**RESIKO HUKUM PENYALAHGUNAAN TEKNOLOGI BIOMETRIK TERHADAP OTENTIKASI TRANSAKSI ELEKTRONIK**

****

**S K R I P S I**

**Diajukan untuk Memenuhi Tugas dan Melengkapi Syarat Guna Memperoleh Gelar Sarjana Strata 1 dalam Ilmu Hukum**

**Oleh:**

**NURUL OKTAFIYANI**

**NPM 5121600239**

**FAKULTAS HUKUM**

**UNIVERSITAS PANCASAKTI TEGAL**

**2025**

****

****



**ABSTRAK**

**Nurul Oktafiyani.** *Resiko Hukum Penyalahgunaan Teknologi Biometrik Terhadap Otentikasi Transaksi Elektronik*. Skripsi. Tegal: Program Studi Ilmu Hukum Fakultas Hukum, Universitas Pancasakti Tegal. 2025.

Latar belakang pada penelitian ini adalah teknologi biometrik telah mengubah cara transaksi elektronik diotentikasi, yang menentukan keabsahan kontrak dari sudut pandang hukum perdata. Metode biometrik seperti pengenalan wajah dan sidik jari lebih aman daripada metode konvensional. Tapi ada masalah dengan tanda tangan elektronik yang dibuat dengan teknologi ini apakah sah atau tidak.

Penelitian ini bertujuan untuk menganalisis keabsahan kontrak yang menggunakan otentikasi biometrik serta mengeksplorasi risiko penyalahgunaan data biometrik yang dapat mempengaruhi keabsahan kontrak dalam transaksi elektronik. Jenis penelitian ini adalah studi kepustakaan *(library research)* dengan menggunakan pendekatan normatif, dan teknik pengumpulan datanya melalui sumber data sekunder dan dianalisis menggunakan pendekatan kualitatif.

Hasil penelitian ini menujukan Undang-Undang tentang Informasi dan Transaksi Elektronik menyatakan bahwa kontrak tertulis dan komunikasi elektronik dapat diberlakukan, dengan keabsahan kontrak diatur dalam KUHPerdata, khususnya Pasal 1320. Kontrak yang menggunakan otentikasi biometrik, seperti tanda tangan elektronik, dapat dianggap sah asalkan memenuhi syarat hukum yang berlaku. Meskipun data biometrik menawarkan keamanan dalam transaksi elektronik, penggunaannya juga membawa risiko penyalahgunaan, seperti pencurian identitas, yang dapat merusak keabsahan kontrak. Cacat kehendak, termasuk penyalahgunaan keadaan, dapat terjadi jika kontrak ditandatangani oleh pihak yang tidak berhak, sehingga mengancam kepercayaan terhadap sistem transaksi digital. Untuk melindungi data pribadi, pemerintah telah mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang bertujuan mencegah penyalahgunaan data biometrik dalam transaksi elektronik.

Berdasarkan hasil penelitian ini diharapkan akan menjadi bahan informasi dan masukan bagi mahasiswa,akademisi,praktisi, dan semua pihak yang membutuhkan di lingkungan Fakultas Hukum Universitas Pancasakti Tegal.

**Kata Kunci: Keabsahan, Kontrak Elektronik, Otentikasi Biometrik, Hukum Perdata**

***ABSTRACT***

**Nurul Oktafiyani***. Legal Risks Of Biometric Technology Misuse On Electronic Transaction Authentication*. Thesis. Tegal: Legal Studies Program, Faculty of Law, Pancasakti University, Tegal. 2025.

*The background of this study is that biometric technology has changed the way electronic transactions are authenticated, which determines the validity of contracts from a civil law perspective. Biometric methods such as facial recognition and fingerprints are more secure than conventional methods. But there is a problem with electronic signatures made with this technology whether they are valid or not.*

*This study aims to analyze the validity of contracts that use biometric authentication and explore the risks of misuse of biometric data that can affect the validity of contracts in electronic transactions. This type of research is a literature study (library research) using a normative approach, and the data collection technique is through secondary data sources and analyzed using a qualitative approach.*

*The results of this study indicate that the Law on Information and Electronic Transactions states that written contracts and electronic communications can be enforced, with the validity of the contract regulated in the Civil Code, specifically Article 1320. Contracts that use biometric authentication, such as electronic signatures, can be considered valid as long as they meet the applicable legal requirements. Although biometric data offers security in electronic transactions, its use also carries the risk of misuse, such as identity theft, which can damage the validity of the contract. Defects of will, including abuse of circumstances, can occur if the contract is signed by an unauthorized party, thus threatening trust in the digital transaction system. To protect personal data, the government has issued Law Number 27 of 2022 concerning Personal Data Protection, which aims to prevent misuse of biometric data in electronic transactions.*

*Based on the results of this study, it is hoped that it will be a source of information and input for students, academics, practitioners, and all parties in need in the Faculty of Law, Pancasakti University, Tegal.*

***Keywords: Validity, Electronic Contract, Biometric Authentication, Civil Law***

**MOTTO**

“Hukum yang Tegas, Keadilan yang Nyata”

“ Memulai dengan penuh keyakinan, dijalani dengan keikhlasan, dan selesai dengan penuh kebahagiaan”

**PERSEMBAHAN**

Dengan penuh rasa syukur, saya mempersembahkan skripsi ini kepada:

1. Allah SWT. karena hanya atas izin dan karunia-Nya maka skripsi ini dapat dibuat dan diselesaikan tepat waktu.
2. Terima kasih kepada kedua orangtua saya, Bapak Kambali dan Ibu Lili Rumandani, yang telah memberikan dukungan, kasih sayang, dan doa yang tiada henti. Terutama untuk ibu saya yang membuat segalanya menjadi mungkin sehingga saya bisa sampai pada tahap ini. Aku sangat bersyukur kalian menjadi orangtuaku.
3. Kakak saya, Lisa Meilani dan keluarga kecilnya, terimakasih sudah membantu segala kebutuhan, serta memberikan tenaga, waktu, pikiran, dan juga motivasi yang telah diberikan. Tanpa dukungan dari mba lisa aku bisa apa. Terimakasih sudah menjadi kakak yang baik ya. Onty sayang Hamza.
4. Untuk teman saya Zahra Shabira, Annisa, Ghina Mufidah, Fiqih Annisa, Elmira Aisyah Fani, dan untuk semua yang menganal saya. Terimakasih atas segala warna yang telah diberikan selama masa perkuliahan ini. Suka maupun duka telah dilewati, semoga kalian selalu sehat, bahagia dan sukses selalu.
5. Kepada Bapak Dr. Sanusi, S.H., M.H. dan Ibu Dr. Tiyas Vika Widyastuti, S.H., M.H. selaku Dosen Pembimbing saya, yang telah membberikan bimbingan, arahan, bantuan, dan motivasi selama proses penulisan skripsi ini. Terimakasih atas kesabaran dan ilmu yang telah diberikan.
6. Terakhir, skripsi ini saya persembahkan untuk diri saya sendiri, sebagai penghargaan atas perjuangan dan perjalanan panjang yang telah saya lewati hingga saat ini. Perjalanan ini bukanlah hal yang mudah, tetapi saya mampu melewatinya. Terima kasih kepada diri saya yang selalu berusaha untuk terus belajar, berkembang, walaupun sering nyerah tapi harus bangkit lagi karena ada orangtua yang menanti di ujung sana.

**KATA PENGANTAR**

Dengan mengucap syukur kehadirat Allah SWT., alhamdulillah penyusunan skrispi ini dapat selesai. Dengan skripsi ini pula penulis dapatmenyelesaikan studi di Program Studi Ilmu Hukum Universitas Pancasakti Tegal. Shalawat dan salam penulisa sampaikan kepada Rasulullah SAW. Yang membawa rahmat sekalian alam.

Penyusunan skripsi ini tidak lepas dari bantuan dan dorongan berbagai pihak yang kedepannya patut diucapkan terima kasih. Ucapan terima kasih penulis sampaikan kepada:

1. Dr. Taufiqullah, M.Hum. selaku Rektor Universitas Pancasakti Tegal
2. Dr. Kus Rizkianto, S.H., M.H selaku Plt. Dekan Fakultas Hukum Universitas Pancasakti Tegal.
3. Dr. Soesi Idayanti, S.H., M.H selaku Wakil Dekan I Fakultas Hukum Universitas Pancasakti Tegal.
4. Fajar Dian Aryani, S.H., M.H selaku Wakil Dekan II Fakultas Hukum Universitas Pancasakti Tegal.
5. Dr. H. Moh. Khamim, S.H., M.H selaku Wakil Dekan III Fakultas Hukum Universitas Pancasakti Tegal.
6. Selviany, S.E., M.H selaku Sekretris Program Studi Ilmu Hukum Fakultas Hukum Universitas Pancasakti Tegal.
7. Dr. H. Sanusi, S.H., M.H., Dr. Tiyas Vika Widyastuti, S.H., M.H selaku Dosen Pembimbing yang telah berkenan memberikan bimbingan dan arahan pada penulis dalam penyusunan skrispsi ini.
8. Segenap dosen Fakultas Hukum Universitas Pancasakti Tegal yang telah memberikan bekal ilmu pengetahuan pada penulis sehingga bisa menyelesaikan studi Strata 1. Mudah-mudahan mendapatkan balasan dari Allah SWT. sebagai amal shalih.
9. Segenap pegawai administrasi/karyawan Universitas Pancasakti Tegal Khususnya di fakultas Hukum yang telah memberikan layanan akademik dengan sabar.
10. Orang Tua, serta saudra-saudra penulis yang memberikan dorongan moriil pada penulis dalam menempuh studi.
11. Kawan-kawan penulis, dan semua pihak yang meberikan motivasi dalam menempuh studi maupun dalam penyusunan skrispi ini yang tidak dapat disebut satu-persatu.

Semoga Allah SWT. membalas semua amal kebaikan mereka dengan balasan yang lebih dari mereka berikan kepada penulis. Akhirnya hnaya kepada Allah SWT. penulis berharap semogra skripsi ini dapat bermanfaat bagi penulis khususnya, dan bagi pembaca umumnya.

Tegal, 08 Februari 2025

Penulis

**DAFTAR ISI**

**HALAMAN JUDUL i**

**HALAMAN PERSETUJUAN PEMBIMBING ii**

**HALAMAN PENGESAHAN iii**

**HALAMAN PERNYATAAN iv**

**ABSTRAK v**

***ABSTRACT vi***

**MOTTO vii**

**PERSEMBAHAN viii**

**KATA PENGANTAR ix**

**DAFTAR ISI xi**

**BAB I PENDAHULUAN 1**

1. Latar Belakang Masalah 1
2. Rumusan Masalah 18
3. Tujuan Penelitian 18
4. Urgensi Penelitian 18
5. Tinjauan Pustaka 19
6. Metode Penelitian 21
7. Sistematika Penelitian 26

**BAB II TINJAUAN KONSEPTUAL 27**

1. Tinjauan tentang Pengertian dan Konsep Teknologi Biometrik dalam Otentikasi Biometrik 27
2. Pengertian Teknologi Biomterik 27
3. Konsep Teknologi Biometrik 31
4. Peran Otentikasi dalam Transaksi Elektronik 35
5. Hubungan antar Teknologi Biometrik dengan Keabsahan Kontrak 38
6. Aspek Hukum Perdata dalam Mengatur Penggunaan Teknologi Biometrik Terhadap Transaksi Elektronik 40
7. Implikasi Hukum dari Penggunaan Teknologi Biometrik dalam Hukum Perdata 40
8. Ketentuana Mengenai Keabsahan Kontrak dalam Hukum Perdata 44
9. Adaptasi Hukum terhadap Perkembangan Teknologi Biometrik dalam Hukum Perdata 48

**BAB III HASIL PENELITIAN DAN PEMBAHASAN 52**

1. Keabsahan Kontrak yang Menggunakan Otentikasi Biometrik dalam Hukum Perdata 52
2. Resiko Penyalahgunaan Data Biometrik ynag Mempengaruhi Keabsahan Kontrak dalam Transaksi Elektronik 69

**BAB IV PENUTUP 95**

1. Simpulan 95
2. Saran 97

**DAFTAR PUSTAKA 98**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang Masalah**

Banyak aspek kehidupan manusia, termasuk profesi hukum, telah mengalami perubahan substansial sebagai hasil dari kemajuan pesat teknologi informasi dan komunikasi.[[1]](#footnote-1) Salah satu dampaknya adalah munculnya transaksi elektronik yang semakin marak di sejumlah daerah, seperti Indonesia, yang secara langsung mempengaruhi munculnya peraturan perundang-undangan, perkembangan baru yang harus diantisipasi oleh pemerintah, setelah itu undang-undang dirancang dan dibuat agar dapat ditegakkan oleh masyarakat secara keseluruhan.[[2]](#footnote-2) Transaksi yang memungkinkan para pihak memenuhi tanggung jawab mereka dan menandatangani perjanjian secara elektronik tanpa harus bertemu secara fisik. Sesuai dengan Pasal 1 Angka 2 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), disebutkan; “Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, atau media elektronik lainnya.”

Hal ini akan memberikan kemudahan dan efisien waktu, tetapi juga menimbulkan tantangan baru terkait keabsahan dan kepastian hukum. Ketentuan legalitas suatu perjanjian juga akan ditentukan oleh karakteristik sistem elektronik yang dimaksud. Keberadaan jaringan komputer internet global semakin memudahkan terjadinya transaksi elektronik, yang pada hakikatnya adalah perjanjian atau hubungan hukum yang dilakukan secara elektronik yang mengintegrasikan sistem informasi berbasis komputer, sistem komunikasi, dan layanan jaringan. Apabila setiap elemen sistem elektronik dapat dipastikan dapat diandalkan dan berfungsi sebagaimana mestinya, maka perjanjian tersebut dianggap sah.[[3]](#footnote-3)

Teknologi biometrik adalah metode untuk mengidentifikasi yang menggunakan ciri fisik atau perilaku khas seseorang untuk mengidentifikasi dan mengkonfirmasi identitas mereka. Istilah "biometrik" berasal dari kata Yunani *"bios",* yang diartikan kehidupan, dan *"metrik",* yang diartikan pengukuran. Dengan demikian, biometrik dapat diartikan sebagai pengukuran dan analisis karakteristik biologi atau perilaku individu. Karena telah menunjukkan identitas biologis manusia, biometrik dapat dianggap sebagai "kemasan kecil dari manusia". Tiga aspek tinjauan digunakan untuk mencapai hal ini: apa yang diketahuinya sebagai seorang individu yang hidup, apa yang dimilikinya dari luar (unsur ekstrinsik), dan apa yang dimilikinya dari dalam (unsur intrinsik).[[4]](#footnote-4) Pengenalan teknologi biometrik dalam konteks keabsahan kontrak telah menjadi topik yang semakin relevan seiring dengan perkembangan transaksi elektronik. Biometrik, yang merupakan teknologi yang memanfaatkan data biologis unik untuk autentikasi, menawarkan metode yang lebih aman dan efisien dalam verifikasi identitas individu. Hanya individu yang berwenang yang dapat menandatangani kontrak atau menyelesaikan transaksi dengan menggunakan biometrik, yang menggunakan ciri fisik seperti sidik jari, wajah, atau iris.[[5]](#footnote-5) Tidak seperti dengan metode identifikasi konvensional yang menggunakan sesuatu yang anda punyai, contoh kartu identitas untuk memasuki suatu gedung, atau sesuatu yang dikenal, seperti kata sandi sistem komputer, dll.[[6]](#footnote-6)

Penerapan autentikasi biometrik dari perspektif hukum perdata menimbulkan pertanyaan kritis tentang hakikat persetujuan dan verifikasi identitas dalam pembentukan kontrak. Data biometrik pada dasarnya bersifat pribadi dan sensitif. Dengan demikian, pengumpulan dan penggunaannya harus mematuhi standar hukum yang ketat untuk melindungi hak privasi individu. Kerangka hukum perdata harus beradaptasi untuk mengakomodasi kemajuan teknologi ini, memastikan bahwa kontrak yang diautentikasi melalui cara biometrik diakui sebagai sah dan dapat diberlakukan. Adaptasi ini penting bukan hanya untuk perlindungan konsumen namun juga untuk menumbuhkan kepercayaan pada sistem keuangan digital. Hal ini tercermin dalam Undang-undang Perlindungan Data Pribadi (UU PDP) yang mensyaratkan persetujuan eksplisit dari pemilik data sebelum melakukan pemrosesan data biometrik.[[7]](#footnote-7) Data biometrik sesuai dengan ketentuan perundang-undangan yang berlaku di Indonesia dikategorikan sebagai data pribadi, yang mana merupakan data pribadi yang bersifat spesifik.[[8]](#footnote-8) Berdasarkan undang-undang Indonesia, hanya *Artificial Intelligence* (AI) dapat mengumpulkan data tanpa persetujuan pemilik data. Jika terjadi pelanggaran, ada pihak yang bertanggung jawab atas kerugian dan pelanggaran. Namun, kedudukan hukum AI yang tidak dapat disamakan dengan manusia atau badan hukum menimbulkan pertanyaan tentang pihak yang bertanggung jawab atas pengumpulan data. Data biometrik sendiri sudah marak digunakan di kalangan masyarakat, hal tersebut diperkirakan pada tahun 2024, 66% dari pengguna telepon genggam di dunia akan menggunakan data biometrik untuk fungsi keamanan maupun pembayaran.[[9]](#footnote-9) Dalam Pasal 1 Ayat 1 UU Perlindungan Data Pribadi (UU PDP), menyebutkan bahwa “Data pribadi didefinisikan sebagai data yang dapat digunakan untuk mengidentifikasi seseorang, baik secara terpisah maupun bersama dengan data elektronik atau non-elektronik lainnya.” Sehingga, data pribadi masuk dalam kategori data biometrik karena data pribadi juga mencakup sidik jari, wajah, tanda tangan, dan lain-lain.

Para pihak menandatangani perjanjian kontrak elektronik ini dengan menggunakan metode elektronik. Kemajuan teknologi digital memungkinkan setiap individu atau badan hukum untuk membuat kontrak tanpa harus bertemu langsung. Kontrak dapat dilaksanakan secara elektronik, misalnya melalui penggunaan komputer, jaringan komputer, internet, atau media lainnya.[[10]](#footnote-10) Syarat sahnya suatu perjanjian menurut hukum positif Indonesia. Menurut Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPer): “Suatu perjanjian adalah sah apabila memenuhi syarat-syarat sebagai berikut: kesepakatan, kecakapan untuk membuat perikatan, suatu hal tertentu, dan sebab yang halal.”

Pentingnya memahami pasal ini karena syarat-syarat tersebut menentukan sah tidaknya sebuah perjanjian. Pada kenyataannya, melanggar salah satu syarat tersebut dapat memiliki konsekuensi hukum yang signifikan, seperti pembatalan perjanjian atau biasa disebut batal demi hukum. Akibatnya, mempelajari Pasal 1320 KUHPer ini sangat penting untuk memahami dasar hukum yang mengatur hubungan kontraktual di Indonesia. Pada Pasal 46 Ayat (2) PP Nomor 71 Tahun 2019[[11]](#footnote-11), diatur bahwa; “Perjanjian elektronik memiliki kekuatan hukum yang sama dengan perjanjian yang dibuat secara tertulis.” Hal ini menunjukkan bahwa perjanjian elektronik diakui secara hukum di Indonesia, asalkan memenuhi syarat-syarat tertentu.

Keabsahan kontrak yang menggunakan otentikasi biometrik, perlu adanya kepatuhan terhadap peraturan perlindungan data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan hak kepada individu untuk melindungi data pribadinya, termasuk data biometrik. Oleh karena itu, proses pengumpulan dan penggunaan data biometrik harus dilakukan secara transparan dan dengan persetujuan yang jelas dari individu tersebut.[[12]](#footnote-12) Jika tidak, dapat timbul masalah hukum terkait keabsahan kontrak tersebut. Transaksi elektronik, yang mengarah pada kontrak yang bersifat elektronik, adalah fenomena baru yang tidak dapat dihindari oleh hukum. Oleh karena itu, transaksi elektronik juga mengandung unsur hukum yang terlihat dalam kontrak atau perjanjian. Karena secara umum diterima bahwa perjanjian atau kontrak merupakan "hukum" bagi para pihak yang terlibat, keberadaannya merupakan faktor yang paling signifikan dalam transaksi pedagang. Menurut Perdata, Pasal 1338 KUHPerdata menyatakan bahwa;

“1. Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya;

1. Perjanjian tidak boleh bertentangan dengan undang-undang, ketertiban umum, atau kesusilaan;
2. Setiap orang yang membuat perjanjian wajib untuk mematuhi isi perjanjian tersebut.”

Pasal ini menegaskan bahwa kontrak atau perjanjian yang dibuat secara sah harus dihormati dan diikuti oleh belah pihak terlibat, juga tidak harus bertentangan dengan standar hukum saat ini. Konsensualitas merupakan prinsip penting dalam hukum perdata. Asas konsensualisme terjadi sejak tercapai kata-kata yang disepakati oleh kedua belah pihak yang terlibat dalam suatu perjanjian, dengan maksud bahwa perjanjian tersebut telah diakui secara hukum dan memiliki konsekuensi hukum karena kedua belah pihak mencapai kesepakatan mengenai ketentuan-ketentuannya yang telah dibuat.[[13]](#footnote-13) Para pihak harus memberikan persetujuan yang jelas dan tanpa paksaan untuk menggunakan otentikasi biometrik. Jika ada unsur paksaan atau penipuan dalam proses persetujuan ini, maka kontrak dapat dianggap tidak sah.

Penggunaan biometrik harus diinformasikan secara jelas kepada semua pihak yang terlibat. Misalnya, prosedur pengumpulan data biometrik dan cara penyimpanannya harus dijelaskan dengan rinci. Jika informasi ini tidak disampaikan dengan baik, maka dapat menimbulkan sengketa di kemudian hari mengenai keabsahan kontrak. Undang-Undang PDP dibuat dengan tujuan memberikan perlindungan hukum yang kuat terhadap informasi pribadi masyarakat. Ini akan memastikan bahwa ada kepastian hukum yang mampu menjamin masalah tersebut, memberikan rasa keadilan kepada korban dan pelaku penyalahgunaan data pribadi.[[14]](#footnote-14) Sistem biometrik harus dilengkapi dengan teknologi keamanan seperti enkripsi untuk melindungi data. Selain itu, pelatihan bagi pengguna juga penting untuk mengurangi kesalahan dalam penggunaan teknologi ini.

Penyalahgunaan teknologi biometrik juga menimbulkan isu privasi dan rentan akan perlindungan data pada korban. Data biometrik adalah informasi sensitif yang harus dikelola dengan hati-hati untuk menghindari penyalahgunaan. Dasar hukum untuk menjaga keamanan data pribadi disediakan oleh Undang-Undang PDP Indonesia, tetapi implementasinya dalam konteks otentikasi biometrik masih memerlukan perhatian lebih. Penggunaan data biometrik tanpa persetujuan yang jelas dari individu dapat berpotensi melanggar hak-hak privasi mereka, sehingga menimbulkan risiko terhadap keabsahan kontrak. Informasi pribadi yang terkait dengan privasi merupakan hak asasi manusia yang mendasar. Perlindungan informasi pribadi menjadi komponen otonomi dan harga diri pribadi.[[15]](#footnote-15)

Teknologi yang memungkinkan penyebaran data informasi dengan cepat dan mudah, tidak ada batasan bagi siapa pun untuk memiliki kontrol atas datanya. Akibatnya, ada kemungkinan pihak lain akan melakukan pelanggaran. Pengaruh dari pelanggaran data pribadi yaitu pelanggaran data pribadi tidak hanya melukai korban secara materil, tetapi juga melukai reputasi dan harga dirinya. Untuk mengevaluasi dampak penggunaan teknologi biometrik terhadap kerangka hukum yang ada, pendekatan hukum yang cermat diperlukan. Regulasi yang tepat diperlukan untuk menyeimbangkan antara kebutuhan akan keamanan dan perlindungan hak-hak individu.[[16]](#footnote-16)

Data pribadi digolongkan menjadi dua penggolongan, yang terdiri dari data umum dan spesifik yang harus dipertimbangkan kembali. Dikarenakan pemrosesan data pribadi dipengaruhi secara tidak langsung. Dengan demikian, terdapat perbedaan yang jelas antara data generik dan data khusus, termasuk data biometrik, dalam instrumen hukum internasional seperti *General Data Protection Regulation* (GDPR), *Oraganisation for Economic Co-Operation*(OECD), dan dokumen hukum Indonesia. Pemisahan yang disebutkan di atas merupakan cara untuk melindungi data umum dan khusus, khususnya data biometrik, yang merupakan representasi dari “keunikan biologis individu” yang membuatnya tidak mungkin digantikan oleh orang lain.[[17]](#footnote-17) Menurut Pasal 1 Ayat 2 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi:

“Data Pribadi adalah setiap data yang berkaitan dengan individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, termasuk tetapi tidak terbatas pada nama, alamat, nomor identitas, dan data lainnya.”

Untuk memastikan hak konstitusional individu yang memberikan data pribadi, perlindungan data pribadi mencakup semua upaya untuk melindungi data pribadi selama pemrosesan..[[18]](#footnote-18)

Kekhawatiran lain terkait keabsahan kontrak adalah kemungkinan kesalahan teknis dalam proses otentikasi biometrik. Meskipun teknologi ini dirancang untuk akurasi tinggi, faktor-faktor seperti kondisi fisik individu atau gangguan teknis dapat menyebabkan kegagalan dalam verifikasi identitas. Jika terjadi kesalahan dalam proses otentikasi yang menyebabkan seorang individu tidak dapat mengakses kontrak atau melakukan transaksi, hal ini dapat menimbulkan sengketa hukum mengenai keabsahan tindakan tersebut. Penyelesaian sengketa diatur dalam Pasal 38 sampai 39 UU ITE[[19]](#footnote-19), Pasal 38 berbunyi;

“(1) Penyelenggara sistem elektronik wajib menjaga kerahasiaan informasi dan data pribadi yang diolahnya. (2) Kerugian yang timbul akibat tidak terjaganya keamanan data pribadi menjadi tanggung jawab penyelenggara sistem elektronik.”

Tanggung jawab penyelenggara sistem elektronik untuk menjamin keamanan informasi dan data pribadi yang diolah dijelaskan dalam pasal ini. Penyelenggara sistem elektronik bertanggung jawab atas kemungkinan terjadinya pelanggaran data dan wajib menjaga kerahasiaan dan integritas data pribadi. Sedangkan, pasal 39 UU ITE berbunyi:

“(1) Gugatan perdata diajukan sesuai dengan ketentuan peraturan perundang-undangan.(2) Para pihak dapat menyelesaikan perselisihan melalui arbitrase atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan, selain gugatan perdata sebagaimana dimaksud pada ayat (1).”

Tugas penyelenggara sistem elektronik jika terjadi penyalahgunaan atau kebocoran data dijelaskan dalam pasal ini. Penyelenggara bertanggung jawab atas segala pelanggaran dan harus mengambil tindakan pencegahan yang diperlukan untuk mengamankan data. Tidak mematuhi ketentuan perlindungan data juga akan dihukum. Contoh langsung dari klausula yang dilarang dalam kontrak elektronik adalah sebagai berikut: Jika ada kerusakan yang terjadi selama pengiriman, penjual tidak bertanggung jawab.; pihak lain yang berafiliasi dengan pengelola situs dapat menggunakan data pribadi; salah satu pihak tidak bertanggung jawab atas kebocoran data pribadi; dan kebijakan dapat diubah tanpa pemberitahuan sebelumnya.[[20]](#footnote-20) Untuk memastikan bahwa kontrak yang menggunakan otentikasi biometrik diakui dan sah secara hukum, regulasi yang jelas diperlukan mengenai pengaplikasian teknologi ini. Pengaturan tentang bagaimana data biometrik dikumpulkan, disimpan, dan digunakan sangat penting untuk memberikan perlindungan bagi semua pihak yang terlibat[[21]](#footnote-21). Dengan adanya regulasi yang tepat dan pemahaman yang baik tentang teknologi biometrik, diharapkan keabsahan kontrak dapat terjamin dalam konteks transaksi elektronik di masa depan.

Penyalahgunaan data biometrik dalam transaksi elektronik dapat menimbulkan risiko signifikan yang berdampak pada keabsahan kontrak. Data biometrik, seperti sidik jari atau pemindaian wajah, merupakan informasi sensitif yang dapat digunakan untuk membedakan orang yang unik. Namun, jika data ini tidak dikelola dengan baik, risiko kebocoran dan penyalahgunaan meningkat, yang pada gilirannya dapat memengaruhi keabsahan kontrak yang didasarkan pada otentikasi biometrik. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengumpulan dan pemrosesan data biometrik hal yang perlu diperhatikan dengan kehati-hatian yang tinggi dan melalui mekanisme yang jelas untuk melindungi hak privasi individu[[22]](#footnote-22).

Terlepas dari ada kemungkinan kekhawatiran yang perlu diperhatikan, perolehan data pribadi ini biasanya dilakukan untuk tujuan bisnis dan pemasaran yang sah..[[23]](#footnote-23) Salah satu masalah utama terkait penyalahgunaan data biometrik adalah potensi terjadinya diskriminasi dan kesalahan identifikasi. Misalnya, kesalahan identifikasi yang mahal dapat diakibatkan oleh sidik jari yang rusak atau wajah yang ditutupi.[[24]](#footnote-24) Ketika sistem otentikasi biometrik gagal mengenali individu secara akurat, hal ini dapat menyebabkan penolakan akses atau kesalahan dalam pengesahan identitas. Dalam konteks kontrak, kesalahan ini dapat mengakibatkan ketidakpastian hukum dan sengketa antara pihak-pihak yang terlibat. Sebagai contoh, jika seseorang tidak dapat mengakses layanan karena kesalahan dalam pengenalan biometrik, mereka mungkin kehilangan hak atau manfaat yang seharusnya diterima berdasarkan kontrak tersebut.

Penyalahgunaan data biometrik memiliki potensi untuk melakukan penipuan dan pencurian identitas. Orang-orang yang tidak berwenang dapat menggunakan data biometrik untuk bertindak melanggar hukum, seperti membuka rekening bank atau melakukan transaksi tanpa sepengetahuan pemilik data. Hal ini membahayakan integritas sistem transaksi elektronik secara keseluruhan, bukan hanya individu. UU ITE, Indonesia mengatur perlindungan informasi pribadi dan menetapkan hukuman atas pelanggaran yang menyebabkan seseorang menderita kerugian.. Tingkat pengetahuan tentang data pribadi berdasarkan kelompok umur menunjukkan bahwa masyarakat semakin memperhatikan data pribadi, baik umum maupun khusus, seiring bertambahnya usia.

Dengan 96,6%, generasi boomer merupakan yang paling berpengetahuan tentang data pribadi, sementara Gen Z memiliki persentase terendah yaitu 91,1%.[[25]](#footnote-25) Hampir setiap rentang usia tahu banyak tentang data pribadi umum, termasuk NIK dan nomor ponsel; generasi boomer, bagaimanapun, adalah yang paling tahu tentang NIK (91,1%) dari semua kelompok usia. Pengetahuan tentang data pribadi juga serupa. Semua kelompok usia menganggap data finansial dan perbankan sebagai yang paling terkenal, termasuk data pribadi khusus. Namun, Gen Z dan Gen Y menganggap data biometrik, seperti sidik jari, wajah, dan tinggi badan, sebagai yang paling diketahui, termasuk data pribadi khusus.[[26]](#footnote-26)

Undang-Undang ITE yang baru dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelaksanaan UU ITE, keduanya memuat ketentuan tentang perlindungan data pribadi di Indonesia. UU ITE yang baru-baru ini disahkan menetapkan hak dan tanggung jawab terkait data pribadi, termasuk data biometrik, dan memberikan sanksi atas penggunaan data tersebut secara tidak sah. Sesuai dengan batasan yang diuraikan dalam UU ITE yang baru, penggunaan data biometrik secara tidak benar dalam transaksi keuangan dapat menjadi pelanggaran dan mengakibatkan sanksi.[[27]](#footnote-27) Namun, UU ITE hanya melindungi data biometrik jika diproses melalui sistem elektronik, yaitu dokumen atau informasi elektronik. Kejahatan komputer dan dunia maya, termasuk penipuan, penggelapan, peretasan, komunikasi, perusakan sistem, dan pelanggaran hak kekayaan intelektual, merupakan penekanan utama undang-undang ITE.[[28]](#footnote-28) Undang-undang Nomor 27 Tahun 2022 (UU PDP) mendefinisikan data biometric sebagai salah satu jenis data pribadi spesifik. Pada pasal 4 ayat (2) UU PDP, menyebutkan bahwa:

“ Data Pribadi yang bersifat spesifik sebagaimana dimaksud pada ayat (l) huruf a meliputi: a. data dan informasi kesehatan; b. data biometrik; c. data genetika; d. catatan kejahatan; e. data anak; f. data keterangan pribadi; dan/ atau g. data lainnya sesuai dengan ketentuan peraturan perundang-undangan.”

Dikarenakan data biometrik dapat menghasilkan efek yang lebih besar kepada subyek pribadi dan memiliki karakteristik yang unik sehingga membutuhkan perlindungan tambahan. Pada sisi lain, aturan UU PDP berfokus pada perlindungan data pribadi milik entitas individu (individu alami), sehingga mencakup hak untuk menghormati kehidupan pribadi makhluk hidup.[[29]](#footnote-29) Meskipun data biometrik pada dasarnya dilindungi oleh UU ITE dan UU PDP, cara penanganan dan pemanfaatan data tersebut berbeda-beda. Perbedaan ini terjadi karena UU ITE dibuat sebagai sarana bagi penegak hukum siber untuk menanggapi berbagai jenis kejahatan daring..[[30]](#footnote-30)

Kesalahan identifikasi dan penipuan merupakan risiko yang signifikan dalam penggunaan data biometrik dalam transaksi elektronik. Jika data biometrik yang digunakan tidak akurat atau telah disalahgunakan, maka identitas pihak yang terlibat dalam kontrak tidak dapat dipastikan dengan jelas. Hal ini dapat menyebabkan kesalahan identifikasi yang berdampak pada keabsahan kontrak. Akibatnya, pemrosesan data dari informasi yang sebelumnya diklasifikasikan hanya dapat digunakan dalam keadaan tertentu, seperti untuk kebutuhan publik, kesehatan, atau keuangan, atau dengan persetujuan tegas dari pemilik data.[[31]](#footnote-31) Selain itu, penipuan yang dilakukan menggunakan data biometrik palsu dapat mengakibatkan kontrak yang dibuat berdasarkan profil palsu tersebut tidak sah. Misalnya, jika seseorang menggunakan sidik jari palsu untuk membuka akun bank online, maka transaksi yang dilakukan dari akun tersebut tidak dapat diakui sebagai sah karena identitas yang digunakan tidak benar. Dengan demikian, kesalahan identifikasi dan penipuan dapat mengganggu proses pembentukan kontrak dan memengaruhi keabsahan kontrak dalam transaksi elektronik. PT Kereta Api Indonesia (PT KAI) selama ini telah memberikan layanan publik di Indonesia dengan memanfaatkan data biometrik dan pengenalan wajah. Namun, 16 Januari 2024, sekelompok peretas menyatakan telah berhasil membobol data khusus PT KAI, dengan informasi sebagai berikut: "Memo umum KAI.ID dapat ditemukan di sini! Harganya 11,69 Bitcoin."[[32]](#footnote-32)

Autentikasi terhadap pengguna adalah salah satu metode perlindungan data yang memungkinkan sistem untuk mengidentifikasi identitas pengguna dan memberikan hak akses yang tepat. Proses validasi yang dilakukan oleh user saat memasuki sistem dikenal sebagai autentikasi. Proses yang mengecek langsung ke daftar orang yang memiliki akses ke sistem mengecek nama dan *password user*. Kemampuan untuk memverifikasi bahwa data yang dikirim dan diterima identik dan bahwa orang yang mengaku sebagai pengirim adalah pengirim yang sebenarnya. Tujuan autentikasi adalah untuk memverifikasi identitas Anda.Apakah itu tepat atau tidak.[[33]](#footnote-33) Jika terjadi kerugian akibat penggunaan otentikasi biometrik, maka klausul tanggung jawab harus jelas dalam kontrak. Biometrik dapat menawarkan tingkat keamanan yang lebih tinggi daripada teknik autentikasi tradisional dengan memanfaatkan ciri fisik atau perilaku khas seseorang, seperti wajah atau sidik jari. Meskipun belum sempurna, penggunaan biometrik sebagai langkah keamanan tambahan dapat membantu melindungi informasi pribadi dan mengurangi kemungkinan terjadinya serangan penipuan.[[34]](#footnote-34)

Jaminan agar data biometrik tidak dieksploitasi, sanksi hukum yang tegas harus diterapkan. Setiap individu yang dengan sengaja dan melanggar hukum mendapatkan atau mengumpulkan data pribadi dianggap melanggar UU PDP dengan tujuan kepentingan pribadi diancam dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp5 miliar (Pasal 67 ayat (1) UU PDP). Dengan adanya permasalahan tersebut penulis ingin memperdalam masalah yang muncul ketika teknologi biometrik digunakan dalam transaksi elektronik, sangat penting untuk mempertimbangkan bagaimana hukum perdata mengatur keabsahan kontrak yang menggunakan otentikasi biometrik. Meski teknologi biometrik menawarkan keamanan tambahan, risiko-risiko spesifik patut dipertimbangkan agar validitas kontrak tidak terancam. Keabsahan kontrak tidak hanya bergantung pada kesepakatan antara pihak-pihak yang terlibat, tetapi juga pada kejelasan identitas mereka yang diotentikasi melalui metode biometrik. Namun, risiko mencakup data biometrik, seperti kesalahan identifikasi dan penipuan, dapat mengancam validitas kontrak tersebut. Data biometrik dapat mengidentifikasi seseorang seumur hidup, jadi membuat database biometrik sulit..[[35]](#footnote-35)

1. **Rumusan Masalah**
2. Bagaimana hukum perdata mengatur keabsahan kontrak yang menggunakan otentikasi biometrik?
3. Bagaimana resiko penyalahgunaan data biometrik dapat memengaruhi keabsahan kontrak dalam transaksi elektronik?
4. **Tujuan Penelitian**
5. Untuk menganalisis keabsahan kontrak yang menggunakan otentikasi biometrik dalam hukum perdata.
6. Untuk menganalisis resiko penyalahgunaan data biometric dapat mempengaruhi keabsahan kontrak dalam transaksi elektronik.
7. **Urgensi Penelitian**

Penelitian ini memiliki urgensi yang signifikan dalam memahami pengaruh teknologi biometrik dalam otentikasi transaksi elektronik terhadap keabsahan kontrak dalam hukum perdata. Dengan meningkatnya adopsi teknologi ini oleh berbagai perusahaan, penting bagi pelaku bisnis dan konsumen untuk mendapatkan kepastian hukum terkait penggunaannya. Penelitian ini tidak hanya bertujuan untuk mengidentifikasi dampak teknologi biometrik terhadap keabsahan kontrak, tetapi juga untuk memberikan wawasan mengenai bagaimana tanggung jawab hukum dapat ditegakkan apabila terjadi penyalahgunaan data biometrik. Dengan pemahaman yang mendalam tentang langkah-langkah yang diperlukan agar penggunaan teknologi ini sah dan sesuai dengan persyaratan undang-undang yang berlaku, penelitian ini diharapkan dapat mendukung praktik bisnis yang etis dan aman, serta berkontribusi pada pengembangan regulasi yang lebih efektif dalam era digital yang semakin kompleks.

1. **Tinjauan Pustaka**
2. Ardi Nur Abdul Hakim (2022) dengan judul *“Keabsahan Dan Kekuatan Hukum Tanda Tangan Elektronik Untuk Legalitas Berdasarkan Undang-Undang Ite Dan Kuhperdata“*Skripsi Ilmu Hukum Universitas Muhammadiyah Sumatera Utara.[[36]](#footnote-36) Menurut skripsi ini, tanda tangan elektronik harus memenuhi sejumlah persyaratan agar dianggap sah menurut hukum. Persyaratan ini meliputi autentikasi dokumen, yang memverifikasi bahwa dokumen digital tersebut asli setelah ditandatangani dan bahwa penanda tangan yang tercantum di dalamnya benar-benar memiliki tanda tangan elektronik, dan autentikasi pemilik, yang memverifikasi bahwa dokumen digital tersebut asli dan tidak dapat dipalsukan. Yang membedakan skripsi ini dengan penelitian penulis yaitu penelitian penulis hanya berbicara tentang keabsahan kontrak dalam hukum perdata, serta penulis akan membahas tentang Biometrik bukan berfokus pada tanda tangan elektronik saja.
3. Patricia Edina Sembiring, Ahmad M. Ramli, dan Laina Rafianti (2024) denga judul *“Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik”* Artikel Hukum Universitas Padjadjaran, Volume 10, Nomor 1, 2024[[37]](#footnote-37) membahas mengenai perlindungan privasi pengguna, keamanan data biometrik menjadi penting. Data biometrik dikategorikan sebagai data khusus berdasarkan Undang-Undang Perlindungan Data Pribadi (UU), artinya karena sifat individu yang tidak dapat dipertukarkan, maka perlu perlindungan lebih lanjut saat diproses. Artikel ini juga membahas mengenai sudut pandang Undang-Undang Informasi-Transaksi Elektronik dan UU Perlindungan Data Pribadi, data biometrik dianggap sebagai data khusus, dan solusi teknis melalui gagasan desain privasi untuk melindungi data biometrik. Yang membedakan artikel ini dengan penelitian penulis yaitu penulis membahas resiko penyalahnagunaan data dapat memengaruhi keabsahan kontrak dalam transaksi elektronik dan perlindungan hukum yang diberikan jika masalah itu terjadi.
4. **Metode Penelitian**
5. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian kepustakaan, juga dikenal sebagai *library reseacrh[[38]](#footnote-38)*. Penelitian kepustakaan atau *(library research)* yaitu penelitian dapat diperoleh melalui penelusuran dokumen. Penelitian kepustakaan atau *(library research)* merupakan penelitian yang dilakukan dengan meneliti bahan- bahan sekunder atau data kepustakaan.[[39]](#footnote-39). Penulis menggunakan metode penelitian kepustakaan *(library research)* karena sumber data tidak selalu dapat ditemukan di lapangan. Sumber data dapat diperoleh dari literatur, jurnal, peraturan perundang-undangan, atau skripsi yang berkaitan dengan topik skripsi. Akibatnya, teknik umum seperti memilih teori secara sistematis, mencari materi di perpustakaan, dan memeriksa makalah yang berisi informasi yang berkaitan dengan topik penelitian semuanya termasuk dalam studi kepustakaan.[[40]](#footnote-40) Selain itu, penulis memiliki keterbatasan waktu dan dana untuk menyelesaikan skripsi.

1. Pendekatan Penelitian

Metode yang digunakan penulis adalah metode normative. Metode ini dilakukan dengan meneliti dan mengkaji hukum sebagai norma, aturan, asas hukum, doktrin hukum, teori hukum, dan berbagai literatur lainnya untuk membahas masalah hukum yang diteliti.[[41]](#footnote-41) Penelitian hukum normatif terkadang disebut sebagai penelitian kepustakaan atau penelitian hukum doktrinal. Penelitian hukum melihat sumber pustaka atau data sekunder, seperti undang-undang *(statute approach)* dan literatur tentang isu yang diteliti *(conceptual approach)*.[[42]](#footnote-42) Pemeriksaan data sekunder atau sumber pustaka, termasuk dokumen hukum primer, sekunder, dan tersier, merupakan bagian dari penelitian.[[43]](#footnote-43)

1. Data Penelitian

Sumber data yang digunakan oleh penulis merupakan sumber data sekunder. Bukti historis, catatan, buku, atau arsip adalah sumber data sekunder. ada penelitian hukum normative, hukum sering digambarkan sebagai apa yang tertulis dalam undang-undang (*law in books)* atau sebagai standar yang menetapkan perilaku manusia yang dianggap baik.[[44]](#footnote-44) Akibatnya, sumber data terbatas pada data sekunder, yang mencakup teks hukum tersier, sekunder, dan primer.

1. Bahan Hukum Primer, merupakan bahan hukum yang mengikat terdiri dari;
2. Undang-Undang Dasar Tahun 1945;
3. Kitab Undang-Undang Hukum Perdata;
4. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE);
5. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi;
6. Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
7. Bahan hukum sekunder adalah bahan hukum yang menjelaskan abahn hukum primer, contohnya temuan dalam penelitian dan pendapat para ahli hukum. Dokumen hukum sekunder memberikan penjelasan yang lebih menyeluruh tentang standar hukum yang ada, bukan mengatur atau menciptakan standar hukum baru.
8. Bahan hukum tersier adalah bahan yang mendukung dan menjelaskan bahan hukum primer dan sekunder.
9. Metode Pengumpulan Data

Metode pengumpulan data pada skripsi ini menggunakan studi pustaka *(literature)* yaitu penelitian ini didasarkan pada undang-undang, buku, studi ilmiah, media massa, dan jurnal hukum yang berkaitan dengan topik skripsi ini.[[45]](#footnote-45) Data pustaka biasanya merupakan sumber sekunder, artinya peneliti mendapatkan bahan dari sumber kedua daripada data asli dari tangan pertama di lapangan.[[46]](#footnote-46) Setelah sumber dipilih, penulis akan membaca secara teliti dan merekap data penting yang berkaitan langsung dengan permasalahan yang penulis teliti. Menurut Soerjono Soekanto[[47]](#footnote-47), penelitian juga dikenal sebagai tiga kategori alat untuk mengumpulkan data: pengamatan, studi dokumen atau bahan pustaka, dan wawancara. Sehingga, pada penelitian ini menggunakan studi dokumen atau bahan Pustaka dan pengamatan sebagai alat pengumpulan data. Studi literatur adalah cara yang efektif dan efisien untuk mengumpulkan data dalam penelitian. Ini memberikan peneliti landasan teoritis yang kuat sebelum melanjutkan penelitian mereka. Dengan menggunakan kata kunci tertentu dalam katalog perpustakaan atau mesin pencari, peneliti mencari sumber yang relevan.

1. Metode Analisis Data

Penelitian ini menggunakan pendekatan kualitatif, yaitu metode penelitian yang mengumpulkan data deskriptif berdasarkan pengamatan terhadap individu dan perilaku mereka..[[48]](#footnote-48) Analisis kualitatif digunakan dalam penelitian hukum normative karena mengutamakan kualitas atau mutu data daripada kuantitas. Ini karena metode data kualitatif lebih mengutamakan kualitas daripada kuantitas.[[49]](#footnote-49) Selanjutnya, data yang telah dikumpulkan diubah menjadi data kualitatif, yang digunakan untuk memeriksa konsep dan prinsip hukum yang relevan, seperti interpretasi dan konstruksi hukum.[[50]](#footnote-50) Kemudian, metode kualitatif digunakan untuk membuat kesimpulan yang umum tentang masalah dan tujuan penelitian pengaruh teknologi biometric dalam otentikasi transaksi elektronik terhadap keabsahan kontrak perspektif hukum perdata. Penelitian ini bertujuan untuk menjawab keragu-raguan tentang kebenaran pengetahuan yang dimiliki penulis.[[51]](#footnote-51) Penelitian kualitatif merupakan salah satu jenis penelitian yang berupaya menginterpretasikan fakta atau realitas secara tepat.[[52]](#footnote-52) Metode penelitian ini memungkinkan peneliti untuk mendapatkan pemahaman yang lebih mendalam tentang subjek penelitian. Peneliti dapat menemukan makna di balik fenomena sosial dengan menggunakan metode pengumpulan dan analisis data yang sistematis. Hasilnya akan memberikan wawasan yang berguna untuk pembangunan praktik atau kebijakan masyarakat.

1. **Sistematika Penulisan**

Sistematika penulisan proposal ini terdiri dari 4 bagian bab sebagai tahapan di dalam penulisan, yaitu :

BAB I PENDAHULUAN, menguraikan tentang latar belakang masalah, rumusan masalah, tujuan penelitian manfaat penelitian, tinjauan pusataka, metode penelitian, sistematika penulisan skripsi.

BAB II TINJAUAN KONSEPTUAL, menguraikan tentang tinjauan umum pengaruh teknologi biometrik dalam otentikasi transaksi elektronik terhadap keabsahan kontrak perspektif hukum perdata.

BAB III HASIL PENELITIAN dan PEMBAHASAN, hasil rumusan masalah tentang pembahasan mengenai pengaruh teknologi biometrik dalam otentikasi transaksi elektronik terhadap keabsahan kontrak perspektif hukum perdata.

BAB IV PENUTUP, memuat simpulan dari hasil rumusan masalah yang akan dihadapi selama penelitian, pernyataan penulis, dan saran.

**BAB II**

**TINJAUAN KONSEPTUAL**

1. **Tinjauan tentang Pengertian dan Konsep Teknologi Biometrik dalam Otentikasi Transaksi Elektronik**
2. **Pengertian Teknologi Biometrik**

Teknologi biometrik menggunakan karakteristik fisik atau perilaku unik seseorang untuk mengidentifikasi dan memverifikasi individu. Dalam bahasa Yunani, “biometrik” diperoleh dari kata *“bios”,* yang berarti “kehidupan,” dan *“metrik”,* yang memiliki arti “pengukuran.”. Di antara berbagai jenis teknologi biometrik yang paling umum diterapkan adalah sidik jari dan pengenalan wajah. Setiap metode biometrik memiliki keunikan dan keunggulan tersendiri, yang membuatnya cocok untuk aplikasi tertentu. Biometrik mengevaluasi ciri-ciri individu untuk membedakan setiap orang, yang membuat mereka berpotensi lebih berhasil dalam mengidentifikasi orang.[[53]](#footnote-53) Dengan menggunakan teknologi ini, keamanan sistem dapat ditingkatkan secara signifikan, meminimalisir risiko pengambilalihan identitas dan akses tidak sah.[[54]](#footnote-54) Selain itu, teknologi biometrik juga menawarkan kemudahan akses bagi pengguna, yang tidak perlu mengingat kata sandi atau PIN.[[55]](#footnote-55) Teknologi biometrik memantau dan mengevaluasi ciri-ciri fisiologis dan perilaku manusia saat digunakan untuk identifikasi pribadi.[[56]](#footnote-56) Mengukur secara langsung tangan, ujung jari, wajah, dan retina serta iris mata seseorang untuk menentukan ciri fisiologisnya*.*[[57]](#footnote-57)Karakteristik biometrik dapat dijelaskan sebagai berikut:

1. Karakteristik Fisik

Karakteristik fisik adalah fitur biologis yang dapat diukur dan diidentifikasi dari tubuh seseorang yang digunakan sebagai tanda pengenal khusus dalam sistem biometrik. Contoh karaktersitik fisik dalam biometrik meliputi sidik jari, pengenalan wajah, iris mata, dan suara.

1. Karakteristik Perilaku

Karakteristik perilaku adalah fitur yang menggunakan pola tindakan atau kebiasaan individu sebagai kode unik untuk pengenalan pada sitem biometrik. Contoh karakteristik perilaku dalam biometrik meliputi ritme mengetik, tanda tangan, dan suara (logat biacara seseorang berbeda-beda).

Perubahan teknologi ini juga memilki relevansi yang penting dalam konteks hukum. Sistem hukum juga harus mampu beradaptasi dengan kemajuan teknologi untuk menangani tantangan dan risiko yang mucul. Perlindungan privasi, pemgaturan kebebasan berekspresi, pertanggungjawaban hukum, dan perlindungan konsumen adalah beberapa area yang terpengaruh oleh perubahan teknologi dalam konteks hukum agar dapat mengembangkan kebijakan yang tepat dan memastikan perlindungan hukum yang memadai di era teknologi yang terus berkembang.[[58]](#footnote-58) Selain itu, terdapat juga peraturan pemerintah yang lebih khusus mengatur tentang perlindungan hak digital dalam, seperti yang diatur dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang “Penyelenggaraan Sistem dan Transaksi Elektronik”.[[59]](#footnote-59)

Kemampuan untuk mengumpulkan dan menyimpan data pribadi dalam jumlah besar merupakan perkembangan teknologi yang signifikan dalam hal perlindungan privasi. Berdasarkan Pasal 28G Ayat (3) UUD 1945 menyatakan bahwa:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Informasi pribadi termasuk dalam data pribadi, seperti nama, alamat, nomor telepon, data keuangan, sejarah kesehatan, kebiasaan berbelanja, dan sebagainya. Seiring kemajuan teknologi, kini mudah untuk mengumpulkan informasi pribadi melalui berbagai metode, termasuk formulir daring, transaksi elektronik, biometrik, dan jejak digital yang ditinggalkan individu selama berinteraksi dengan dunia digital.[[60]](#footnote-60) Dengan meningkatnya kebutuhan akan keamanan dan perlindungan data, teknologi biometrik semakin banyak diterapkan dalam berbagai bidang, termasuk perbankan, keamanan, dan perangkat mobile.

Teknologi biometrik yang menggunakan karakteristik fisik atau perilaku individu untuk identifikasi dan verifikasi, memiliki keunggulan dan kelemahan yang perlu dipertimbangkan sebagai berikut;

1. Keunggulan Teknologi Biometrik
2. Karena ciri biometrik lebih sulit dipalsukan, biometrik menawarkan tingkat keamanan yang lebih baik daripada teknik yang lebih konvensional seperti kata sandi atau PIN.[[61]](#footnote-61)
3. Pengguna tidak perlu mengingat kata sandi atau PIN, sehingga proses autentikasi menjadi lebih cepat dan mudah.[[62]](#footnote-62)
4. Risiko penipuan dapat diminimalkan, karena identitas pengguna dapat diverifikasi secara akurat.
5. Proses autentikasi yang cepat dapat meningkatkan efisiensi dalam berbagai aplikasi, seperti akses ke perangkat, sistem keamanan, dan layanan keuangan.
6. Kelemaham Teknologi Biometrik
7. Pengumpulan dan penyimpanan data biometrik dapat menimbulkan masalah privasi, dan jika data ini bocor, individu dapat berisiko kehilangan privasi dan identitas.[[63]](#footnote-63)
8. Sistem biometrik tidak selalu akurat. Kesalahan identifikasi dapat terjadi, misalnya ketika sidik jari terluka atau wajah tertutup
9. Data biometrik yang tersimpan dalam sistem dapat menjadi target serangan siber.[[64]](#footnote-64)
10. **Konsep Teknologi Biometrik**

Kontrol akses digital dan fisik, serta identifikasi manusia, telah berhasil menggunakan teknologi biometrik. Teknologi biometrik ini mengidentifikasi orang dengan menggunakan ciri fisik atau perilaku mereka.[[65]](#footnote-65)

1. Pengenalan Sidik Jari *(Fingerprint Recognition).*

Sidik jari atau fingerprint merupakan identitas yang dimiliki manusia dan uniknya setiap manusia sidik jari semua orang di dunia berbeda satu sama lain.[[66]](#footnote-66) Identifikasi menggunakan sidik jari melalui akuisisi citra, tahapan preprosesing, ekstrasi ciri dengan metode fractal, dan terakhir adalah pencocokan.[[67]](#footnote-67) Jika sidik jari cocok, akses akan diberikan, sedangan jika data sidik jari tidak cocok, akses ditolak, menjadikan proses ini cepat dan efisien.

1. Pengenalan Wajah *(Face Recognition).*

Pengenalan wajah merupakan metode pengenalan yang menggunakan karakteristik fisik individu dari wajah seseorang, seperti bentuk wajah, struktur mata, hidung, dan bibir.[[68]](#footnote-68) Salah satu keunggulan pengenalan wajah adalah kemampuannya untuk berfungsi tanpa kontak fisik, sehingga meningkatkan kenyamanan pengguna. Namun, teknologi ini juga menghadapi tantangan terkait akurasi dan potensi kesalahan identifikasi.

1. Pengenalan Iris Mata *(Iris Recognition).*

Pengenalan iris adalah teknik autentikasi biometrik yang menggunakan algoritma pengenalan pola yang didasarkan pada foto beresolusi tinggi dari iris mata seseorang.[[69]](#footnote-69) Salah satu keuntungan utama pengenalan iris adalah stabilitasnya, atau umur panjang template, karena satu pendaftaran dapat bertahan seumur hidup.

1. Pengenalan Suara *(**Voice Recognition).*

Teknik dan sistem yang memungkinkan mesin atau komputer menerima dan mempelajari informasi dalam bentuk suara yang dikelompokkan menjadi kata-kata atau kalimat yang diucapkan disebut pengenalan ucapan, sering disebut sebagai *Voice Recognition*.[[70]](#footnote-70) Ada tiga metode pendekatan untuk pengenalan suara: pendekatan akustik-fonetik, pendekatan kecerdasan buatan, dan pendekatan pengenalan pola.[[71]](#footnote-71)

1. Pengenalan Tanda Tangan Elektronik *(**Handwriting Recognition).*

Pengenalan tanda tangan elektronik, juga dikenal sebagai *Handwriting Recognition*, adalah teknologi biometrik yang digunakan untuk mengidentifikasi seseorang berdasarkan tanda tangan mereka. Sistem biometrik analisis tulisan tangan dengan memperhatikan tindakan menulis, seperti tekanan, kecepatan, dan ritme.[[72]](#footnote-72)

"Perbuatan hukum yang dilakukan dengan menggunakan komputer, dan/atau media elektronik lainnya" adalah definisi transaksi elektronik menurut Pasal 1 angka 1 UU ITE. Tujuan dari regulasi ini adalah untuk melindungi hak konsumen dan memberi pelaku usaha dan konsumen keamanan hukum saat melakukan transaksi secara elektronik. Perbuatan hukum merupakan kegiatan yang dilakukan oleh subjek hukum dalam rangka memperoleh akibat hukum yang diinginkan, yaitu hak dan kewajiban yang dibebankan kepada orang yang melakukan perbuatan tersebut, misalnya nasabah dan pelaku usaha.[[73]](#footnote-73) Transaksi ini mencakup berbagai kegiatan seperti pembelian barang dan jasa secara online, pengiriman dokumen, serta interaksi bisnis lainnya yang dilakukan secara digital.[[74]](#footnote-74) Dengan demikian, transaksi elektronik merupakan bagian integral dari perkembangan teknologi informasi yang memudahkan interaksi bisnis dan konsumen di era digital saat ini.

1. **Peran Otentikasi dalam Transaksi Elektronik**

Otentikasi biometrik memainkan peran yang sangat penting dalam meningkatkan keamanan transaksi elektronik di era digital saat ini. Kinerja tinggi dan kemampuan beradaptasi terhadap berbagai skenario penggunaan dan keadaan lingkungan sangat penting untuk sistem biometrik.[[75]](#footnote-75) Autentikasi pengguna adalah proses yang digunakan untuk mengidentifikasi seseorang yang meminta akses ke sistem, jaringan, atau perangkat.[[76]](#footnote-76) Proses ini dikenal sebagai autentikasi pengguna.[[77]](#footnote-77) Setiap akses dan aktivitas dapat dicatat secara otomatis oleh sistem komputer, sehingga memudahkan pelacakan dan audit jika terjadi masalah atau pelanggaran keamanan. Penggunaan teknologi biometrik dalam transaksi elektronik membuat pengguna lebih aman.. Data biometrik dapat digunakan untuk melacak dan mengaudit transaksi, memberikan jejak yang jelas tentang siapa yang melakukan transaksi dan kapan, yang sangat berguna dalam investigasi jika terjadi pelanggaran.

Beberapa pihak, termasuk penyedia layanan, pengembang teknologi, pemerintah, dan pengguna, harus berkolaborasi untuk menjamin manfaat maksimal teknologi biometrik. Kerja sama ini diperlukan untuk menjamin bahwa teknologi tersebut dapat diandalkan, aman, dan sesuai dengan persyaratan dan harapan pengguna.[[78]](#footnote-78) Dengan hanya menambahkan sidik jari atau menatap kamera perangkat seluler, misalnya, biometrik membuat prosedur autentikasi menjadi cepat dan sederhana.[[79]](#footnote-79) Verifikasi identitas yang lebih akurat dan cepat dimungkinkan oleh sistem biometrik.[[80]](#footnote-80) Meskipun demikian, menjaga privasi data pribadi sulit, terutama mencegah penyadapan oleh pihak tak berwenang.[[81]](#footnote-81) Sehingga, penting untuk terus memperhatikan aspek privasi dan keamanan data dalam penerapannya.

Salah satu contoh penerapan teknologi biometrik adalah dalam proses verifikasi nasabah pada layanan perbankan digital. Teknologi biometrik digunakan oleh bank dan pemerintah Indonesia untuk meningkatkan keamanan transaksi nasabah. Faktor sosial dapat mendorong kejahatan, dan penegakan hukum yang lemah meningkatkan risiko, terutama dalam kasus penipuan perbankan.[[82]](#footnote-82) Dalam sektor perbankan, penerapan otentikasi biometrik telah terbukti efektif dalam melindungi data dan transaksi pelanggan. Dengan meningkatnya ancaman kejahatan siber, metode otentikasi konvensional semakin dianggap tidak memadai. Pada awal tahun 2018, terjadi pencurian informasi kartu debit melalui teknik skimming pada 64 bank di seluruh dunia, 13 di antaranya adalah bank pemerintah dan swasta di Indonesia.[[83]](#footnote-83) Dengan demikian, bank yang terkena dampak harus mengembalikan dana nasabah sebesar 18 miliar.[[84]](#footnote-84)

Otentikasi biometrik juga meningkatkan keamanan transaksi yang dilakukan secara online. Dengan meningkatnya penggunaan aplikasi mobile banking, penyedia layanan keuangan menghadapi masalah baru, sehingga banyak sektor perbankan menggunakan teknologi biometrik untuk meningkatkan kenyamanan dan keaman pengguna atau nasabah. Misalnya, saat melakukan pembelian di platform *e-commerce* atau transfer dana melalui aplikasi *mobile banking*, pengguna dapat menggunakan sidik jari atau pemindaian wajah untuk memverifikasi identitas individu.[[85]](#footnote-85) Karena akses yang sangat mudah dan jelas, pengguna tidak lagi perlu menginstal aplikasi atau pelatihan tambahan untuk penggunaan biometrik.[[86]](#footnote-86) Karena berbeda dengan metode otentikasi lainnya yang memerlukan berbagai prosedur verifikasi, seperti kata sandi dan QR.

1. **Hubungan antar Teknologi Biometrik dengan Keabsahan Kontrak**

Teknologi biometrik memiliki hubungan yang erat dengan keabsahan kontrak elektronik, terutama dalam konteks penggunaan tanda tangan elektronik. Autentikasi ini dapat digunakan untuk mengakses sistem yang aman dan sangat bermanfaat saat mengonfirmasi identitas untuk tanda tangan. Sebagai contoh, suatu organisasi dapat memastikan bahwa seseorang dapat menandatangani dokumen dari jarak jauh dengan menggunakan berbagai metode autentikasi biometrik. Autentikasi biometrik memungkinkan pengguna untuk menandatangani dokumen dari jarak jauh tanpa memerlukan ID fisik.[[87]](#footnote-87) Tanda tangan elektronik berkualitas (QES) memungkinkan pengesahan saksi jarak jauh dan verifikasi identitas fisik dengan tingkat keamanan yang samaTanda tangan elektronik yang menggunakan metode biometrik, seperti pemindaian wajah atau sidik jari, dapat digunakan untuk perjanjian sah menurut Pasal 1320 KUHPerdata, yang mencakup kesepakatan para pihak dan kecakapan hukum untuk membuat perjanjian. Sebagai contoh, metode ini digunakan oleh aplikasi digital seperti Form Digital FIFGroup untuk memastikan bahwa hukum yang berlaku berlaku untuk setiap jual beli online.[[88]](#footnote-88)

Undang-undang ITE dan Peraturan Pemerintah Nomor 71 Tahun 2019 mengatur tanda tangan elektronik di sistem hukum Indonesia.[[89]](#footnote-89) Pada Pasal 46 Ayat (2) PP 71/2019 menyatakan bahwa;

“ (2) Kontrak elektronik dianggap sah jika: a. terdapat kesepakatan antara para pihak; b. dilakukan oleh subjek hukum yang cakap atau yang berwenang mewakili sesuai dengan peraturan perundang-undangan; dan c. objek transaksi tidak boleh melanggar hukum, kesusilaan, atau ketertiban umum.”

Dalam artikel tersebut dijelaskan bahwa klausul baku yang digunakan dalam kontrak elektronik harus mematuhi peraturan perundang-undangan.[[90]](#footnote-90) Pasal 5 Ayat (1) Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik menyatakan bahwa:

“ 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 Undang-Undang ini.

4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku dalam hal diatur lain dalam Undang-Undang.”

Dengan pengakuan ini, pihak-pihak yang terlibat dalam transaksi elektronik memiliki jaminan hukum saat informasi dan dokumen elektronik digunakan dalam proses pembuktian di pengadilan.

1. **Aspek Hukum Perdata dalam Mengatur Penggunaan Teknologi Biometrik Terhadap Transaksi Elektronik**
2. **Implikasi Hukum dari Penggunaan Teknologi Biometrik dalam Hukum Perdata**

Teknologi biometrik mempunyai sistem otentikasi yang dapat meningkatkan keabsahan transaksi elektronik. Dalam sengketa hukum, dokumen transaksi elektronik juga bisa digunakan sebagai pembuktian di Pengadilan. Namun, perlu ada standar yang jelas mengenai data biometrik dikumpulkan, disimpan, dan digunakan untuk memastikan bahwa dokumen elektronik yang digunakan untuk pembuktian dapat diterima di Pengadilan. Misalnya, penghitung elektronik digunakan sebelum tanda tangan elektronik dalam perdagangan elektronik atau transaksi *e-commerce*, tanda tangan digital dalam pengiriman pesan, dan penawaran produk dan layanan digital.[[91]](#footnote-91) Informasi elektronik, dokumen elektronik, dan/atau hasil cetakannya adalah alat bukti yang sah menurut Pasal 5 ayat (1) UUITE yang telah dibahas sebelumnya. Pada Pasal 1875 Kitab Undang-Undang Hukum Perdata berbunyi;

“ Perjanjian yang dibuat dengan syarat atau cara yang tidak sesuai dengan ketentuan undang-undang adalah batal, kecuali apabila undang-undang menentukan lain. ”

Pasal ini menegaskan bahwa apabila suatu perjanjian dibuat dengan syarat atau cara yang melanggar ketentuan undang-undang, maka perjanjian tersebut dapat dianggap batal. Sehingga, keabsahan kontrak yang di tanda tangan secara elektronik didasarkan pada pengakuan orang yang membubuhakna tanda tanagn tersebut.[[92]](#footnote-92)

Penggunaan data biometrik sebagai data pribadi dalam hukum perdata menjadi penting terutama terkait dengan perlindungan privasi dan hak-hak inidividu. Implikasi hukum dari penggunaan teknologi biometrik juga mencakup tanggung jawab hukum bagi penyelenggara sistem. informasi biometrik sebagai informasi pribadi yang berbeda sesuai dengan peraturan Indonesia.[[93]](#footnote-93) Di era big data, data pribadi sangat berharga secara ekonomis, sehingga rentan untuk dimanipulasi untuk keuntungan pihak lain.[[94]](#footnote-94) Tindakan memperoleh, berbagi, menjual, dan memanfaatkan informasi yang bukan milik sendiri adalah bagian dari tindakan untuk mendapatkan keuntungan dari penyalahgunaan data pribadi.[[95]](#footnote-95) Contoh kasus penyalahgunaan atau pembobolan akun yaitu Peretas Bjorka yang mengaku menguasai 44 juta data MyPertamina, kemudian meminta pembayaran dalam bentuk Bitcoin senilai 25 ribu dolar, yang setara dengan Rp 392 juta..[[96]](#footnote-96)

Pengakuan hak pribadi sebagai hak asasi manusia dalam Pasal 28G Ayat (1) UUD 1945 adalah dasar dari kebutuhan untuk melindungi data pribadi:

“ Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi ”

Mayoritas individu menyadari hak-hak pribadi mereka yang tidak dibatasi secara hukum dan moral, termasuk hak privasi..[[97]](#footnote-97) Menurut KUHPerdata adalah benda, sehingga memiliki hak kebendaan dan hak relatif.[[98]](#footnote-98) Hak perdata absolut, yang memberikan otoritas langsung kepada subjek hukum, termasuk hak kebendaan dan hak untuk mempertahankan tuntutannya. Definisi lain dari hukum kebendaan adalah rangkaian peraturan yang menentukan hubungan hukum secara langsung antara individu dan bendanya. Karena adanya asas droit de suite, kepemilikan data pribadi dapat dipersamakan dengan hak kebendaan.

Terdapat empat kategori meliputi klasifikasi objek dalam Kitab Undang-Undang Hukum Perdata: komponen berwujud, tak berwujud, bergerak, dan tak bergerak. Ciri-ciri berikut mencirikan makna hak milik: 1) Hak yang tidak dapat dicabut yang dilindungi dari pihak ketiga; 2) Hak orang-orang yang bertanggung jawab atas sesuatu; 3) Dalam hal pembayaran utang, hak milik memberi orang kesempatan untuk memprioritaskan pembayaran utang; dan 4) Hak milik juga memberi orang kemampuan untuk menuntut.[[99]](#footnote-99) Sebab itu, dalam isi KUHPerdata tidak disebutkan bahwa informasi pribadi dapat digolongkan sebagai objek. Namun, karena data pribadi merupakan bagian dari data besar dan tidak memiliki bentuk atau nilai moneter yang nyata, maka pemiliknya berhak untuk menyimpannya. Pada pasal 1365 KUHPerdata berbunyi:

“ Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut ”.

Pasal ini mengatur tanggung jawab perdata yang timbul dari tindakan ilegal (seperti melakukan sesuatu yang menyebabkan cedera pada orang lain). Jika seseorang melakukan sesuatu yang salah dan merugikan orang lain, orang itu harus mengganti kerugian yang disebabkan oleh perbuatannya. Pasal ini menjadi dasar hukum dalam hal ganti rugi dan berhubungan erat dengan prinsip keadilan serta perlindungan hak-hak individu dalam sistem hukum Indonesia. Pihak yang merasa dirugikan atas PMH “perbuatan melawan hukum”, baik oleh Penyelenggara Sistem Elektronik maupun pihak ketiga, berhak untuk mengajukan tuntutan ganti rugi dan diproses secara perdata di pengadilan negeri yang memiliki kewenangan sesuai dengan ketentuan pasal tersebut.[[100]](#footnote-100)

Data biometrik, yang termasuk dalam data pribadi memiliki memiliki sifat yang sensitif. Data biometrik termasuk dalam kategori data pribadi yang meliputi informasi tentang kesehatan, genetika, riwayat kriminal, data anak, serta data keuangan individu. Keseluruhan proses pemrosesan data biometrik harus transparan, mulai dari pengumpulan, penyimpanan, perbaikan, pengiriman, dan penghapusan. Transparansi sangat diperlukan agar dapat mencegah penyalahgunaan dikemudian hari, misalnya Informasi biometric individu yang dikumpulkan secara diam-diam tanpa persetujuan dan partisipasi pengguna menimbulkan risiko pelanggaran privasi konsumen.[[101]](#footnote-101) Kurangnya informasi yang jelas dan transparan dapat menyebabkan ketidakpercayaan di antara pengguna, yang merasa bahwa privasi mereka terancam tanpa persetujuan yang memadai.

1. **Ketentuan Mengenai Keabsahan Kontrak dalam Hukum Perdata**

Bentuk interaksi manusia, perjanjian atau kontrak selalu berkembang. Perkembangan mereka mengikuti bentuk interaksi manusia itu sendiri. Perjanjian tradisional dapat berupa sepenuhnya lisan (Perjanjian verbal) atau sepenuhnya tertulis (Perjanjian yang dibuat secara tertulis), atau keduanya. Mereka juga dapat terdiri dari gabungan antara keduanya, sebagian dalam bentuk tertulis dan sebagian lisan.[[102]](#footnote-102) Dua orang yang bertindak untuk dan atas nama diri mereka sendiri atau bisnis yang mereka wakili dapat membuat perjanjian secara langsung atau tidak langsung. Sergio Meldonado mengklasifikasikan kontrak online menjadi tiga (tiga) jenis: pertama, kontrak yang dibuat antara dua orang fisik (orang nyata), kedua, perjanjian yang dibuat antara sebuah sistem komputer dan orang fisik, dan ketiga, perjanjian yang dibuat antara dua sistem komputer.[[103]](#footnote-103)

KUHperdata tidak secara spesifik menyebut kata kontrak, mealainka *verbintenissen* (perikatan) atau *overeenkoms* (perjanjian) sementara dalam banyak ketentuan lainnya dan juga yang dianut dalam hukum internasional disebut dengan kontrak.[[104]](#footnote-104) Pasal 1313 Buku III KUHPerdata menyatakan bahwa "Perjanjian adalah suatu perbuatan dengan mana satu orang atau lebih mnegikatkan dirinya terhadap satu orang atau lebih." Ini adalah definisi perjanjian menurut KUHPerdata. Dalam pasal ini, "perjanjian" didefinisikan sebagai tindakan hukum yang dilakukan oleh satu atau lebih pihak dengan tujuan untuk mencapai kesepakatan atau ikatan hukum dengan pihak lain. Pihak yang terlibat dalam sebuah perjanjian bisa berupa orang atau badan hukum selama pihak tersebut memiliki kapasitas hukum yang memadai unutuk melakukannya. Sangat penting untuk memahami bagaimana perjanjian dapat dilaksanakan dengan benar.[[105]](#footnote-105) Di mana harus diperhatikan beberapa syarat agar perjanjian dapat dianggap sah.[[106]](#footnote-106) Pasal 1320 KUHPerdata mengatur tentang syarat sahnya perjanjian, Pasal 1320 berbunyi:

" Suatu perjanjian berlaku sebagai undang-undang bagi mereka yang membuatnya, apabila memenuhi syarat-syarat sebagai berikut::

1. Kesepakatan mereka yang mengikatkan dirinya.
2. Kecakapan untuk membuat perikatan.
3. Suatu hal tertentu.
4. Suatu sebab yang halal."

Untuk mencapai kesuksesan kedua belah pihak, sebuah transaksi harus mempertimbangkan elemen-elemen dalam kontrak yang berfungsi sebagai landasan untuk menjaga arah dan tujuan kontrak, serta untuk mengevaluasi apakah kontrak tersebut telah dilaksanakan dengan benar dan melindungi transaksi dengan baik. Dengan demikian, kontrak elektronik harus dianggap sah secara hukum. Maka, apabila persyaratan pada pasla 1320 tidak terpenuhi bagi pelaksanaan kontrak tersebut, sebuah kontrak dapat batal demi hukum. [[107]](#footnote-107) Jika objek kontrak tidak ada dan penyebabnya ternyata haram, kontrak tersebut batal demi hukum.[[108]](#footnote-108)

Para pihak menginginkan atau bermaksud untuk menciptakan akibat hukum. Komitmen atau kesepakatan yang dibuat oleh seseorang hanya akan menghasilkan kewajiban sosial; kesepakatan belum tentu memiliki konsekuensi hukum.[[109]](#footnote-109) Faktanya, ada perbedaan antara kewajiban moral yang memiliki konsekuensi hukum dan kewajiban yang tidak. Perjanjian harus menarik bagi satu pihak dari pihak lain. Hanya pihak-pihak yang secara langsung berpartisipasi dalam suatu perjanjian yang akan tunduk pada konsekuensi dan tugas hukumnya; pihak-pihak lain yang tidak terlibat langsung dalam perjanjian tersebut tidak akan terikat oleh hak atau kewajiban apa pun yang timbul daripadanya. [[110]](#footnote-110) Selain itu, perjanjian yang dibuat oleh dua pihak atau lebih tidak boleh merugikan pihak ketiga yang tidak berpartisipasi atau tidak terlibat dalam kesepakatan. Hal ini menunjukkan bahwa hak dan kewajiban yang muncul hanya terbatas pada pihak-pihak yang berkontrak dan tidak boleh merugikan pihak lain yang tidak terikat oleh perjanjian.

Prinsip kebebasan berkontrak, yang diakui dalam hukum perdata Indonesia, memungkinkan para pihak untuk mengubah isi kontrak sesuai keinginan mereka selama tidak bertentangan dengan ketentuan hukum yang berlaku. Kebebasan berkontrak, yang diatur dalam Pasal 1338 KUHPerdata, adalah salah satu prinsip utama hukum kontrak.

“(1) Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya.

(2) Perjanjian tidak dapat dibatalkan selain atas dasar kesepakatan para pihak atau alasan yang diatur dalam undang-undang.”

Hukum perjanjian Indonesia didasarkan pada pasal ini. Perjanjian yang sah dapat diberlakukan kepada para pihak selama tidak melanggar kesusilaan dan ketertiban umum. Meskipun harus mematuhi pedoman yang ditetapkan dalam Pasal 1320 Kitab Undang-Undang Hukum Perdata, hal ini juga memberikan kebebasan kepada para pihak yang ingin membuat perjanjian untuk memilih ketentuan dan struktur perjanjian.

1. **Adaptasi Hukum Terhadap Perkembangan Teknologi Biometrik dalam Hukum Perdata**

Penggunaan teknologi biometrik ini menimbulkan tantangan hukum, terutama dalam ranah hukum perdata. Beberapa Undang-Undang Perdata, terutama Undang-Undang ITE dan Undang-Undang PDP, mengatur transaksi elektronik. Untuk mendukung transaksi elektronik, undang-undang ITE mengakui tanda tangan elektronik dalam teknologi biomterik sebagai sah dan mengikat secara hukum.[[111]](#footnote-111) Undang-undang ITE juga mengatur hak dan kewajiban pengguna serta penyelenggara layanan termasuk perlindungan data pribadi yang dikumpulkan selama proses transaksi.

Implikasi dari undang-undnag perlindungan data pribadi adalah adanya perlindungan yang lebih baik bagi privasi individu. [[112]](#footnote-112) Pengguna memiliki hak untuk mrngrtahui bagaimana data pribadi pengguna digunakan dan dapat memberikan atau menarik persetujuan pengguna kapan saja, sehingga dapat menjaga kepercayaan dalam transaksi elektronik. Semua orang yang menangani atau memanfaatkan data pribadi untuk tujuan tertentu harus mematuhi hukum pada peraturan perundang-undangan ini tanpa kecuali, sesuai dengan akibat hukum yang timbul setelah pembentukannya. [[113]](#footnote-113) Undang-undang yang berkaitan dengan perlindungan data pribadi memiliki dampak besar dalam menjaga privasi individu, memberi orang kendali atas informasi pribadi mereka, dan meminta pertanggungjawaban bisnis atas data pribadi mereka.[[114]](#footnote-114) Perlindungan privasi, kontrol data, dan tanggung jawab organusasi merupakan tujuan utama undnag-undang perlindungan data pribadi.[[115]](#footnote-115) Pasal 28G ayat (1) UUD 1945 menyatakan bahwa:

“ Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. ”

Pasal ini mengungkapkan bahwa setiap individu berhak mendapatkan perlindungan di berbagai bidang kehidupan, seperti perlindungan terhadap diri pribadi, keluarga, martabbat, kehormatana, serta harta benda yang dikuasainySelain itu, juga pasal ini memberikan hak atas rasa aman, sehingga setiap warga negara merasa aman dalam menjalani kehidupannya. Hal ini sebagai pagian dari penghormatan terhadap hak asasi manusia (HAM).

Undang-undang ITE menjamin pemanfaatan teknologi informasi dan media komunikasi yang aman dan lancar.[[116]](#footnote-116) Salah satu cara untuk mencegah ketidakrukunan umat beragama di Indonesia adalah dengan membuat UU ITE.[[117]](#footnote-117) Pasal 28 Ayat (2) UU ITE berbunyi:

“ Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik. ”

Menurut pasal ini, dilarang menyebarluaskan materi yang bertujuan untuk menimbulkan permusuhan atau kebencian terhadap seseorang atau suatu kelompok tertentu atas dasar ras, agama, suku, dan antarsub (SARA).[[118]](#footnote-118) UU ITE yang menerapkan prinsip-prinsip seperti kepastian hukum, manfaat, kehati-hatian, itikad baik, serta kebebasan dalam memilih teknologi atau prinsip netralitas teknologi pada dasarnya dirancang untuk menciptakan kepastian hukum dalam dunia digital.[[119]](#footnote-119) Selain itu, undang-undang ini juga bertujuan untuk mengatasi masalah hukum yang terkait dengan kegiatan yang dilakukan secara virtual melalui langkah-langkah preventif. Dengan asumsi-asumsi ini, UU ITE dimaksudkan untuk memastikan bahwa segala bentuk interaksi dan transaksi elektronik di internet berjalan dengan cara yang adil dan tidak merugikan pihak-pihak yang terlibat.

1. Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. (2023). *Ilmu Hukum Implikasi Teknologi Dalam Perubahan Hukum*. PTT. Literasi Nusantara Abadi Grup [↑](#footnote-ref-1)
2. Barkatullah, A. H. (2019). *Hukum Transaksi Elektronik di Indonesia: sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia*. Bandung. Nusamedia. Hlm. 2 [↑](#footnote-ref-2)
3. Krista Yitawati, Haryani, Nugroho. (2017). *Hukum dan Teknologi: Perlindungan Hukum Jual Beli Melalui Transaksi Elektronik (E-Commerce)*. Solo. Pustaka Iltizam. Hlm. 14 [↑](#footnote-ref-3)
4. Anil Jain, Ruud Bole, Sharath Pankanti. (2011). *Introduction to Biometrics*. Springer US. hlm. 2 [↑](#footnote-ref-4)
5. Authme, A. (2024). *Apa Itu Biometrik? Pahami Fungsi, Jenis, Manfaat, dan Aplikasinya*. <https://authme.com/id/blog/what-is-biometric-authentication/> (diakses pada 09 Oktober 2024, pukul 20.32 WIB) [↑](#footnote-ref-5)
6. Sumijan, S., Widya Purnama, P. A., & Arlis, S. (2021). *Buku-Teknologi Biometrik: Impementasi pada Bidang Medis Menggunakan Matlabs.* hlm. 25 [↑](#footnote-ref-6)
7. Rizki, M. F., & Salam, A. (2023). Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris). *Lex Patrimonium*, 2(2), 9.<https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/9?utm_source=scholarhub.ui.ac.id%2Flexpatri%2Fvol2%2Fiss2%2F9&utm_medium=PDF&utm_campaign=PDFCoverPages> [↑](#footnote-ref-7)
8. *Ibid*  [↑](#footnote-ref-8)
9. *Ibid* [↑](#footnote-ref-9)
10. Salim HS. (2021). *Hukum Kontrak Elektronik: E-contract Law.* Jakarta. Rajawali Persada. hlm. 1. [↑](#footnote-ref-10)
11. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 146, Tambahan Lembaran Negara Nomor 6388). [↑](#footnote-ref-11)
12. Sip Law Firm. (2024). Hak, kewajiban dan sanksi hukum penggunaan biometrik. <https://siplawfirm.id/penggunaan-biometrik/?lang=id> (diakses pada 09 Oktober 2024, pukul 21.53 WIB) [↑](#footnote-ref-12)
13. Lokania, L. (2022*). Keabsahan Hukum Penggunaan Tanda Tangan Elektronik Dalam Perjanjian Jual Beli Online Melalui Aplikasi FIFGROUP Digital Form* (Skripsi, Program Studi Hukum, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Tidar). [↑](#footnote-ref-13)
14. Pramana, A. A., Hamzani, A. I., & Taufik, M. (2023). Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Indonesia Bagi Pengguna Vaksin. *Pancasakti Law Journal (PLJ*), 1(1), 45-54. [↑](#footnote-ref-14)
15. Evelyn de Souza. (2018). The Era of Homo Digitus, *in Women in Security: Changing the Face of Technology and Innovation,* pp.47-52. [↑](#footnote-ref-15)
16. Silalahi, R. N. (2024). Implikasi hukum dari penggunaan teknologi pengenalan biometrik dalam sistem keamanan di Indonesia. Tugas *Mahasiswa Fakultas Hukum*, 1(2). <https://coursework.uma.ac.id/index.php/fakum/article/view/833> (diakses pada 11 Oktober 2024, pukul 13.47 WIB) [↑](#footnote-ref-16)
17. Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik. *Veritas et Justitia*, 10(1), 127-152. [↑](#footnote-ref-17)
18. Asliri. (2022). Pentingnya Perlindungan Data Biometrik Untuk Bisnis Digital. <https://asliri.id/blog/pentingnya-perlindungan-data-biometrik-untuk-bisnis-digital/> (diakses pada 11 Oktober 2024, pukul 14.22 WIB) [↑](#footnote-ref-18)
19. Dahlia, M., & Susetio, W. (2023). Tinjauan Yuridis Penggunaan Tanda Tangan Digital Dalam Perjanjian Jual Beli. *Jurnal Multidisiplin Indonesia, 2*(8). [↑](#footnote-ref-19)
20. Rahmawati, S. (2024). Tingkat Keabsahan Kontrak Elektronik Berdasarkan Hukum Positif di Indonesia. *INNOVATIVE: Journal of Social Science Research, 4*(4), 7561-7572. [↑](#footnote-ref-20)
21. Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial *Technology* di Indonesia. *REFLEKSI HUKUM: Jurnal Ilmu Hukum, 3*(2), 145-160. [↑](#footnote-ref-21)
22. Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia. *Jurnal RechtsVinding, 12*(2), 261–279. [↑](#footnote-ref-22)
23. *Ibid* [↑](#footnote-ref-23)
24. Dimensy.id. (2023). *Verifikasi Biometrik: Fungsi, Cara Kerja, Kelebihan & Kelemahannya*. <https://dimensy.id/article/verifikasi-biometrik-fungsi-cara-kerja-kelebihan--kelemahannya> (diakses pada 12 Oktober 2024, pukul 20.50 WIB) [↑](#footnote-ref-24)
25. Delphia, R., & Harjono, M. K. (2021). *Persepsi Masyarakat Atas Pelindungan Data Pribadi: Survei Nasional*. hlm. 25. [↑](#footnote-ref-25)
26. *Ibid* [↑](#footnote-ref-26)
27. Priambodo, B. W., & Wadjoeono, D. (2023). Perlindungan Hukum Terhadap Penggunaan Teknologi Biometrik dalam Transaksi Perbankan Untuk Meningkatkan Keamanan. *Madani: Jurnal Ilmiah Multidisipline, 1*(11), 325. [↑](#footnote-ref-27)
28. Suparni, N. (2009). *Cyberspace, Problematika dan Antisipasi Pengaturannya*. Jakarta. Sinar Grafika. hlm. 5-6. [↑](#footnote-ref-28)
29. Rosadi, S. D., & Pratama, G. G. (2018). Urgensi Perlindungandata Privasi dalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, 4(1), 88-110. [↑](#footnote-ref-29)
30. Edrisy, I. F. (2019). *Pengantar Hukum Siber*. Lampung. Sei Wawai Publishing. hlm. 42. [↑](#footnote-ref-30)
31. Haryanto, J. (2018). *Klasifikasi Data Untuk Pelindungan Data Pribadi*, Yogyakarta, Center for Digital Society, hlm. 14 [↑](#footnote-ref-31)
32. Rizki, M. F., & Salam, A. (2023). Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi kasus Clearview AI Inc. di Yunani dan Inggris). *Lex Patrimonium, 2*(2), Article 9.<https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/9?utm_source=scholarhub.ui.ac.id%2Flexpatri%2Fvol2%2Fiss2%2F9&utm_medium=PDF&utm_campaign=PDFCoverPages> [↑](#footnote-ref-32)
33. Permana, R. I. (2021). Analisis Faktor Penggunaan Dompet Digital Di Kalangan Mahasiswa Perguruan Tinggi Surabaya. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 8*(1), 312-322. [↑](#footnote-ref-33)
34. Nadhotul Sufi’, F. Y., Putri, D. K., & Suhartini, D. (2023). Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review. *Prosiding Senapan, 3*(1), 19-29.. [↑](#footnote-ref-34)
35. Rofiq Hidayat. (2020). Pengumpulan Data Biometrik, Ancaman Perlindungan Data Pribadi, *Hukumonline*, <https://www.hukumonline.com/berita/a/pengumpulan-data-biometrik--ancaman-perlindungan-data-pribadi-lt5e2ab2ce33ef5/>. (Diakses pada tanggal 13 Oktober 2024, Pukul 20.42 WIB) [↑](#footnote-ref-35)
36. Hakim, A. N. A. (2022). *Keabsahan dan Kekuatan Hukum Tanda Tangan Elektronik Untuk Legalitas Berdasarkan Undang-Undang ITE dan Kuhperdata* (Skripsi, Universitas Muhammadiyah Sumatera Utara). [↑](#footnote-ref-36)
37. Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi Desain Privasi Sebagai Pelindungan Privasi Atas Data Biometrik. *Artikel Hukum, 10*(1). [↑](#footnote-ref-37)
38. Hamzani, A. I., Idayanti, S., & Widyastuti, T. V. (2020). *Buku Panduan Penulisan Skripsi*. Yogyakarta. Tanah Air Beta [↑](#footnote-ref-38)
39. Zainuddin Ali. (2016). *Metode Penelitian Hukum*. Jakarta. Sinar Grafika. hlm.68. https://inlislite.uin-suska.ac.id/opac/detail-opac?id=12346 (Diakses pada tanggal 27 September 2024 Pukul 12.55 WIB) [↑](#footnote-ref-39)
40. M. Nazir. (2003). *Metode Penelitian*. Ghalia Indonesia, hlm. 27. [↑](#footnote-ref-40)
41. Muhaimin, M. (2020). *Metode Penelitian Hukum*. Nusa Tenggara Barat. Mataram University Press. hlm. 47-48 [↑](#footnote-ref-41)
42. Soekanto, S., & Mamudja, S. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers. Hlm. 13-14 [↑](#footnote-ref-42)
43. Zainuddin Ali, *op.cit.,* hlm. 69 [↑](#footnote-ref-43)
44. Amiruddin dan Zainal Asikin. (2004*). Pengantar Metode Penelitian Hukum,* Jakarta. PT RajaGrafindo Persada. hlm. 119 [↑](#footnote-ref-44)
45. Wahyudin Darmalaksana. (2020). *Cara Menulis Proposal Penelitian*. Bandung. Fakultas Ushuluddin UIN. hlm.25 [↑](#footnote-ref-45)
46. Mestika Zed. (2014). *Metode Penelitian Kepustakaa.,* Yayasan Pustaka Obor Indonesia. hlm. 5. [↑](#footnote-ref-46)
47. Amiruddin, A. & Zainal Asikin, *Ibid,* hlm. 67 [↑](#footnote-ref-47)
48. Ajat Rukayat. (2018). *Pendekatan Penelitian Kualitatif*. Yogyakarta. CV Budi Utama. hlm. 6 [↑](#footnote-ref-48)
49. Salim, H. S., & Nurbani, E. S. (2013)*. Penerapan Teori Hukum Pada Penelitian Tesis Dan Disertasi*. Jakarta. PT RajaGrafindo Persada. Hlm. 19 [↑](#footnote-ref-49)
50. Widyastuti, T. V., Marsisno, W., Udin, A. F., & Sutaguna, I. N. T. (2024). *Penelitian Transformatif; Mengatasi Isu-Isu Kontemporer Dengan Kombinasi Metode Kuantitatif dan Kualitatif.* Media Penerbit Indonesia. [↑](#footnote-ref-50)
51. Sirajuddin Saleh. (2017). *Analisis Data Kualitatif*. Bandung. Pustaka Ramadhan. hlm. 9 [↑](#footnote-ref-51)
52. Ulfah, A. K., Razali, R., Rahman, H., Ghofur, A., Bukhory, U., Wahyuningrum, S. R., ... & Muqoddam, F. (2022). *Ragam Analisis Data Penelitian (Sastra, Riset dan Pengembangan)*. IAIN Madura Press. hlm. 99 [↑](#footnote-ref-52)
53. Sumijan, S., Widya Purnama, P. A., & Arlis, S. (2021). *Buku-Teknologi Biometrik: Impementasi pada Bidang Medis Menggunakan Matlabs*. Insan Cendikia Mandiri. hlm. 25 [↑](#footnote-ref-53)
54. AWS Amazon. (2024). Apa itu Pengenalan Wajah? <https://aws.amazon.com/id/what-is/facial-recognition/> (diakses pada tanggal 15 November 2024 pukul 13.41 WIB) [↑](#footnote-ref-54)
55. Verihubs. (2023). Biometrik Wajah, Seperti Apa Cara Kerja dan Keunggulannya? <https://verihubs.com/blog/biometrik-wajah> (diakses pada tanggal 15 November 2024 pukul 13.50 WIB) [↑](#footnote-ref-55)
56. Sumijan, S., Widya Purnama, P. A., & Arlis, S, *op.cit, Hlm. 25-26* [↑](#footnote-ref-56)
57. *Ibid* [↑](#footnote-ref-57)
58. Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. (2023). *Ilmu Hukum Implikasi Teknologi Dalam Perubahan Hukum*. PTT. Literasi Nusantara Abadi Grup. Hlm. 2-3 [↑](#footnote-ref-58)
59. Siboro, S., & Hadiningrum, S. (2024). Tantangan Penegakan Hukum Perdata di Era Digital. *Public Service and Governance Journal*, *5*(2), 52-59. [↑](#footnote-ref-59)
60. Pakarti, M. H. A., Farid, D., Saepullah, U., & Sucipto, I. (2023). Pengaruh Perkembangan Teknologi Terhadap Perlindungan Privasi Dalam Hukum Perdata. *SULTAN ADAM: Jurnal Hukum dan Sosial*, *1*(2), 204-212. [↑](#footnote-ref-60)
61. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction To Biometric Recognition. *IEEE Transactions On Circuits and Systems For Video Technology*, *14*(1), 4-20. [↑](#footnote-ref-61)
62. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing Security and Privacy In Biometrics-Based Authentication Systems. *IBM systems Journal*, *40*(3), 614-634. DOI [10.1147/sj.403.0614](https://doi.org/10.1147/sj.403.0614) [↑](#footnote-ref-62)
63. European Union Agency for Fundamental Rights. (2018). "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement." [↑](#footnote-ref-63)
64. Santoso, E. (2023). Hukum Siber: Permasalahan Hukum Bisnis di Bidang Teknologi Informasi dan Komunikasi. Kencana. [↑](#footnote-ref-64)
65. Sumijan, S., Widya Purnama, P. A., & Arlis, S, *op.cit,* Hlm. 146 [↑](#footnote-ref-65)
66. Ba'abud, M. F. R., & Heriyanto, D. S. N. (2024). Application Of The Principles Of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders. *Uti Possidetis: Journal of International Law*, *5*(1), 106–139. [↑](#footnote-ref-66)
67. Gunawan, I. (2024). Upaya Preventif dan Represif dalam Penanggulangan Kebocoran Data Pada Penyelenggaraan Pinjaman Online. *Officium Notarium*, *4*(1), 25-49. [↑](#footnote-ref-67)
68. Murad, M. R. (2023). Pemodelan Matematis untuk Pengembangan Sistem Pengenalan Wajah dalam Keamanan Biometrik. *Jurnal Dunia Ilmu*, *3*(7). [↑](#footnote-ref-68)
69. Sumijan, S., Widya Purnama, P. A., & Arlis, S, *Ibid,* Hlm. 52. [↑](#footnote-ref-69)
70. Ridho, A. Z. (2019). *Coefficient Dan Dynamic Time Warping K Nearest Neighbour dalam Rekognisi Aksen Suku di Indonesia* (Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim Malang). [↑](#footnote-ref-70)
71. Adhinata, F. D., Rakhmadani, D. P., & Segara, A. J. T. (2021). Pengenalan Jenis Kelamin Manusia Berbasis Suara Menggunakan MFCC dan GMM. *Journal Data Sci. IoT, Mach. Learn. Informatics*, *1*(1), 1–12. [↑](#footnote-ref-71)
72. Annisadev. (2023). Mengenal Teknologi Biometrik Dalam Melindungi Identitas Pribadi <https://annisadev.com/news/read/709/mengenal-teknologi-biometrik-dalam-melindungi-identitas-pribadi.html> (diakses pada tanggal 17 November 2024 pukul 11.40 WIB) [↑](#footnote-ref-72)
73. Priowirjanto, E. S. (2014). Pengaturan Transaksi Elektronik dan Pelaksanaannya Di Indonesia Dikaitkan Dengan Perlindungan E-Konsumen. *Padjadjaran Jurnal Ilmu Hukum*, 1(2). [↑](#footnote-ref-73)
74. *Ibid* [↑](#footnote-ref-74)
75. Sufi, F. Y. N., Putri, D. K., & Suhartini, D. (2023). Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review. In *Seminar Nasional Akuntansi dan Call for Paper*. Vol. 3, No. 01, pp. 19-29. [↑](#footnote-ref-75)
76. Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). Sistem keamanan informasi. [↑](#footnote-ref-76)
77. *Ibid* [↑](#footnote-ref-77)
78. Saputri, V. D. (2023). Implementation Of Biometric-Based Security System On Mobile Banking Application. *Jurnal Komputer Indonesia*, *2*(1), 25-32. [↑](#footnote-ref-78)
79. *Ibid* [↑](#footnote-ref-79)
80. Priambodo, B. W., & Wahjoeono, D. (2023). Perlindungan Hukum terhadap Penggunaan Teknologi Biometrik dalam Transaksi Perbankan untuk Meningkatkan Keamanan. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(11). [↑](#footnote-ref-80)
81. *Ibid* [↑](#footnote-ref-81)
82. *Ibid* [↑](#footnote-ref-82)
83. Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. Cyber Security Dan Forensik Digital, 1(2), 57-61. [↑](#footnote-ref-83)
84. *Ibid* [↑](#footnote-ref-84)
85. Saputri, V. D. *Op.cit* [↑](#footnote-ref-85)
86. Bank Mas. (2022). Aktifkan Otentifikasi Biometrik di MAS Mobile Kamu Agar Transaksi Lebih Aman!. <https://www.bankmas.co.id/id/blog/otentifikasi-biometrik/> (diakses pada 17 November 2024 pukul 18.04 WIB) [↑](#footnote-ref-86)
87. DocuSign. (2024). Peran otentikasi biometrik dalam tanda tangan elektronik. DocuSign. <https://www.docusign.com/en-gb/blog/the-role-of-biometric-authentication-in-e-signatures> (diakses pada 17 November 2024 pukul 18.25 WIB) [↑](#footnote-ref-87)
88. Lokania, L. (2022). *Keabsahan Hukum Penggunaan Tanda Tangan Elektronik Dalam Perjanjian Jual Beli Online Melalui Aplikasi FIFGROUP Digital Form* (Skripsi, Program Studi Hukum, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Tidar). [↑](#footnote-ref-88)
89. Munawaroh, N. (2022). Keabsahan perjanjian elektronik dan syaratnya. *Hukum Online*. <https://www.hukumonline.com/> (diakses pada 17 November 2024 pukul 18.37 WIB) [↑](#footnote-ref-89)
90. Kejaksaan Republik Indonesia. (2023). Perjanjian elektronik. *Halo JPN*. <https://halojpn.id/publik/d/permohonan/2023-17f0> (diakses pada 17 November 2024 pukul 18.50 WIB) [↑](#footnote-ref-90)
91. Khairandy, R. (2001). Pembaharuan Hukum Kontrak sebagai Antisipasi Transaksi Electronic Commerce. *Jurnal Hukum IUS QUIA IUSTUM*, *8*(16), 42-57. [↑](#footnote-ref-91)
92. Daffa, M. F., Rahman, S., & Qahar, A. (2023). Kekuatan Pembuktian Tanda Tangan Elektronik sebagai Alat Bukti dalam Perkara Perdata. *Journal of Lex Philosophy (JLP)*, *4*(1), 205-221. [↑](#footnote-ref-92)
93. Rizki, M. F., & Salam, A. *Op.cit* [↑](#footnote-ref-93)
94. Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39-57. [↑](#footnote-ref-94)
95. *Ibid* [↑](#footnote-ref-95)
96. Dewi, I. R. (2022). Hacker Bjorka is back, data apa saja yang pernah dibocorkan? CNBC Indonesia. <https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan> (diakses pada tanggal 25 November 2024, Pukul 12.18 WIB) [↑](#footnote-ref-96)
97. Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis, 7*(1), 105–119. <https://doi.org/10.35814/selisik.v6i1.1699> [↑](#footnote-ref-97)
98. Fikri, M., & Rusdiana, S. *Op.cit* [↑](#footnote-ref-98)
99. Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia. *Jurnal Hukum & Pembangunan*, *48*(4), 814-825. [↑](#footnote-ref-99)
100. *Ibid*  [↑](#footnote-ref-100)
101. Sirait, R. M., Ginting, R. F., & Ginting, C. D. B. (2023). Tantangan Hukum Penggunaan Data Biometrik Dalam Keperluan Bisnis. *Jurnal Konseling Pendidikan Islam*, *4*(2 Juli), 467-477. [↑](#footnote-ref-101)
102. Artanti, D. A., & Widiatno, M. W. (2020). Keabsahan Kontrak Elektronik Dalam Pasal 18 Ayat 1 UU ITE Ditinjau Dari Hukum Perdata Di Indonesia. *JCA of Law*, *1*(1). [↑](#footnote-ref-102)
103. *Ibid* [↑](#footnote-ref-103)
104. Marpi, Y., & Kom, S. (2020). *Perlindungan Hukum Terhadap Konsumen Atas Keabsahan Kontrak Elektronik Dalam Transaksi E-Commerce*. PT. Zona Media Mandiri. [↑](#footnote-ref-104)
105. Wijayanti, N. L. P. E. (2019). Keabsahan Sebuah Perjanjian Berdasarkan Dari Kitab Undang-Undang Hukum Perdata. *Bagian Hukum Bisnis Fakultas Hukum Universitas Udayana*, *1*, 1-5. [↑](#footnote-ref-105)
106. *Ibid* [↑](#footnote-ref-106)
107. Keabsahan Kontrak Elektronik Dalam UU ITE Ditinjau Dari Pasal 1320 KUHPerdata dan UNCITRAL Model Law On Electronic Commerce. (2020). *Risalah Hukum*, *7*(2), 64-76. <https://e-journal.fh.unmul.ac.id/index.php/risalah/article/view/189> [↑](#footnote-ref-107)
108. *Ibid* [↑](#footnote-ref-108)
109. Lie, C., Clarosa, V., Yonatan, Y. A., & Hadiati, M. (2023). Pengenalan Hukum Kontrak dalam Hukum Perdata Indonesia. *Jurnal Kewarganegaraan*, *7*(1), 918-924. [↑](#footnote-ref-109)
110. *Ibid* [↑](#footnote-ref-110)
111. SIPPN. (2023). Mengenal Undang-Undang ITE. <https://sippn.menpan.go.id/berita/58352/rumah-tahanan-negara-kelas-iib-pelaihari/mengenal-undang-undang-ite> (diakses pada tanggal 29 November 2024 pukul 02.47 WIB) [↑](#footnote-ref-111)
112. Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. *Op.cit* [↑](#footnote-ref-112)
113. Sisca, K. A. (2024). Penegakan Hukum Notaris Yang Menggunakan Data Pribadi Orang Lain Dalam Akta: Perspektif Perlindungan Data. *Repertorium: Jurnal Ilmiah Hukum Kenotariatan*, *13*(1), 95-103. [↑](#footnote-ref-113)
114. Sanusi, S., La Dee, M., Widyastuti, T. V., & Lubis, A. F. *Op.cit* [↑](#footnote-ref-114)
115. *Ibid* [↑](#footnote-ref-115)
116. Nabilah, W., Putri, D., Rizal, D., & Warman, A. B. (2022). Implikasi Undang-Undang Informasi dan Transaksi Elektronik (UU-ITE) terhadap Kerukunan Kehidupan Beragama di Ruang Digital. *Dialog*, *45*(1), 69-80. [↑](#footnote-ref-116)
117. Ibid [↑](#footnote-ref-117)
118. Ibid [↑](#footnote-ref-118)
119. Ibid [↑](#footnote-ref-119)