PERLINDUNGAN HUKUM TEKNOLOGI IDENTITAS DIGITAL MELALUI SISTEM VERIFIKASI IDENTITAS BERBASIS BIOMETRIK

LEGAL PROTECTION OF DIGITAL IDENTITY TECHNOLOGY THROUGH IDENTITY VERIFICATION SYSTEM BIOMETRIC-BASED

Oleh:

Nabilla Zahra[1], Recca Ayu Hapsari[2], Melisa Safitri[3]

[1]nabilla.19211409@student.ubl.ac.id; [2]Recca@ubl.ac.id; [3]Melisa@ubl.ac.id
[1, 2, 3] Universitas Bandar Lampung

ABSTRAK: Identitas digital merupakan sebuah refleksi dari diri seseorang yang dibuat dalam bentuk dan sistem digital. Di era digitalisasi yang saat ini berkembang pesat, sistem verifikasi identitas digital di dalam dunia teknologi juga ikut berkembang. Salah satunya adalah verifikasi identitas digital menggunakan sistem biometrik. Biometrik merupakan pengenalan individu yang berdasarkan karakteristik anatomi dan perilaku seperti sidik jari, wajah, iris, dan suara. Biometrik juga sangat relevan dengan teknologi karena biometrik digunakan untuk menganalisa fisik dan kelakuan manusia. Sistem verifikasi mempunyai tujuan untuk menerima atau menolak identitas yang diklaim sesorang. Pendekatan masalah yang akan digunakan dalam penelitian ini adalah pendekatan yuridis normatif. Jadi, Sistem verifikasi identitas digital berbasis biometrik ini merupakan salah satu solusi untuk keamanan verifikasi data pribadi seseorang karena cara penggunaanya hanya dapat terverifikasi oleh karakteristik anatomi seseorang sehingga sangat sulit untuk dipalsukan.

KATA KUNCI: Teknologi, Sistem Verifikasi, Identitas Digital, Biometrik

ABSTRACT: Digital identity is a reflection of one's self made in digital forms and systems. In the era of digitalization which is currently developing rapidly, digital identity verification systems in the world of technology are also developing. One of them is digital identity verification using a biometric system. Biometrics is the recognition of individuals based on anatomical and behavioral characteristics such as fingerprints, faces, irises, and voices. Biometrics is also very relevant to technology because biometrics is used to analyze human physique and behavior. The verification system aims to accept or reject the identity claimed by someone. The problem approach that will be used in this study is the normative juridical approach. So, this biometric-based digital identity verification system is one of the solutions for the security of verifying someone's personal data because the way it is used can only be verified by a person's anatomical characteristics so it is very difficult to fake.

KEYWORDS: Technology, Verification Systems, Digital Identity, Biometrics

PENDAHULUAN

Perkembangan teknologi yang terjadi saat ini cukup berkembang pesat. Tak heran jika kita sering kali menemukan hal-hal baru yang berkaitan dengan sistem teknologi dalam kehidupan sehari-hari. Bahkan teknologi pun hadir untuk memberikan sistem keamanan untuk menyimpan identitas seseorang. Salah satunya adalah menggunakan sistem verifikasi identitas biometrik. Sistem verifikasi identitas biometrik adalah sistem verifikasi yang menggunakan identitas biologis seseorang. Tujuannya untuk memverifikasi identitas seseorang dengan akurat. Dalam penggunaan sistem verifikasi identitas biometrik ini membutuhkan berbagai macam data. Di antaranya seperti foto wajah, rekaman suara, atau menggunakan rekam sidik jari yang kemudian data-data tersebut akan disimpan untuk selanjutnya digunakan jika pihak bersangkutan berusaha mendapat akses. Pengaksesan tersebut hanya dapat digunakan oleh pengakses yang data-datanya mampu dicocokan oleh sistem verifikasi tersebut.[1]

Identitas merupakan refleksi diri atau cerminan diri yang berasal dari keluarga, gender, budaya, etnis dan proses sosialisasi.[2] Identitas merupakan karakteristik yang dimiliki setiap orang untuk membedakan yang satu dan yang lainnya. Karakteristik yang dimiliki setiap orang menjadi suatu kumpulan informasi yang membedakan dan mengidentifikasikan setiap orang. Identitas juga merupakan rangkuman karakteristik yang tidak pernah berubah, seperti tempat dan tanggal lahir, sekolah yang pernah diikuti dan lain sebagainya atau bisa juga berhubungan dengan privasi seseorang. Namun, bebrapa hal juga dapat berubah seperti usia, warna rambut, atau alamat tempat tinggal.

Identitas digital adalah cara elektronik untuk mengidentifikasi seseorang yang di dalamnya terdapat sertifikat umum yang berisi kunci umum dari identitas seseorang, yang dapat dilihat, dan kunci pribadi dari identitas seseorang yang tidak dapat terlihat. Melansir dari laman resmi Direktorat Jendral Kependudukan dan Pencatatan Sipil Kementrian dalam Negeri Republik Indonesia, Identitas digital adalah instrument berupa QR Code yang berisi informasi identitas penduduk dan dapat disimpan di berbagai perangkat.[3] Instrumen yang dimaksudkan memuat semua informasi identitas yang ada di dunia digital. Identitas digital juga merupakan salah satu solusi untuk mengatasi tantangan utama dalam era digitalisasi saat ini, berupa Keamanan Data Pengguna. Sederhananya juga, Identitas digital merupakan kumpulan informasi tentang individu atau organisasi yang tersedia secara daring. Berbeda dengan identitas konvensional seperti KTP atau Paspor, identitas digital bisa di autentikasikan dari mana pun melalui kanal digital.[4]

Laporan dari McKisney yang bertajuk Digital Identification, Identitas digital harus memenuhi standar pemerintah atau sektor swasta saat digunakan untuk beberapa keperluan.[5]

---

[1] Verihubs, 2022, *Sistem Biometrik adalah Upaya Verifikasi Digital yang Aman*, *https://verihubs.com/blog/biometrik-adalah/* di akses pada tanggal 27 Agustus 2022.

[2] *Larry A. Samovar, Richard E. Porter, Edwin R. McDaniel. (2010). Communication Between Cultures. Wadsworth and Cengage Learning, Boston, hlm. 154-161.*

[3] DUKCAPIL KEMENDAGRI, 2022, *Yuk, Kenali Identitas Kependudukan Digital*, *https://dukcapil.kemendagri.go.id/berita/baca/1327/yuk-kenali-identitas-kependudukan-digital* diakses pada tanggal 27 Agustus 2022.

[4] Dian Harni, 2022, *Apa Itu Identitas Digital dan Manfaattnya bagi Perkembangan Bisnis*, *https://id.techinasia.com/apa-itu-identitas-digital-dan-manfaatnya* diakses pada tanggal 27 Agustus 2022.

[5] McKisney Global Institute, 2019, *Digital Identification*, *https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-*

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

Misalnya pembukaan rekening bank hingga pendaftaran sekolah atau pekerjaan. Beberapa protokol kredensial yang bisa digunakan untuk autentikasi ini adalah verifikasi berbasis Biometrik dan QR Code. Seseorang juga hanya bisa memiliki satu identitas untuk digunakan. Identitas yang digunakan tersebut harus dalam persetujuan individu yang secara sadar telah di daftarkan dan mengetahui bagaimana cara menggunakannya. Selain keamanan identitas diri, sistem identitas digital juga perlu memastikan bahwa pengguna memiliki akses ke data pribadinya sendiri termasuk juga kontrol atas siapa saja yang dapat mengakses data tersebut. Pada laporan tersebut disebutkan salah satu protokol kredensial untuk sebuah autentikasi yaitu sistem verifikasi identitas berupa verifikasi berbasis biometrik. Identitas biometrik merupakan identitas digital dengan autentifikasi analisis tubuh seseorang yang dimana hasil analisis tersebut akan direkam sehingga identitas pembuat tidak dapat digunakan oleh orang lain.

Di dalam dunia bisnis digital, risiko kebocoran data atau identitas digital pelaku bisnis digital terus meningkat seiring bertumbuhnya nilai transaksi bisnis digital di Indonesia. Data yang bocor bisa sangat merugikan perusahaan ataupun pelaku bisnis digital perorangan, karena dapat digunakan pihak-pihak yang tidak bertanggung jawab untuk melakukan tindak kejahatan (cybercrime). Karena kemungkinan sejumlah risiko yang bisa terjadi, verifikasi digital sangatlah penting dan harus ada perlindungan yang maksimal untuk menjaga keamanan identitas digital pengguna. Kebutuhan akan sistem keamanan yang tangguh merupakan salah satu faktor penting kenapa teknologi biometrika terus dikembangkan.[6] Keamanan dalam perlindungan data pribadi dalam teknologi digital juga sangat di perlukan agar terhindar dari perbuatan melawan hukum seperti penyalahgunaan data pribadi seseorang.

METODE PENELITIAN

Pendekatan digunakan dalam penelitian ini adalah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah pendekatan melalui studi kepustakaan (*library research*). Studi pustaka dilakukan dengan beberapa metode yaitu dengan mencari referensi terhadap semua hal yang bersifat teoritis dengan mencari dan mempelajari referensi buku, *e-book*, artikel-artikel baik nasional maupun internasional, jurnal dan karya ilmiah, asas-asas hukum dalam teori/pendapat sarjana dan peraturan perundang-undangan yang berlaku. Sehingga membuat teori-teori yang telah digunakan dapat saling berkaitan dan menjadi sebuah kerangka konsepsional yang konkret.

HASIL DAN PEMBAHASAN

Perlindungan Hukum terhadap Para Pengguna Teknologi Identitas Digital melalui Sistem Verifikasi Identitas Berbasis Biometrik

Teknologi informasi berkembang sangat pesat dan dampaknya telah kita rasakan. Berbagai kemudahan yang kita terima, seperti kemudahan untuk memperoleh informasi melalui telepon seluler maupun internet, kemudahan dalam bertransaksi dengan menggunakan kartu kredit atau kartu debit, dan kemudahan untuk mengambil uang melalui ATM. Peran yang dapat diberikan oleh aplikasi teknologi

identification-a-key-to-inclusive-growth diakses pada tanggal 27 Agustus 2022.

[6] Darma Putra, Adi Resmawan. 2011. *Verifikasi Biometrika Suara Menggunakan Metode MFCC dan DTW*. Lontar Komputer, Bali, hlm. 9.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

informasi ini adalah mendaptkan informasi kehidupan pribadi seperti informasi tentang kesehatan, hobi, rekreasi, dan rohani. Perkembangan teknologi informasi memacu suatu cara baru dalam kehidupan, dari kehidupan dimulai sampai dengan berakhir, kehidupan seperti itu dikenal dengan *e-life* yang artinya kehidupan ini sudah dipengaruhi oleh berbagai kebutuhan secara elektronik. Teknologi informasi, meliputi segala hal yang berkaitan dengan proses, penggunaan sebagai alat bantu, manipulasi dan pengelolaan informasi.[7]

Teknologi informasi yaitu ilmu yang mencakup teknologi komunikasi untuk memproses, menyimpan data dan mengirimkan informasi melalui jalur komunikasi yang cepat.[8] Menurut Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elekronik (ITE), Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi. Teknologi informasi memiliki manfaat untuk sumber informasi dan untuk mencari informasi yang akan dibutuhkan, teknologi informasi sebagai media, sebagai alat bantu yang memfasilitasi penyampaian suatu informasi agar dapat diterima dan dimengerti dengan mudah, teknologi informasi sebagai pengembang keterampilan pembelajaran, pengembangan keterampilan-keterampilan berbasis teknologi informasi dengan aplikasi-aplikasi dalam kurikulum. Dari beberapa manfaat teknologi informasi yang telah disebutkan, pengembangan keterampilan berbasis teknologi informasi saat ini, perkembangannya sangat berpengaruh dalam kehidupan manusia, terutama untuk kepentingan penyimpanan data seseorang di berbagai perangkat.

Perlindungan privasi atas informasi pribadi berkembang disebabkan oleh penggunaan internet dan banyaknya transaksi melalui perdagangan elektronik *(e-commerce)* yang mengakibatkan banyaknya informasi pribadu dapat di proses, diprofilkan, dan kemudian disebarkan kepada pihak lain guna kepenetingan transaksi elektronik sebagaimana yang telah disepakati oleh para pihak.[9] Pengumpulan dan pengolahan data rentan menimbulkan intervensi terhadap privasi. Data pribadi seseorang mudah terpapar dan dipindahtangankan secara semena-mena tanpa kontrol dari pemilik data. Terlebih dimungkinkannya aliran data *(data flow)* yang melibatkan lebih dari satu yuridiksi menjadi perhatian, terutama dalam perspektif keamanan nasional. Dengan mempertimbangkan globalisasi dan perkembangan teknologi yang cepat, pengaturan di level nasional saja tidak cukup, namun juga memerlukan pengaturan di level nasional.

Perlindungan data sendiri secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya.[10] Pemilik data juga harus dapat mengambil

[7] Aziz, A. 2012. *Pemanfaatan Teknologi Informasi dalam Pengembangan Bisnis Pos*. Buletin Pos dan Telekomunikasi, 10(1), pp.35-50.
[8] Tri Rachmadi. 2020. *Teknologi Informasi*. TIGA Ebook, Padang, hlm. 1.
[9] Nitayanti, N.G.A.P. and Griadhi, N.M.A.Y. 2014. *Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Kertha Negara: Journal Ilmu Hukum, 2*(5), pp.1-6.
[10] Djafar, W. 2019. *Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. Makalah disampaikan sebagai materi dalam kuliah umum "Tantangan Hukum dalam Era*

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

keputusan dengan tepat, apakah ingin membagikan beberapa informasi atau tidak, siapa yang bisa memiliki akses, jangka waktu, untuk alasan apa, dan dapat memodifikasi beberapa informasi ini atau tidak. Perlindungan hukum terhadap teknologi informasi di atur dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) pada Pasal 26 Ayat (1) : "Kecuali ditentukan lain oleh peraturan perundang-undangan, pengguna setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan." Lalu dilanjutkan Ayat (2) : "Setiap Orang yang dilanggar haknya sebagaimana dimaksud [ada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini."

Saat ini Indonesia sedang menuju akselerasi digital. Menurut ketua umum Asosiasi Penyedia Jasa Internet Indonesia (APJII) Muhammad Arif, pertumbuhan pengguna internet di Indonesia sebelum pandemi penggunanya hanya 175 juta, tapi saat ini data terbarunya sekitar 220 juta.[11] Banyaknya perpindahan aktivitas manusia ke dunia maya tentu harus diimbangi dengan teknologi serta regulasi untuk melindungi masyarakat, seperti melindungi dari ancaman kejahatan siber yang semakin banyak terjadi. Kejahatan siber yang paling sering terjadi adalah pencurian data pribadi, penyalahgunaan data, sampai memalsukan dokumen yang banyak menimbulkan kerugian. Karena hal tersebut sangat penting literasi digital untuk masyarakat awam, serta peran identitas digital di dalamnya.

Identitas digital memuat segala informasi online yang tersedia di ruang digital dan terikat kepada seorang individu, organisasi, maupun perangkat elektronik. Informasi yang di maksud, mulai dari informasi pribadi seperti tanggal lahir, nomor paspor, riwayat medis, dan lain-lain. Selain itu juga identitas digital juga dapat mencakup rekam jejak aktivitas digital melalui postingan-postingan di media sosial. Seluruh catatan online ini baik secara sendiri-sendiri maupun kumulatif membentuk suatu identitas digital. Penjelasan lebih singkatnya, Identitas digital berfungsi sebagai pembeda antara satu individu atau organisasi ketika beraktivitas di ruang digital.

Kehadiran identitas digital bagi penggunanya akan memberikan kemudahan ketika akan melakukan aktivitas di ruang digital yang membutuhkan pendaftaran. Dengan adanya identitas digital, pengguna tak perlu repot untuk mengisi data pribadi, cukup memasukkan identitas digital untuk kemudian diverifikasi. Sedangkan untuk penyedia layanan, kehadiran identitas digital yang terintegrasi akan memudahkan pemberian layanan.

Kehadiran identitas digital tak hanya selalu memberi manfaat, namun juga bayangan peretasan. Semua aktivitas yang ada di ruang digital sangat berpotensi untuk mengalami serangan siber tanpa terkecuali, sehingga pemerintah atau otoritas terkait perlu memperhatikan sisi keamanan ketika identitas digital ini nantinya sudah diterapkan secara luas di masyarakat.

Seiring perkembangan teknologi, sistem verifikasi identitas digital juga selalu di perbaharui manfaatnya agar dapat memudahkan kegiatan manusia. Identitas digital adalah sebuah representasi identitas seseorang dalam

---

Analisis Big Data". Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada.

[11] Asti. 2022. *Memahami Esensi Identitas Digital Dalam Ekosistem Teknologi di Indonesia*. *https://dailysocial.id/post/memahami-esensi-identitas-digital-dalam-ekosistem-teknologi-di-indonesia.* Diakses pada tanggal 23 Desember 2022.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

suatu jaringan sistem informasi dan teknologi digital. Melalui sistem verifikasi identitas biometrik para pengguna jauh lebih mudah untuk mengakses sesuatu. Keterlibatan identitas digital di dalam kehidupan sehari-hari akan menimbulkan sebuah kebiasaan baru pada masyarakat.

Biometrik berarti mengukur karakteristik pembeda *(distinguishing traits)* pada badan atau perilaku seseorang yang digunakan untuk melakukan pengenalan secara otomatis terhadap identitas orang tersebut.[12] Identitas biometrik termasuk identitas seseorang yang dimaksudkan sebagai data pribadi. Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Salah satu Hak Asasi Manusia (HAM) adalah berupa bentuk perlindungan data pribadi, karena hal tersebut termasuk bagian dari perlindungan diri pribadi.

Teknologi identitas biometrik adalah sistem yang menggunakan bagian tubuh manusia untuk kepastian pengenalan.[13] Teknologi identitas biometrik yang paling sering digunakan biasanya rekam sidik jari dan pengenalan wajah. Untuk identitas biometrik lainnya seperti rekaman suara, iris, ataupun retina masih jarang atau bahkan belum pernah digunakan untuk verifikasi identitas biometrik. Di Indonesia, verifikasi biometrik sudah lama digunakan dan dikembangkan. Verifikasi biometrik bekerja dengan cara mencocokan pengguna dengan data-data biometrik yang ada pada Kartu Tanda Penduduk (KTP). Biasanya, sistem akan mengecek atau sinkronisasi ke database DUKCAPIL. Sehingga, verifikasi ini sangat akurat dan sulit untuk dipalsukan.

Sistem verifikasi identitas biometrik bisa mengenali seseorang dengan tepat, akurat dan konsisten. Sehingga bisa mengurangi kesalahan dalam mengenali seseorang hanya sebab memiliki kemiripan ataupun pemalsuan. Prosesnya yang bisa terjadi secara masif membuat sistem verifikasi ciri-ciri biometrik sangat efisien. Efisiensi biaya juga dapat terjadi karena tidak lagi membutuhkan proses yang panjang dan melibatkan banyak pihak. Kemudahan akses menggunakan pembuktian identitas biometrik bisa terjadi karena seseorang tidak perlu buat membawa-bawa indera verifikasi berbentuk kartu ataupun perangkat lainnya. Hanya menggunakan data biometrik yang melekat pada tubuh, maka verifikasi identitas bisa dilakukan.

Kata sandi ataupun angka identifikasi eksklusif (PIN) merupakan sistem pembuktian identitas yang sangat mudah terlupakan, sebagai akibatnya pengguna perlu menuliskannya disuatu tempat seperti menuliskannya di kertas atau mengetiknya di aplikasi catatan yang ada di smartphone-nya. Tetapi hal tersebut justru meningkatkan risiko pencurian akses.

Pada era digital saat ini, data pribadi seseorang yang sengaja diunggah oleh sang pemilik data maupun yang disalahgunakan oknum yang sangat tidak bertanggung jawab dapat ditemukan dengan mudah di dunia maya. Karena hal tersebut, negara juga wajib untuk melindungi data pribadi warga negaranya. Pada tanggal 20 September 2022, dalam Rapat Paripurna DPR RI Masa Persidangan I Tahun Sidang 2022-2023, Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi (PDP) telah resmi disahkan menjadi Undang-Undang (UU). Pada tanggal 17 Oktober

[12] Putra, D. 2009. *Sistem Biometrika: Konsep Dasar, Teknik Analisis Citra, dan Tahapan Membangun Aplikasi Sistem Biometrika.* Andi Offset, Yogyakarta, hlm. 34.

[13] Fatoni, F. 2022. *Teknik Presensi Karyawan Berbasis Biometrik Menggunakan Sensor Sidik Jari.* Universitas Bina Darma, Palembang, hlm. 2.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

2022, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah disahkan dan ditandatangani oleh Presiden Joko Widodo. Undang-Undang Perlindungan Data Pribadi dibuat dan disahkan untuk dapat melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik ataupun mencegah penyalahgunaan dari oknum yang tidak bertanggung jawab.

Pengertian Data Pribadi dijelaskan di dalam Pasal 1 Angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam pasal tersebut data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Pada Pasal 4 Ayat (1) yang berbunyi "Data Pribadi terdiri atas : a. Data Pribadi yang bersifat spesifik; dan b. Data Pribadi yang bersifat umum." Pada Ayat (2) pada Pasal 4 tersebut, data biometrik disebutkan sebagai salah satu data pribadi yang bersifat spesifik. Data biometrik yang dimaksudkan merupakan data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku seseorang yang memungkinkan identifikasi unik. Identifikasi yang dimaksud adalah wajah atau sidik jari.

Dalam Undang-Undang Perlindungan Data Pribadi disebutkan juga ketentuan pidana bagi para setiap orang yang sengaja menyalahgunakan data pribadi milik orang lain. Pada Pasal 67 Ayat (2) yang menjelaskan bagi setiap orang yang dengan sengaja membocorkan data pribadi milik orang lain akan dipidana penjara paling lama 4 (empat) tahun dan/atau dipidana denda paling banyak empat miliar rupiah. Kemudian ayat 3 dari pasal tersebut yang menjelaskan seseorang yang dengan sengaja dan melawan hukum menggunakan data pribadi milik orang lain akan mendapatkan sanksi pidana paling lama 5 (lima) tahun penjara dan/atau pidana denda paling banyak lima miliar rupiah.

Konstitusi Indonesia juga tidak secara terus terang mengatur mengenai perlindungan data didalam Undang-Undang Dasar Republik Indonesia 1945. Dalam Undang-Undang Dasar Republik Indonesia 1945 ketentuan mengenai data dapat ditemukan dalam pasal 28 F Undang-Undang Dasar Republik Indonesia 1945 yang berbunyi :
"Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan infromasi dengan menggunakan segala jenis saluran yang tersedia".

Pasal 28 G ayat 1 Undang-Undang Dasar RI 1945 berbunyi: ""Setiap orang berhak atas perlindungan data pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman kekuatan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Perlindungan hukum terhadap para pengguna teknologi identitas digital melalui sistem verifikasi identitas berbasis biometrik yang mana identitas biometrik termasuk data pribadi yang harus dijaga keamanannya dalam penggunaannya di berbagai bidang teknologi dan juga di berbagai kebutuhan. Saat ini Indonesia sudah mempunyai peraturan yang berlaku dimana identitas biometrik menjadi salah satu data pribadi yang bersifat spesifik di dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Sebelumnya identitas biometrik belum mempunyai

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

perlindungan hukum yang khusus ataupun jelas. Identitas biometrik sendiri saat itu masih termasuk data pribadi yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE).

Sistem Keamanan Data yang Diberikan oleh Para Pengguna Teknologi Identitas Digital melalui Sistem Verifikasi Identitas Berbasis Biometrik

Dalam era digital saat ini, komunikasi melalui jaringan sosial memegang peranan penting. Karna saat ini banyak kegiatan yang dilakukan melalui internet atau dalam jaring (daring). Melalui komunikasi elektronik, seseorang dapat melakukan transaksi atau berkomunikasi dengan praktis dan juga sangat cepat. Hal tersebut merupakan pengaruh dari perkembangan yang sangat signifikan dalam teknologi informasi, dimana jumlah kapasitas maksimum dari suatu kegiatan komunikasi antara server dan client di internet semakin besar dan dengan biaya akses yang semakin murah. Risikonya adalah keamanan informasi semakin meningkat.

Sistem keamanan data adalah praktik melindungi informasi digital dari akses tidak sah, korupsi, atau pencurian di seluruh siklus hidupnya.[14] Keamanan dan kerahasiaan data menjadi sangat penting saat data memiliki nilai. Sebagai contoh data pribadi kita sebagai warga negara perlu dilindungi karena data tersebut bisa digunakan oleh orang yang tidak berhak dan tidak bertanggung jawab untuk berbuat kejahatan, akibatnya pemilik data yang harus bertanggung jawab. Keamanan data ini juga meliputi 4 aspek utama dalam keamanan data dan informasi, diantaranya adalah: (1) *Privacy/Confidentiality* yaitu usaha menjaga data informasi yang bersifat pribadi dari orang yang tidak berhak mengakses. (2) *Integrity* yaitu usaha untuk menjaga data informasi tidak diubah oleh yang tidak berhak. (3) *Authentication* yaitu usaha atau metode untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar atau layanan dari server yang diberikan benar berasal dari server yang dimaksud. (4) *Availability* berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Teknologi di abad kedua puluh satu telah mengubah dunia dengan berbagai cara, menarik dan tidak terduga. Memfasilitasi arus informasi, modal, dan layanan yang cepat di seluruh dunia, hal tersebut yang secara dramatis merevolusi cara kita bekerja, berkomunikasi, dan berinteraksi satu sama lain. Perjalanan yang lebih terjangkau, perangkat komunikasi seluler, media sosial, dan konektivitas online telah memungkinkan pola gerakan dan bentuk partisipasi sosial baru. Di dunia yang terhubung secara digital ini, orang-orang bergerak dengan lancar melintasi ruang online dan offline, mengaburkan batas ruang dan waktu dan mengubah gagasan tentang domain publik dan pribadi.[15] Konsep ruang telah menjadi lebih tertanam dalam imajinasi orang, yang mengarah pada identifikasi, kesetiaan, dan hubungan baru.[16] Ketika teknologi terus menembus semua aspek kehidupan manusia dan mengubah tatanan sosial, teknologi telah berdampak

[14] Ahmad Ashifuddin Aqham. 2022. *Pentingnya Keamanan Data/Data Security Di Era 4.0*. http://komputerisasi-akuntansi-d4.stekom.ac.id/informasi/baca/Pentingnya-Keamanan-Data-Data-Security-di-era-4.0/5dd42b08460dae46456ca6e3cf9db621b59e67b6. Diakses pada tanggal 27 Desember 2022.

[15] Gee,J.P. dan Hayes, E.R. (2011). *Language and learning in the digital age*. Routledge. Abingdon, hlm. 523.

[16] Warriner, D.S. 2007. *Transnational Literacies : Immigration, Language Learning and Identity.* Linguistics and Education. United States, hlm. 523.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

pada bahasa dan identitas secara signifikan. ‘

Identitas digital diciptakan untuk pengguna internet di masyarakat digital. Kunci yang membuka portal situs web ada dua bentuk, yang pertama adalah nama asli yang menunjukkan kepribadian asli kita yang kita tangani di lapangan, dan yang kedua didasarkan pada nama palsu (pinjaman) yang tidak mempengaruhi kenyataan, dan formulir ini lebih disukai oleh mayoritas pengguna situs web melalui internet untuk tetap anonim.[17]

Identitas digital adalah jumlah dari semua informasi yang tersedia secara digital tentang seorang individu.[18] Identitas di era modern semakin bergantung pada internet, terutama yang berkaitan dengan informasi, forum, situs jejaring sosial, game, dan aplikasi yang disediakan. Hal ini telah mengakibatkan meningkatnya permintaan akan hak privasi yang melindungi penciptaan identitas digital tanpa kesulitan dan permasalahan, terutama dengan meningkatnya jumlah orang yang membentuk identitas mereka di internet dan hal ini akan lebih baik melindungi perkembangan identitas digital yang independen dan tidak terpengaruh di jejaring sosial, mengakui identitas digital sebagai aset terpisah dan mengalokasikan hak privasi para penggunanya secara digital memberikan kesempatan untuk mengatur ruang siber dengan cara yang inovatif.

Dengan meningkatnya interaksi individu dengan dunia digitalisasi, privasi pengguna menjadi terancam dan data pribadi pengguna telah menjadi sebuah materi yang digunakan secara komersial untuk melakukan iklan pemasaran, atau pemantauan lembaga pemerintah, atau mengekspos ke pencurian dan menggunakannya untuk satu tujuan yang berbahaya bagi pemilik data tersebut. Karena menjaga privasi di dunia digital adalah masalah yang sering kali terjadi di era yang serba digital saat ini, menangani pelanggaran yang memengaruhinya oleh pemerintah atau pihak lain membutuhkan banyak arahan dan waktu tentang cara melindunginya melalui pembaruan kerangka hukum yang relevan.

Dalam sistem informasi saat ini, pengguna memiliki beragam senyawa *login-name* dan *password* untuk setiap *online service* atau bahkan kredensial yang berbeda untuk peran yang berbeda di dalamnya layanan yang tersedia untuk mereka. Hal ini dapat mengakibatkan risiko privasi bagi pengguna akhir dan membahayakan penyedia layanan ancaman keamanan. Di era *big data* yang terjadi saat, keamanan data menjadi sebuah hal yang sangat diperhatikan oleh semua individu. Setiap harinya orang-orang akan menyimpan aset dan melakukan transaksi yang terhubung dengan data pribadi mereka sebagaimana. Verifikasi identitas biometrik merupakan sebuah sistem yang dapat mempermudah berbagai keperluan manusia di berbagai tempat. Mulai dari verifikasi transaksi yang dapat digunakan melalui aplikasi di *smartphone,* akses komputer pribadi, akses membuka ruang penyimpanan, akses untuk transaksi melalui mesin ATM, dan juga dapat digunakan untuk kepentingan akses layanan kependudukan atau akses layanan lainnya yang disediakan oleh pemerintah. Penggunaan verifikasi identitas biometrik terbilang *simple* atau mudah. Para penggunanya hanya di minta untuk melakukan *scan* pada karakteristik anatomi yang di minta, seperti sidik jari

[17] Majeed, Majeed & Adisaputera, Abdurahman & Ridwan, Muhammad. 2020. *Digital Identity*. Konfrontasi: Jurnal Kultural, Ekonomi dan Perubahan Sosial. 7. 246-252. 10.33258/konfrontasi2.v7i4.122.

[18] Deborah Gonzales. 2015. *In Managing Online Risk : Apps Mobile, and Social Media Security.* Elsevier. United Kingdom, hlm. 56.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

(finger print), wajah *(face)*, selaput pelangi *(iris)*, retina mata, suara *(voice)*, geometri tangan *(hand geometry)*. Karena hal tersebut sistem verifikasi identitas melalui verifikasi biometrik dinilai jauh lebih aman, cepat dan praktis, di karenakan sistem verifikasi membutuhkan data pengenalan biometrik seseorang yang bersangkutan untuk dapat terverifikasi. Verifikasi identitas berbasis biometrik juga sangat sulit untuk di manipulasi karena ciri-ciri biometrik sangat berhubungan erat dan relatif permanen antara pengguna dan identitasnya.

Sistem verifikasi identitas biometrik berbeda dari sistem verifikasi identitas tradisional, seperti kata sandi dan sistem berbasis pengetahuan, karena mereka menggunakan karakteristik biologis unik seseorang untuk memverifikasi identitas mereka.[19] Tidak seperti sistem verifikasi identitas tradisional, yang sering dapat dibodohi oleh penipu, verifikasi biometrik bersifat tunggal bagi individu dan oleh karena itu jauh lebih efektif dalam mengkonfirmasi identitas mereka.

Dalam sistem biometrik, identifikasi pengguna dilakukan berdasarkan karakter fisik dan perilakunya.

Proses identifikasi tersebut terdiri dari dua tahap utama yaitu: (1) Tahap Pendaftaran; Dalam tahap ini, informasi biometrik dari seseorang akan disimpan dalam database bersama dengan identitas pendaftar. Data yang telah diperoleh tersebut selanjutnya diproses untuk mengekstrak fitur yang menonjol dan khas. (2) Tahap Pengenalan; Dalam tahap ini, data biometrik diambil kembali dari pendaftar lalu dibandingkan dengan data yang telah disimpan untuk menentukan identitas dari pendaftar. Sistem biometrik pada dasarnya merupakan pengenalan atau pencocokan pola yang terdiri dari 4 bagian, yaitu sensor, fitur ekstraktor, database, dan pencocokan biometrik.

Identitas digital berbasis biometrik hanya bisa diakses oleh pengguna yang bersangkutan atau si pemilik data. Akses pada data juga dapat diatur sehingga privasi para penggunanya akan sangat terjaga dengan aman. Sistem keamanan data pengguna, disimpan pada sistem yang aman dan di lindungi. Hanya pemilik data yang dapat mengetahui bagaimana dan kapan data tersebut digunakan termasuk pula dengan segala perubahan yang dilakukan pada sistem tersebut. Di India dan Eropa, identitas digital berbasis biometrik sudah berlaku dan berhasil mengurangi penyalahgunaan dan penipuan data pribadi. Sedangkan Indonesia sedang dalam proses untuk menggunakan teknologi tersebut. Identitas biometrik dikatakan sangat efektif untuk mencegah penipuan, karena setiap individu atau setiap orang hanya dapat menggunakan satu identitas untuk segala kegunaannya.

Setiap sistem keamanan teknologi pasti memiliki kelebihan dan kekurangannya. Sama halnya dengan sistem verifikasi identitas berbasis biometrik ini, sistem verifikasi identitas memiliki kelebihan yaitu: (1) Verifikasi Identitas Masif; Teknologi biometrik mampu melakukan banyak verifikasi identitas dalam waktu yang singkat. Karena hal tersebut sistem verifikasi ini sudah diterapkan di berbagai hal, seperti pemerintahan, perbankan, finansial, dan kegiatan lain yang memerlukan keamanan tinggi. (2) Akurasi Tinggi; Sistem ini mampu mengenali individu dengan akurat, tepat, dan konsisten. Kesalahan identitas karena mirip atau pemalsuan jadi bisa berkurang

[19] Jay Raol. 2022. *How Biometric Authentication Can Be The Ultimate Identity Verification Solution?. https://www.idmerit.com/blog/how-biometric-authentication-can-be-the-ultimate-identity-verification-solution/*

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

kejadiannya. (3) Hemat Biaya; Karena sistem ini bisa melakukan banyak verifikasi sekaligus dengan otomatis, jadi tidak perlu lagi melakukan verifikasi manual yang membutuhkan banyak tenaga manusia dan proses yang berbelit-belit. (4) Kemudahan Akses; Verifikasi identitas berbasis biometrik menggunakan data yang melekat pada tubuh manusia, sehingga tidak perlu lagi untuk membawa alat verifikasi lain seperti kartu atau perangkat lainnya. (5) Sulit Dipalsukan; Seperti yang sudah disebutkan, verifikasi identitas berbasis biometrik memakai data yang melekat pada tubuh manusia. Hal ini tentu saja sangat sulit untuk dipalsukan dan aman dari kebocoran data karena setiap manusia itu unik. Berbeda dengan verifikasi melalui PIN, password, dan sejenisnya.

Secanggih apapun suatu sistem keamanan teknologi, pasti tetap akan memiliki kekurangan, di antaranya: (1) Isu Privasi Identitas; Sistem verifikasi identitas berbasis biometrik melakukan verifikasilangsung pada tubuh manusia, sehingga privasi otomatis langsung terbongkar. Berbeda dengan sistem verifikasi lain yang bisa dilakukan secara anonim, seperti hanyan perlu memasukkan password, pin, dan sejenisnya tanpa harus menampilkan diri. (2) Keamanan Penyimpanan Data; Sistem verifikasi identitas berbasis biometrik memang aman, tetapi tempat penyimpanan data tersebut masih rentan terkena cyber crime. Maka dari itu, penting bagi penyedia layanan yang menggunakan teknologi tersebut untuk menggunakan sistem keamanan berlapis yang tentu saja membutuhkan biaya untuk mengimplementasikannya.

Sistem keamanan data yang diberikan oleh para pengguna teknologi identitas digital melalui sistem verifikasi identitas berbasis biometrik adalah data pengguna yang disimpan pada sistem yang aman dan dilindungi. Identitas biometrik saat ini sangat jarang terjadi dalam penyalahgunaan atau pemalsuan data. Data biometrik yang sudah tersimpan dalam sistem tersebut hanya bisa terverifikasi jika si pemilik data ingin menggunakan atau merubah sistem tersebut. Identitas biometrik yang sudah terdaftar hanya bisa digunakan oleh pemilik data sesungguhnya.

PENUTUP

Perlindungan hukum terhadap para pengguna teknologi identitas digital melalui sistem verifikasi identitas berbasis biometrik dibuat untuk melindungi privasi atas informasi pribadi yang berkembang disebabkan oleh penggunaan internet dan banyaknya transaksi melalui perdagangan elektronik (e-commerce) yang mengakibatkan banyaknya informasi pribadu dapat di proses, diprofilkan, dan kemudian disebarkan kepada pihak lain guna kepentingan transaksi elektronik sebagaimana yang telah disepakati oleh para pihak. Perlindungan data sendiri secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Pada era digital saat ini, data pribadi seseorang yang sengaja diunggah oleh sang pemilik data maupun yang disalahgunakan oknum yang sangat tidak bertanggung jawab dapat ditemukan dengan mudah di dunia maya. Undang-Undang Perlindungan Data Pribadi dibuat dan disahkan untuk dapat melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik ataupun mencegah penyalahgunaan dari oknum yang tidak bertanggung jawab. Pada Pasal 4 Ayat 2 Undang-Undang No.27

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

Tahun 2022 tentang Perlindungan Data Pribadi data biometrik menjadi salah satu data pribadi seseorang yang dilindungi kerahasiaannya oleh Undang-Undang.

Sistem keamanan data yang diberikan oleh para pengguna teknologi identitas digital melalui sistem verifikasi identitas berbasis biometrik adalah data pengguna yang disimpan pada sistem yang aman dan dilindungi karena sistem yang digunakan untuk verifikasi ini hanya dapat terverifikasi oleh individu yang memiliki identitas tersebut. Identitas biometrik bersifat unik, karena setiap individu memiliki keunikan biometriknya sendiri. Verifikasi identitas melalui identitas biometrik adalah bentuk sebuah ide teknologi yang sangat efeketif karna identitas biometrik dapat mencegah dan mengurangi kasus penyalahgunaan atau pemalsuan data yang sering terjadi. Data biometrik yang sudah tersimpan dalam sistem tersebut hanya bisa terverifikasi jika si pemilik data ingin menggunakan atau merubah sistem tersebut. Identitas biometrik yang sudah terdaftar hanya bisa digunakan oleh pemilik data sesungguhnya. Tetapi, secanggih apapun sebuah teknologi pasti memiliki manfaat dan kelemahannya. Maka dari itu untuk meminimalisir hal-hal yang tidak diinginkan terjadi, setiap penyelenggara atau pembuat sebuah sistem teknologi harus bisa membuat perlindungan extra terutama teknologi verifikasi identitas.

DAFTAR PUSTAKA

Undang-Undang Dasar Republik Indonesia 1945.

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

Ahmad, A. A. 2022. Pentingnya Keamanan Data/Data Security Di Era 4.0. http://komputerisasi-akuntansi-d4.stekom.ac.id/informasi/baca/Pentingnya-Keamanan-Data-Data-Security-di-era-4.0/5dd42b08460dae46456ca6e3cf9db621b59e67b6,diakses:27 Desember 2022.

Asti. 2022. Memahami Esensi Identitas Digital Dalam Ekosistem Teknologi di Indonesia. https://dailysocial.id/post/memahami-esensi-identitas-digital-dalam-ekosistem-teknologi-di-indonesia, diakses: 23 Desember 2022.

Aziz, A. 2012. Pemanfaatan Teknologi dalam Pengembangan Bisnis Pos. *Buletin Pos dan Komunikasi*, 10(1), pp.35-50.

Darma, P., Adi, R. 2011. *Verifikasi Biometrika Suara Menggunakan Metode MFCC dan DTW*. Lontar Komputer, Bali.

Deborah, G. 2015. *In Managing Online Risk : Apps Mobile, and Social Media Security*. Elsevier. United Kingdom.

Dian, H. 2022, Apa Itu Identitas Digital dan Manfaattnya bagi Perkembangan Bisnis, https://id.techinasia.com/apa-itu-identitas-digital-dan-manfaatnya, diakses: 27 Agustus 2022.

DUKCAPIL KEMENDAGRI, 2022, Yuk, Kenali Identitas Kependudukan Digital, https://dukcapil.kemendagri.go.id/berita/baca/1327/yuk-kenali-identitas-kependudukan-digital diakses: 27 Agustus 2022.

Fatoni, F. 2022. *Teknik Presensi Karyawan Berbasis Biometrik Menggunakan Sensor Sidik Jari*. Universitas Bina Darma, Palembang.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**

Gee, J. P. dan Hayes, E. R. (2011). *Language and learning in the digital age*. Routledge. Abingdon.

Harun, M. 2018. *Kriptografi Untuk Keamanan Data*. Deepublish, Yogyakarta.

Jay, R. 2022. *How Biometric Authentication Can Be The Ultimate Identity Verification Solution?*. https://www.idmerit.com/blog/how-biometric-authentication-can-be-the-ultimate-identity-verification-solution/.

Larry A. Samovar, Richard E. Porter, Edwin R. McDaniel. (2010). *Communication Between*

Cultures. Wadsworth and Cengage Learning, Boston.

Majeed, Majeed & Adisaputera, Abdurahman & Ridwan, Muhammad. 2020. Digital Identity. *Konfrontasi: Jurnal Kultural, Ekonomi dan Perubahan Sosial*. 7. 246-252. 10.33258/konfrontasi2.v7i4.122.

McKisney Global Institute, 2019, *Digital* Identification, https://www.mckinsey.com/business functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth diakses: 27 Agustus 2022.

Nitayanti, N.G.A.P. and Griadhi, N.M.A.Y. 2014. Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Kertha Negara: Journal Ilmu Hukum*, 2(5), pp.1-6.

Putra, D. 2009. *Sistem Biometrika: Konsep Dasar, Teknik Analisis Citra, dan Tahapan Membangun Aplikasi Sistem Biometrika.* Andu Offset, Yogyakarta.

Tri, R. 2020. *Teknologi Informasi.* TIGA Ebook, Padang.

Verihubs, 2022, Sistem Biometrik adalah Upaya Verifikasi Digital yang Aman, https://verihubs.com/blog/biometrik-adalah/ di akses: 27 Agustus 2022.

Warriner, D.S. 2007. *Transnational Literacies: Immigration, Language Learning and Identity.* Linguistics and Education. United States.

p-ISSN **1412 – 517X**
e-ISSN **2720 – 9369**