

PELINDUNGAN DATA PRIBADI DALAM PENGGUNAAN *SMART*
***CONTRACT* DI INDONESIA**
PERSONAL DATA PROTECTION IN THE USE OF SMART CONTRACTS
IN INDONESIA

Angela Claudia Scolastika Manurung, Tengku Keizerina Devi Azwar dan
Joiverdia Arifiyanto

Magister Ilmu Hukum, Universitas Sumatera Utara

Korespondensi Penulis: angelascolastika16@gmail.com, keizerina.devi@usu.ac.id,
joiverdia@usu.ac.id

Citation Structure Recommendation :

Manurung, Angela Claudia Scolastika, Tengku Keizerina Devi Azwar dan Joiverdia Arifiyanto.
Pelindungan Data Pribadi dalam Penggunaan Smart Contract di Indonesia. Jurnal Hukum Lex
Generalis. Vol.7. No.4 (2026).

ABSTRAK

Perkembangan blockchain melahirkan smart contract yang mengeksekusi perjanjian secara otomatis, transparan dan efisien, tetapi sekaligus menimbulkan persoalan perlindungan data pribadi karena sifatnya yang permanen, immutable dan terdesentralisasi. Penelitian ini bertujuan menganalisis kerangka hukum, tantangan penerapan dan bentuk perlindungan hukum ideal bagi pengguna smart contract di Indonesia. Dengan metode yuridis normatif dan pendekatan perundang-undangan serta konseptual, penelitian ini bersifat deskriptif analitis berbasis data sekunder. Hasilnya menunjukkan bahwa perlindungan hukum bertumpu pada UU PDP, UU ITE, KUH Perdata, namun belum ada pengaturan khusus. Diperlukan *lex specialis*, Privacy by Design dan penguatan kelembagaan pengawas. Upaya tersebut diharapkan mampu menjamin kepastian hukum sekaligus menyeimbangkan inovasi teknologi blockchain dengan pemenuhan hak privasi pengguna.

Kata Kunci: Blockchain, Data Pribadi, Pelindungan Hukum, *Smart Contract*

ABSTRACT

Blockchain's development has given rise to smart contracts that execute agreements automatically, transparently and efficiently, but at the same time it creates personal data protection issues because of their permanent, immutable and decentralized nature. This study aims to analyze the legal framework, implementation challenges and the ideal form of legal protection for smart contract users in Indonesia. Using a normative juridical method with statutory and conceptual approaches, this descriptive-analytical study is based on secondary data. The results show that legal protection is currently grounded in the PDP Law, the ITE Law and the Civil Code, yet no specific regulation has been

established. Therefore, a lex specialis, Privacy by Design and stronger supervisory institutions are needed. These efforts are expected to guarantee legal certainty while balancing blockchain technological innovation with the fulfillment of users' privacy rights.

Keywords: *Blockchain, Legal Protection, Personal Data, Smart Contract*

A. PENDAHULUAN

Teknologi dan informasi diciptakan untuk melayani dan memberikan kemudahan bagi setiap warga negara. Karena sifatnya yang terus berkembang dan menjangkau konteks kerja sama internasional, harus dicatat bahwa ada batasan agar tidak melanggar identitas manusia, hak asasi manusia, privasi dan kebebasan individu atau publik.¹ Perkembangan teknologi digital dalam beberapa dekade terakhir telah membawa perubahan fundamental dalam berbagai sektor kehidupan. Salah satu inovasi yang muncul dari perkembangan teknologi *blockchain* adalah *Smart contract* atau kontrak pintar, yang merupakan protokol komputer yang dirancang untuk memverifikasi, mengontrol, atau mendokumentasikan peristiwa dan tindakan secara digital sesuai dengan ketentuan kontrak atau perjanjian.² *Smart contract* telah mulai diadopsi di berbagai sektor seperti keuangan, rantai pasok, *real estate* dan berbagai industri lainnya karena kemampuannya untuk mengotomatisasi proses bisnis dan mengurangi kebutuhan akan perantara.³

Kecepatan dan efisiensi dalam pelaksanaan kontrak dapat meningkat, sejalan dengan asas kebebasan berkontrak. Namun, kendati *Smart contract* memberikan kebebasan dalam perjanjian, perlu diperhatikan juga bahwa kemungkinan terjadinya pelanggaran kontrak secara otomatis memunculkan pertanyaan hukum tertentu. Ketidakpastian hukum yang berkaitan dengan keabsahan keberadaan *Smart contract* dan penegakan hukum terkait dengan teknologi ini menjadi fokus analisis yuridis.⁴

¹ Joiverdia Arifiyanto, *Pelindungan Data Pribadi dan Regulasi Fintech (Penerapan di Prancis dan Indonesia)*, Tri Selaras Cendekia, Medan, 2024.

² Korintus Wilson Horas Hutapea dan Adi Sulistiyono, *Keabsahan Smart Contract dengan Teknologi Blockchain Menurut Kitab Undang-Undang Hukum Perdata*, Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora, Vol.1, No.3 (2024).

³ Bima Danubrata Adhijoso, *Legalitas Penerapan Smart Contract Dalam Asuransi Pertanian di Indonesia*, Jurist-Diction, Vol.2, No.2 (2019).

⁴ Andini Eka Budiyanto, *Analisis Yuridis Penggunaan Smart Contract dalam Perspektif Asas Kebebasan Berkontrak*, Jurnal Sains Student Research, Vol.1, No.1 (2023).

Di tengah era transformasi digital yang semakin intensif, keamanan data pribadi menjadi perhatian utama bagi masyarakat dan pemerintah di seluruh dunia. Data pribadi, yang meliputi identitas personal, informasi keuangan, riwayat kesehatan dan berbagai informasi sensitif lainnya, menjadi komoditas berharga dalam ekosistem digital.⁵ Seiring dengan meningkatnya volume dan kompleksitas data yang dihasilkan, dikumpulkan dan diproses setiap harinya, potensi penyalahgunaan data juga semakin tinggi, yang dapat mengakibatkan kerugian finansial, pencurian identitas, pelanggaran privasi, hingga dampak psikologis bagi individu.⁶

Indonesia, sebagai negara dengan populasi pengguna internet yang besar dan pertumbuhan ekonomi digital yang pesat, menghadapi tantangan yang signifikan.⁷ Masyarakat Indonesia semakin aktif dalam menggunakan layanan digital, mulai dari *e-commerce*, perbankan digital, *transportasi online*, hingga layanan kesehatan digital, yang kesemuanya melibatkan pertukaran dan pemrosesan data pribadi.⁸ Namun, kesadaran akan pentingnya perlindungan data pribadi masih relatif rendah di kalangan masyarakat, sementara regulasi yang komprehensif baru saja disahkan pada 2022 melalui Undang-Undang Pelindungan Data Pribadi.

Ekonomi global saat ini bergeser ke arah ekonomi berbasis pengetahuan, di mana informasi dan pengetahuan menjadi faktor utama dalam mendorong pertumbuhan ekonomi.⁹ Di tengah kondisi ini, perkembangan teknologi *blockchain* dan *Smart contract* di Indonesia yang juga semakin pesat. Berbagai lembaga keuangan, *startup* teknologi dan bahkan instansi pemerintah mulai mengeksplorasi dan mengaplikasikan teknologi ini guna meningkatkan efisiensi,

⁵ Elsa Daniella Simbolon, dkk., *Pelindungan Korban Pemalsuan Data Diri dalam Transaksi Pinjaman Online melalui Penegakan Hak untuk Dilupakan*, Neoclassical Legal Review: Journal of Law and Contemporary Issues, Vol.3, No.2 (2024).

⁶ Tia Deja Pohan dan Muhammad Irwan Padli Nasution, *Perlindungan Hukum Data Pribadi Konsumen dalam Platform E Commerce*, Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, Vol.1, No.3 (2023).

⁷ Sakirman, dkk., *Kepastian Hukum Smart Contract dalam Perspektif Hukum Perdata*, Rewang Rencang: Jurnal Hukum Lex Generalis, Vol.5, No.10 (2024).

⁸ Erna Priliasari, *Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia*, Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, Vol.12, No.2 (2023).

⁹ Joiverdia Arifiyanto, *Konsep Data Pribadi dalam Fintech (Perspektif Hukum dan Hak Asasi Manusia)*, Tri Selaras Cendekia, Medan, 2024.

transparansi dan keamanan dalam berbagai proses bisnis dan layanan publik.¹⁰ *Smart contract* menawarkan potensi besar untuk revolusi dalam berbagai sektor, namun juga menimbulkan pertanyaan dan kekhawatiran.¹¹

Karakteristik utama dari *blockchain*, termasuk *immutability* (tidak dapat diubah) dan transparansi, menimbulkan tantangan tersendiri dalam konteks pelindungan data pribadi. Di satu sisi, sifat tidak dapat diubah dari *blockchain* memberikan jaminan keamanan dan integritas data. Namun di sisi lain, hal ini dapat bertentangan dengan beberapa prinsip pelindungan data, seperti hak untuk dilupakan (*right to be forgotten*) dan hak untuk memodifikasi data pribadi yang tidak akurat.¹² Selain itu, transparansi *blockchain*, meskipun menjadi kekuatan dalam mencegah manipulasi data, dapat menimbulkan risiko terhadap kerahasiaan data pribadi jika tidak dirancang dengan tepat.¹³

Tujuan dari pengaturan ini adalah untuk melindungi privasi, keamanan dan hak-hak konsumen dalam penggunaan data pribadi mereka. Terkait dengan pelindungan hukum, Isnaenil mengatakan bahwa berdasarkan sumbernya pelindungan hukum dapat dibagi menjadi 2 (dua) jenis yaitu pelindungan internal dan pelindungan eksternal. Pelindungan hukum internal dapat diwujudkan oleh para pihak, disaat kedudukan hukum antara kedua pihak relatif seimbang, artinya mereka memiliki *bargaining power* yang berimbang, sehingga atas dasar hak asasi manusia, para pihak mempunyai keleluasaan untuk menyatakan kehendak sesuai kepentingannya. Hal ini menjadi landasan saat para pihak menyusun klausul-klausul kesepakatan, sehingga pelindungan hukum dapat terwujud sesuai kebutuhan para pihak. Pelindungan hukum eksternal yang dibuat oleh penguasa lewat regulasi dapat memberikan pelindungan bagi kepentingan pihak yang lemah. Hakekat peraturan perundang-undangan harus seimbang dan tidak boleh berat sebelah.¹⁴

¹⁰ Willion Lim, dkk., *Smart Contracts: Validitas Hukum dan Tantangan di Masa Depan Indonesia*, Jurnal Kewarganegaraan, Vol.8, No.1 (2024).

¹¹ Jecelyn Amanda Dethan dan Yericia Evadne Giralani Irianto, *Analisis Keabsahan Smart Contract dalam Perjanjian Bisnis di Indonesia*, UNES Law Review, Vol.7, No.1 (2024).

¹² SIP Law Firm, *Penggunaan Smart contract dalam Perbankan dan Implikasinya*, diakses dari <https://siplawfirm.id/penggunaan-smart-contract-dalam-perbankan-dan-implikasinya/?lang=id>, diakses pada 30 Agustus 2025.

¹³ Imelda Martinelli, dkk., *Legalitas dan Efektivitas Penggunaan Teknologi Blockchain terhadap Smart Contract Pada Perjanjian Bisnis di Masa Depan*, UNES Law Review, Vol.6, No.4 (2024).

¹⁴ Moch. Isnaeni, *Seberkas Diaroma Hukum Kontrak*, Revka Petra Media, Surabaya, 2017.

Pelindungan data pribadi dalam penggunaan *Smart contract* menjadi semakin relevan mengingat adopsi teknologi *blockchain* yang terus meningkat. Baik pemerintah, pelaku bisnis, maupun masyarakat umum perlu memahami implikasi penggunaan *Smart contract* terhadap privasi dan keamanan data pribadi, serta bagaimana menyeimbangkan inovasi teknologi dengan pelindungan hak individu atas data mereka.¹⁵

Permasalahan pelindungan data pribadi dalam penggunaan *Smart contract* di Indonesia menjadi semakin kompleks karena beberapa faktor. Pertama, kerangka hukum untuk pelindungan data pribadi di Indonesia masih relatif baru dan dalam tahap implementasi. Undang-Undang Pelindungan Data Pribadi (UU PDP) yang disahkan pada September 2022 menjadi tonggak penting dalam upaya melindungi data pribadi warga negara Indonesia. Namun, UU ini masih memerlukan berbagai peraturan pelaksana untuk mengatur aspek-aspek teknis, termasuk bagaimana prinsip-prinsip pelindungan data pribadi diterapkan dalam konteks teknologi spesifik seperti *blockchain* dan *Smart contract*.

Kedua, masih terdapat kesenjangan pengetahuan dan kesadaran di antara pemangku kepentingan mengenai implikasi penggunaan *Smart contract* terhadap pelindungan data pribadi. Banyak pelaku bisnis dan pengembang teknologi yang fokus pada manfaat dan efisiensi dari *Smart contract*, tanpa mempertimbangkan secara mendalam aspek privasi dan keamanan data. Di sisi lain, regulator dan pembuat kebijakan juga dihadapkan pada tantangan untuk memahami kompleksitas teknologi ini dan merumuskan kebijakan yang seimbang antara mendorong inovasi dan melindungi hak-hak individu.

Ketiga, *Smart contract* yang beroperasi pada jaringan *blockchain* publik bersifat lintas batas, yang berarti data dapat disimpan dan diproses di berbagai yurisdiksi dengan aturan pelindungan data yang berbeda-beda. Hal ini menimbulkan pertanyaan tentang yurisdiksi dan penegakan hukum dalam kasus pelanggaran data pribadi. Selain itu, prinsip-prinsip dasar pelindungan data pribadi seperti transparansi, persetujuan (*consent*) dan pembatasan tujuan penggunaan data perlu diterjemahkan ke dalam konteks *Smart contract*, yang memiliki karakteristik unik seperti otomatisasi dan *immutability*.

¹⁵ Farens Sebastian Fahlevi dan Zuhda Mila Fitriana, *Keabsahan Smart Contract Sebagai Solusi Praktik Manipulasi Kontrak di Indonesia*, Kabilah: Journal of Social Community, Vol.9, No.2 (2024).

Di sisi teknis, tantangan juga muncul dalam perancangan *Smart contract* yang memenuhi prinsip-prinsip pelindungan data pribadi. Misalnya, bagaimana memastikan bahwa data pribadi yang sensitif tidak tersimpan secara langsung pada *blockchain* yang bersifat publik, atau bagaimana mengimplementasikan mekanisme persetujuan yang efektif dalam konteks transaksi yang terautomatisasi. Inovasi dalam "*privacy by design*" untuk *Smart contract* menjadi penting, di mana pertimbangan privasi dan pelindungan data diintegrasikan sejak tahap awal perancangan.¹⁶

Di tengah kompleksitas ini, terdapat peluang bagi Indonesia untuk mengembangkan pendekatan regulasi dan praktik terbaik yang dapat menjadi model bagi negara-negara lain. Dengan memadukan pemahaman mendalam tentang teknologi *blockchain*, prinsip-prinsip pelindungan data pribadi dan konteks sosial-budaya Indonesia, para pemangku kepentingan dapat bersama-sama menciptakan ekosistem di mana *Smart contract* dapat berkembang tanpa mengorbankan privasi dan keamanan data pribadi warga negara.

Latar belakang ini menunjukkan bahwa pelindungan data pribadi dalam penggunaan *Smart contract* di Indonesia bukan hanya masalah teknis atau hukum semata, tetapi juga melibatkan aspek sosial, etika dan tata kelola yang kompleks. Diperlukan pendekatan kolaboratif dan multi-disiplin untuk mengatasi tantangan ini, dengan melibatkan pemerintah, sektor swasta, akademisi, masyarakat sipil dan pengguna teknologi itu sendiri. Melalui dialog dan kerjasama yang berkelanjutan, Indonesia dapat memanfaatkan potensi *Smart contract* sambil tetap melindungi hak-hak fundamental warganya atas privasi dan keamanan data pribadi mereka.

Penelitian ini dijamin keasliannya dan belum pernah diteliti sebelumnya. Meskipun terdapat lima penelitian terdahulu, seperti karya M. Ulil Azmi (2023) tentang risiko hukum *smart contract* di Ethereum, Ilena Prinindyta Harum (2020) mengenai *e-commerce* dan perbandingan hukum Singapura, M. Rizqon Baihaiqi (2021) terkait pengembangan *Artificial Intelligence*, Andrew G.A Pelealu (2018) mengenai *e-commerce* berbasis UU ITE, serta Andi S. Putri terkait kontrak bisnis,

¹⁶ Gabriella Rachel Mansula, *Pelindungan Hukum Atas Penyelesaian Hukum Tidak Berfungsinya Proses Transaksi Melalui Smart Contract Pada Sistem Blockchain*, Al Qodiri: Jurnal Pendidikan, Sosial dan Keagamaan, Vol.21, No.2 (2023).

penelitian ini secara fundamental berbeda karena fokus utamanya secara spesifik mengkaji aspek perlindungan data pribadi pengguna *smart contract* pasca-pengesahan UU PDP 2022, khususnya interaksi antara sifat *blockchain* yang *immutable* dan terdesentralisasi dengan prinsip privasi seperti *Privacy by Design* serta pertanggungjawaban hukumnya.

Berdasarkan hal tersebut, ada tiga permasalahan yang diteliti dalam penelitian ini yaitu:

1. Bagaimana kerangka hukum perlindungan data pribadi pengguna *smart contract* di Indonesia?
2. Apa saja tantangan hukum dalam penerapan perlindungan data pribadi pengguna *smart contract* di Indonesia?
3. Bagaimana bentuk perlindungan hukum yang ideal bagi pengguna *smart contract* di Indonesia?

Penelitian hukum normatif yang bersifat deskriptif-analitis ini menggunakan pendekatan perundang-undangan, konseptual dan kasus untuk mengkaji perlindungan data pribadi dalam penggunaan *smart contract* di Indonesia. Data yang digunakan berupa data sekunder, terdiri atas bahan hukum primer (seperti UUD 1945, KUHPerdata, UU PDP, UU ITE dan PP No. 71/2019), bahan hukum sekunder (jurnal dan literatur ilmiah), serta bahan hukum tersier, yang dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara yuridis-kualitatif berbasis metode interpretasi hukum.

B. PEMBAHASAN

1. Kerangka Hukum Pelindungan Data Pribadi Pengguna *Smart Contract* di Indonesia

Kehadiran UU PDP yang mulai diberlakukan secara penuh setelah berakhirnya masa transisi dua tahun menandai tonggak sejarah perlindungan privasi di Indonesia. UU PDP ini berasaskan perlindungan, kepastian hukum, pertanggungjawaban dan kerahasiaan untuk menjamin hak fundamental warga negara atas data pribadinya.¹⁷ Namun, ketika prinsip-prinsip UU PDP dihadapkan pada arsitektur teknis *blockchain* yang menopang *smart contract*,

¹⁷ Andini Eka Budiyo, *Op.Cit.*.

timbul benturan yuridis yang sangat mendasar. Karakteristik *blockchain* yang terdesentralisasi dan tidak dapat diubah secara langsung bertentangan dengan pilar-pilar pelindungan data modern.¹⁸

Titik benturan paling krusial terletak pada pemenuhan hak subjek data untuk meminta penghapusan datanya, atau dikenal sebagai hak untuk dihapus sebagaimana diatur dalam Pasal 8 UU PDP. Karakteristik dasar *blockchain* mengasumsikan bahwa setelah suatu data divalidasi dan dimasukkan ke dalam blok, data tersebut bersifat permanen dan tidak dapat diubah atau dihapus oleh pihak manapun. Ketidakmampuan teknis ini menciptakan ketidakpatuhan bawaan terhadap hak subjek data untuk menarik kembali persetujuan pemrosesan atau meminta pemusnahan data mereka.¹⁹ Benturan kedua berkaitan dengan prinsip minimalisasi data (*data minimization*) yang termaktub dalam UU PDP, di mana pengumpulan data harus dibatasi hanya pada informasi yang diperlukan sesuai dengan tujuan pemrosesan yang sah. Sebaliknya, dalam arsitektur *blockchain* publik, setiap transaksi disebarluaskan ke seluruh node dalam jaringan global untuk mencapai konsensus.²⁰

Hal ini tidak hanya melanggar prinsip minimalisasi, tetapi juga menabrak ketentuan transfer data pribadi lintas batas negara dalam Pasal 56 UU PDP, yang mewajibkan adanya kesetaraan tingkat pelindungan data di negara penerima sebelum data ditransfer. Selain itu, UU PDP membebankan tanggung jawab hukum utama pada Pengendali Data Pribadi, yaitu pihak yang menetapkan tujuan dan melakukan kendali atas pemrosesan data. Dalam ekosistem aplikasi terdesentralisasi (*decentralized applications*) yang dijalankan oleh *smart contract*, ketiadaan dari otoritas pusat membuat ketentuan dari penetapan Pengendali Data menjadi sangat kabur. Ketika terjadi kegagalan pelindungan data atau kebocoran informasi sensitif,

¹⁸ Alfred Ariyanto, dkk., *Analisis Kelemahan dan Kekuatan UU No. 27 Tahun 2022 dalam Melindungi Data Pribadi Pasien Telemedicine*, LABEL: Law, Accounting, Business, Economics and Language, Vol.2, No.1 (2025).

¹⁹ Juliana Ananda Rukman, dkk., *Legalitas dan Pemanfaatan Teknologi Blockchain terhadap Smart Contract pada Perjanjian Bisnis di Indonesia*, RIGGS: Journal of Artificial Intelligence and Digital Business, Vol.4, No.2 (2025).

²⁰ Stanislaus Wisnu Putra Hans, dkk., *Analisis Yuridis Keabsahan Smart Contract dalam Prespektif Hukum Perdata Indonesia*, Jurnal Kepastian Hukum dan Keadilan, Vol.7, No.1 (2025).

struktur terdesentralisasi ini menyulitkan aparat penegak hukum untuk meminta pertanggungjawaban hukum secara administratif maupun pidana.²¹

Hingga tahun 2026, ekosistem pengawasan perlindungan data pribadi di Indonesia berada dalam fase transisi kelembagaan yang dinamis. Pasal 58 UU PDP secara eksplisit mengamanatkan pembentukan sebuah Lembaga Pelindungan Data Pribadi (sering disebut sebagai Otoritas PDP atau *Data Protection Authority*) yang ditunjuk oleh dan bertanggung jawab langsung kepada Presiden. Namun, pembentukan lembaga independen ini mengalami keterlambatan yang signifikan akibat rumitnya proses harmonisasi draf Peraturan Presiden (Perpres) serta koordinasi lintas kementerian, termasuk Kementerian Sekretariat Negara dan Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB).²²

Kekosongan lembaga pengawas independen ini bahkan memicu gugatan uji materiil di Mahkamah Konstitusi melalui Permohonan Nomor 153/PUU-XXIV/2026, yang mempersoalkan dampak kekosongan kelembagaan terhadap penegakan hukum perlindungan data yang kurang optimal.²³ Selama masa transisi dan kekosongan operasional Lembaga PDP ini, fungsi pengawasan sementara dilaksanakan secara aktif oleh Komdigi. Dalam menjalankan fungsi penegakan hukum sementara, aparat kepolisian (Bareskrim Polri) aktif meminta bantuan keterangan ahli dari Direktorat Strategi dan Kebijakan Pengawasan Ruang Digital di bawah Komdigi untuk menangani kasus-kasus pelanggaran data pribadi.²⁴ Di sisi lain, setiap pengembang atau operator aplikasi terdesentralisasi berbasis *smart contract* yang menyediakan layanan di wilayah hukum Indonesia wajib

²¹ Ariyanto, *Perkembangan Pernyataan Kehendak dan Keabsahannya dalam Smart Contract*” (*Development of the Statement of Will and Its Validity in Smart Contract*), Jurnal Penelitian Hukum De Jure, Vol.24, No.2 (2024).

²² Saliki Dwi Saputra, *Lembaga PDP Belum Ada Hilalnya, Menkomdigi Bilang Begini*, diakses dari <https://investortrust.id/national/81021/lembaga-pdp-belum-ada-hilalnya-menkomdigi-bilang-begini>, diakses pada 2 Juni 2026.

²³ Mimi Kartika, *Urgensi Sistem Pelindungan Data Pribadi di Indonesia*, diakses dari <https://www.mkri.id/berita/urgensi-sistem-pelindungan-data-pribadi-di-indonesia-25088>, diakses pada 2 Juni 2026.

²⁴ Andreas Ricky Febrian, *Polri Soroti Isu Worldcoin dan WorldID, Siap Ambil Langkah Penegakan Hukum*, diakses dari <https://kumparan.com/kumparannews/polri-soroti-isu-worldcoin-dan-worldid-siap-ambil-langkah-penegakan-hukum-250fFxcTCVn/full>, diakses pada 2 Juni 2026.

mendaftarkan diri sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Privat melalui sistem *Online Single Submission* (OSS). Kewajiban registrasi ini diatur dalam PP 71/2019 dan Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2021. Komdigi memegang otoritas penuh untuk menjatuhkan sanksi administratif berupa pemutusan akses (*access blocking*) terhadap platform atau aplikasi terdesentralisasi yang melalaikan kewajiban pendaftaran PSE ini.²⁵

Sementara itu, pengawasan pada sektor keuangan digital mengalami konsolidasi struktural yang masif. Berdasarkan Undang-Undang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) serta Peraturan Pemerintah Nomor 49 Tahun 2024 yang ditetapkan pada 31 Desember 2024, kewenangan pengawasan terhadap Aset Keuangan Digital termasuk Aset Kripto resmi dialihkan secara bertahap dari Bappebti ke Otoritas Jasa Keuangan (OJK) terhitung sejak 10 Januari 2025. OJK kemudian menerbitkan Peraturan OJK (POJK) Nomor 27 Tahun 2024 tentang Penyelenggaraan Perdagangan Aset Keuangan Digital termasuk Aset Kripto, yang mulai berlaku efektif sejak tanggal peralihan tersebut. POJK ini kemudian disesuaikan kembali melalui POJK Nomor 23 Tahun 2025 pada Desember 2025 guna memberikan fleksibilitas kriteria aset keuangan digital dan memfasilitasi perdagangan derivatif kripto dalam lingkungan pengawasan yang aman.²⁶

UU PDP memperkenalkan mekanisme sanksi yang berlapis dan komprehensif, mencakup tanggung jawab administratif, perdata dan pidana, yang berlaku secara mutlak bagi setiap individu, korporasi, maupun badan publik yang bertindak selaku Pengendali Data Pribadi. Dalam konteks penggunaan *smart contract*, pengembang atau operator aplikasi terdesentralisasi tidak dapat membebaskan diri dari tuntutan hukum dengan dalih bahwa pelanggaran terjadi karena kesalahan logika kode otomatis,

²⁵ Putu Raditya Nugraha, *What Is PSE in Indonesia: Who Must Register, OSS Process, TDPSE & How to Avoid Blocking*, diakses dari <https://globallawexperts.com/what-is-pse-in-indonesia/>, diakses pada 2 Juni 2026.

²⁶ Dewi Arum, dkk., *OJK Takes the Lead in Regulating Digital Financial Assets and Crypto Assets*, diakses dari <https://www.arma-law.com/news-event/newsflash/ojk-takes-the-lead-in-regulating-digital-financial-assets-and-crypto-assets#fn12>, diakses pada 2 Juni 2026.

sebab penentuan tanggung jawab hukum tetap melekat pada subjek hukum manusia atau badan hukum yang mengoperasikan sistem tersebut.²⁷

Sanksi administratif diatur secara ketat dalam Pasal 57 UU PDP dan draf PP turunan UU PDP. Apabila terjadi kebocoran data pribadi konsumen, Lembaga PDP atau Komdigi berwenang menjatuhkan denda administratif maksimal sebesar 2% dari pendapatan tahunan terhadap variabel pelanggaran perusahaan pelanggar. Variabel penentu besaran denda dihitung berdasarkan matriks kepatuhan yang ketat, yaitu :²⁸

- a. Dampak negatif dan kerugian konkret yang ditimbulkan akibat kebocoran data.
- b. Durasi waktu berlangsungnya pelanggaran sistem keamanan.
- c. Kategori data pribadi yang terdampak, baik data umum maupun data spesifik seperti biometrik atau keuangan.
- d. Jumlah subjek data pribadi yang terdampak pelanggaran.
- e. Tingkat keterbukaan dan kooperatifnya Pengendali Data dalam membantu proses penyelidikan otoritas.
- f. Skala usaha dan kemampuan finansial korporasi membayar denda.

Selain denda finansial, sanksi administratif dapat berupa peringatan tertulis, penghentian sementara seluruh aktivitas pemrosesan data, hingga pencabutan izin usaha PSE secara permanen. Dari aspek hukum perdata, Pasal 12 UU PDP memberikan hak kepada pemilik data pribadi untuk mengajukan gugatan perdata dan menuntut ganti rugi atas kerugian material maupun imaterial yang diderita akibat kelalaian Pengendali Data dalam menjaga kerahasiaan dan integritas data. Sengketa perdata ini dapat diselesaikan melalui jalur pengadilan umum atau penyelesaian sengketa alternatif.²⁹

²⁷ Derry Angling Kesuma, *Simbiosis Mutualisme Badan Publik dan Pengendali Data Pribadi terhadap Perlindungan Hukum Kebocoran Atas Privasi dan Data Pribadi*, Lex Librum: Jurnal Ilmu Hukum, Vol.10, No.2 (2024).

²⁸ Lita Paromita Siregar dan Arivigo Pranata, *Data Pribadi Konsumen Bocor? Siap-Siap Lembaga PDP Dibawah Komdigi Berikan Sanksi Ke Pelaku Usaha*, diakses dari <https://bplawyers.co.id/2025/02/26/data-pribadi-konsumen-bocor-siap-siap-lembaga-pdp-dibawah-komdigi-berikan-sanksi-ke-pelaku-usaha/>, diakses pada 2 Juni 2026.

²⁹ Sih Yuliana Wahyuningtyas, *Implikasi Algorithmic Decision-Making (ADM) Terhadap Otonomi Subyek Data dan Legalitasnya dalam Pemrosesan Big Data*, Jurnal Paradigma Hukum Pembangunan, Vol.9, No.2 (2024).

Sementara itu, sanksi pidana yang diatur dalam Pasal 67 hingga Pasal 69 UU PDP, yang diperkuat oleh penyesuaian ketentuan pidana dalam Undang-Undang Nomor 1 Tahun 2026, menetapkan hukuman penjara yang sangat berat bagi pelaku kejahatan data :

a. Pengumpulan Data Ilegal

Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri atau orang lain diancam dengan pidana penjara paling lama 5 tahun dan/atau denda maksimal Rp5.000.000.000,00.

b. Pengungkapan Data Ilegal

Tindakan mengungkapkan data pribadi orang lain secara sengaja dan melawan hukum diancam pidana penjara maksimal 4 tahun dan/atau denda maksimal Rp4.000.000.000,00.

c. Penyalahgunaan Data

Penggunaan data pribadi milik orang lain secara melawan hukum diancam dengan pidana penjara maksimal 5 tahun dan/atau denda maksimal Rp5.000.000.000,00.

d. Pemalsuan Data

Tindakan membuat data pribadi palsu atau memalsukan data pribadi dengan tujuan menguntungkan diri sendiri yang menimbulkan kerugian bagi orang lain diancam pidana penjara maksimal 6 tahun dan/atau denda pidana maksimal Rp6.000.000.000,00.

Penegakan hukum perlindungan data pribadi dalam ekosistem *smart contract* di Indonesia menghadapi tantangan ganda berupa kekosongan kelembagaan pengawas independen dan benturan bawaan antara karakteristik *blockchain* dengan hukum positif. Meskipun secara normatif kedudukan *smart contract* diakui setara dengan kontrak elektronik perdata, ketegasan penegakan hukum administratif maupun pidana di lapangan masih sangat tergantung pada kecepatan pemerintah dalam merampungkan regulasi turunan UU PDP dan pembentukan Lembaga PDP independen.

2. Tantangan Hukum dalam Penerapan Pelindungan Data Pribadi Pengguna *Smart Contract* di Indonesia

Penegakan hukum terhadap pelanggaran data pribadi pada ekosistem *smart contract* di Indonesia menghadapi tantangan kelembagaan yang masif. Hal ini disebabkan oleh adanya tumpang tindih regulasi sektoral serta terjadinya kekosongan struktural pada lembaga pengawas pelindungan data pribadi yang diamanatkan undang-undang.³⁰ UU PDP menetapkan masa transisi penyesuaian bagi seluruh pengendali data di Indonesia selama dua tahun sejak undang-undang tersebut diundangkan, yang berarti batas akhir kepatuhan jatuh pada Oktober 2024. Kendati batas masa transisi tersebut telah terlampaui, hingga pertengahan tahun 2026, Lembaga Pengawas Pelindungan Data Pribadi (Lembaga PDP) belum juga dibentuk oleh pemerintah.

Keterlambatan pembentukan lembaga khusus ini memicu terjadinya kekosongan otoritas struktural (*structural authority vacuum*) yang melumpuhkan dua fungsi utama penegakan hukum, yaitu :

a. Fungsi Pencegahan (Preventif)

Sebagaimana diatur dalam Pasal 59 jo. Pasal 60 UU PDP, Lembaga PDP seharusnya memiliki wewenang untuk menetapkan kebijakan teknis pelindungan data, melakukan pengawasan kepatuhan berkala, menerbitkan aturan mengenai penilaian dampak pelindungan data (*Data Protection Impact Assessment/DPIA*), serta memberikan sertifikasi keandalan sistem. Ketiadaan lembaga ini menyebabkan tidak adanya standar baku bagi industri dalam menyelaraskan arsitektur *blockchain* dengan hukum nasional.

b. Fungsi Penyelesaian Sengketa (Represif)

Lembaga PDP diamanatkan untuk bertindak sebagai fasilitator penyelesaian sengketa data pribadi di luar pengadilan. Di tengah kekosongan struktural ini, kasus-kasus kebocoran data yang masif terpaksa ditarik ke ranah hukum pidana konvensional, salah satunya diselesaikan melalui Putusan MA Nomor 7509K/Pid.Sus/2024.

³⁰ Hesti Ayu Wahyuni, dkk., *Penggunaan Smart Contract pada Transaksi E-Commerce dalam Perspektif Hukum Perdata di Indonesia*, Jurnal Hukum In Concreto, Vol.2, No.1 (2023).

Namun, penyelesaian kasus demi kasus secara parsial melalui jalur peradilan tidak mampu menyentuh perbaikan sistemik pada tata kelola teknologi.³¹

Kekosongan pengawas independen ini sangat krusial mengingat mayoritas kasus kebocoran data skala besar di Indonesia sering kali melibatkan instansi pemerintah atau Badan Usaha Milik Negara (BUMN) yang bertindak sebagai pengendali data raksasa (seperti kebocoran data eHAC Kementerian Kesehatan memaparkan 1,3 juta data pengguna, kegagalan sistem pada Pusat Data Nasional Sementara/PDNS, kebocoran data kependudukan Dukcapil, PLN dan Bank BSI). Situasi ini melahirkan risiko konflik kepentingan struktural apabila otoritas pengawas berada di bawah kendali rumpun eksekutif secara langsung.³²

Di tengah kelumpuhan penegakan hukum data pribadi secara umum, sektor keuangan digital menunjukkan pergerakan regulasi yang jauh lebih agresif. Sejak disahkannya UU P2SK, pengawasan terhadap aset keuangan digital dan aktivitas perdagangan kripto dialihkan dari Bappebti ke Otoritas Jasa Keuangan (OJK), dengan masa transisi penuh yang efektif berjalan sejak 10 Januari 2025. OJK merespons pelimpahan wewenang ini dengan merancang ekosistem kepatuhan baru melalui penerbitan POJK Nomor 3 Tahun 2024 tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan (ITSK) serta POJK Nomor 27 Tahun 2024 tentang Perdagangan Aset Keuangan Digital.³³

Perubahan arah regulasi melalui POJK No. 23 Tahun 2025 mencerminkan sikap pragmatis OJK dalam memandang teknologi *blockchain*. Dengan menghapus kewajiban mutlak penggunaan *Distributed Ledger Technology* (DLT), regulator membuka ruang bagi integrasi sistem hibrida yang meminimalkan risiko penyimpanan data sensitif secara

³¹ Salsa Hardafi, *Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Preventif Kebocoran Data Pribadi*, Jurnal Hukum & Pembangunan, Vol.55, No.3 (2025).

³² *Ibid.*, p.543.

³³ Ali Budiardjo, dkk., *Indonesia Greenlights Crypto Derivatives: A Look at the New OJK Framework*, diakses dari <https://www.abnrlaw.com/news/indonesia-greenlights-crypto-derivatives-a-look-at-the-new-ojk-framework>, diakses pada 3 Juni 2026.

permanen pada rantai publik. Penegakan hukum terhadap pelanggaran data pribadi dalam ekosistem *smart contract* dilakukan melalui penerapan sanksi administratif, pidana dan perdata yang diatur dalam berbagai undang-undang sektoral.

Pasal 55 UU PDP menjatuhkan konsekuensi hukum administratif yang berat bagi Pengendali Data yang melanggar kewajiban kepatuhan, mulai dari peringatan tertulis, penghentian sementara kegiatan pemrosesan data, hingga denda administratif paling tinggi 2% dari pendapatan tahunan variabel perusahaan yang melanggar. Dalam ekosistem *smart contract* yang dijalankan oleh startup teknologi, denda finansial berbasis persentase ini dapat mengancam kelangsungan hidup bisnis, terutama bagi Usaha Mikro, Kecil dan Menengah (UMKM) yang belum memahami peran dan tanggung jawab hukum mereka sebagai pengendali data.³⁴

Ketentuan pidana diatur secara ketat dalam Bab 14 UU PDP (Pasal 67 hingga Pasal 69), yang menetapkan ancaman hukuman bagi setiap orang atau korporasi yang terbukti melakukan pelanggaran dengan sengaja :

- a. Setiap pihak yang secara melawan hukum memperoleh atau mengumpulkan data pribadi milik orang lain untuk menguntungkan diri sendiri atau orang lain diancam dengan pidana penjara paling lama 5 tahun atau denda maksimal Rp 5 miliar.
- b. Pihak yang secara sengaja mengungkapkan data pribadi yang bukan miliknya kepada publik terancam dengan hukuman pidana yang sama, yaitu 5 tahun penjara atau denda Rp 5 miliar.
- c. Pelaku pemalsuan atau penciptaan data pribadi palsu guna menimbulkan kerugian bagi pihak lain diancam dengan hukuman pidana paling lama 6 tahun penjara atau denda maksimal Rp 6 miliar.³⁵

³⁴ Taufik Safar Hidayat dan Lukman Abdurrahman, *Keamanan dan Privasi Teknologi Pembayaran Digital pada UMKM dengan Menggunakan Platform Blockchain Hyperledger Fabric*, JITTER: Jurnal Ilmiah Teknologi Informasi Terapan, Vol.9, No.2 (2023).

³⁵ Michael Tanley, dkk., *Analisis Potensi dan Tantangan Teknologi Blockchain dalam Mendukung Digitalisasi Ekonomi di Indonesia*, Indonesian Journal of Education and Computer Science, Vol.2, No.3 (2024).

Bagi subjek hukum korporasi yang terlibat dalam pelanggaran data melalui *smart contract*, UU PDP memberikan kewenangan kepada hakim untuk menjatuhkan pidana tambahan berupa pembekuan sebagian atau seluruh kegiatan usaha korporasi, penutupan tempat usaha, hingga pencabutan izin usaha secara permanen.³⁶

UU PDP memberikan hak kepada subjek data untuk menuntut ganti rugi perdata atas pelanggaran data pribadi yang dialaminya. Dalam hukum perdata nasional, kepemilikan data pribadi diposisikan setara dengan hak kebendaan imateriel karena berlakunya asas *droit de suite*, di mana hak tersebut terus melekat pada pemilik aslinya ke mana pun data tersebut dipindahkan.³⁷ Apabila terjadi kebocoran atau manipulasi data akibat kelalaian sistem penyedia layanan *smart contract*, subjek data dapat mengajukan gugatan perdata Perbuatan Melawan Hukum (PMH) berdasarkan Pasal 1365 KUHPerdata untuk menuntut ganti rugi materiil maupun imateriil. Namun, mengingat kompleksitas pembuktian unsur kesalahan dalam teknologi *blockchain* terdesentralisasi, muncul wacana teoretis kuat untuk menerapkan konsep pertanggungjawaban mutlak (*strict liability*).³⁸

Lewat doktrin *strict liability*, korban pelanggaran data pribadi berhak mendapatkan ganti rugi secara instan tanpa perlu memikul beban pembuktian yang berat mengenai di mana letak kesalahan teknis dalam jaringan komputer terdistribusi tersebut. Penyelenggaraan *smart contract* di Indonesia berada di persimpangan jalan antara tuntutan inovasi teknologi dan kedaulatan perlindungan data pribadi warga negara.³⁹ Benturan karakteristik dasar *blockchain* dengan asas-asas UU PDP tidak boleh diselesaikan dengan melarang penggunaan teknologi buku besar terdistribusi,

³⁶ Bambang Hadi Purnomo, dkk., *Adopsi Blockchain sebagai Solusi Keamanan dan Transparansi Transaksi Digital di Industri Fintech*, Jurnal Minfo Polgan, Vol.13, No.2 (2025).

³⁷ Fiona dan Nazilatur Rizqiyah, *Perlindungan Data Pribadi Klien pada Era Digital: Harmonisasi Regulasi Kenotariatan dan Hukum Perlindungan Data Pribadi*, Jurnal Minuta: Jurnal Kenotariatan, Vol.7, No.2 (2025).

³⁸ Muhammad Fikri dan Shelvi Rusdiana, *Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia*, Ganesha Law Review, Vol.5, No.1 (2023).

³⁹ M. Nu'man Arif H, dkk., *Studi Komparasi Perlindungan Hukum Data Pribadi Uni Eropa dan Indonesia dalam Prinsip The Right to Be Forgotten Menurut Pasal 26 UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Yuriyaya: Jurnal Ilmiah Hukum, Vol.6, No.2 (2024).

melainkan harus dijembatani melalui harmonisasi hukum yang progresif dan pemanfaatan arsitektur kriptografi modern.⁴⁰

3. Bentuk Pelindungan Hukum yang Ideal bagi Pengguna *Smart Contract* di Indonesia

Pelindungan hukum yang ideal bagi pengguna smart contract dalam perspektif hukum nasional tidak dapat dipahami secara sempit hanya sebagai upaya memberikan kepastian terhadap berlakunya perjanjian elektronik. Pelindungan hukum yang ideal harus ditempatkan sebagai sarana untuk memastikan bahwa perkembangan teknologi tetap berada dalam koridor keadilan, kemanfaatan dan penghormatan terhadap hak-hak subjek hukum.⁴¹ Dalam konteks smart contract, persoalan yang muncul tidak hanya menyangkut sah atau tidaknya perjanjian, tetapi juga menyangkut perlindungan data pribadi, pertanggungjawaban para pihak, penegakan hukum dan kemampuan hukum nasional untuk merespons dinamika teknologi blockchain yang bergerak sangat cepat.⁴² Oleh karena itu, pendekatan yang paling tepat untuk membaca kebutuhan pelindungan hukum ini adalah teori hukum progresif, karena teori ini memandang hukum sebagai sarana untuk membahagiakan manusia, bukan sebaliknya.

Teori hukum progresif menolak pandangan bahwa hukum harus dibaca secara kaku, formalistik dan berhenti pada teks undang-undang semata. Bagi teori ini, hukum harus selalu bergerak mengikuti perkembangan masyarakat dan menjawab kebutuhan riil manusia dalam konteks sosial yang terus berubah. Dalam isu smart contract, pendekatan progresif menjadi sangat relevan karena teknologi blockchain telah melahirkan bentuk hubungan hukum baru yang tidak sepenuhnya dapat dijangkau oleh pengaturan konvensional. Apabila hukum hanya dipahami secara tekstual dan mempertahankan format lama tanpa adaptasi, maka hukum akan tertinggal dari realitas sosial yang dihadapinya. Akibatnya,

⁴⁰ Sinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama, Bandung, 2022.

⁴¹ Elsa Daniella Simbolon, dkk., *Op.Cit.*.

⁴² Monika Esterina Situmorang dan Abdul Salam, *Analisis Aspek Hukum Kontrak Pintar dalam Transaksi Kebendaan Digital: Tantangan Anonimitas dan Peran Identitas Digital*, Lex Patrimonium, Vol.4, No.1 (2025).

pelindungan hukum bagi pengguna smart contract menjadi tidak efektif. Dalam kerangka hukum progresif, justru hukum harus berani melakukan pembaruan, penyesuaian dan reinterpretasi agar mampu melindungi manusia sebagai pusat dari seluruh proses hukum.

Pelindungan hukum yang ideal bagi pengguna smart contract harus dimaknai sebagai perlindungan yang hidup, responsif dan berorientasi pada pemecahan persoalan nyata. Karena itu, hukum nasional tidak cukup hanya mengakui smart contract sebagai bentuk perjanjian digital, tetapi juga harus aktif membangun perangkat normatif yang mampu menyesuaikan karakteristik blockchain.⁴³ Di sinilah pentingnya pembentukan *lex specialis* yang secara khusus mengatur smart contract. Kebutuhan akan peraturan khusus ini bukan sekadar keinginan akademik, melainkan konsekuensi logis dari pendekatan progresif terhadap hukum. Hukum progresif menuntut agar kekosongan norma tidak dibiarkan terus-menerus, terutama ketika kekosongan itu berpotensi merugikan masyarakat. Oleh sebab itu, pembentukan regulasi khusus yang memuat pengakuan smart contract, standar keamanan data, tanggung jawab pengembang, mekanisme audit dan penyelesaian sengketa merupakan langkah yang sejalan dengan semangat progresif.

Kberadaan *lex specialis* menjadi penting karena hukum yang umum sering kali tidak cukup memadai untuk menangani kompleksitas teknologi baru. Smart contract memiliki karakter yang berbeda dari kontrak elektronik biasa. Ia berjalan secara otomatis, berbasis kode, terdistribusi dan sering kali sulit diubah setelah aktif. Karena itu, pengaturan umum dalam KUH Perdata, UU ITE dan UU PDP memang menjadi dasar awal, tetapi belum cukup untuk menjawab seluruh problem teknis dan yuridis yang timbul. Hukum progresif menuntut agar pembentuk undang-undang tidak sekadar mempertahankan kerangka lama, melainkan menciptakan aturan baru yang sesuai dengan kebutuhan riil masyarakat digital. Dengan demikian, pelindungan hukum yang ideal tidak berhenti pada pengakuan normatif,

⁴³ Bambang Fitrianto, dkk., *Analisis Yuridis Penggunaan Smart Contracts dalam Perjanjian Pembiayaan Bank*, Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory, Vol.3, No.4 (2025).

tetapi bergerak menuju pembentukan regulasi yang lebih adaptif, spesifik dan fungsional.⁴⁴

Selain aspek regulatif, teori hukum progresif juga menuntut adanya pendekatan teknis yang konkret. Salah satu wujudnya adalah kewajiban penerapan *Privacy by Design* dalam pengembangan smart contract. Dalam pandangan hukum progresif, perlindungan hukum tidak boleh hanya bekerja setelah pelanggaran terjadi, tetapi harus hadir sejak awal dalam desain sistem. Karena itu, pengembang smart contract harus diwajibkan untuk merancang sistem yang sejak awal sudah memperhitungkan risiko privasi, pembatasan data dan keamanan informasi. Prinsip minimisasi data, enkripsi, pemisahan data on-chain dan off-chain, serta penggunaan teknologi seperti *zero-knowledge proof* merupakan bentuk konkret dari perlindungan hukum yang progresif. Teknologi ini memungkinkan verifikasi dilakukan tanpa harus membuka seluruh data pribadi, sehingga transparansi blockchain tetap terjaga tanpa mengorbankan privasi pengguna.⁴⁵

Pendekatan teknis semacam ini sangat sejalan dengan hukum progresif karena menunjukkan bahwa hukum tidak bekerja secara abstrak, melainkan mendorong perubahan dalam praktik. Hukum progresif tidak puas dengan larangan atau perintah umum, tetapi menuntut solusi yang benar-benar dapat diterapkan. Jika smart contract dibangun tanpa memperhitungkan *privacy by design*, maka hukum akan selalu tertinggal satu langkah di belakang teknologi. Sebaliknya, jika prinsip privasi telah diintegrasikan sejak tahap desain, maka perlindungan hukum menjadi jauh lebih efektif. Dalam konteks ini, *zero-knowledge proof*, enkripsi dan minimalisasi data bukan sekadar opsi teknis, melainkan bagian dari rekayasa perlindungan hukum yang progresif. Dengan kata lain, hukum harus mendorong teknologi untuk bekerja melayani perlindungan manusia, bukan sekadar mengejar efisiensi sistem.

⁴⁴ I Putu Ayanda Rizki, dkk., *Tanggung Jawab Hukum Platform Digital Worldapp terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia*, Al-Zayn: Jurnal Ilmu Sosial & Hukum, Vol.4, No.1 (2026).

⁴⁵ Siti Azijah Alisia dan Abdul Halim Barkatullah, *Legalitas Bitcoin dan Teknologi Blockchain dalam Sistem Keuangan Indonesia: Analisis Tatanan Hukum*, Al-Zayn: Jurnal Ilmu Sosial & Hukum, Vol.3, No.3 (2025).

Lebih jauh, teori hukum progresif juga menekankan pentingnya dimensi kelembagaan dalam pelindungan hukum. Dalam kasus smart contract, keberadaan otoritas pengawas pelindungan data pribadi yang independen menjadi sangat penting. Hukum progresif memandang lembaga hukum bukan sebagai struktur administratif yang pasif, tetapi sebagai instrumen aktif yang harus mampu bergerak cepat merespons perubahan sosial. Karena itu, amanat pembentukan otoritas pelindungan data pribadi dalam UU PDP harus direalisasikan secara serius, bukan sekadar formalitas kelembagaan. Otoritas ini harus memiliki kewenangan yang jelas untuk melakukan audit teknologi, mengawasi kepatuhan, memeriksa insiden pelanggaran data, serta menjatuhkan sanksi yang proporsional. Tanpa lembaga yang kuat, pelindungan hukum hanya akan berhenti pada teks hukum, sementara pelanggaran terus terjadi dalam praktik.

Kelembagaan yang efektif juga harus dapat bekerja secara lintas sektor. Smart contract tidak hanya bersinggungan dengan perlindungan data pribadi, tetapi juga dengan hukum perjanjian, hukum elektronik, hukum sektor keuangan dan bahkan hukum pidana.⁴⁶ Oleh karena itu, lembaga pengawas tidak boleh bekerja secara terfragmentasi. Ia harus memiliki kemampuan koordinatif untuk menjembatani berbagai rezim hukum yang saling berkaitan. Ini penting agar perlindungan hukum tidak terputus-putus dan tidak menimbulkan kekosongan tanggung jawab. Pendekatan progresif memandang lembaga hukum sebagai bagian dari solusi, bukan sekadar alat administratif. Karena itu, keberadaan otoritas independen yang mampu melakukan audit teknologi dan mengawasi pemrosesan data dalam smart contract merupakan syarat utama bagi perlindungan hukum yang ideal.

Arah perlindungan hukum yang ideal bagi pengguna smart contract di Indonesia dapat dijelaskan melalui tiga dimensi besar yang semuanya selaras dengan teori hukum progresif. Pertama, dimensi regulatif, yaitu perlunya pembentukan *lex specialis* yang mengatur smart contract secara terpisah dari kontrak elektronik konvensional.

⁴⁶ I Made Marta Wijaya, *The Application of Blockchain Technology in Cross-Border Personal Data Transfer Activities in Indonesia: Opportunities and Challenges*, Jurnal Magister Hukum Udayana, Vol.14, No.1 (2025).

Peraturan ini harus memuat klausul tanggung jawab pengembang, standar keamanan, perlindungan data pribadi, validitas kontrak dan mekanisme penyelesaian sengketa. Dalam perspektif progresif, pembentukan aturan ini adalah bentuk keberanian hukum untuk menyesuaikan diri dengan perkembangan teknologi dan kebutuhan masyarakat digital.

Kedua, dimensi teknis, yaitu kewajiban penerapan *Privacy by Design*. Hukum progresif menuntut agar perlindungan hukum tidak hanya disusun pada tataran abstrak, tetapi diwujudkan dalam desain teknis sistem. Oleh karena itu, minimisasi data, enkripsi, pemisahan data dan zero-knowledge proof harus dijadikan bagian dari standar perlindungan smart contract. Dengan cara ini, privasi tidak dikorbankan atas nama efisiensi teknologi. Justru teknologi diarahkan agar menjadi sarana perlindungan, bukan ancaman, terhadap data pribadi pengguna.⁴⁷

Ketiga, dimensi kelembagaan, yaitu pembentukan otoritas pengawas perlindungan data pribadi yang independen dan efektif. Dalam kerangka hukum progresif, lembaga ini harus mampu melampaui fungsi administratif biasa dan benar-benar aktif dalam penegakan, pengawasan, serta audit teknologi. Lembaga yang kuat akan menjamin bahwa hukum tidak berhenti sebagai norma tertulis, tetapi hidup dalam praktik. Dengan demikian, perlindungan hukum bagi pengguna smart contract menjadi nyata, bukan ilusi normatif.

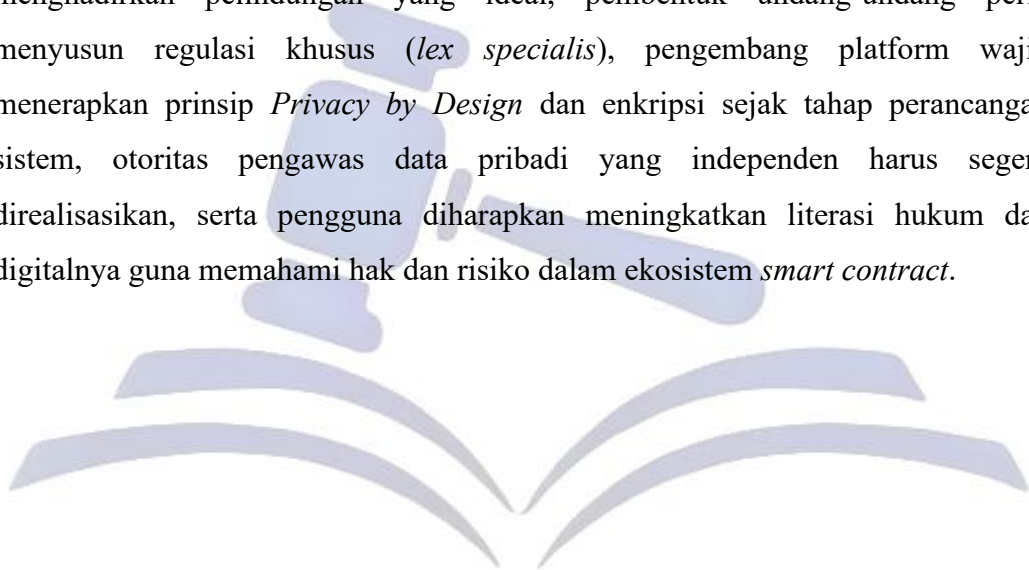
Secara keseluruhan, teori hukum progresif memberikan dasar yang sangat tepat untuk merumuskan perlindungan hukum yang ideal bagi pengguna smart contract. Teori ini menegaskan bahwa hukum harus berpihak pada manusia, mampu beradaptasi dengan perkembangan teknologi dan berani melakukan pembaruan ketika kerangka hukum yang ada tidak lagi memadai. Dalam konteks smart contract, perlindungan hukum yang ideal bukanlah perlindungan yang menolak teknologi, melainkan perlindungan yang mengarahkan teknologi agar tetap tunduk pada nilai keadilan, kemanfaatan dan kepastian hukum. Sehingga oleh karena itu,

⁴⁷ Zandra Azelia Savitri, dkk., *Urgensi Sertifikat Keandalan Privasi dalam Menghadapi Kebocoran Data Pribadi*, Jurnal USM Law Review, Vol.8, No.1 (2025).

pembentukan *lex specialis*, penerapan Privacy by Design, penggunaan teknologi privasi yang lebih canggih dan penguatan lembaga pengawas independen merupakan wujud konkret dari hukum progresif dalam bidang pelindungan data pribadi pengguna smart contract di Indonesia.

C. PENUTUP

Kerangka hukum pelindungan data pribadi pengguna *smart contract* di Indonesia saat ini masih bersifat sektoral dan belum spesifik (*lex specialis*), sehingga menghadapi tantangan besar terkait kekosongan hukum, karakteristik *blockchain* yang *immutable* dan terdesentralisasi, ketidakjelasan pengontrol data, hingga belum optimalnya literasi digital serta kelembagaan pengawas. Untuk menghadirkan pelindungan yang ideal, pembentuk undang-undang perlu menyusun regulasi khusus (*lex specialis*), pengembang platform wajib menerapkan prinsip *Privacy by Design* dan enkripsi sejak tahap perancangan sistem, otoritas pengawas data pribadi yang independen harus segera direalisasikan, serta pengguna diharapkan meningkatkan literasi hukum dan digitalnya guna memahami hak dan risiko dalam ekosistem *smart contract*.



DAFTAR PUSTAKA

Buku

- Arifiyanto, Joiverdia. 2024. *Konsep Data Pribadi dalam Fintech (Perspektif Hukum dan Hak Asasi Manusia)*. (Medan: Tri Selaras Cendekia).
- _____. 2024. *Pelindungan Data Pribadi dan Regulasi Fintech (Penerapan di Prancis dan Indonesia)*. (Medan: Tri Selaras Cendekia).
- Isnaeni, Moch. 2017. *Seberkas Diaroma Hukum Kontrak*. (Surabaya: Revka Petra Media).
- Rosadi, Sinta Dewi. 2022. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*. (Bandung: Refika Aditama).

Publikasi

- Adhijoso, Bima Danubrata. *Legalitas Penerapan Smart Contract dalam Asuransi Pertanian di Indonesia*. Jurist-Diction. Vol.2. No.2 (2019).
- Alisia, Siti Azijah dan Abdul Halim Barkatullah. *Legalitas Bitcoin dan Teknologi Blockchain dalam Sistem Keuangan Indonesia: Analisis Tatahan Hukum*. Al-Zayn: Jurnal Ilmu Sosial & Hukum. Vol.3. No.3 (2025).
- Ariyanto. *Perkembangan Pernyataan Kehendak dan Keabsahannya dalam Smart Contract” (Development of the Statement of Will and Its Validity in Smart Contract)*. Jurnal Penelitian Hukum De Jure. Vol.24. No.2 (2024).
- Ariyanto, Alfred, dkk.. *Analisis Kelemahan dan Kekuatan UU No. 27 Tahun 2022 dalam Melindungi Data Pribadi Pasien Telemedicine*. LABEL: Law, Accounting, Business, Economics and Language. Vol.2. No.1 (2025).
- Budiyanto, Andini Eka. *Analisis Yuridis Penggunaan Smart Contract dalam Perspektif Asas Kebebasan Berkontrak*. Jurnal Sains Student Research. Vol.1. No.1 (2023).
- Dethan, Jecelyn Amanda dan Yericia Evadne Giralhani Irianto. *Analisis Keabsahan Smart Contract dalam Perjanjian Bisnis di Indonesia*. UNES Law Review. Vol.7. No.1 (2024).
- Fahlevi, Farens Sebastian dan Zuhda Mila Fitriana. *Keabsahan Smart Contract Sebagai Solusi Praktik Manipulasi Kontrak di Indonesia*. Kabilah: Journal of Social Community. Vol.9. No.2 (2024).
- Fikri, Muhammad dan Shelvi Rusdiana. *Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia*. Ganesha Law Review. Vol.5. No.1 (2023).
- Fiona dan Nazilatur Rizqiyah. *Perlindungan Data Pribadi Klien pada Era Digital: Harmonisasi Regulasi Kenotariatan dan Hukum Perlindungan Data Pribadi*. Jurnal Minuta: Jurnal Kenotariatan. Vol.7. No.2 (2025).
- Fitrianto, Bambang, dkk.. *Analisis Yuridis Penggunaan Smart Contracts dalam Perjanjian Pembiayaan Bank*. Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory. Vol.3. No.4 (2025).
- H, M. Nu'man Arif, dkk.. *Studi Komparasi Perlindungan Hukum Data Pribadi Uni Eropa dan Indonesia dalam Prinsip The Right to Be Forgotten Menurut Pasal 26 UU Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Yurijaya: Jurnal Ilmiah Hukum. Vol.6. No.2 (2024).

- Hans, Stanislaus Wisnu Putra, dkk.. *Analisis Yuridis Keabsahan Smart Contract dalam Prespektif Hukum Perdata Indonesia*. Jurnal Kepastian Hukum dan Keadilan. Vol.7. No.1 (2025).
- Hardafi, Salsa. *Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Preventif Kebocoran Data Pribadi*. Jurnal Hukum & Pembangunan. Vol.55. No.3 (2025).
- Hidayat, Taufik Safar dan Lukman Abdurrahman. *Keamanan dan Privasi Teknologi Pembayaran Digital pada UMKM dengan Menggunakan Platform Blockchain Hyperledger Fabric*. JITTER: Jurnal Ilmiah Teknologi Informasi Terapan. Vol.9. No.2 (2023).
- Hutapea, Korintus Wilson Horas dan Adi Sulistiyono. *Keabsahan Smart Contract dengan Teknologi Blockchain Menurut Kitab Undang-Undang Hukum Perdata*. Aliansi: Jurnal Hukum, Pendidikan dan Sosial Humaniora. Vol.1. No.3 (2024).
- Kesuma, Derry Angling. *Simbiosis Mutualisme Badan Publik dan Pengendali Data Pribadi terhadap Perlindungan Hukum Kebocoran Atas Privasi dan Data Pribadi*. Lex Librum: Jurnal Ilmu Hukum. Vol.10. No.2 (2024).
- Lim, Willion, dkk.. *Smart Contracts: Validitas Hukum dan Tantangan di Masa Depan Indonesia*. Jurnal Kewarganegaraan. Vol.8. No.1 (2024).
- Mansula, Gabriella Rachel. *Perlindungan Hukum Atas Penyelesaian Hukum Tidak Berfungsinya Proses Transaksi Melalui Smart Contract Pada Sistem Blockchain*. Al Qodiri: Jurnal Pendidikan, Sosial dan Keagamaan. Vol.21. No.2 (2023).
- Martinelli, Imelda, dkk.. *Legalitas dan Efektivitas Penggunaan Teknologi Blockchain terhadap Smart Contract Pada Perjanjian Bisnis di Masa Depan*. UNES Law Review. Vol.6. No.4 (2024).
- Pohan, Tia Deja dan Muhammad Irwan Padli Nasution. *Perlindungan Hukum Data Pribadi Konsumen dalam Platform E Commerce*. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen. Vol.1. No.3 (2023).
- Priliasari, Erna. *Perlindungan Data Pribadi Konsumen dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan di Indonesia*. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional. Vol.12. No.2 (2023).
- Purnomo, Bambang Hadi, dkk.. *Adopsi Blockchain sebagai Solusi Keamanan dan Transparansi Transaksi Digital di Industri Fintech*. Jurnal Minfo Polgan. Vol.13. No.2 (2025).
- Rizki, I Putu Ayanda, dkk.. *Tanggung Jawab Hukum Platform Digital Worldapp terhadap Pelanggaran Perlindungan Kerahasiaan Data Biometrik Berdasarkan Sistem Hukum Indonesia*. Al-Zayn: Jurnal Ilmu Sosial & Hukum. Vol.4. No.1 (2026).
- Rukman, Juliana Ananda, dkk.. *Legalitas dan Pemanfaatan Teknologi Blockchain terhadap Smart Contract pada Perjanjian Bisnis di Indonesia*. RIGGS: Journal of Artificial Intelligence and Digital Business. Vol.4. No.2 (2025).
- Sakirman, dkk.. *Kepastian Hukum Smart Contract dalam Perspektif Hukum Perdata*. Rewang Rencang: Jurnal Hukum Lex Generalis. Vol.5. No.10 (2024).
- Savitri, Zandra Azelia, dkk.. *Urgensi Sertifikat Keandalan Privasi dalam Menghadapi Kebocoran Data Pribadi*. Jurnal USM Law Review. Vol.8. No.1 (2025).

- Simbolon, Elsa Daniella, dkk.. *Pelindungan Korban Pemalsuan Data Diri dalam Transaksi Pinjaman Online melalui Penegakan Hak untuk Dilupakan*. Neoclassical Legal Review. Vol.3. No.2 (2024).
- Situmorang, Monika Esterina dan Abdul Salam. *Analisis Aspek Hukum Kontrak Pintar dalam Transaksi Kebendaan Digital: Tantangan Anonimitas dan Peran Identitas Digital*. Lex Patrimonium. Vol.4. No.1 (2025).
- Tanley, Michael, dkk.. *Analisis Potensi dan Tantangan Teknologi Blockchain dalam Mendukung Digitalisasi Ekonomi di Indonesia*. Indonesian Journal of Education and Computer Science. Vol.2. No.3 (2024).
- Wahyuni, Hesti Ayu, dkk.. *Penggunaan Smart Contract pada Transaksi E-Commerce dalam Perspektif Hukum Perdata di Indonesia*. Jurnal Hukum In Concreto. Vol.2. No.1 (2023).
- Wahyuningtyas, Sih Yuliana. *Implikasi Algorithmic Decision-Making (ADM) terhadap Otonomi Subyek Data dan Legalitasnya dalam Pemrosesan Big Data*. Jurnal Paradigma Hukum Pembangunan. Vol.9. No.2 (2024).
- Wijaya, I Made Marta. *The Application of Blockchain Technology in Cross-Border Personal Data Transfer Activities in Indonesia: Opportunities and Challenges*. Jurnal Magister Hukum Udayana. Vol.14. No.1 (2025).

Website

- Arum, Dewi, dkk.. *OJK Takes the Lead in Regulating Digital Financial Assets and Crypto Assets*. diakses dari <https://www.arma-law.com/news-event/newsflash/ojk-takes-the-lead-in-regulating-digital-financial-assets-and-crypto-assets#fn12>. diakses pada 2 Juni 2026.
- Budiardjo, Ali, dkk.. *Indonesia Greenlights Crypto Derivatives: A Look at the New OJK Framework*. diakses dari <https://www.abnrlaw.com/news/indonesia-greenlights-crypto-derivatives-a-look-at-the-new-ojk-framework>. diakses pada 3 Juni 2026.
- Febrian, Andreas Ricky. *Polri Soroti Isu Worldcoin dan WorldID, Siap Ambil Langkah Penegakan Hukum*. diakses dari <https://kumparan.com/kumparannews/polri-soroti-isu-worldcoin-dan-worldid-siap-ambil-langkah-penegakan-hukum-250fFxcTCVn/full>. diakses pada 2 Juni 2026.
- Kartika, Mimi. *Urgensi Sistem Pelindungan Data Pribadi di Indonesia*. diakses dari <https://www.mkri.id/berita/urgensi-sistem-pelindungan-data-pribadi-di-indonesia-25088>. diakses pada 2 Juni 2026.
- Nugraha, Putu Raditya. *What Is PSE in Indonesia: Who Must Register, OSS Process, TDPSE & How to Avoid Blocking*. diakses dari <https://globallawexperts.com/what-is-pse-in-indonesia/>. diakses pada 2 Juni 2026.
- Saputra, Saliki Dwi. *Lembaga PDP Belum Ada Hilalnya, Menkomdigi Bilang Begini*. diakses dari <https://investortrust.id/national/81021/lembaga-pdp-belum-ada-hilalnya-menkomdigi-bilang-begini>. diakses pada 2 Juni 2026.
- Siregar, Lita Paromita dan Arivigo Pranata. *Data Pribadi Konsumen Bocor? Siap-Siap Lembaga PDP Dibawah Komdigi Berikan Sanksi Ke Pelaku Usaha*. diakses dari <https://bplawyers.co.id/2025/02/26/data-pribadi-konsumen-bocor-siap-siap-lembaga-pdp-dibawah-komdigi-berikan-sanksi-ke-pelaku-usaha/>. diakses pada 2 Juni 2026.

SIP Law Firm. *Penggunaan Smart contract dalam Perbankan dan Implikasinya*. diakses dari <https://siplawfirm.id/penggunaan-smart-contract-dalam-perbankan-dan-implikasinya/?lang=id>. diakses pada 30 Agustus 2025.

Sumber Hukum

Undang-Undang Dasar Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Perdata.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

