkan Kepmenkes No. HK.01.07/Menkes/249/2020 tentang PSBB di wilayah Tangerang, Tangerang Selatan, Provinsi Banten; Jo. Kepmenkes No. HK.01.07/Menkes/248/2020 tentang PSBB di wilayah Kab. Bogor, Kota Bogor, Kota Depok, Kab. Bekasi dan Kota Bekasi, Provinsi Jawa Barat. Untuk wilayah Provinsi Daerah Istimewa Yogyakarta (DIY), Pemda secara resmi memperpanjang kebijakan Pengetatan Secara Terbatas Kegiatan Masyarakat (PTKM) di Provinsi DIY mulai tanggal 26 Januari 2021 sampai dengan 8 Februari 2021, yang tertuang dalam Instruksi Gubernur DIY No. 4/INSTR/2021, kebijakan ini diambil guna menindaklanjuti Instruksi Menteri Dalam Negeri No. 02 Tahun 2021 tentang Perpanjangan Pemberlakuan Pembatasan Kegiatan Masyarakat untuk Pengendalian Penyebaran Covid-19.

Pemberlakuan PSBB tersebut, juga memberikan batasan bahkan penghentian sementara pelaksanaan tugas dan jabatan pejabat umum yakni, notaris dan PPAT. Di lain pihak, kebijakan dimaksud menimbulkan berbagai ketidakpastian hukum dan ruang hukum yang kosong terhadap tindakan hukum yang seharusnya dilakukan oleh pihak yang berkepentingan. Terlebih, jika melihat ketentuan yang mengatur tentang pembuatan akta autentik baik dalam UU No. 2 Tahun 2014 tentang Perubahan Atas UU No. 30 Tahun 2004 tentang Jabatan Notaris (UU Jabatan Notaris) maupun Peraturan Pemerintah (PP) No. 37 Tahun 1998 tentang Pejabat Pembuat Akta Tanah dan Perubahannya, yang mana secara prinsipil menuntut untuk interaksi secara langsung, yaitu tatap muka dan kehadiran para pihak yang berkehendak dengan notaris. Ketentuan itu sebagaimana diatur pada Pasal 1868 Kitab Undang-Undang Hukum Perdata (KUHPerdato) yang menyatakan bahwa suatu akta disebut akta autentik bilamana memenuhi syarat, yaitu bentuk akta ditentukan dalam peraturan perundang-undangan, dibuat oleh atau

⁶ Komite Penanganan Covid-19 Dan Pemulihan Ekonomi Nasional, 'Peta Sebaran COVID-19' (Komite Penanganan Covid-19 Dan Pemulihan Ekonomi Nasional) <<https://covid19.go.id/peta-sebaran-covid19>> diakses pada tanggal 26 November 2020.

dihadapan pejabat umum yang berwenang dan tempat pembuatan akta merupakan wilayah kewenangan pejabat tersebut⁷.

Kehadiran para pihak sebagai penghadap di depan (dihadapan) notaris dan PPAT, merupakan sebuah permasalahan tersendiri jika melihat dan memperhatikan ketentuan pemerintah tentang PSBB tersebut. Untuk itulah, permasalahan ini kami usulkan dalam Hibah Penelitian Kemenristekdikti tahun 2020, Skema Penelitian Tesis Magister, dimaksudkan untuk mencari jalan keluar atau solusi, agar masyarakat yang membutuhkan akta-akta notarial tetap terpenuhi. Sedangkan bagi notaris dan PPAT, tidak mengabaikan ketentuan pemerintah tentang PSBB tersebut, dan akta-akta tersebut tetap mempunyai kekuatan hukum mengikat. Tentunya, aspek lain yang perlu diperhatikan adalah, pada layanan publik dan layanan komersial yang membutuhkan dan memerlukan pendampingan dari notaris dan pejabat pembuat akta autentik. Seperti halnya: perbankan, badan-badan di sektor kesehatan, investasi, pasar modal dan sebagainya yang masih tetap diizinkan melaksanakan kegiatan untuk memenuhi kebutuhan penanggulangan pandemi ini.

Apakah dimungkinkan, dengan memperhatikan permasalahan tersebut digunakan *cyber notary*? Tentunya yang dimaksud dengan *cyber notary* adalah akta notarial yang dibuat tanpa hadirnya para pihak di hadapan pejabat pembuat akta. Konsep ini sebenarnya tidaklah asing, notaris sebagai salah satu pilar penegakan hukum nasional melalui UU Jabatan Notaris, berfungsi menjalankan prinsip-prinsip negara hukum yakni menjamin kepastian, ketertiban, dan perlindungan hukum yang berintikan pada kebenaran dan keadilan⁸. Sebagai pejabat umum yang terpercaya, akta-akta yang dibuatnya harus menjadi alat bukti yang kuat apabila terjadi sengketa hukum di pengadilan⁹. Hal inilah yang tidak boleh dilanggar mengingat dalam UU Jabatan Notaris, notaris wajib membacakan akta yang dibuatnya, dihadapan para pihak serta menandatangani akta tersebut.

Jika melihat bunyi Pasal 15 UU Jabatan Notaris, menyebutkan, notaris memiliki tugas dan kewenangan yang beberapa diantaranya adalah selain membuat akta otentik, juga berwenang untuk mengesahkan tanda tangan dan menetapkan kepastian tanggal surat dibawah tangan, membukukan surat dibawah tangan, melakukan pengesahan, dan kewenangan lain yang diatur dalam peraturan perundang-undangan. Kewenangan lain yang dimaksud dalam Pasal 15 ayat (3) ini dijelaskan dalam Penjelasan Pasal 15 ayat (3) yang salah satunya adalah mensertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*). Sampai disini, kewenangan notaris dalam hal *cyber notary* tersebut belum ada pengaturan lebih lanjut, sehingga akibatnya menghambat perkembangan profesi kenotariatan dalam melayani kebutuhan masyarakat pada masa pandemi Covid-19 ini.

Ketertinggalan atau keterlambatan pengaturan *cyber notary* dalam sektor pelayanan jasa pembuatan akta ini, menyebabkan timbulnya permasalahan yang menyebabkan konsep *cyber notary* tidak diterapkan secara keseluruhan dalam pelaksanaan tugas notaris. Bahkan Negara Belgia menyatakan sah penggunaan

⁷ Andi Suci Wahyuni, 'Urgensi Kebutuhan Aka Otentik di Masa Pandemi Covid-19' (2020) 18 (1) Jurnal Hukum dan Dinamika Masyarakat 2.

⁸ Sunarto Siswanto, 'Peranan Kode Etik Profesi Dalam Pemuliaan Jabatan Notaris' (Tesis, Universitas Gadjah Mada Yogyakarta 2007) 5.

⁹ Marsudi Triatmojo, 'Fakultas Hukum UGM sebagai Lembaga Pendidikan Notaris' Harian Kedaulatan Rakyat (Yogyakarta, 4 Juni 2007) 17

video *conference* dengan klien pada masa pandemi Covid-19 ini, sedangkan Perancis sejak tahun 2004 telah memperkenalkan penggunaan tanda tangan elektronik dan teknologi kriptografi¹⁰. Selama pandemi Covid-19, dari bulan Maret sampai Desember 2020 ini, beberapa instansi telah mengadakan seminar online (*daring*) tentang konsep *cyber notary* ini. Bahwa sebelum pandemi Covid-19, konsep *cyber notary* (e-notary) sudah diterapkan, selain penggunaan media *teleconference* dalam RUPS dengan merujuk pada Pasal 12 Peraturan Otoritas Jasa Keuangan (POJK) No. 16/POJK.04/2020, juga diterapkan pada pengesahan badan hukum dan jaminan fidusia online.¹¹

Tuntutan penggunaan *cyber notary* sudah sangat mendesak, menjalankan program dan ketentuan pemerintah dalam mencegah penyebaran Covid-19 menjadi sebuah prioritas yang tidak dapat dikesampingkan. Namun, prioritas tersebut tidak diimbangi dengan pengaturan yang jelas penggunaan *cyber notary* dalam pembuatan akta otentik, sedangkan masyarakat juga berada dalam kondisi “terdesak” membutuhkan akta otentik dalam setiap transaksi, khususnya dalam kondisi resesi¹² akibat pandemi Covid-19.

Oleh karena itu, artikel hasil dari penelitian ini sangat penting, karena notaris memiliki peran yang sentral dalam membuat akta dan kekuatan akta yang sempurna sebagai alat pembuktian dipersidangan. Namun, berkembangnya teknologi dan perubahan peraturan perundang-undangan yang mengadopsi IT, serta tuntutan akan efisiensi dan kepraktisan dari masyarakat, membuat notaris berada pada ruang yang tidak terlindungi. Banyak kontrak atau dokumen hukum yang dibuat dan/atau melalui proses digitalisasi, namun praktik digitalisasi akta masih menjadi larangan dalam UU Jabatan Notaris. Jika nantinya terdapat gugatan atas akta digitalisasi sebagai konsep *cyber notary* menjadikan posisi notaris sebagai buah simalakama. Di sisi lain, akta sebagai produk dari *cyber notary* tersebut, masih harus diuji kekuatan otentiknya sebagai alat bukti surat dalam persidangan pidana, sebagaimana dimaksud dalam Pasal 184 ayat (1) UU No. 8 Tahun 1981 tentang Hukum Acara Pidana. Masalah yang diangkat dalam penulisan ini adalah bagaimana keabsahan akta notaris yang dilakukan melalui media internet (*cyber notary*), dan bagaimana kekuatan pembuktian akta tersebut dalam persidangan?

Penelitian ini menggunakan jenis penelitian hukum normatif menggunakan metode dimana kualitas dari suatu norma hukum yang berkaitan dengan isu hukum yang terjadi itu diuji dengan dasar pembenaran dari undang-undang, pendapat para ahli hukum, dan buku-buku mengenai teks hukum. Data yang dipergunakan lebih diutamakan data sekunder, dan dikuatkan dengan data primer, yang kami dapatkan secara langsung melalui Interview dengan metode *non-probability purposive sampling*, yaitu menentukan narasumber yang kompeten dengan topik praktik *cyber notary* dengan menggunakan teknik *Focus Group*

¹⁰ Cahyo Rahardian Muzar, 'Notaris dan Kebutuhan Saat Ini' (Seminar Online E-Notary Dalam Era Industri 4.0 dan Sosial 5.0: Kebutuhan atan Ancaman, Oktober 2020).

¹¹ Aulia Taufani, 'E-Notary: Praktek Kenotariatan Menghadapi Era Industri 4.0 dan Sosial 5.0' (Seminar Online E-Notary Dalam Era Industri 4.0 dan Sosial 5.0: Kebutuhan atan Ancaman, Oktober 2020).

¹² Chairul Iksan Burhanuddin, Muhammad Nur Abdi, 'Ancaman Krisis Ekonomi Global dari Dampak Penyebaran Virus Corona (Covid-19)' (2020) 17 (1) Jurnal Akmen 90, 92.

Discussion (FGD)¹³, antara lain: Robinson Halim (Notaris wilayah Jawa Barat), Maria Pranatia (Notaris wilayah Jakarta Barat), Susi Susantijo (Pengajar Magister Kenotariatan) dan Risky Karo-Karo (ahli hukum telematika). Selain itu, mengikuti seminar online dan bertanya langsung dengan para narasumber.

PEMBAHASAN

Kewenangan Notaris dalam Pembuatan *Cyber Notary* sebagai Akta Otentik

Sebagaimana telah disampaikan dalam latar belakang di atas, bahwa dalam Penjelasan Pasal 15 ayat (3) UU Jabatan Notaris, "... salah satunya adalah mensertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*)", yang merupakan kewenangan lain, artinya bukan kewenangan utamanya. Kewenangan utama notaris, sebagaimana diatur dalam Pasal 15 ayat (1) dan (2), antara lain membuat akta otentik. Selain membuat akta otentik, notaris berwenang pula antara lain untuk mengesahkan tanda tangan dan menetapkan kepastian tanggal surat di bawah tangan (legalisasi), membukukan surat-surat di bawah tangan (*waarmerking*), membuat kopi dari asli surat-surat di bawah tangan berupa salinan yang memuat uraian sebagaimana ditulis dan digambarkan dalam surat yang bersangkutan (akta penyimpanan) dan melakukan pengesahan kecocokan fotokopi sesuai dengan surat aslinya (fotokopi sesuai asli)¹⁴.

Dalam Pasal 15 ayat (3) UU Jabatan Notaris tersebut tidak disebutkan adanya mensertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*), kalimat tersebut diketemukan dalam penjelasannya, sehingga fokus utama dari kewenangan notaris bukan pada mensertifikasi akta secara elektronik¹⁵. Apabila dilihat konsep tentang *cyber notary* yang dikemukakan oleh Theodore Sedwick, manajer dari *cyber notary Project-US Council for International Business* menjelaskan bahwa istilah *cyber notary* dipakai untuk menggambarkan suatu kombinasi dari fungsi *notary public* secara konvensional dan aplikasinya dalam transaksi elektronik. *Cyber notary* diibaratkan sebagai pengaman dalam lalu lintas transaksi elektronik melalui internet. Hal ini dapat terjadi melalui penerapan fungsi *notary public* secara konvensional, yaitu otentik secara otomatis atau elektronik dengan memanfaatkan infrastruktur umum yang ada serta tanda tangan elektronik. Untuk itu, seorang *cyber notary* dikatakan harus memiliki kualifikasi yang tinggi di bidang teknologi informasi, selain dari kemampuan hukum yang dimilikinya sebagai landasan¹⁶.

Fungsi utama dari *cyber notary* adalah melakukan *certification* dan *authentication* dalam lalu lintas transaksi elektronik. Fungsi *certification* dalam hal ini memiliki arti kewenangan untuk bertindak sebagai *certification authority (trusted*

¹³ Agus Budiarto, 'Legal Research Methodology Reposition In Research On Social Science' (2020) 9 International Journal of Criminology and Sociology 1339–1346.

¹⁴ Dewa Ayu Widya Sari, R.A Retno Murni dan I Made Udiana, 'Kewenangan Notaris di Bidang Cyber Notary Berdasarkan Pasal 15 ayat (3) Undang-Undang No. 2 Tahun 2014 tentang Perubahan Atas Undang-Undang No. 30 Tahun 2004 tentang Jabatan Notaris' (2017) 2 Acta Comitas 219, 220.

¹⁵ Robinson Halim, 'Notaris dan Cyber Notary' (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

¹⁶ Agung Fajar Matra, 'Penerapan Cyber Notary di Indonesia Ditinjau Dari Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notaris' (Tesis, Universitas Indonesia 2012) 57.

third-party) yang dapat mengeluarkan digital *certificate* dan *public key* kepada para pihak yang memerlukan. Sedangkan fungsi *authentication* dalam hal ini berkaitan dengan aspek hukum yang dipersyaratkan bagi transaksi elektronik tersebut. Aspek hukum ini dalam prakteknya biasanya berupa kepastian tanggal dan waktu terjadinya transaksi yang disahkan oleh *cyber notary* dengan cap notaris elektronik (*electronic Notary seal*) dan disimpan dalam protokolnya untuk keperluan pengarsipan, tanpa menyinggung mengenai status akta autentik sebagaimana yang dikenal dalam praktek notariat *civil law*. Aspek hukum inilah yang membedakan *cyber notary* dengan *certification authority* yang hanya mampu menjamin keamanan transaksi hanya dari segi teknis¹⁷.

Gagasan untuk menerapkan *cyber notary* di Indonesia sudah muncul sejak tahun 1995, tetapi dengan berbagai keterbatasan peraturan serta tidak adanya dasar hukum yang mendukung untuk memfasilitasi hal tersebut, maka *cyber notary* tersebut hanya menjadi sebuah konsep saja. Sebenarnya, dengan perkembangan teknologi informasi di bidang komputer dan jaringan internet, kewenangan membuat akta dalam bentuk digital tidak dapat dilepaskan dengan tugas-tugas seorang notaris. Sebagaimana disebutkan, bahwa seorang *cyber notary* adalah sekaligus seorang ahli computer dan ahli hukum. Peran seorang *cyber notary* “*would be to bind the private key of the particular sender with the public key of the intended recipient and to envelope the entire transaction in an umbrella of trust*”. *Cyber notary* melakukan verifikasi tanggung jawab finansial, kewenangan, serta kedudukan hukum dari para pihak dengan kesimpulan bahwa notaris elektronik seharusnya *attorneys*, demikian *The American Bar Association’s Information Security Committee*.

Namun demikian, jika memang diterapkan di Indonesia, syarat formil yang harus dipenuhi dari akta *cyber notary* untuk menjadi akta notariil adalah data pendukung seperti KTP, kartu keluarga, akta perkawinan, akta lahir, dan sebagainya harus terverifikasi dalam suatu sistem yang diselenggarakan oleh pemerintah. Sebab, dalam praktiknya notaris kesulitan untuk membuktikan apakah data tersebut benar atau palsu. Selain itu, syarat materilnya adalah menghadap kepada penghadap, mengesahkan tanda tangan, wilayah yang tidak melanggar jabatan dan lain sebagainya. *Cyber notary* perlu diselenggarakan untuk membuktikan dokumen pendukung dari suatu akta. Tetapi, media tersebut wajib dilengkapi dengan tanda tangan elektronik yang terdaftar¹⁸.

Kewenangan notaris dalam membuat *cyber notary* tidak terlepas dari ketentuan tentang penerapan sistem elektronik, yaitu PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, sebagai ketentuan pelaksana dari UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (UU ITE). PP ini dimaksudkan untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan keamanan dan ketertiban umum dalam suatu masyarakat yang demokratis. Terdapat sebanyak 11 (sebelas) muatan dalam pengaturan PP ini, namun yang berkaitan dengan kewenangan notaris dalam pembuatan *cyber notary*, antara lain terkait dengan

¹⁷ Susi Susantijo, ‘Notaris dan Cyber Notary’ (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

¹⁸ Maria Pranatia, ‘Perluah Cyber Notary?’ (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

penyelenggara sertifikasi elektronik, penyelenggara sistem elektronik dan penyelenggara transaksi elektronik.

Melihat pada terminologinya, sertifikasi transaksi yang dilakukan secara elektronik ini adalah berupa sertifikat. Dalam PP No. 71 Tahun 2019, definisi sertifikat elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Dengan kata lain, sertifikasi transaksi yang dilakukan secara elektronik adalah pembuatan sertifikat elektronik hasil dari transaksi yang dilakukan dengan cara dan ciri *paperless*, *borderless* dan tanpa harus bertatap muka. Dengan mengacu kepada terminologi sertifikasi transaksi yang dilakukan secara elektronik di atas, maka kewenangan lain yang diberikan oleh UU Jabatan Notaris kepada notaris adalah kewenangan bagi notaris untuk mengesahkan suatu transaksi elektronik dengan menerbitkan suatu bukti pengesahan berupa sertifikat elektronik. Adapun unsur-unsur kewenangan notaris tersebut adalah sebagai berikut: 1) Kewenangan mengesahkan; 2) Dengan bukti pengesahan berupa sertifikat elektronik; dan 3) Atas suatu transaksi elektronik.

Berdasarkan PP No. 71 Tahun 2019 tersebut, kewenangan sertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*) dan penyelenggaraan sertifikasi elektronik, memiliki sifat dan/atau prinsip yang sama dengan kewenangan notaris berupa kewenangan mengesahkan tanda tangan dan menetapkan kepastian tanggal surat di bawah tangan dengan mendaftar dalam buku khusus (yang dalam praktiknya, kewenangan ini dinamakan legalisasi tanda tangan atau pengesahan tanda tangan). Dalam legalisasi tanda tangan, kepastian yang diberikan oleh notaris adalah kepastian atas pihak yang membubuhkan tanda tangan; dan kepastian atas tanggal penandatanganan surat dibawah tangan tersebut. Dalam memberikan kepastian atas pihak yang membubuhkan tanda tangan, notaris harus melakukan pengecekan identitas dari pihak penandatanganan.

Meskipun pembuktian notaris dalam hal pengecekan identitas bersifat formal, dimana data identitas dalam bentuk asli (bukan fotokopi) dan terdapat kesesuaian antara nama, foto dan tanda tangan pada identitas dengan pihak penandatanganan. Tanggal penandatanganan surat akan menjadi tanggal legalisasi (tanggal pengesahan tanda tangan) yang diberikan oleh notaris. Sama hal dengan kewenangan sertifikasi transaksi yang dilakukan secara elektronik (*cyber notary*) dan penyelenggaraan sertifikasi elektronik berdasarkan PP No. 71 Tahun 2019 dimana sertifikasi transaksi tersebut adalah untuk menjamin kepastian atas pihak yang melakukan transaksi dan kepastian tanggal serta waktu transaksi. Selain terdapat PP No. 71 Tahun 2019, juga diberlakukan PP No. 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, yang menyatakan juga, bahwa penyelenggaraan transaksi elektronik dalam lingkup publik atau privat yang menggunakan sistem elektronik untuk kepentingan pelayanan publik wajib menggunakan sertifikat keandalan dan/atau sertifikat elektronik.

Barcoding Digital Signature Authencity dalam Cyber Notary

Sebagaimana disampaikan Dirjen AHU Kementrian Hukum dan HAM bahwa di Perancis sudah memperkenalkan kriptografi (*cryptography*) dalam *cyber notary*.

Pengertian *cryptography* ditemukan pada Oxford Advanced Learner's Dictionary, sebagai “*the art of writing or solving codes*” atau suatu seni untuk menulis dan memecahkan sandi. Kriptografi ini terdiri dari dua unsur, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). *Encryption* adalah proses untuk membuat suatu informasi menjadi tidak dapat dipahami (*unintelligible*) bagi para pihak yang tidak berwenang. Sedangkan *decryption* adalah proses untuk membalik *encryption* kepada bentuk aslinya sehingga informasi tersebut dapat dibaca kembali. Kriptografi sudah dikenal sejak zaman Romawi dan digunakan oleh Julius Caesar untuk pengiriman informasi rahasia¹⁹.

Untuk penggunaan dengan metode jaringan internet, terdapat dua jenis sistem kriptografi, *Pertama*, kriptografi simetris (*symmetric cryptography*) yang dikenal juga dengan *secret key cryptography*. Yaitu kriptografi yang didasarkan pada penggunaan kunci rahasia tunggal (*single secret key*), digunakan oleh kedua belah pihak yang terlibat dalam suatu hubungan komunikasi, dimana pihak pengirim menggunakan kunci tersebut untuk melakukan enkripsi dan pihak penerima juga menggunakan kunci yang sama untuk melakukan dekripsi²⁰. Masalah yang muncul pada penggunaan sistem ini adalah tingkat kecerobohan *single secret key* yang cukup tinggi, dikarenakan pertukaran kunci yang sama diantara kedua belah pihak dalam praktiknya sulit dijamin keamanannya. *Kedua*, kriptografi asimetris (*asymmetric cryptography*). Kriptografi asimetris yang disebutkan juga dengan *public key infrastructure* (PKI) yaitu kriptografi yang didasarkan pada penggunaan sepasang kunci berpasangan, yang disebut *private key* dan *public key*²¹. Kemungkinan yang terjadi dalam praktik adalah apabila kunci-kunci tersebut hilang atau terlupakan oleh pihak-pihak yang berkepentingan, pesan yang dikirimkan akan menjadi tidak dapat dibaca atau dimengerti.

Dalam penulisan ini, lebih memfokuskan dengan penggunaan tanda tangan digital dengan metode barcoding. Tanda tangan digital adalah satu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim dari suatu pesan atau penandatanganan dari suatu dokumen dan untuk memastikan isi dari pesan atau dokumen dikirim tanpa perubahan. *Digital Signature* bukanlah tanda tangan biasa berupa goresan tinta atau pena yang dimasukkan ke dalam dokumen komputer dengan cara dilakukan *scan* terlebih dahulu (*digitalized image of handwritten signature*). Kristel Kreek menyebutkan *digital signature* sebagai “...*a digital signature is one that is specially based on asymmetric cryptography, coupled with a one-way hash function*”²². Jadi, suatu digital signature didapatkan dengan berlandaskan pada sistem *asymmetric cryptography* dengan terlebih dahulu menciptakan suatu *hash* atau *message digest* yaitu berupa *mathematical summary* dari dokumen bersangkutan yang akan dikirimkan.

Pemindaian *digital signature* pada suatu akta elektronik dapat dilakukan dengan tahapan, antara lain: 1) pengirim harus membuat “*hash*” dari pesan (*original plaintext*) dengan melalui *hash function* tertentu secara *Secure Hash Algorithm-1*

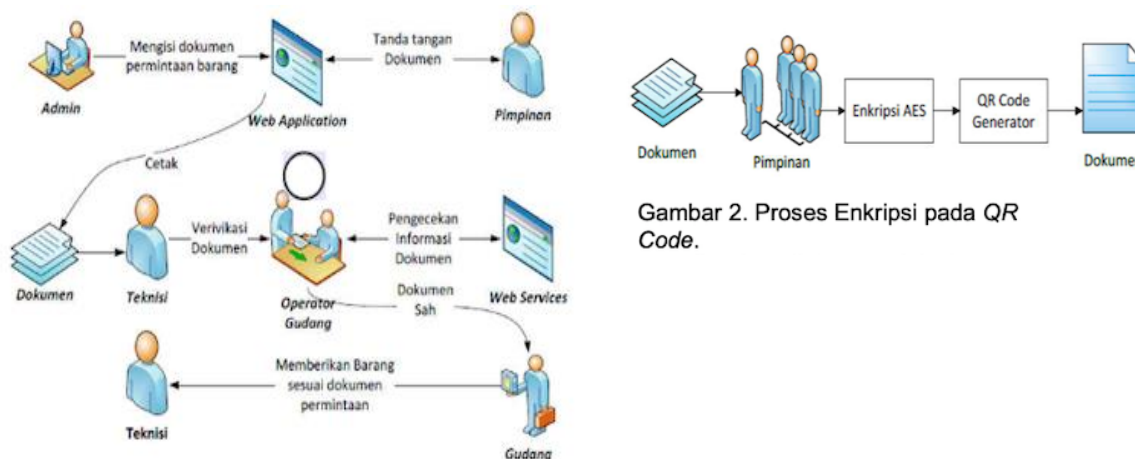
¹⁹ Ian J. Lloyd, *Informasi Technology Law* (Ed. 2, Butterworths 1997) 482.

²⁰ Sutan Remy Sjahdeini, ‘Sistem Pengamanan E-Commerce’ (2002) 18 (1) Jurnal Hukum Bisnis 9.

²¹ Ian J. Lloyd (n 19) 45.

²² Arvind K. Sharma, Satish K. Mittal, ‘A Comprehensive Study on Digital-Signature with Hash-Fanction’ (2019) 7 (4) International Journal of Computer Sciences and Engineering 604, 604-605.

(SHA-1), dan saat ini sering digunakan oleh protokol *Secure Electronic Transaction* (SET). SET sendiri merupakan protokol yang dikembangkan oleh Master Card dan Visa yang khusus dirancang untuk memberikan kepastian kepada *merchants* dan *cardholders* untuk dapat melaksanakan transaksi secara aman melalui internet; 2) *Hash* tersebut kemudian di enkripsi dengan menggunakan *private key* milik si pengirim untuk memperoleh suatu *digital signature*²³, sebagaimana gambar 1 & 2 berikut²⁴.



Gambar 1. Proses tanda tangan digital.

Gambar 2. Proses Enkripsi pada QR Code.

Dengan kata lain, yang di enkripsi dalam hal ini bukanlah pesan aslinya melainkan *hash* dari pesan asli yang telah melalui suatu *hash function* tertentu. Apabila suatu pesan yang telah dibubuhi *digital signature* telah diubah, sekalipun hanya sedikit saja, maka pesan tersebut tidak akan dapat di dekripsi dengan benar. apabila hal tersebut terjadi, maka pesan tersebut telah diubah atau dipalsukan pada saat pengiriman berlangsung. Sederhananya, untuk setiap pesan yang dikirimkan berbeda, maka *message digest*-nya pasti berbeda pula. Sehingga, *digital signature* tidak hanya berfungsi untuk memverifikasi *authentication* atau identitas para pihak, tetapi juga untuk memverifikasi integritas pesan itu sendiri (*message integrity*).

Secara yuridis, pembubuhan penandatanganan merupakan suatu fakta hukum (*rechtsfeit*) yang mempunyai arti suatu pernyataan kehendak pembuat tanda tangan, bahwa ia dengan membubuhkan tandatangannya tersebut dibawah suatu tulisan, menghendaki agar tulisan itu dalam hukum dianggap sebagai tulisannya sendiri. Dengan demikian, suatu tanda tangan digital telah memenuhi unsur yuridis dari tanda tangan secara konvensional dan seseorang yang membutuhkan tanda tangan digitalnya dianggap mengakui apa yang dituliskannya secara keseluruhan dalam dokumen elektronik yang bersangkutan. Dalam hal ini, *digital signature* mengandung makna juga sebagai *one signature for one document*, yaitu bilamana terjadi perubahan sedikit saja pada tulisan yang dikirimkan maka tanda tangan digitalnya pun juga akan berubah dan akan menjadi tidak *valid* lagi dalam kaitannya dengan si penandatanganan.

²³ Asril Sitompul, *Hukum Internet-Pengenalan Mengenai Masalah Hukum di Cyberspace* (Citra Aditya Bakti 2001) 45.

²⁴ Abdul Gani Putra Suratma & Abdul Aziz, 'Tanda Tangan Digital Menggunakan QR Code dengan Metode Advanced Encryption Standard' (2017) 18 (1) Jurnal Techno 59, 60 - 61.

Pada gambar 2 tersebut diatas, proses selanjutnya adalah pembuatan barcode (barcoding) dalam bentuk QR (*Quick Response*) Code. Barcode merupakan instrumen yang bekerja berdasarkan asas kerja digital, oleh karenanya bagi kita yang menyukai dunia komputer pasti tertarik memahami cara kerjanya. Kode baris atau barcode ini terdiri dari deretan-deretan garis hitam tebal dan tipis berselang-seling, dengan huruf atau deretan angka dibawahnya yang dapat memberi informasi tentang identitas atau jenis barang dengan lebih cepat dan akurat, karena informasi ini disimpan dalam komputer. Kemudian, informasi tersebut dibaca dengan scanner.²⁵ Tentunya pembuatan *digital signature* ini ke dalam bentuk QR Code hanya dapat dilakukan pada sebuah aplikasi.

Dengan demikian, sebuah dokumen yang telah di enkripsi dengan *digital signature* dengan memenuhi tahapan tersebut diatas, dapat menjadi dokumen asli yang berkaitan dengan hubungan hukum antar pihak sebagai dokumen elektronik legal. Menurut UU ITE, menyebutkan bahwa dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Sementara itu, yang di maksud dengan tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Fungsi tanda tangan elektronik menurut PP No. 82 Tahun 2012 sebagai alat autentikasi dan verifikasi atas identitas penanda tangan serta keutuhan dan keautentikan informasi elektronik. Menurut Pasal 60 ayat (2) PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, terdapat 2 (dua) jenis tanda tangan elektronik, yaitu tanda tangan elektronik yang tersertifikasi dan tanda tangan elektronik tidak tersertifikasi. Penggunaan QR Code saja sebagai tanda tangan elektronik merupakan jenis tanda tangan elektronik yang tidak tersertifikasi, sehingga tidak direkomendasikan karena dengan mudah untuk dipalsukan.

Oleh karena itu, penggunaan tanda tangan elektronik berbentuk QR Code dalam akta notaris, wajib dilakukan sertifikasi lebih lanjut oleh jasa²⁶ penyelenggara sertifikasi elektronik indonesia dan dibuat dengan menggunakan perangkat pembuat tanda tangan elektronik tersertifikasi. Instansi resmi yang ditunjuk oleh pemerintah, untuk menyelenggarakan sertifikasi tanda tangan elektronik tersebut, salah satunya adalah Badan Siber dan Sandi Negara (BSSN) dan Balai Sertifikasi Elektronik (BSE).

²⁵ B. T. Atmojo, S. R. Sulistyanti, and E. Nasrullah, 'Model Sistem Kendali Pintu Otomatis Menggunakan Barcode Berbasis PC (Personal Computer) Pada Gerbang Laboratorium Teknik Elektro Unila' (2013) 7 (2) Jurnal Rekayasa dan Teknologi Elektro 47, 55.

²⁶ Daftar Penyelenggara Sertifikasi Elektronik bisa di lihat di Penyelenggara Sertifikat Elektronik, 'Status Pengakuan Penyelenggara Sertifikasi Elektronik' (Kominfo PsrE) <https://tte.kominfo.go.id/listPSrE/_/> diakses pada tanggal 19 Desember 2020.

Cyber Notary sebagai Alat Bukti “Surat” menurut Pasal 184 ayat (1) UU No. 8 Tahun 1981 tentang Kitab Hukum Acara Pidana

Pembuktian merupakan tahap yang menentukan dalam proses perkara, karena dari hasil pembuktian dapat diketahui benar atau tidaknya suatu dakwaan atau tuntutan tersebut dengan menunjuk pada alat bukti. Alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan terdakwa. Pembuktian sendiri ialah perbuatan membuktikan, membuktikan berarti memberi atau memperlihatkan bukti, melakukan sesuatu sebagai kebenaran, melaksanakan, menandakan, menyaksikan, dan meyakinkan²⁷.

Merujuk pada sistem pembuktian dan alat-alat bukti sebagaimana pada Pasal 184 ayat (1) UU No. 8 Tahun 1981 tentang Kitab Hukum Acara Pidana (KUHP), bahwa alat bukti yang sah, ialah: a. Keterangan saksi; b. Keterangan ahli; c. Surat; d. Petunjuk; e. Keterangan terdakwa, yang dimaksud dengan alat bukti adalah segala sesuatu yang ada hubungannya dengan suatu perbuatan, dimana dengan alat-alat bukti tersebut, dapat dipergunakan sebagai bahan pembuktian guna menimbulkan keyakinan hakim atas kebenaran adanya suatu tindak pidana yang telah dilakukan terdakwa, sedangkan sistem pembuktian merupakan sebagian dari hukum acara pidana yang mengatur macam-macam alat bukti yang sah menurut hukum, sistem yang dianut dalam pembuktian, syarat-syarat dan tata cara mengajukan alat bukti tersebut serta kewenangan Hakim untuk menerima, menolak, dan menilai suatu pembuktian²⁸.

Dalam UU ITE *juncto* PP No. 82 Tahun 2012 dan PP No. 71 Tahun 2019, tidak mengatur istilah alat bukti elektronik. Pasal 54 ayat (1) UU ITE menggunakan termonologi data elektronik dapat dijadikan sebagai alat bukti. Namun demikian, jika merujuk pada Pasal 44 *jo.* Pasal 5 UU ITE, dengan menyebut “informasi elektronik” dan “bukti dokumen” oleh karenanya, bukti elektronik pada dasarnya adalah informasi atau dokumen, atau dapat disebut secara umum “data” bukan alat. Sejalan dengan hal tersebut, terdapat dalam Pasal 26 A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi, menyebut alat bukti lain, yang kemudian disebut bukti elektronik adalah berbentuk informasi dan dokumen, dan mendudukan sebagai bagian dari alat bukti petunjuk.

Demikian juga dalam Pasal 73 UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (UU TPPU), menyebutkan: Alat bukti yang sah dalam pembuktian tindak pidana pencucian uang ialah: a. alat bukti sebagaimana dimaksud dalam hukum acara pidana; dan/atau b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau alat yang serupa optik dan dokumen. Insan Pribadi²⁹ menambahkan, keberagaman pengaturan mengenai bukti elektronik

²⁷ Eddy O.S Hiariej, *Teori & Hukum Pembuktian* (Erlangga 2012) 3

²⁸ Hari Sasangka dan Lily Rosita, *Hukum Pembuktian Dalam Perkara Pidana* (Mandar Maju 2003) 10.

²⁹ Insan Pribadi, ‘Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana’ (2018) 3 (1) *Lex Renaissance* 109, 118.

sebagai alat bukti sebagaimana Pasal 184 (1) KUHPdata, tentunya kembali pada asas legalitas dalam UU ITE itu sendiri. Pasal 5 UU ITE menyebutkan:

- [1] Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
- [2] Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
- [3] Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam UU ini.
- [4] Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
 - a. Surat yang menurut UU harus dibuat dalam bentuk tertulis, dan
 - b. Surat beserta dokumennya yang menurut UU harus dibuat dalam bentuk akta notariil atau akta yang dibuat oleh pejabat pembuat akta.

Dengan demikian, akta yang dibuat oleh notaris, atau dibuat di hadapan notaris yang telah dipindai (*scan*) untuk kepentingan arsip digital para pihak dapat secara sah sebagai surat dan dikategorikan sebagai alat bukti dalam persidangan pidana apabila akta yang asli dapat diperlihatkan.

Jika, akta asli tidak dapat diperlihatkan maka dapat dikategorikan sebagai petunjuk³⁰. Hal demikian juga disampaikan oleh Mahkamah Agung pada tahun 1988, dengan mengeluarkan surat kepada Menteri Kehakiman No. 39/TU/88/102/Pid tanggal 14 Januari 1988 menyatakan “*microfilm* atau *microfiche*” dapat dipergunakan sebagai alat bukti yang sah dalam perkara pidana di pengadilan mengganti alat bukti surat, dengan catatan *microfilm* tersebut sebelumnya dijamin keotentikasiannya yang dapat ditelusuri kembali dari registrasi.³¹

Kembali kepada permasalahan di atas, terkait dengan implementasi Pasal 15 ayat (3) UU Jabatan Notaris yang menjadi permasalahan saat ini, sehingga mendesak untuk diperhatikan adanya sinergitas antara Kemenkumham, Ikatan Notaris Indonesia (INI) dengan Balai Sertifikasi Elektronik (BSE), terkait bentuk keamanan akta siber (termasuk namun tidak terbatas pada apakah ada sistem *barcode*, sistem hologram, tanda tangan digital yang dapat divalidasi), membuat payung hukum terkait *digital deeds*, akta apa saja yang dapat dibuat dalam bentuk dokumen elektronik. Jika melihat pada Pasal 5 ayat (1), (2) *Juncto* Pasal 44 UU ITE, ditafsirkan lebih lanjut menggunakan interpretasi gramatikal dan sistematis maka informasi elektronik, bukti elektronik dan hasil cetaknya (*screenshot*-nya) adalah alat bukti hukum yang sah dan merupakan perluasan alat bukti yang sah yang berbentuk ‘surat’ dan bukan merupakan ‘petunjuk’. Apabila mengacu pada Pasal 188 ayat (2) KUHP bahwa petunjuk sebagaimana dimaksud dalam ayat (1) hanya dapat diperoleh dari : a. keterangan saksi; b. surat; c. keterangan terdakwa. Dan berdasarkan Pasal 188 ayat (3) KUHP bahwa penilaian atas kekuatan pembuktian dari suatu petunjuk dalam setiap keadaan tertentu dilakukan oleh hakim dengan

³⁰ Rizky Karo-Karo ‘Cyber Notary dalam UU ITE’ (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

³¹ Triyanti, ‘Kekuatan Pembuktian Dokumen Elektronik Sebagai Pengganti Minuta Akta Notaris’ (2015) 2 (2) Jurnal Repertorium 20, 26.

arif lagi bijaksana setelah ia mengadakan pemeriksaan dengan penuh kecermatan dan kesaksamaan berdasarkan hati nuraninya.

Akibatnya dokumen elektronik adalah bukti langsung (*direct evidence/real evidence*) dan bukan merupakan bukti pelengkap. Mengutip pendapat Josua Sitompul, informasi dan dokumen elektronik dapat dijadikan alat bukti hukum yang sah, UU ITE telah mengatur bahwa adanya syarat formil dan syarat materil yang harus terpenuhi. Syarat formil diatur dalam Pasal 5 ayat (4) UU ITE, yaitu bahwa Informasi atau dokumen elektronik bukanlah dokumen atau surat yang menurut perundang-undangan harus dalam bentuk tertulis. Sedangkan syarat materil diatur dalam Pasal 6, Pasal 15, dan Pasal 16 UU ITE, yang pada intinya Informasi dan dokumen elektronik harus dapat dijamin keotentikannya, keutuhannya, dan ketersediaannya³².

Mengacu pada *Good Practice Guide for Digital Evidence* dari *Association of Chief Police Officers (ACPO)* di Inggris, Wales & Northern Ireland, bahwa terdapat 4 (empat) prinsip dalam bukti elektronik yakni:

1. *No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.*
(Terjemahan bebas: Tidak ada tindakan yang diambil oleh APH, orang yang dipekerjakan dalam instansi tersebut agar mereka mengubah data yang kemudian dapat diajukan di Pengadilan).
2. *In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.*
(Terjemahan Bebas: Jika setiap orang dirasa perlu untuk mengakses data asli, orang tersebut harus kompeten dalam melakukannya dan dapat memberikan bukti yang menjelaskan relevansi dan implikasi dari tindakan tersebut).
3. *An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.*
(Terjemahan bebas: Jejak/catatan audit dari semua proses yang diterapkan pada bukti digital harus disimpan. Pihak ketiga yang independent harus dapat memeriksa proses tersebut dan mencapai hasil yang sama).
4. *The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.*
(Terjemahan bebas: orang yang bertanggung jawab atas investigasi memiliki tanggung jawab keseluruhan untuk memastikan bahwa hukum dan prinsip dalam aturan ini ditaati).

Demikian juga, yang disampaikan oleh Edmon Makarim bahwa setidaknya terdapat 3 (tiga) dasar agar informasi maupun dokumen elektronik dapat dikatakan sama dengan bukti tertulis, yakni “dapat disimpan dan ditemukan kembali, tidak berubah substansinya atau yang dimaksud terjamin keotentikannya, serta bertandatangan apabila terdapat informasi yang menjelaskan adanya suatu objek hukum yang bertanggung jawab di atasnya atau terdapat sistem autentikasi yang

³² Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. (Tatanusa 2012) 15.

reliable yang menjelaskan identitas dan otoritas atau verifikasi dari pihak tersebut.³³ Pasal 11 UU ITE menyebutkan adanya 6 (enam) syarat, suatu tanda tangan elektronik dapat memiliki kekuatan hukum dan akibat hukum yang sah sebagai dokumen hukum, antara lain:

1. data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan;
2. data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penanda tangan;
3. segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
4. segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui;
5. terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penanda-tangannya; dan
6. terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap Informasi elektronik yang terkait.

Keenam syarat sebagaimana diatur dalam Pasal 11 UU ITE tersebut, harus tetap dijaga dan dipertahankan keasliannya oleh penegak hukum, dalam hal ini penyidik dan jaksa penuntut umum sampai pada pemeriksaan alat bukti dipersidangan oleh hakim. Hal demikian, mengingat alat bukti dokumen elektronik tersebut rentan untuk dirubah, dihapus atau bahkan di *cloning*, sehingga tidak lagi mempunyai kekuatan pembuktian atau diragukan *authenticity* nya sebagai alat bukti.

Oleh karena itu, prosedur untuk menjaga keaslian alat bukti elektronik, antara lain³⁴: *Pertama*, Proses *Acquiring* dan *Imaging*. Dalam hal ini, setelah penyidik menerima barang bukti digital, maka harus dilakukan proses *acquiring* dan *imaging* yang mengkopi (mengkloning/menduplikat) secara tepat dan presisi 1:1 dari hasil kopi tersebutlah maka seorang ahli forensik dapat melakukan analisis karena analisis tidak boleh dilakukan dari barang bukti digital yang asli karena dikhawatirkan akan mengubah barang bukti. *Kedua*, Melakukan Analisis. Setelah melakukan proses *Acquiring* dan *Imaging*, maka dapat dilanjutkan untuk menganalisis isi data terutama yang sudah dihapus, disembunyikan, di-enkripsi, dan jejak *log-file* yang ditinggalkan. Hasil dari analisis barang bukti digital tersebut yang akan dilimpahkan penyidik kepada Kejaksaan untuk selanjutnya dibawa ke Pengadilan.

Terakhir, tentunya dari apa yang telah diuraikan diatas, bahwa kehadiran *digital signature* akta-akta notaris yang telah tersertifikasi secara elektronik menjadi kebutuhan yang mendesak. Di samping mengantisipasi penyebaran Covid-19 sebagaimana konsekuensi dari Pasal 1 angka 7 UU Jabatan Notaris, bahwa mengurangi datangnya para pihak dan saksi pada akta yang dibuat oleh notaris. Namun, yang lebih penting dari hal tersebut adalah menghindari penggunaan tanda tangan basah oleh staf notaris atau notaris pengganti secara tidak bertanggung jawab.

³³ Edmon Makarim, 'Keautentikan Dokumen Publik Elektronik dalam Administrasi Pemerintahan dan Pemerintahan Publik' (2015) 45 (4) Jurnal Hukum dan Pembangunan 508, 532.

³⁴ Cahyo Handoko, 'Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan' (2016) 6 (1) Jurisprudence 13.

PENUTUP

Permasalahan tentang *cyber notary* belum diatur dalam UU Jabatan Notaris, sementara tuntutan masyarakat akan kebutuhan akta notaris semakin meningkat, bahkan cenderung naik ketika Indonesia berada pada masa pandemi Covid-19. Terbatasnya ruang gerak pelaku usaha terbentur dengan peraturan pemerintah untuk menjalankan protokol kesehatan, seperti menjaga jarak, larangan berpergian dan pembatasan berskala besar. Secara langsung, kebijakan ini menghambat kebutuhan masyarakat akan jasa notaris. Sementara itu, dalam UU Jabatan Notaris, pembuatan akta secara elektronik, dengan tanda tangan elektronik tidak diatur secara jelas, termasuk ketentuan Pasal 15 ayat (3) UU Jabatan Notaris. Sebuah *digital signature* didapatkan dengan sistem *asymmetric cryptography* dengan terlebih dahulu menciptakan suatu *hash* atau *message digest* yaitu berupa *mathematical summary* dari dokumen bersangkutan. Pemindaian *digital signature* pada suatu akta elektronik dapat dilakukan dengan tahapan, antara lain: 1) pengirim harus membuat “*hash*” dari pesan (*original plaintext*) dengan melalui *hash function* tertentu secara *Secure Hash Algorithm-1* (SHA-1), dan saat ini sering digunakan oleh protokol Secure Electronic Transaction (SET); 2) *Hash* tersebut kemudian di enkripsi dengan menggunakan *private key* milik si pengirim untuk memperoleh suatu *digital signature*. Oleh karena itu, *digital signature* mengandung makna juridis sebagai *one signature for one document*. Menurut ketentuan UU ITE *Juncto* PP No. 71 Tahun 2019 dan PP No. 82 Tahun 2012 dengan jelas dinyatakan bahwa tanda tangan elektronik yang telah tersertifikasi oleh lembaga yang ditunjuk Pemerintah (BSSN dan BSE) untuk melakukan sertifikasi tanda tangan elektronik, maka dokumen tersebut sah secara hukum sebagai alat bukti surat sebagaimana disebutkan dalam Pasal 184 ayat (1) UU No. 8 Tahun 1981 tentang Kitab Hukum Acara Pidana dan digunakan sebagai alat pembuktian dalam perkara pidana. Saran yang disampaikan dalam penelitian ini adalah tidak ada alasan lagi bagi Kementerian Hukum dan HAM cq. Ikatan Notaris Indonesia untuk menunda-nunda kebijakan pelaksanaan transaksi elektronik oleh notaris dalam akta elektroniknya, sehingga mendesak untuk segera dilakukan amandemen kedua terhadap UU Jabatan Notaris.

Ucapan Terima Kasih

Tim Peneliti merupakan dosen tetap FH UPH mengucapkan terima kasih sebesar-besarnya kepada Kementerian Ristek dan Pendidikan Tinggi atas terpilihnya topik penelitian ini dalam Hibah Kemenristekdikti Tahun Anggaran 2020, skema Penelitian Tesis Magister, berdasarkan Surat Keputusan No. 26/E1/KPT/2020 dan Perjanjian/Kontrak No. 425/LPPM-UPH/IX/2020.

DAFTAR REFERENSI

Buku

Hiariej EOS, *Teori & Hukum Pembuktian* (Erlangga 2012)

- Komisi Kesehatan Nasional RRC, *Guidance for Corona Virus Disease 2019: Prevention, Control, Diagnosis and Management* (Forum Academia NTT ed, People's Medical Publishing House 2019)
- Lloyd IJ, *Informasi Technology Law* (Ed. 2, Butterworths 1997)
- Ramdhan HE, *Startup Lessons* (Penebar Plus 2016)
- Sasangka H dan Rosita L, *Hukum Pembuktian Dalam Perkara Pidana* (Mandar Maju 2003)
- Sitompul A, *Hukum Internet-Pengenalan Mengenai Masalah Hukum di Cyberspace* (Citra Aditya Bakti 2001)
- Sitompul J, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* (Tatanusa 2012)
- Yudhanto Y, *Information Technology Business Start-Up* (Elex Media Komputindo 2019)

Artikel Jurnal

- Atmojo BT, Sulistyanti SR, and Nasrullah E, 'Model Sistem Kendali Pintu Otomatis Menggunakan Barcode Berbasis PC (Personal Computer) Pada Gerbang Laboratorium Teknik Elektro Unila' (2013) 7 (2) *Rekayasa dan Teknol. Elektro*.
- Sari AW, Dewa. Murni RAR dan Udiana IM, 'Kewenangan Notaris di Bidang Cyber Notary Berdasarkan Pasal 15 ayat (3) Undang-Undang No. 2 Tahun 2014 tentang Perubahan Atas Undang-Undang No. 30 Tahun 2004 tentang Jabatan Notaris' (2017) 2 *Acta Comitatus*.
- Budianto, Agus. 'Legal Research Methodology Reposition In Research On Social Science' (2020) 9 *International Journal of Criminology and Sociology*.
- Burhanuddin C I dan Abdi M N, 'Ancaman Krisis Ekonomi Global dari Dampak Penyebaran Virus Corona (Covid-19)' (2020) 17 (1) *Jurnal Akmen*.
- Cahyo H. 'Kedudukan Alat Bukti Digital dalam Pembuktian Cybercrime di Pengadilan' (2016) 6 (1) *Jurisprudence*.
- Makarim E, 'Keautentikan Dokumen Publik Elektronik dalam Administrasi Pemerintahan dan Pemerintahan Publik' (2015) 45 (4) *Jurnal Hukum dan Pembangunan*.
- Pribadi, Insan. 'Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana' (2018) 3 (1) *Lex Renaissance*.
- Rohimah A. 'Era Digitalisasi Media Pemasaran Online dalam Gugurnya Pasar Ritel Konvensional' (2018) 6 (2) *KANAL (Jurnal Ilmu Komunikasi)*
- Sharma A K, Mittal S K, 'A Comprehensive Study on Digital-Signature with Hash-Fanction' (2019) 7 (4) *International Journal of Computer Sciences and Engineering*.
- Sjahdeini S R, 'Sistem Pengamanan E-Commerce' (2002) 18 *Jurnal Hukum Bisnis*.
- Suratma A G P dan Aziz A, 'Tanda Tangan Digital Menggunakan QR Code dengan Metode Advanced Encryption Standard' (2017) 18 (1) *Jurnal Techno*.

Triyanti, 'Kekuatan Pembuktian Dokumen Elektronik Sebagai Pengganti Minuta Akta' (2015) 11 (2) Jurnal Repertorium.

Wahyuni A S, 'Urgensi Kebutuhan Aka Otentik di Masa Pandemi Covid-19' (2020) 18 (1) Jurnal Hukum dan Dinamika Masyarakat.

Tesis/Disertasi

Matra A F, 'Penerapan Cyber Notary di Indonesia Ditinjau Dari Undang-Undang Nomor 30 Tahun 2004 Tentang Jabatan Notaris' (Tesis, Universitas Indonesia 2012).

Siswanto S, "Peranan Kode Etik Profesi Dalam Pemuliaan Jabatan Notaris" (Tesis, Universitas Gadjah Mada 2007).

Artikel Koran

Triatmojo M, 'Fakultas Hukum UGM sebagai Lembaga Pendidikan Notaris' *Harian Kedaulatan Rakyat* (Yogyakarta, 4 Juni 2007)

Seminar

Muzar C R, 'Notaris dan Kebutuhan Saat Ini' (Seminar Online E-Notary Dalam Era Industri 4.0 dan Sosial 5.0: Kebutuhan dan Ancaman, Oktober 2020).

Taufani A, 'E-Notary: Praktek Kenotariatan Menghadapi Era Industri 4.0 dan Sosial 5.0' (Seminar Online E-Notary Dalam Era Industri 4.0 dan Sosial 5.0: Kebutuhan dan Ancaman, Oktober 2020).

Halim R, 'Notaris dan Cyber Notary' (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

Susantijo S, 'Notaris dan Cyber Notary' (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

Pranatia M, 'Perluakah Cyber Notary?' (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

Karo-Karo R, 'Cyber Notary dalam UU ITE' (FGD Penelitian Hibah Kemenristekdikti Pascamagister UPH, September 2020).

Website

WHO, 'WHO Coronavirus Disease (Covid-19) Dashboard' (world Health Organization) <https://covid19.who.int/?gclid=EAIaIQobChMI9p7lvKOf7QIVDyUrCh0jqAPT EAAAYASAAEgI8OPD_BwE> diakses pada tanggal 25 November 2020.

Komite Penanganan Covid-19 Dan Pemulihan Ekonomi Nasional, 'Peta Sebaran COVID-19' (Komite Penanganan Covid-19 Dan Pemulihan Ekonomi Nasional) <<https://covid19.go.id/peta-sebaran-covid19>> diakses pada tanggal 25 November 2020.

Daftar Penyelenggara Sertifikasi Elektronik bisa di lihat di Penyelenggara Sertifikat Elektronik, 'Status Pengakuan Penyelenggara Sertifikasi Elektronik' (Kominfo PsrE) <https://tte.kominfo.go.id/listPSrE/_> diakses pada tanggal 19 Desember 2020.

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 8 Tahun 1981 tentang Hukum Acara Pidana.

Undang-Undang Republik Indonesia Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang No. 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi.

Undang-Undang Republik Indonesia Nomor 40 Tahun 2007 tentang Perseroan Terbatas.

Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Undang-Undang Republik Indonesia Nomor 2 Tahun 2014 tentang Perubahan Atas UU No. 30 Tahun 2004 tentang Jabatan Notaris.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas UU Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 6 Tahun 2018 tentang Keekarantinaan Kesehatan.

Peraturan Pemerintah Republik Indonesia Nomor 37 Tahun 1998 tentang Pejabat Pembuat Akta Tanah dan Perubahannya.

Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Peyelenggaraan Sistem dan Transaksi Elektronik.

Keputusan Presiden Republik Indonesia Nomor 12 Tahun 2020 tentang Penetapan Bencana Nonalam Penyebaran *Corona Virus Disease 2019 (Covid 19)* Sebagai Bencana Nasional.

Keputusan Kepala Badan Nasional Penanggulangan Bencana (BNPB) Republik Indonesia Nomor 13A Tahun 2020 tentang Perpanjangan Status Keadaan Tertentu Darurat Bencana Wabah Penyakit Akibat Virus Corona di Indonesia.

Keputusan Menteri Kesehatan Republik Indonesia Nomor HK.01.07/Menkes/239/2020 tentang Penetapan Pembatasan Sosial Berskala Besar (PSBB) di Wilayah Provinsi DKI Jakarta Dalam Rangka Percepatan Penanganan *Corona Virus Disease 2019 (Covid-19)*.

Peraturan Menteri Kesehatan Republik Indonesia Nomor HK.01.07/Menkes/249/2020 tentang PSBB di wilayah Tangerang, Tangerang Selatan, Provinsi Banten.

Peraturan Menteri Kesehatan Republik Indonesia Nomor HK.01.07/Menkes/248/2020 tentang PSBB di wilayah Kab. Bogor, Kota Bogor, Kota Depok, Kab. Bekasi dan Kota Bekasi, Provinsi Jawa Barat.

