TRANSFORMASI SISTEM KEAMANAN DATA MELALUI BIOMETRIK DI INDONESIA PERSPEKTIF TEKNOLOGI HUKUM

ANJAR SETIARMA[1], ELFRIDA RATNAWATI GULTOM[2]
Magister Ilmu Hukum, Universitas Trisakti
Anjarsetiarma@outlook.com[1], Elfrida.r@trisakti.ac.id[2]

Abstract: *Technological advances have driven the growth of e-commerce in Indonesia, which has had an impact on the development of data security systems in the e-commerce sector, such as biometric technology which is the most practical mechanism for identifying and authenticating human individuals in a reliable and fast way through the unique characteristics of each individuals and has been used in many applications to identify humans using fingerprints, faces, iris patterns, facsimile signatures, facsimile signatures, fac Cases of crimes against personal data are still rife in Indonesia, indicating weaknesses in the country's data security framework. The study methodology employed is normative legal research utilizing secondary data, followed by an analytical approach and a deductive approach to legislation. The results of this study indicate that by type of biometric data can be divided into three types namely physical, physical, and behavioral. Legal technology that can be utilized in data security systems such as online dispute resolution features, board governance, cybersecurity, and data privacy compliance. In establishing the legal system, it is hoped that the government will not only focus on legal substance and legal structure, the government must elaborate on the legal culture by utilizing national biometric technology and legal technology in the data security system, thus the effectiveness and standardization of national personal data protection can be realized immediately.*
Keywords: *biometric, legal technology, and Indonesia.*

Abstrak: Kemajuan teknologi telah mendorong pertumbuhan *e-commerce* di Indonesia, yang berdampak pada perkembangan sistem keamanan data di sektor *e-commerce*, seperti teknologi biometrik yang merupakan mekanisme paling praktis untuk mengidentifikasi dan mengotentikasi individu manusia di cara yang handal dan cepat melalui karakteristik yang unik pada setiap individu dan telah digunakan dalam banyak aplikasi untuk mengidentifikasi manusia menggunakan sidik jari, wajah, pola iris, tanda tangan faksimili, tanda tangan faksimili, tanda tangan faksimili, fac Kasus kejahatan terhadap data pribadi masih marak di Indonesia, menunjukkan kelemahan dalam kerangka keamanan data negara. Metodologi kajian yang digunakan adalah penelitian hukum normatif dengan memanfaatkan data sekunder, dilanjutkan dengan pendekatan analitis dan pendekatan deduktif peraturan perundang-undangan. Penelitian ini menghasilakan bahwa secara jenis data biometrik dapat dibagi menjadi tiga jenis yakni *physical, physiological,* dan *behavioural.* Teknologi hukum yang dapat dimanfaatkan dalam sistem keamanan data seperti fitur *online dispute resolution, board governance, cybersecurity, dan data privacy compliance.* Dalam pembentukan sistem hukum, pemerintah diharapkan tidak hanya fokus pada substansi hukum dan struktur hukum, pemerintah harus mengelaborasi budaya hukum dengan cara memanfaatkan teknologi biometrik dan teknologi hukum dalam sistem keamanan data nasional, dengan demikian efektivitas dan standarisasi perlindungan data pribadi nasional dapat segera terwujud.
Kata Kunci: biometrik, teknologi hukum, dan Indonesia.

A. Pendahuluan

Kemajuan pada bidang teknologi telah memiliki implikasi terhadap kemajuan dalam sistem perdagangan di Indonesia, salah satu dampaknya ialah lahirnya sistem perdagangan melalui internet atau disebut *e-commerce* (Eka Nadia Septiani Ady, et.al. 2022:45). Masifnya penggunaan internet telah menimbulkan potensi kejahatan terhadap data pribadi (Muhamad Hasan Rumulus dan Hanif Hartadi. 2020:290). Bahaya terhadap kebocoran data pribadi juga semakin nyata bagi masyarakat dengan berkembanganya

jual beli melalui *e-commerce* di Indonesia, para pelaku usaha di bidang *e-commerce* telah mengumpulkan data pribadi konsumen secara masif, termasuk data perilaku belanja atau aktivitas para konsumen. Data pribadi yangdikumpulkan oleh pelaku usaha seperti nama, nomor induk kependudukan, alamat, sebagian atau data biometrik seperti potongan data dari anggota tubuh (data biometrik) (Wahyudi Djafar. 2019:14). Kejahatan terhadap data pribadi umumnya akan terkait dengan pencurian yang mengakibatkan kerugian secara materi bagi penggunanya. Dalam hal ini, cukup banyak kasus yang terjadi, contohnya pencurian data pribadi yang dialami oleh *platform* Tokopedia, data pengguna Tokopedia yang dijual dalam situs Raid Forums dengan harga 5.000 USD (lima ribu dolar Amerika Serikat)(Edy Santoso dan Sukendar. 2020).

Berdasarkan fakta dalam penerapan hukum, sebagaimana adagium hukum "*het recht hinjt achterde faiten aan*", maksudnya ialah hukum selalu tertinggal dari sebuah peristiwa yang akan diatur atau dalam hal ini berarti hukum tertinggal dan dianggap kurang membersamai kemajuan teknologi. Penggunaan data eksponsional dan perkembangan teknologi sangat perlu perhatian dalam aspek-aspek seperti kesenjangan antara teknologi, sosial dan hukum, keamanan data, kepatuhan hukum dan aspek lainnya. Perkembangan teknologi dan hukum apabila dilihat menggunakan teori konvergensi, maka teknologi dan hukum seperti sebuah persimpangan antara pertumbuhan ekonomi dengan pembangunan negara. Teori ini menitikberatkan pada pertemuan interdisiplin antara hukum dengan teknologi yang masing-masing memiliki karakteristik (Nalom Kurniawan dan Mery Christian Putri. 2021:21-57).

Sebagai salah satu data yang dikumpulkan oleh pelaku usaha *e-commerce*, biometrik memiliki peran yang sangat penting dalam sistem keamanan data sebagai suatu metode yang dimanfaatkan sebagai alat untuk mengidentifikasi manusia berdasarkan ciri-ciri fisik atau tingkah laku yang khas (Aprilia Ayu Andarinny, et.al. 2017:305). Teknologi biometrik dapat dikategorikan mejadi tiga kelompok antara lain: (a) *physical*, yaitu mengacu pada data tentang karakteristik tubuh yang bersifat tetap dan unik, contohnya DNA, sidik jari, pola iris, retina dan lainnya; (b) *physiological*, yaitu data tentang fisiologis seseorang, contohnya detakjantung, tekanan darah, kadar oksigen dan penggunaan otot; dan (c) *behavioural*, yaitu data yang mengacu pada pola perilaku manusia, contohnya *keystroke*, *signature*, dan *voice* (Mia Hoffmann dan Mario Mariniello. 2021:4). Data biometrik sangat penting untuk dilindungi karena data tersebut dapat mengidentifikasi secara khusus dan spesifik pemilik datanya, hal tersebut karena terdapat perbedaan yang mendasar atas kejahatan terhadap nomor kartu kredit dengan kejahatan pencurian data biometrik seperti sidik jari, wajah, suara dan lainnya (Tiffany C.Li. 2021:862)

Teknologi biometrik telah digunakan untuk mengotentikasi pengguna di berbagai aplikasi dalam mengakses atau log in pada suatu aplikasi. Di masa depan, teknologi biometrik diharapkan dapat diterapkan pada otentikasi pengguna jarak jauh melalui jaringan, namun hal tersebut akan memiliki beberapa masalah yang muncul seperti masalah keamanan yang disebabkan karena fitur biometrik seperti pola sidik jari yang tidak dapat diubah atau digantikan, masalah lainnya yaitu terkait privasi, karena biometrik sangat berhubungan dengan identitas seseorang, maka dapat diprediksi beberapa pengguna tidak akan mengungkapkan data biometriknya ke server suatu jaringan (David Chek Ling Ngo, et.al. 2015).

Adanya perkembangan teknologi pada akhirnya berdampak pada perubahan dan penyesuaian aturan, asas dan hukum yang berlaku. Misalnya dalam penggunaan *e-signature* sebagai tanda bukti kesepakatan dalam sebuah transaksi. Hal tersebut juga didukung atas pengakuan terhadap dokumen elektronik sebagai alat bukti yang sah dalam hukum pembuktian. Pada saat ini, isu mengenai teknologi hukum telah muncul sebagai topik penelitian yangpenting di industri hukum dan teknologi, teknologi hukum dapat didefinisikan sebagai penggunaan teknologi modern yang digunakan untuk membantu dalam mengidentifikasi, menafsirkan dan menerapkan hukum dalam beberapa jenis layanan hukum (Ryan Whalen. 2022:6). Salah satunya yaitu penggunaan teknologi

keamanan data yang bertujuan untuk melindungi data pribadi dalam suatu domain hukum dari serangan atau ancaman kejahatan siber. Dengan demikian, harapannya dengan adanya bantuan teknologi hukum tersebut dapat berdampak dalam mendukung sektor bisnis dan proses rekayasa ulang hukum, baik dalam hal substansi hukum, struktur hukum, maupun budaya hukum (Rahmat Dwi Putranto. 2022:1168; So-Hui Park, et.al. 2021;2).

Dalam ketentuan hukum di Indonesia, isu terkait sistem keamanan data melalui biometrik telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU No. 27/2022). Dalam Pasal 1 angka (1) UU No. 27/2022, menyebutkan definsi data pribadi yakni:*"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 non elektronik."* Merujuk pada kutipan tersebut, maka data biometrik termasuk dalam jenis data pribadi yang bersifat spesifik, oleh karena itu dalam pengendaliannya termasuk memiliki potensi risiko yang tinggi.

Lawrence M. Friedman telah memberikan konsep mengenai teori sistem hukum, teori tersebut meliputi tiga aspek seperti struktur hukum, substansi hukum, dan budaya hukum (Farida Sekti Pahlevi: 2022: 31). Berkaitan dengan isu perlindungan data pribadi, pemerintah telah mengeluarkan UU No. 27/2022 yang merupakan bagian dari aspek substansi hukum menurut Lawrence M. Friedman, adapun dalam ketentuan yang diatur dalam peraturan tersebut menyebutkan mengenai kewajiban pemerintah untuk membentuk lembaga perlindungan data pribadi. Adapun pokok permasalahan tulisan ini ialah bagaimana transformasi sistem keamanan data melalui teknologi biometrik di Indonesia dalam perspektif teknologi hukum. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan menganalisis bagaimana teknologi biometrik mengubah sistem keamanan data di Indonesia dari sudut pandang teknologi hukum.

B. Metodologi Penelitian

Penelitian ini menggunakan teknik penelitian hukum normatif dan menggunakan data sekunder, seperti: Bahan hukum primer, yaitu UU No. 27/2022 dan undang-undang lainnya yang relevan. Bahan hukum sekunder, yaitu buku, jurnal, dan/atau literatur hukum, data dari media internet yang relevan dengan penelitian mengenai transformasi sistem keamanan data melalui biometrik di Indonesia perspektif teknologi hukum. Bahan hukum tersier, yaitu data-data yang mendukung bahan hukum primer dan bahan hukum sekunder. Pendekatan analitis dan undang-undang diterapkan dalam proses penelitian ini. Data penelitian diperiksa secara kualitatif, dan proses pengumpulan data diperoleh dari informasi yang dikumpulkan berdasarkan fakta lapangan, khususnya mengenai transformasi sistem keamanan data di Indonesia melalui penggunaan biometrik. Penarikan kesimpulan menggunakan logika deduktif.

C. Hasil dan Pembahasan

1.Tinjauan Umum Perlindungan Data Pribadi

Masalah mengenai perlindungan data pribadi di masa sekarang telah berkembang cukup signifikan, hal ini sebanding dengan adanya kemajuan dunia digital. Relevansi data pribadi sebagai bagian dari ruang privat merupakan akibat langsung dari kemajuan teknologi informasi dan komunikasi (Ananthia Ayu D. et.al. 2019: 24). Gagasan tentang hak atas perlindungan data pribadi didasarkan pada gagasan bahwa setiap orang memiliki hak untuk menghormati privasi mereka sendiri. Gagasan tersebut berhubungan dengan manusia sebagai makhluk hidup, maka setiap orang dianggap sebagai pemilik utama hak atas data pribadinya (Sinta Dewi Rosadi dan Garry Gumelar Pratama. 2018: 94)

Pada tahun 2020 berdasarkan laporan *Policy Brief* telah terjadi kebocoran data pribadi masyarakat sebanyak 2,3 juta, kemudian pada bulan Mei 2020 terjadi kebocoran data lembaga BPJS Kesehatan sebanyak 279 juta. Adanya kasus-kasus tersebut menunjukkan adanya sistem keamanan data yang belum dibangun dengan layak dan baik. Hal ini terjadi pada lembaga publik dan privat yang memiliki *database* masih belum

 P-ISSN 2622-9110
E-ISSN 2654-8399

memiliki *server* yang baik untuk melindungi data tersebut. Sistem untuk melindungi data pribadi tersebut mencakup *server* atau *domain* yang digunakan dalam sistem penyimpanan data atau sumber daya manusia yang membuat dan menjalankannya (Naylawati Bachtiar. 2022). Menindaklanjuti kasus-kasus kebocoran data pribadi yang sering terjadi, pemerintah pada akhir tahun 2022 telah menetapkan dan mengundangkan UU No. 27/2022, pemerintah percaya bahwa sangat penting untuk menegakkan hak individu atas perlindungan privasi, meningkatkan kesadaran publik, dan memastikan pentingnya menjaga informasi pribadi.

Berdasarkan Pasal 4 UU No. 27/2022 data pribadi dikategorikan dalam dua jenis, yaitu (i) data pribadi yang bersifat spesifik, yakni data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, dan data keuangan pribadi; dan (ii) data pribadi yang bersifat umum, yakni nama lengkap, jenis kelamin, kewarganegaraan, agama, dan status perkawinan. Dalam menggunakan atau memproses data pribadi tersebut wajib dilaksanakan berdasarkan asas pelindungan, asas kepastian hukum, asas kepentingan umum, asas kemanfaatan, asas kehati-hatian, asas keseimbangan,asas pertanggung-jawaban, dan asas kerahasiaan. Selain itu, pengendali data pribadi yang akan menggunakan data pribadi diwajibkan memiliki dasar pemrosesan yang meliputi: a. persetujuan yang sah secara eksplisit dari pemilik data pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh pengendali data pribadi kepada pemilik data pribadi; b. pemenuhan kewajiban perjanjian; c. pemenuhan kewajiban hukum dari pengendali data pribadi; d. pemenuhan perlindungan kepentingan vital pemilik data pribadi; dan/atau e. pelaksanaan tugas dengan tujuan kepentingan umum dan pelayanan publik.

Konsep perlindungan data pribadi saat ini juga telah mewajibkan pengendali data pribadi untuk menghentikan pemrosesan data pribadi paling lambat dalam waktu 3 x 24 jam apabila pemilik data pribadi menarik kembali persetujuannya. Pemilik data pribadi juga dapat mengajukan penundaan dan pembatasan pemrosesan data pribadi kepada pengendali data pribadi, tetapi tidak berlaku apabila membahayakan keselamatan pihak lain, terdapat peraturan atau perjanjian tertulis yang tidak memungkinkan dilakukan penundaan dan pembatasan oleh pengendali data pribadi. Apabila data pribadi tidak lagi diperlukan, pemilik data menarik kembali persetujuan pemrosesan data pribadi, adanya permintaan dari pemilik data pribadi, atau data pribadi diperoleh dengan perbuatan melawan hukum, maka sebagai konsekuensi hukumnya pengendali data pribadi wajib menghapus data pribadi tersebut.

Di negara-negara maju, isu perlindungan data peribadi merupakan bagian dari perlindungan hukum terhadap hak asasi. Oleh sebab itu, negara-negara maju menganggap bahwa dibutuhkan suatu regulasi yang komperhensif yang dapat mengakomodasinya. Pengakuan terhadap perlindungan data pribadi di sejumlah negara diberikan dalam bentuk "*hebeas data*", yaitu hak seseorang untuk mendapatkan pengamanan terhadap data pribadinya dan memperoleh suatu perlindungan hukum jika terjadi pelanggaran pada data pribadinya (Hari Sutra Disemadi. 2021: 186) Di Indonesia sendiri upaya untuk melindungi data pribadi merupakan amanat konsitusi sesuai dengan Pasal 28G Undang-Undang Dasar Republik Indonesia Tahun 1945 yang berbunyi: *"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."*

Dengan demikian, disahkannya UU No. 27/2022 selain menjalankan amanah konstitusi, regulasi tersebut juga mengatasi adanya tumpang tindih peraturan perundang-undangan yang sebelumnya tersebar di beberapa undang-undang, sehingga dengan adanya peraturan yang jelas efektivitas dan standarisasi perlindungan data pribadi masyarakat dapat segera terwujud.

2.Transformasi Sistem Keamanan Data Melalui Teknologi Biometrik

Keamanan data adalah upaya dan tindakan untuk melindungi unsur paling penting dari lingkungan digital, seperti ketersediaan data, integritas data, dan kerahasiaan. Sejak akhir 1970-an, ketika seorang peretas terkenal bernama Kevin Mitnick mulai melakukan kejahatan komputer, pada saat itu lah teknologi keamanan data telah berkembang pesat. Pada usia 13 tahun, Kevin Mitnick menggunakan strategi *social engineering* dan *trash dumpster* untuk melakukan kejahatan di sekolahnya dengan tujuan mengendarai gratis bus sekolah. Kejahatan lain yang dilakukan oleh Kevin Mitnick antara lain meretas jaringan komputer Palo Alto Research Center, dan serangkaian kejahatan *cyber* ke jaringan *Federal Bureau of Investigation* (FBI) dan banyak sistem komputer di dunia lainnya. Salah satu dampak atas kejahatan Kevin Mitnick tersebut telah membuat sistem keamanan data mengalami perkembangan pesat. Sistem keamanan data yang paling umum digunakan adalah metode *cryptography* (ilmu penyandian) dan metode *encryption* (penyandian) (Indra Gunawan. 2021). Saat ini bantuan teknologi telah memiliki banyak keunggul jika dibandingkan dengan metode tradisional, hal ini juga terjadi pada pemrosesan data modern, namun kemajuan tersebut juga memiliki dampak buruk seperti hak atas privasi yang semakin terancam (Ananthia Ayu D. et.al. 2019: 74).

Ancaman terhadap data pribadi dapat mengakibatkan penurunan atau hilangnya tujuan keamanan data, seperti: (i) kehilangan integritas, yang mengacu pada persyaratan untuk melindungi informasi dari modifikasi yang tidak pantas, seperti pembuatan, penyisipan, pembaruan, perubahan status data, atau penghapusan; (ii) hilangnya ketersediaan data berdasarkan pemberian informasi kepada pengguna yang memiliki hak akses legal; dan (iii) hilangnya kerahasiaan data berdasarkan perlindungan data dari pengungkapan yang tidak berwenang (Gatot Susilo. 2016: 81). Keamanan data menggunakan metode *password* saat ini telah banyak kelemahannya, fungsi *password* pada umumnya untuk melakukan verifikasi dan banyak masyarakat yang menggunakan *password* yang sama untuk mengakses berbagai aplikasi. Untuk mengatasi kelemahan perlindungan data menggunakan *password* kemudian dikembangkanlah teknologi biometrik sebagai perlindungan data modern (Adhi Kusmantoro. 2006: 34).

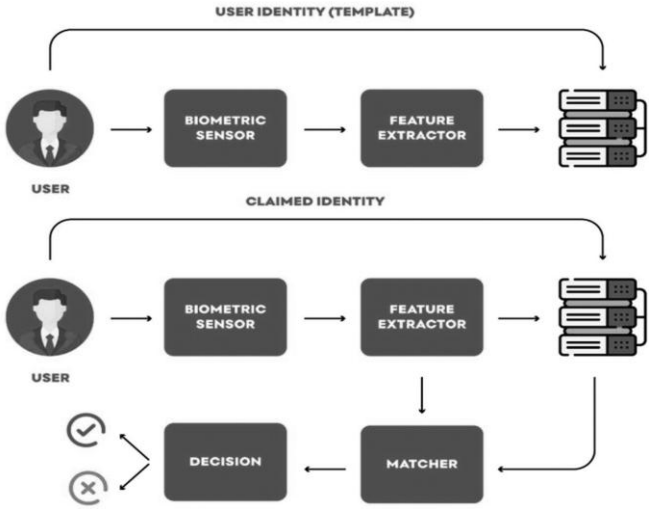
Tujuan dari dilakukannya pengembangan terhadap teknologi biometrik yakni untuk memenuhi dua manfaat yakni identifikasi dan verifikasi, di sisi lain data biometrik juga memiliki ciri khas seperti sulit hilang, tidak dapat lupa, dan sulit dipalsukan karena data biometrik antara satu orang dengan lainnya berbeda (Nicco dan Iman Fahruzi. 2016). Dikutip dari Asosiasi Industri Teknologi Biometrik, definisi biometrik adalah metode paling dasar untuk mengidentifikasi dan memverifikasi seseorang dengan cepat dan akurat berdasarkan sifat masing-masing. Identifikasi menggunakan teknologi biometrik ditentukan dari verifikasi identitas seseorang, dengan maksud untuk mendapatkan data biometrik seseorang tersebut seperti wajah, suara, dan sidik jari. Kemudian data yang telah diperoleh akan dilakukan perbandingan menggunakan data biometrik orang lain yang tersimpan di database, dalam proses tersebut sistem biometrik akan melakukan verifikasi kebenaran data yang diberikan asli atau palsu.

Berdasarkan sejarahnya, penggunaan teknologi biometrik sudah ada sejak tahun 1800-an, data biometrik dimanfaatkan secara teratur untuk mengidentifikasi pelaku kejahatan dan penandatanganan perjanjian, pemanfaatan teknologi biometrik jenis ini dikembangkan oleh Edward Henry. Pada tahun 1960-an metode identifikasi menggunakan wajah semi otomatis mulai dikembangkan, kemudian memasuki 1969, mulai berkembang teknologi biometrik sidik jadi dan identifikasi wajah dalam penegakan hukum. Sementara teknologi biometrik melalui suara mulai dikembangkan di Institut Nasional Standar dan Teknologi pada tahun 1980-an, yang disusul dengan pengembangan penggunaan biometrik sidik jari dan iris padatahun 1985. Kemudian pada tahun 1991, pengembangan teknologi biometrik melalui identifikasi wajah mulai dikembangkan, meskipun proses perkembangannya dianggap cukup rumit, tetapi teknologi biometrik wajah menjadi jenis biometrik yang mendapat dukungan dari berbagai pihak. Ahli di bidang biometrik memprediksi bahwa akan terjadi kemajuan dibidang teknologi

P-ISSN 2622-9110
E-ISSN 2654-8399

biometrik dengan munculnya banyak pilihan sistem teknologi biometrik. Para ahli pun memprediksi pada tahun 2030 penggunaan metode *password* dalam pengamanan data tidak akan lagi digunakan sepenuhnya. Hal ini karena keberadaan teknologi biometrik yang dianggap sangat membantu dalam menjaga keamanan data seseorang dan dapat mengurangi tindak kejahatan seperti penipuan dan pemalsuan data.

Gambar di bawah ini menunjukkan cara kerja sistem keamanan data berbasis teknologi biometrik:



Gambar 1 Mekanisme Kerja Teknologi Biometrik

Berdasarkan mekanisme kerja teknologi biometrik di atas, pengguna wajib melakukan pendaftaran dan verifikasi, pada tahap pendaftaran akan menghasilkan data biometrik yang disimpan dalam database. Pada tahap verifikasi, pengguna terdaftar mengklaim identitasnya, data tersebut diverifikasi oleh sistem berdasarkan rangkaian fitur biometrik pengguna (Barbara Mroz-Gorgon, et.al. 2022: 4).

3.Proyeksi Teknologi Hukum Terhadap Sistem Keamanan Data

Dalam teorinya tentang sistem hukum, Lawrence M. Friedman berpendapat bahwa hukum memiliki tiga komponen utama: struktur hukum, substansi hukum, dan budaya hukum. Secara fundamental proses pembentukan sistem hukum harus mencakup pembangunan dalam segi materi (*substance*), kelembagaan (*structure*) dan budaya (*culture*), ketiganya harus saling mempengaruhi, oleh karenanya hukum harus dibangun secara terintegrasi antara satu aspek dengan aspek lainnya, serta berkelanjutan dan berwawasan global (Priyo Hutomo dan Markus Marselinus Soge. 2021: 53). Berdasarkan hal tersebut, khususnya mengenai isu perlindungan data pribadi, maka yang menjadi fokus dalam pembahasan ini adalah aspek substansi hukum (UU No. 27/2022) dan struktur hukum yang telah diatur dalam UU No. 27/2022, tetapi sampai saat ini lembaga tersebut belum ditetapkan oleh pemerintah.

Apabila merujuk ketentuan Pasal 58 UU No. 27/2022, pemerintah memiliki kewajiban untuk menindaklanjuti terkait ketentuan pelaksana, salah satunya yaitu membentuk lembaga atau otoritas yang bertugas untuk mengawasi penyelenggaraan perlindungan data pribadi di Indonesia. Lembaga tersebut dibentuk oleh pemerintah dan akan bertanggung jawab secara langsung kepada presiden, akan tetapi sampai dengan saat ini lembaga tersebut belum dibentuk oleh pemerintah. Secara tugas dan wewenang lembaga tersebut telah diatur dalam Pasal 59 dan Pasal 60 UU No. 27/2022 dan mengenai mekanisme pelaksanaan wewenangnya akan diatur dalam peraturan pelaksana UU No. 27/2022. Adapun tugas dari lembaga tersebut antara lain: a) mengembangkan dan menerapkan kebijakan dan strategi perlindungan data pribadi yang menjadi pedoman bagi pemilik data pribadi, pengontrol data pribadi, dan pengolah data pribadi; b) mengawasi atas pelaksanaan perlindungan data pribadi secara nasional; c) penegakan hukum administrasi terhadap pelanggaran hukum; dan d) memfasilitasi penyelesaian sengketa perlindungan data pribadi di luar pengadilan.

Selain empat tugas tersebut di atas, lembaga tersebut juga akan memiliki sejumlah wewenang lain, termasuk kemampuan untuk membuat dan menerapkan aturan nasional untuk administrasi data pribadi dan memantau kepatuhan pengendali data pribadi, memberikan sanksi terhadap pelanggaran perlindungan data pribiadi, membantu aparat penegak hukum dalam penanganan tindak pidana kejahatan siber yang melibatkan data pribadi, melaksanakan kerjasama dengan lembaga negara lain dalam rangka penyelesaian sengketa lintas negara, melaksanakan analisa dan penilaian terhadap pemenuhan persyaratan transfer data pribadi ke luar wilayah hukum Indonesia, melaksanakan publikasi hasul pelaksanaan pengawasan, menerima laporan dan aduan, serta melakukan pemeriksaan dan penelusuran terkait dugaan pelanggaran, memanggil dan menghadirkan pihak termasuk ahli terkait dugaan pelanggaran, meminta keterangan, data, informasi, dan dokumen kepada pihak hukum terkait dugaan pelanggaran, melakukan pemeriksaan dan penelusuran sistem elektronik, fasilitas, ruang, dan lokasi yang digunakan oleh pengendali atau pemroses.

Pasca pengesahan UU No. 27/2022, saat ini Indonesia sangat membutuhkan lembaga pengawas di bidang perlindungan data pribadi yang memiki peran sebagai *state auxiliary organ* yang independen dan setingkat dengan kementerian lainnya. Tujuan dari lembaga tersebut yakni untuk memastikan sistem keamanan terkait perlindungan data pribadi sesuai dengan aturan-aturan yang ditentukan dalam UU No. 27/2022 (Imas Novita Juaningsih, et.al, 2021: 478). Selain itu, sebagai langkah preventif, lembaga tersebut juga seharusnya dapat membentuk direktorat perizinan atau setidaknya bekerja sama dengan lembaga sertifikasi nasional dan Badan Koordinasi Penanaman Modal/ Kementerian Investasi untuk menerbitakan izin kelayakan terhadap pengendali data pribadi dan prosesor data pribadi agar memiliki standarisasi keamanan data nasional yang aman dan handal.

Menurut Esther Salmeron Manzano, teknologi hukum secara arti ialah penggunaan teknologi dalam layanan jasa hukum untuk menciptakan disrupsi pada jasa hukum tradisional, untuk mempercepat pekerjaan seorang profesional hukum, dan untuk menyederhanakan atau memodifikasi bentuk komunikasi antara profesional hukum dengan calon klien melalui platform digital (Esther Salmeron-Manzano. 2021: 2). Sementara Ryan Whalen memberikan definisi teknologi hukum sebagai semua perangkat yang mampu digunakan sebagai sarana untuk berinteraksi dengan substansi hukum atau membantu penggunanya untuk berinteraksi dengan hukum, termasuk semua teknologi yang mampu dimanfaatkan untuk mencapai dari tujuan hukum (Ryan Whalen. 2022).

Selain pembentukan substansi hukum dan struktur hukum, pemerintah diharapkan juga mengelaborasi budaya hukum dengan cara memanfaatkan teknologi biometrik dan teknologi hukum dalam sistem keamanan data nasional. Dengan merujuk pada tugas dan wewenang lembaga perlindungan data pribadi sebagaimana diatur UU No. 27/2022, maka terdapat fitur teknologi hukum yang memungkinkan untuk diterapkan di lembaga perlindungan data pribadi, yaitu (Jim Leason. Et.al. 2019): 1) *Online dispute resolution* (ODR), yaitu penyelesaian sengketa alternatif yang bersifat khusus dan tersendiri (*sui generis*). Manfaat yang dapat diperoleh apabila lembaga perlindungan data pribadi menyediakan penyelesaian melalui internet sebagai salah satu pilihan dalam penyelesaian sengketa, yakni waktu dan biaya yang lebih efisien dan murah, pemanfaatan sistem *asynchronous* ODR berbasis teknologi modern yang akan memudahkan para pihak untuk saling bertukar argumentasi dengan leluasa, dan dalam proses ODR tidak memandang teritorial (Armansyah. 2021: 46). Selain itu sesuai dengan Pasal 64 angka (4) yang mengatur hukum acara dari perkara perlindungan data pribadi dilakukan secara tertutup, maka dengan adanya pemanfaatan sidang melalui ODR akan sangat terbantu, terutama dengan sistem *asynchronous;* 2) *Board governance,* yakni fitur yang dapat membantu lembaga perlindungan data pribadi untuk mengelola pemberian izin dan disrtibusi secara online kepada pengendali dan prosesor data pribadi; 3) *Cybersecurity,* yakni fitur yang melayani perlindungan keamanan data pribadi dan informasi dari ancaman *hacking,* lembaga perlindungan data pribadi bisa menggunakan fitur ini untuk mengedukasi

pemilik data pribadi; 4) *Data privacy compliance,* yakni fitur yang dapat digunakan oleh lembaga perlindungan data pribadi untuk mengelola kepatuhan sistem keamanan data dari pengendali dan prosesor data pribadi dalam rangka tugas pengawasan.

D. Penutup

Adanya perkembangan teknologi dan informasi dan kasus-kasus kejahatan siber terkait pencurian data pribadi telah memberikan dampak kepada kemajuan sistem keamanan data pribadi, dampak paling nyata yakni dengan disahkannya UU No. 27/2022 oleh pemerintah. Jenis-jenis data pribadi terdiri atas data bersifat umum dan data berifat spesifik, adapun biometrik termasuk dalam data yang bersifat spesifik, maka dalam pengendaliannya masuk ke dalam risiko tingkat tinggi. Data biometrik dibagi dua, yaitu: (a) *physical*, contohnya DNA, sidik jari, pola iris, retina dan lainnya; (b) *physiological*, contohnya detak jantung, tekanan darah, kadar oksigen dan penggunaan otot; dan (c) *behavioural*, contohnya *keystroke, signature,* dan *voice.* Pada masa serba digital saat ini, teknologi biometrik semakin dibutuhkan karena dapat secara bersamaan berfungsi untuk mengidentifikasi dan verifikasi. Selain itu, gagasan perlindungan data pribadi saat ini telah memberikan opsi kepada pemilik data seperti meminta pengendali dan pemroses data untuk berhenti memproses data mereka, mengajukan penundaan dan pembatasan pemrosesan data, dan menarik persetujuan untuk memproses data mereka. Untuk membangun sistem keamanan data nasional, pemerintah saat ini perlu menindaklanjuti UU No. 27/2022 dengan membentuk otoritas atau lembaga perlindungan data pribadi. Diharapkan pada masa depan, lembaga tersebut dapat memanfaatkan bantuan teknologi modern seperti teknologi biometrik dan teknologi hukum seperti menyediakan fitur *online dispute resolution, board governance, cybersecurity,* dan *data privacy compliance*, sehingga bukan hanya struktur hukum dan substansi hukum saja yang dibangun, tetapi pembangunan budaya hukum pun dilaksanakan dalam rangka mewujudkan efektivitas dan standarisasi perlindungan data pribadi masyarakat.

Daftar Pustaka

Armansyah. "Online Dispute Resolution Sebagai Alternatif Penyelesaian Sengketa Transaksi Digital". *Jurnal Selisik,* Vol. 7, No. 2, pp. 34-52, 2021.

Ayu Andarinny, Aprili, Perancangan Sistem Identifikasi Biometrik Jari Tangan Menggunakan Laplacian of Gaussian dan Ektraksi Kontur. *Youngster Physics Journal,* 6 (4). 2017.

Ayu D., Ananthia, et.al. "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital," Mahkamah Konstitusi. Jakarta, 2019.

Bachtiar, Naylawati. *Darurat Kebocoran Data: Kebutuhan Regulasi Pemerintah*. Lab. RisetKebijakan Manajemen Publik Universitas Hasanuddin. Makassar, 2022.

C.Li.. Tiffany. *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis. Loyola University Chicago Law Journal,* 52 (3) : 862, 2021.

Chek Ling Ngo, David, et.al. *Biometric Security*. Edisi Pertama. Newcastle: Cambridge Scholars Publishing, 2015.

Dewi Rosadi, Sinta dan Garry Gumelar Pratama. "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia," *Jurnal VeJ*, Vol. 4, No. 1, pp. 88-110, 2018.

Dwi Putranto, Rahmat. *Legal Digitalization Analysis: Study of National Legal System Renewal. Literatus,* 4 (3): 1168, 2022.

Gunawan, Indra. *Keamanan Data: Teori dan Implementasi*. Sukabumi.CV Jejak, 2021.

Hasan Rumlus, Muhamad dan H. Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadidalam Media Elektronik". *Jurnal HAM,* Vol. 11, No. 2, pp. 285-299, 2020.

Hoffmann, Mia dan Mario Mariniello.. *Biometric Technologies at Work: A Proposed Use-Based Taxonomy*. *Policy Contribution 23/2021,* Bruegel, p. 19, 2021.

Hui Park, So, et.al. *A Survey of Research on Data Analytics Based Legal Tech. Sustainability,* 13 (8085): 1-2, 2021.

Hutomo, Priyo dan Markus Marselinus Soge. "Perspektif Teori Sistem Hukum dalam Pembaharuan Pengaturan Sistem Permasyarakatan Militer", *Legacy: Jurnal Hukum dan Perundang-Undangan*, Vol. 1, No. 1, pp. 46-68, 2021.

Industri Teknologi Biometrik, Asosiasi. 2021. Apa itu Biometrik? Ini Definisi dan Jenis-Jenisnya. Diunduh tanggal 7 Mei 2022 dari *https://biometrik.org/biometrik-adalah/.*

Kusmantoro, Adhi. "Teknologi Biometrik dengan Metode Sidik Jari untuk Sistem Keamanan Database". *Jurnal Teknik Elektro*, Vol 4, No. 1, pp. 34, 2006.

Leason, Jim. et.al. "Legal Tech Startup Report 2019 A Maturing Market". *Thomson Reuters& Legal Geek*, United Kingdom, 2019.

Nicco dan Iman Fahruzi. "Rancang Bangun Sistem Biometrik Pengenalan Wajah Menggunakan Principal Component Analysis". *Jurnal Integrasi*, Vol. 7, No. 2, 2015.

Novita Juaningsih, Imas, et.al. "Rekonsepsi Lembaga Pengawas terkait Perlindungan Data Pribadi oleh Korporasi sebagai Penegakan Hak Privasi Berdasarkan Konstitusi". *Jurnal Sosial dan Budaya Syari Salam*, Vol. 8, No. 2, pp. 467-484, 2021.

Salmerón Manzano, Eshter. "Legaltech and Lawtech: Global Perspectives, Challenges, and Opportunities". *MDP*I *Laws*, 10 (2), pp. 24, 2021.

Santoso, Edy dan Sukendar. Hukum Bisnis (Kumpulan Undang-Undang di Bidang Teknologi Informasi dan Komunikasi). Cetakan Pertama. Sleman: Deepublish, 2020.

Sekti Pahlevi, Farida. "Pembrantasan Korupsi di Indonesia: Perspektif Legal System Lawrence M. Friedman", *Jurnal El-Dusturie*, Vol. 1, No. 1, Juni 2022, pp. 24-42, 2022.

Septiani Ady, Nadia, et.al. Urgensi KUHD dalam Menangani Risiko Kejahatan Siber pada Transaksi E-Commerce. *Jurnal of Law, Administration, Social Science*, 2 (1): 4, 2022.

Susilo, Gatot. "Keamanan Basis Data Pada Sistem Informasi di Era Global". *Jurnal Transformasi*, Vol. 12, No. 2, pp. 78-87, 2016.

Sutra Disemadi, Hari. "Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia". *Jurnal Wawasan Yuridika*,Vol. 5, No. 2, pp. 177-199, 2021.

Whalen, Ryan. *Defining Legal Technology and Its Implications, International Journal of Law and Information Technology*, 00 (17): 6, 2022.