

Perlindungan Data Pribadi dalam Sistem Blockchain: Tantangan Normatif dan Implikasi Hukum di Indonesia

Emmy Febriani Thalib^{1*}, Ni Putu Suci Meinarni², Happy Budyana Sari³

^{1,2*,3} Institut Bisnis dan Teknologi Indonesia, Denpasar, Indonesia

¹emmy.f@instiki.ac.id *, ²sucimeinarni@instiki.ac.id, ³happy.budyana@instiki.ac.id

INFO ARTIKEL

Article history:

Received Juni 2026

Published Juli 2026

ABSTRAK

Perkembangan teknologi blockchain telah mendorong transformasi dalam pengelolaan dan pertukaran data digital melalui sistem pencatatan yang terdesentralisasi, transparan, dan imutabel. Meskipun menawarkan tingkat keamanan dan integritas data yang tinggi, karakteristik tersebut juga menimbulkan tantangan hukum, khususnya dalam konteks perlindungan data pribadi. Penelitian ini bertujuan untuk menganalisis kesesuaian kerangka hukum perlindungan data pribadi di Indonesia terhadap karakteristik blockchain serta mengidentifikasi implikasi hukumnya. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur ilmiah, dan dokumen hukum yang relevan. Hasil penelitian menunjukkan adanya tiga tantangan utama, yaitu konflik antara hak penghapusan data dan karakter imutabel blockchain, ketidakjelasan penentuan pengendali data dalam sistem terdesentralisasi, serta kompleksitas yurisdiksi pada jaringan blockchain lintas batas. Temuan tersebut menunjukkan bahwa kerangka hukum perlindungan data pribadi yang berlaku saat ini masih berorientasi pada sistem pemrosesan data yang terpusat sehingga menghadapi berbagai kendala ketika diterapkan pada ekosistem blockchain. Oleh karena itu, diperlukan pendekatan regulasi yang lebih adaptif guna menjamin perlindungan data pribadi tanpa menghambat inovasi teknologi blockchain.

Kata Kunci: Blockchain, Hukum Siber, Regulasi Digital, Yurisdiksi, Perlindungan Data Pribadi.

ABSTRAK

The rapid development of blockchain technology has transformed digital data management through a decentralized, transparent, and immutable ledger system. While blockchain offers enhanced security, integrity, and transparency of information, its fundamental characteristics also create legal challenges, particularly in the context of personal data protection. This study aims to examine the compatibility of Indonesia's personal data protection framework with the characteristics of blockchain technology and to analyze the legal implications arising from their interaction. The research employs a normative legal research method using statutory, conceptual, and comparative approaches. Data were collected through a literature review of relevant laws and regulations, academic literature, and legal documents concerning blockchain and personal data protection. The findings reveal three major normative challenges. First, the immutability of blockchain conflicts with data subjects' rights, particularly the

right to erasure and data rectification. Second, the decentralized structure of blockchain creates ambiguity in determining data controllers and data processors, thereby complicating legal accountability. Third, the cross-border nature of blockchain networks raises jurisdictional challenges for the enforcement of personal data protection laws. These findings indicate that Indonesia's current personal data protection framework remains largely oriented toward centralized data processing systems and therefore encounters significant limitations when applied to decentralized blockchain environments. Consequently, a more adaptive regulatory approach is required to ensure effective personal data protection while supporting the continued development and adoption of blockchain technology.

Keywords: Blockchain, Cyber Law, Digital Regulation, Jurisdiction, Personal Data Protection.

©2026 Authors. Licensed Under [CC-BY-NC-SA 4.0](#)

1. Pendahuluan

Perkembangan teknologi blockchain sebagai sistem pencatatan terdistribusi (*distributed ledger technology*) telah membawa perubahan signifikan dalam pengelolaan dan pertukaran data digital. Karakteristik utama blockchain yang bersifat terdesentralisasi, transparan, dan imutabel menjadikannya sebagai salah satu inovasi teknologi yang banyak diadopsi dalam berbagai sektor, mulai dari layanan keuangan digital, rantai pasok (*supply chain*) (Baktygul, 2023), hingga layanan publik berbasis elektronik. Melalui mekanisme kriptografi dan konsensus jaringan, blockchain mampu menyediakan tingkat integritas dan keamanan data yang tinggi karena setiap transaksi yang tercatat sulit untuk dimanipulasi atau diubah secara sepihak. Kemampuan tersebut menjadikan blockchain dipandang sebagai solusi yang menjanjikan dalam menciptakan sistem informasi yang lebih aman, transparan, dan terpercaya dibandingkan sistem penyimpanan data konvensional yang terpusat (Holden & Malani, 2022).

Pemanfaatan blockchain saat ini tidak lagi terbatas pada transaksi aset kripto, tetapi telah berkembang ke berbagai aplikasi yang melibatkan pemrosesan data pribadi. Sejumlah negara mulai mengimplementasikan blockchain dalam sistem identitas digital, rekam kesehatan elektronik, sertifikasi pendidikan, layanan administrasi publik, hingga pengelolaan kontrak pintar (*smart contract*). Dalam berbagai implementasi tersebut, data yang diproses sering kali berkaitan langsung dengan identitas individu dan informasi pribadi yang memerlukan perlindungan hukum. Meskipun blockchain menawarkan jaminan keamanan dan keutuhan data yang lebih baik, karakteristiknya yang permanen dan tersebar pada banyak node jaringan menimbulkan pertanyaan mengenai kesesuaiannya dengan prinsip-prinsip perlindungan data pribadi yang berkembang dalam berbagai rezim hukum modern.

Di Indonesia, penguatan perlindungan data pribadi memperoleh landasan hukum yang lebih komprehensif melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022). Regulasi ini mengatur berbagai hak subjek data, termasuk hak untuk memperoleh informasi, memperbaiki data, membatasi pemrosesan data, menarik persetujuan, serta menghapus data pribadi dalam kondisi tertentu. Selain itu, UU PDP juga menetapkan kewajiban bagi pengendali dan prosesor data dalam memastikan pemrosesan data dilakukan secara sah, adil, dan bertanggung jawab. Permasalahan muncul ketika prinsip-prinsip tersebut dihadapkan pada karakteristik blockchain yang dirancang untuk menyimpan data secara permanen dan sulit diubah maupun dihapus. Kondisi ini berpotensi menimbulkan konflik normatif, khususnya terkait pemenuhan hak penghapusan data (*right to erasure*), hak perbaikan data, serta hak untuk menarik persetujuan atas pemrosesan data pribadi yang telah tercatat dalam jaringan blockchain (Gruber et al., 2023).

Selain persoalan hak subjek data, blockchain juga menghadirkan tantangan terhadap konsep pertanggungjawaban hukum dalam rezim perlindungan data pribadi. Struktur blockchain yang terdesentralisasi menyebabkan tidak adanya satu entitas tunggal yang secara jelas dapat dikualifikasikan sebagai pengendali data (*data controller*) atau prosesor data (*data processor*) sebagaimana dimaksud dalam UU PDP. Dalam sistem konvensional, tanggung jawab hukum dapat ditelusuri kepada penyelenggara sistem elektronik yang mengelola data (Abidin, 2023). Sebaliknya, pada blockchain publik, data tersimpan dan

diverifikasi oleh banyak pihak yang tersebar di berbagai lokasi geografis. Situasi ini menimbulkan ketidakpastian hukum dalam menentukan pihak yang bertanggung jawab apabila terjadi pelanggaran data pribadi, kebocoran informasi, maupun penyalahgunaan data. Di samping itu, karakter lintas batas (*cross-border*) dari jaringan blockchain juga mempersulit penerapan yurisdiksi hukum nasional karena data dapat tersimpan dan diproses pada node yang berada di berbagai negara dengan rezim hukum yang berbeda.

Beberapa penelitian sebelumnya telah membahas hubungan antara blockchain dan perlindungan data pribadi, khususnya terkait konflik antara karakteristik imutabilitas blockchain dengan prinsip perlindungan data modern. Sebagian penelitian menyoroti tantangan penerapan hak penghapusan data dalam sistem blockchain, sementara penelitian lainnya membahas persoalan penentuan pengendali data dalam lingkungan yang terdesentralisasi. Namun demikian, kajian yang secara khusus menganalisis kesesuaian kerangka hukum perlindungan data pribadi Indonesia terhadap karakteristik blockchain masih relatif terbatas. Sebagian besar penelitian nasional lebih berfokus pada manfaat teknologi blockchain atau pembahasan normatif mengenai UU PDP secara umum, tanpa mengkaji secara mendalam konflik normatif yang muncul ketika kedua rezim tersebut dipertemukan. Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis kesesuaian kerangka hukum perlindungan data pribadi di Indonesia terhadap karakteristik blockchain, mengidentifikasi potensi konflik normatif yang muncul, serta menjelaskan implikasi hukumnya terhadap kepastian hukum dan perlindungan hak subjek data. Hasil penelitian diharapkan dapat memberikan kontribusi akademik dalam pengembangan kajian hukum siber sekaligus menjadi bahan pertimbangan dalam penyusunan kebijakan perlindungan data pribadi yang lebih adaptif terhadap perkembangan teknologi blockchain (Durovic & Willett, 2023).

2. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan kualitatif. Metode penelitian hukum normatif dipilih karena penelitian berfokus pada analisis norma hukum yang mengatur perlindungan data pribadi dalam kaitannya dengan karakteristik teknologi blockchain. Blockchain dalam penelitian ini tidak diposisikan sebagai objek kajian teknis, melainkan sebagai fenomena teknologi yang menimbulkan implikasi hukum terhadap perlindungan data pribadi dan kepastian hukum dalam sistem digital.

Pendekatan penelitian yang digunakan meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan perbandingan (*comparative approach*). Pendekatan perundang-undangan dilakukan melalui analisis terhadap berbagai regulasi yang berkaitan dengan perlindungan data pribadi dan penyelenggaraan sistem elektronik di Indonesia, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2024 (Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, n.d.) tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik. Pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang berkaitan dengan hak subjek data, tanggung jawab hukum, pengendali data, prosesor data, serta prinsip perlindungan data pribadi dalam lingkungan digital. Sementara itu, pendekatan perbandingan digunakan untuk menelaah pengaturan perlindungan data pribadi dalam sistem blockchain pada beberapa yurisdiksi lain sebagai bahan pembandingan dalam mengevaluasi kerangka hukum Indonesia.

Bahan hukum yang digunakan terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi dan transaksi elektronik. Adapun bahan hukum sekunder diperoleh dari jurnal ilmiah, buku, prosiding, laporan penelitian, serta publikasi akademik yang membahas blockchain, perlindungan data pribadi, dan hukum siber. Seluruh bahan hukum dikumpulkan melalui studi kepustakaan (*library research*) dan penelusuran dokumen hukum yang relevan (Rusdin Tahir, I Gde Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiharti, 2023).

Analisis dilakukan secara kualitatif melalui tahapan identifikasi isu hukum, inventarisasi norma hukum yang relevan, analisis konflik normatif, serta sintesis hasil penelitian. Fokus analisis diarahkan pada tiga isu utama, yaitu pemenuhan hak subjek data dalam sistem blockchain, penentuan tanggung jawab hukum dalam lingkungan terdesentralisasi, dan tantangan yurisdiksi hukum terhadap jaringan blockchain yang bersifat lintas batas. Hasil analisis kemudian disusun secara deskriptif-analitis untuk menjelaskan kesesuaian maupun potensi konflik antara karakteristik blockchain dan kerangka hukum perlindungan data pribadi di Indonesia (Benuef & Azhar, 2020).

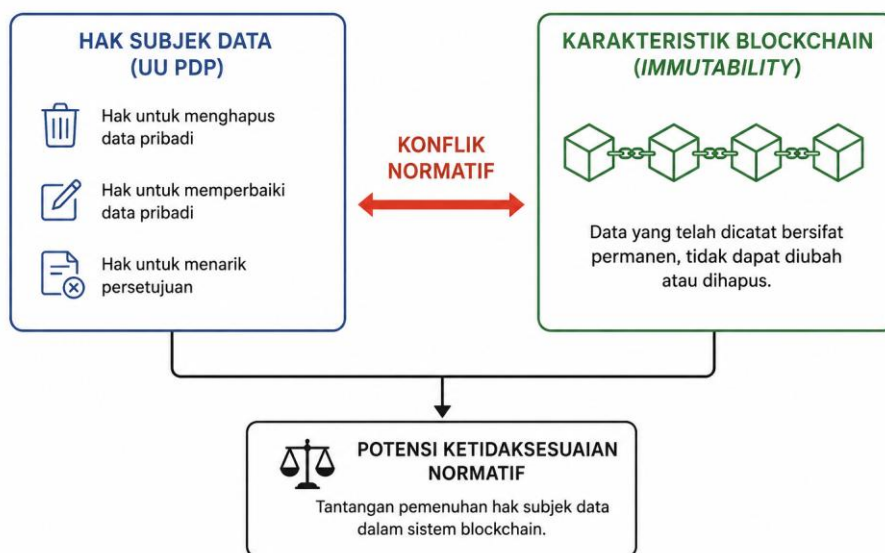
Tahapan penelitian dimulai dengan identifikasi permasalahan hukum melalui studi literatur dan penelusuran regulasi, dilanjutkan dengan analisis normatif terhadap ketentuan hukum yang berlaku. Selanjutnya dilakukan kajian perbandingan terhadap praktik pengaturan di beberapa yurisdiksi lain guna memperoleh perspektif yang lebih komprehensif. Tahap akhir penelitian berupa sintesis temuan dan perumusan rekomendasi konseptual mengenai penguatan perlindungan data pribadi dalam pemanfaatan teknologi blockchain di Indonesia.

3. Hasil dan Pembahasan

a. Konflik antara Hak dan Penghapusan Data dan Karakter Imutabel Blockchain

Salah satu tantangan utama dalam penerapan teknologi blockchain terhadap perlindungan data pribadi terletak pada konflik antara hak penghapusan data (*right to erasure*) yang diakui dalam rezim perlindungan data pribadi dengan karakteristik imutabilitas (*immutability*) yang menjadi fondasi utama blockchain. Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, subjek data diberikan sejumlah hak yang berkaitan dengan kendali atas data pribadinya, termasuk hak untuk memperbaiki, memperbarui, dan menghapus data pribadi dalam kondisi tertentu. Ketentuan tersebut mencerminkan prinsip bahwa individu tetap memiliki kontrol terhadap data pribadinya meskipun data tersebut telah diproses oleh pihak lain.

Di sisi lain, blockchain dirancang sebagai sistem pencatatan terdistribusi yang mengutamakan integritas dan keaslian data melalui mekanisme pencatatan permanen. Setiap data yang telah divalidasi dan dimasukkan ke dalam blok akan terhubung dengan blok lainnya menggunakan mekanisme kriptografi sehingga perubahan atau penghapusan data menjadi sangat sulit dilakukan. Karakteristik ini menjadi salah satu keunggulan utama blockchain karena mampu mencegah manipulasi data dan meningkatkan kepercayaan antar pengguna jaringan (Chen et al., 2023). Namun demikian, sifat permanen tersebut berpotensi bertentangan dengan prinsip perlindungan data pribadi yang memberikan hak kepada individu untuk meminta penghapusan atau koreksi terhadap data yang dimilikinya. Perbedaan karakteristik antara hak subjek data yang dijamin oleh UU PDP dan sifat imutabel blockchain dapat digambarkan sebagaimana ditunjukkan pada Gambar 1.



Gambar 1. Konflik antara Hak Penghapusan Data dalam UU PDP dan Karakter Imutabel Blockchain

Sebagaimana ditunjukkan pada Gambar 1, konflik normatif muncul karena UU PDP memberikan hak kepada subjek data untuk mengendalikan dan menghapus data pribadinya, sedangkan blockchain dirancang untuk mempertahankan integritas data melalui mekanisme pencatatan permanen. Konflik normatif muncul ketika data pribadi tersimpan secara langsung maupun tidak langsung dalam jaringan blockchain. Apabila seorang subjek data mengajukan permintaan penghapusan data sebagaimana dijamin dalam UU PDP, pelaksanaannya dapat menghadapi kendala teknis karena data yang telah tercatat pada

blockchain tidak dapat dihapus tanpa memengaruhi integritas keseluruhan rantai blok. Situasi ini menimbulkan pertanyaan mengenai sejauh mana hak penghapusan data dapat dilaksanakan dalam sistem yang secara desain justru dibangun untuk mempertahankan data secara permanen. Dengan demikian, terdapat ketidaksesuaian antara prinsip kontrol data oleh subjek data dengan prinsip ketidakberubahan data yang menjadi karakteristik utama blockchain.

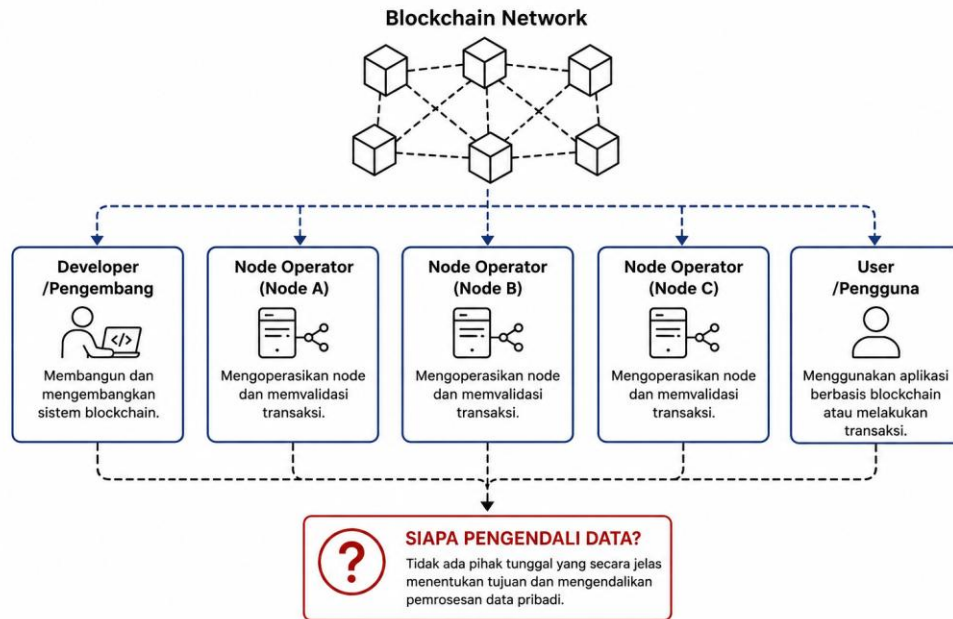
Meskipun demikian, beberapa pendekatan teknis telah dikembangkan untuk mengurangi konflik tersebut, seperti penggunaan *off-chain storage*, penyimpanan data dalam bentuk hash, maupun penerapan blockchain privat (*private blockchain*). Dalam model ini, data pribadi tidak disimpan secara langsung pada blockchain, melainkan ditempatkan pada sistem penyimpanan terpisah sehingga memungkinkan penghapusan atau perubahan data tanpa mengganggu integritas jaringan blockchain (Sari, Ningsih, et al., 2024). Namun, pendekatan tersebut belum sepenuhnya menyelesaikan persoalan dari perspektif hukum karena masih terdapat perdebatan mengenai apakah hash data dapat dikategorikan sebagai data pribadi apabila tetap memungkinkan identifikasi terhadap individu tertentu.

Berdasarkan analisis tersebut, dapat dipahami bahwa konflik antara hak penghapusan data dan karakter imutabel blockchain bukan sekadar persoalan teknis, melainkan juga persoalan normatif yang menunjukkan adanya ketidaksesuaian antara paradigma perlindungan data pribadi yang berpusat pada kontrol individu dengan desain blockchain yang berorientasi pada permanensi dan integritas data. Oleh karena itu, diperlukan interpretasi hukum maupun pengaturan yang lebih spesifik untuk menjamin bahwa pemanfaatan blockchain tetap sejalan dengan prinsip-prinsip perlindungan data pribadi tanpa menghilangkan manfaat utama teknologi tersebut.

b. Tantangan Penentuan Pengendali Data dalam Sistem Blockchain

Salah satu prinsip fundamental dalam rezim perlindungan data pribadi adalah adanya pihak yang bertanggung jawab terhadap pemrosesan data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi membedakan pihak yang terlibat dalam pemrosesan data menjadi pengendali data pribadi (*data controller*) dan prosesor data pribadi (*data processor*). Pengendali data merupakan pihak yang menentukan tujuan dan melakukan kendali terhadap pemrosesan data pribadi, sedangkan prosesor data menjalankan pemrosesan atas nama pengendali data. Pembagian peran tersebut menjadi dasar dalam menentukan tanggung jawab hukum apabila terjadi pelanggaran terhadap hak subjek data maupun kegagalan dalam pelindungan data pribadi (Sari, Thalib, et al., 2024).

Konsep tersebut relatif mudah diterapkan pada sistem informasi konvensional yang bersifat terpusat. Dalam sistem tersebut terdapat organisasi atau penyelenggara sistem elektronik yang secara jelas memiliki kewenangan untuk mengumpulkan, menyimpan, mengelola, dan menghapus data pribadi. Namun, kondisi yang berbeda ditemukan pada sistem blockchain, khususnya blockchain publik yang beroperasi melalui jaringan terdesentralisasi. Data dalam blockchain tidak dikelola oleh satu entitas tunggal, melainkan disimpan dan diverifikasi oleh banyak node yang tersebar dalam jaringan. Setiap peserta jaringan memiliki peran tertentu dalam menjaga konsistensi dan validitas data, sehingga struktur pengelolaan data menjadi lebih kompleks dibandingkan sistem elektronik konvensional (Beduschi, 2019).



Gambar 2. Ketidakjelasan Penentuan Pengendali Data dalam Sistem Blockchain

Sebagaimana terlihat pada Gambar 2, berbagai pihak dalam ekosistem blockchain memiliki keterlibatan dalam pemrosesan data, mulai dari pengembang sistem, operator node, hingga pengguna jaringan. Namun, tidak terdapat satu entitas yang secara eksklusif menentukan tujuan dan mengendalikan keseluruhan proses pemrosesan data sebagaimana diasumsikan dalam konsep pengendali data pada UU PDP.

Permasalahan muncul ketika terjadi pelanggaran data pribadi atau sengketa terkait pemrosesan data dalam jaringan blockchain. Dalam kondisi tersebut, sulit untuk menentukan pihak yang dapat dimintai pertanggungjawaban hukum karena tidak terdapat satu entitas yang secara eksklusif mengendalikan seluruh proses pemrosesan data. Pengembang sistem blockchain, operator node, penyedia aplikasi berbasis blockchain, maupun pengguna jaringan sama-sama memiliki keterlibatan dalam proses pemrosesan data, namun tingkat kendali yang dimiliki masing-masing pihak berbeda. Akibatnya, penerapan konsep pengendali data dan prosesor data sebagaimana diatur dalam UU PDP menjadi tidak sederhana ketika dihadapkan pada lingkungan blockchain yang terdesentralisasi (Anastasia et al., 2021).

Beberapa pendekatan telah dikembangkan untuk menjawab persoalan tersebut. Salah satu pendekatan adalah mengidentifikasi penyelenggara aplikasi berbasis blockchain sebagai pengendali data karena pihak tersebut umumnya menentukan tujuan pemrosesan data dan menyediakan layanan kepada pengguna. Pendekatan lain berupaya membagi tanggung jawab kepada beberapa pihak yang memiliki pengaruh terhadap pengelolaan data dalam jaringan. Namun demikian, hingga saat ini belum terdapat kesepakatan yang sepenuhnya diterima mengenai siapa yang seharusnya bertanggung jawab dalam sistem blockchain publik. Kondisi tersebut menunjukkan bahwa konsep pertanggungjawaban hukum yang berkembang dalam rezim perlindungan data pribadi masih berorientasi pada sistem yang memiliki struktur pengelolaan data yang jelas dan terpusat (Acerbi, 2022).

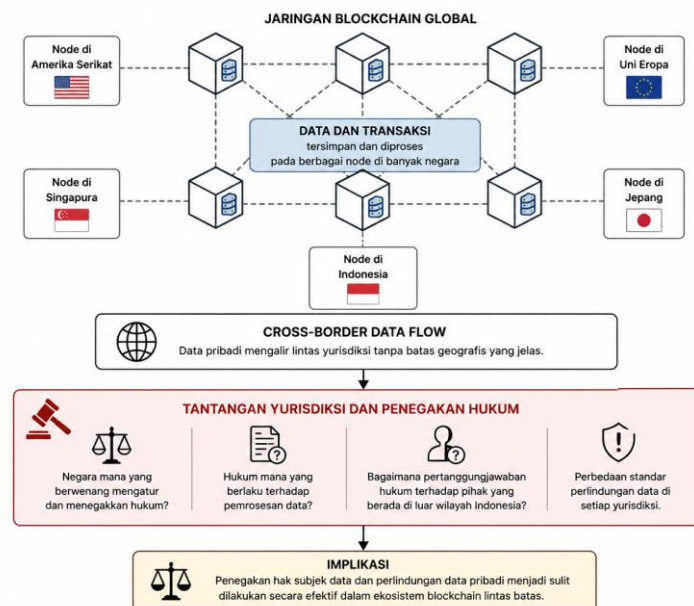
Berdasarkan analisis tersebut, dapat dipahami bahwa tantangan utama dalam penerapan UU PDP terhadap blockchain tidak hanya berkaitan dengan hak penghapusan data, tetapi juga menyangkut ketidakjelasan subjek hukum yang bertanggung jawab atas pemrosesan data pribadi. Karakter terdesentralisasi blockchain menyebabkan batas antara pengendali data dan prosesor data menjadi semakin kabur. Oleh karena itu, diperlukan interpretasi hukum maupun pedoman regulasi yang lebih spesifik untuk menentukan model pertanggungjawaban yang sesuai dengan karakteristik sistem blockchain tanpa mengurangi efektivitas perlindungan data pribadi.

c. Yurisdiksi dan Penegakan Hukum pada Blockchain Lintas Batas

Selain menimbulkan persoalan terkait hak subjek data dan penentuan pengendali data, blockchain juga menghadirkan tantangan terhadap penerapan yurisdiksi hukum nasional. Berbeda dengan sistem informasi konvensional yang umumnya dikelola dalam wilayah hukum tertentu, blockchain beroperasi

melalui jaringan terdistribusi yang memungkinkan data tersimpan dan diproses pada berbagai node yang berada di negara berbeda. Karakteristik ini menyebabkan aktivitas pemrosesan data tidak lagi terikat pada satu wilayah geografis tertentu sehingga menimbulkan kompleksitas dalam penentuan hukum yang berlaku (Ahmed & Pathan, 2020; Baktygul, 2023; Blockchain et al., 2019).

Dalam konteks perlindungan data pribadi, yurisdiksi memiliki peran penting dalam menentukan kewenangan negara untuk mengatur, mengawasi, dan menegakkan hukum terhadap pemrosesan data pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada dasarnya ditujukan untuk melindungi data pribadi warga negara Indonesia, termasuk dalam aktivitas pemrosesan data yang melibatkan pihak asing (Kominfo.go.id, n.d.). Namun demikian, penerapan ketentuan tersebut dapat menghadapi kendala ketika data pribadi tersimpan pada jaringan blockchain yang tersebar di berbagai negara dengan sistem hukum dan standar perlindungan data yang berbeda. Karakter lintas batas yang melekat pada blockchain serta implikasinya terhadap yurisdiksi dan penegakan hukum dapat digambarkan sebagaimana ditunjukkan pada Gambar 3.



Gambar 3. Tantangan Yurisdiksi dan Penegakan Hukum pada Jaringan Blockchain Global

Permasalahan semakin kompleks apabila terjadi pelanggaran data pribadi atau sengketa hukum yang melibatkan lebih dari satu yurisdiksi. Dalam kondisi tersebut, muncul pertanyaan mengenai negara mana yang memiliki kewenangan untuk melakukan penegakan hukum, hukum mana yang harus diterapkan, serta bagaimana mekanisme pertanggungjawaban dapat dilaksanakan terhadap pihak-pihak yang berada di luar wilayah Indonesia. Karakter anonim dan terdesentralisasi yang melekat pada blockchain juga berpotensi menyulitkan proses identifikasi pihak yang terlibat dalam pemrosesan data (Thalib et al., 2024).

Sebagaimana terlihat pada praktik pemanfaatan blockchain secara global, data dan transaksi dapat mengalir melintasi berbagai wilayah hukum tanpa batas yang jelas. Kondisi ini menunjukkan bahwa pendekatan regulasi yang hanya berfokus pada batas teritorial negara menjadi kurang memadai ketika dihadapkan pada teknologi blockchain. Oleh karena itu, perlindungan data pribadi dalam lingkungan blockchain memerlukan pendekatan yang tidak hanya mengandalkan regulasi nasional, tetapi juga memperhatikan prinsip kerja sama lintas negara dan harmonisasi standar perlindungan data.

Berdasarkan analisis tersebut, dapat dipahami bahwa tantangan yurisdiksi merupakan konsekuensi logis dari sifat blockchain yang bersifat global dan terdesentralisasi. Meskipun UU PDP telah memberikan dasar hukum bagi perlindungan data pribadi di Indonesia, efektivitas penegakannya masih menghadapi berbagai kendala ketika diterapkan pada jaringan blockchain lintas batas. Oleh karena itu, diperlukan penguatan mekanisme kerja sama internasional serta pengembangan kebijakan yang mampu

mengakomodasi karakter global teknologi blockchain tanpa mengurangi perlindungan terhadap hak-hak subjek data.

d. Implikasi dan Arah Penguatan Regulasi Perlindungan Data Pribadi dalam Sistem Blockchain

Hasil analisis menunjukkan bahwa penerapan teknologi blockchain dalam pengelolaan data pribadi menghadirkan sejumlah tantangan yang belum sepenuhnya dapat diakomodasi oleh kerangka hukum perlindungan data pribadi yang berlaku di Indonesia. Setidaknya terdapat tiga isu utama yang muncul, yaitu konflik antara hak penghapusan data dan karakter imutabel blockchain, ketidakjelasan penentuan pengendali data dalam sistem terdesentralisasi, serta kompleksitas yurisdiksi dalam jaringan blockchain lintas batas. Ketiga isu tersebut menunjukkan bahwa perkembangan teknologi blockchain tidak hanya menimbulkan persoalan teknis, tetapi juga memunculkan tantangan normatif yang memerlukan respons hukum yang memadai.

Temuan penelitian ini memperlihatkan bahwa konsep perlindungan data pribadi yang diadopsi dalam UU PDP pada dasarnya masih berorientasi pada sistem pemrosesan data yang terpusat. Dalam model tersebut, terdapat pihak yang secara jelas berperan sebagai pengendali data dan memiliki kemampuan untuk melakukan pengelolaan, perubahan, maupun penghapusan data sesuai dengan hak yang dimiliki oleh subjek data. Sebaliknya, blockchain dikembangkan berdasarkan prinsip desentralisasi dan permanensi data yang dalam beberapa kondisi justru menyulitkan pelaksanaan hak-hak tersebut. Akibatnya, terdapat kesenjangan antara asumsi yang digunakan dalam regulasi perlindungan data pribadi dengan karakteristik teknologi blockchain yang berkembang saat ini.

Meskipun demikian, kondisi tersebut tidak serta-merta menunjukkan bahwa blockchain tidak dapat diterapkan dalam kerangka hukum Indonesia. Sebaliknya, temuan penelitian ini mengindikasikan perlunya pendekatan regulasi yang lebih adaptif terhadap perkembangan teknologi digital. Penguatan regulasi dapat dilakukan melalui penyusunan pedoman khusus mengenai pemrosesan data pribadi pada sistem blockchain, penegasan mekanisme pertanggungjawaban hukum dalam lingkungan terdesentralisasi, serta pengaturan yang lebih jelas mengenai pemrosesan data pribadi yang melibatkan jaringan lintas negara. Pendekatan tersebut penting untuk memberikan kepastian hukum bagi penyelenggara sistem berbasis blockchain sekaligus menjamin perlindungan hak-hak subjek data.

Selain itu, pengembangan kebijakan di masa mendatang perlu mempertimbangkan keseimbangan antara perlindungan data pribadi dan dukungan terhadap inovasi teknologi. Regulasi yang terlalu ketat berpotensi menghambat pemanfaatan blockchain dalam berbagai sektor, sementara regulasi yang terlalu longgar dapat menimbulkan risiko terhadap hak privasi individu. Oleh karena itu, diperlukan pendekatan yang proporsional sehingga perlindungan data pribadi dapat berjalan seiring dengan perkembangan teknologi blockchain yang semakin luas digunakan dalam berbagai aktivitas digital (Judijanto et al., 2024).

Berdasarkan hasil penelitian ini, dapat dipahami bahwa tantangan utama perlindungan data pribadi dalam sistem blockchain tidak terletak pada teknologinya semata, melainkan pada kebutuhan untuk menyesuaikan kerangka hukum yang ada dengan karakteristik sistem terdesentralisasi. Dengan demikian, penguatan regulasi dan interpretasi hukum yang adaptif menjadi langkah penting untuk memastikan bahwa pemanfaatan blockchain di Indonesia tetap memberikan manfaat inovatif tanpa mengurangi efektivitas perlindungan data pribadi.

4. Kesimpulan

Penelitian ini menunjukkan bahwa penerapan teknologi blockchain dalam pengelolaan data pribadi menghadirkan tantangan normatif terhadap kerangka hukum perlindungan data pribadi di Indonesia. Konflik utama muncul dari perbedaan karakteristik antara prinsip perlindungan data pribadi yang menempatkan subjek data sebagai pihak yang memiliki kendali atas data pribadinya dengan karakter blockchain yang bersifat terdesentralisasi dan imutabel. Kondisi tersebut terlihat dari sulitnya pelaksanaan hak penghapusan dan perbaikan data, ketidakjelasan penentuan pengendali data dalam jaringan blockchain, serta kompleksitas yurisdiksi pada pemrosesan data yang berlangsung lintas batas negara.

Hasil penelitian menunjukkan bahwa kerangka hukum perlindungan data pribadi yang berlaku saat ini pada dasarnya masih berorientasi pada sistem pemrosesan data yang terpusat, sehingga menghadapi berbagai tantangan ketika diterapkan pada ekosistem blockchain. Oleh karena itu, diperlukan pendekatan regulasi yang lebih adaptif melalui penguatan interpretasi hukum, penyusunan pedoman khusus mengenai pemrosesan data pribadi dalam sistem blockchain, serta pengembangan mekanisme kerja sama lintas

yurisdiksi untuk mendukung efektivitas perlindungan data pribadi. Penelitian selanjutnya dapat diarahkan pada kajian yang lebih spesifik mengenai model pertanggungjawaban hukum dalam blockchain maupun evaluasi implementasi teknologi blockchain pada sektor-sektor yang memproses data pribadi secara intensif, seperti layanan keuangan digital, identitas digital, dan layanan publik berbasis elektronik.

5. Ucapan Terima Kasih

Penulis menyampaikan apresiasi dan terima kasih kepada Institut Bisnis dan Teknologi Indonesia (INSTIKI) atas dukungan pendanaan dan fasilitasi penelitian melalui skema **INSTIKI Research and Development Program (IRD P) Tahun 2026**. Dukungan tersebut telah memberikan kesempatan bagi penulis untuk melaksanakan penelitian mengenai perlindungan data pribadi dalam sistem blockchain serta menghasilkan luaran ilmiah yang diharapkan dapat berkontribusi pada pengembangan kajian hukum siber dan regulasi teknologi digital di Indonesia.

Daftar Pustaka

- Abidin, M. I. (2023). Legal Review of the Validity of the Use of Smart Contracts in Business Transactions in Indonesia and Its Regulation in Various Countries. *Unnes Law Journal*, 9(2), 289–310. <https://doi.org/10.15294/ulj.v9i2.74957>
- Acerbi, P. (2022). Is blockchain technology a challenge for antitrust law? *Competition Law & Policy Debate*, 5(3). <https://doi.org/10.4337/clpd.2019.03.09>
- Ahmed, M., & Pathan, A.-S. K. (2020). Blockchain: Can It Be Trusted? *Computer*, 53(4), 31–35. <https://doi.org/10.1109/MC.2019.2922950>
- Anastasia, L., Dewi, T., Kenotariatan, M., Putu, N., & Meinarni, S. (2021). ANALISIS EKONOMI TERHADAP HUKUM DALAM KEGAGALAN PERLINDUNGAN DATA PRIBADI PENGGUNA E-COMMERCE ECONOMIC ANALYSIS OF LAW IN FAILURE TO PERSONAL DATA PROTECTION OF E-COMMERCE USERS I Dewa Gede Dana Sugama. *Jurnal IUS Kajian Hukum Dan Keadilan*, 9(3). <http://jurnalius.ac.id/ojs/index.php/jurnalIUSDOI:http://dx.doi.org/10.29303/ius.v9i3.978>
- Baktygul, K. (2023). International Law in The Era of Blockchain: Law Semiotics. *International Journal for the Semiotics of Law*, 36(6). <https://doi.org/10.1007/s11196-023-10017-y>
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data and Society*, 6(2). <https://doi.org/10.1177/2053951719855091>
- Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Gema Keadilan*, 7(1), 20–33. <https://doi.org/10.14710/gk.2020.7504>
- Blockchain, T., Law ; Quintais, J., Bodo, B., Giannopoulou, A., & Ferrari, V. (2019). Blockchain and the Law: Critical Evaluation. In *Stanford Journal of Blockchain Law & Policy* (Vol. 86, Issue 1).
- Chen, C., Huang, H., Zhao, B., Shu, D., & Wang, Y. (2023). The Research of AHP-Based Credit Rating System on a Blockchain Application. *Electronics (Switzerland)*, 12(4). <https://doi.org/10.3390/electronics12040887>
- Durovic, M., & Willett, C. (2023). A Legal Framework for Using Smart Contracts in Consumer Contracts: Machines as Servants, Not Masters. *Modern Law Review*, 86(6). <https://doi.org/10.1111/1468-2230.12817>
- Gruber, J., Hargreaves, C. J., & Freiling, F. C. (2023). Contamination of digital evidence: Understanding an underexposed risk. *Forensic Science International: Digital Investigation*, 44, 301501. <https://doi.org/10.1016/j.fsidi.2023.301501>
- Holden, R., & Malani, A. (2022). The Law and Economics of Blockchain. *Annual Review of Law and Social Science*, 18. <https://doi.org/10.1146/annurev-lawsocsci-011921-060322>
- Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20–29. <https://doi.org/10.58812/eslhr.v3i01.351>

- Kominfo.go.id. (n.d.). *Sesditjen IKP : Perlu segera UU Perlindungan Data Pribadi*. 2013. Retrieved June 18, 2018, from https://kominfo.go.id/index.php/content/detail/1337/Sesditjen+IKP+%3A+Perlu+segera+UU+Perlindungan+Data+Pribadi/0/berita_satker
- Rusdin Tahir, I Gde Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiharti, S. R. P. (2023). *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori dan Praktek*. Sonpedia.
- Sari, H. B., Ningsih, N. M. A. P. C., Kristina, N. M. Y., Rismayanti, N. P. I., Thalib, E. F., Meinarni, N. P. S., & Julianti, L. (2024). DIGITAL ETHICS AND CITIZENSHIP CHALLENGES IN CYBERSPACE: AN OVERVIEW FROM PERSPECTIVE MORALS AND LAWS. *NOTARIIL Jurnal Kenotariatan*, 9(1), 33–39. <https://doi.org/10.22225/jn.9.1.2024.33-39>
- Sari, H. B., Thalib, E. F., & Meinarni, N. P. S. (2024). IMPLEMENTATION OF SMART CONTRACTS IN INDONESIA: AN ANALYSIS OF FINANCIAL REGULATION, TAXATION, AND CONSUMER PROTECTION. *NOTARIIL Jurnal Kenotariatan*, 9(2), 65–70. <https://doi.org/10.22225/jn.9.2.2024.65-70>
- Thalib, E. F., Sari, H. B., & Meinarni, N. P. S. (2024). Analysis of the Internet of Things (IoT) and Its Impact on Individual Privacy from the Perspective of Indonesian Law. In *ISAR Journal of Arts, Humanities and Social Sciences* (Vol. 2, Issue 11, pp. 153–157). <https://isarpublisher.com/journal/isarjahss>
- Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Retrieved August 4, 2024, from <https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024>
- Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).