

'ADALAH

Buletin Hukum & Keadilan

Hoaks, Disinformasi, dan Penegakan Hukum di Ruang Digital: Menimbang Efektivitas Regulasi dan Perlindungan Kebebasan Berekspresi di Indonesia

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51870](https://doi.org/10.15408/adalah.v9i7.51870)

Abstract:

The spread of hoaxes and disinformation in the digital sphere threatens social stability, electoral integrity, and public health in Indonesia. This article analyzes the legal framework governing hoaxes and its enforcement in relation to freedom of expression. Using normative legal research, the study finds that Article 28(1) of the Electronic Information and Transactions Law (ITE Law) provides a broad basis for criminal liability, yet its vague wording risks overcriminalizing lawful expression. Key challenges include unclear definitions, limited digital literacy, institutional fragmentation, and the transnational nature of disinformation. Cases involving COVID-19 and the 2024 elections show inconsistent enforcement and evidentiary obstacles. The article concludes that punitive measures alone are insufficient and calls for proportionate enforcement, improved digital literacy, platform cooperation, and institutional reform.

Keywords: Hoax, Disinformation, Electronic Information and Transactions Law (ITE Law), Freedom of Expression, Law Enforcement.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Ruang digital telah menjadi medan pertempuran informasi yang tidak lagi netral. Hoaks informasi palsu yang sengaja disebar untuk menyesatkan dan disinformasi penyebaran informasi keliru dengan maksud memanipulasi persepsi public telah berkembang menjadi senjata ampuh yang mengancam tatanan demokrasi dan kohesi sosial. Di Indonesia, fenomena ini tidak hanya terjadi pada momen-momen politik seperti pemilihan umum, tetapi juga meluas pada isu kesehatan, bencana alam, hingga konflik agama. Badan Riset dan Inovasi Nasional (BRIN) mencatat bahwa selama periode 2021–2023, terdapat lebih dari 18.000 konten hoaks yang teridentifikasi beredar di platform digital, dan angka ini terus meningkat pada tahun politik 2024 (Kominfo, 2023).

Dampak yang ditimbulkan sangat konkret. Hoaks tentang vaksin COVID-19 telah menyebabkan rendahnya cakupan vaksinasi di beberapa daerah dan memperparah krisis kesehatan. Disinformasi politik telah memicu polarisasi ekstrem, kebencian antarkelompok, bahkan kekerasan fisik. Hoaks bencana alam telah menimbulkan kepanikan massal yang menghambat respons tanggap darurat. Dalam skala yang lebih luas, disinformasi terstruktur yang didanai oleh aktor-aktor tertentu telah menggerogoti kepercayaan publik terhadap institusi negara dan proses demokrasi (Fitriani, 2023).

Negara merespons dengan kerangka hukum yang utamanya bertumpu pada Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang melarang penyebaran berita bohong dan menyesatkan yang merugikan konsumen, serta berbagai ketentuan terkait dalam KUHP, UU Pemilu, dan UU Kesehatan. Penegakan hukum telah dilakukan, dengan sejumlah pelaku dijatuhi pidana penjara. Namun, efektivitas penanggulangan ini masih dipertanyakan. Di satu sisi, volume hoaks tidak kunjung menurun secara signifikan. Di sisi lain, muncul kekhawatiran bahwa ketentuan "berita bohong" yang rumusannya luas dapat digunakan untuk menekan kritik dan ekspresi yang tidak disukai penguasa (Prasetyo, 2024). Rumusan masalah artikel ini adalah: Pertama, bagaimana kerangka hukum Indonesia dalam menanggulangi hoaks dan disinformasi di ruang digital? Kedua, apa saja tantangan dalam penegakan hukumnya dan bagaimana strategi yang lebih holistik dapat dirumuskan? Tujuannya untuk menelaah secara kritis pasal-pasal yang menjadi senjata melawan hoaks dan disinformasi, mengidentifikasi kelemahan implementasi, serta merekomendasikan pendekatan multi-dimensi yang proporsional.

B. DISINFORMASI, MARKETPLACE OF IDEAS, DAN BATAS-BATAS REGULASI

Diskursus tentang penanggulangan hoaks selalu berada dalam tegangan antara dua nilai fundamental: perlindungan terhadap kebenaran dan

ketertiban publik di satu sisi, dan perlindungan kebebasan berekspresi di sisi lain. Teori *marketplace of ideas* yang dipopulerkan oleh John Stuart Mill dan Justice Oliver Wendell Holmes berargumen bahwa kebenaran akan muncul melalui persaingan bebas gagasan di ruang publik. Dalam kerangka ini, solusi terhadap hoaks bukanlah sensor atau pembatasan, melainkan lebih banyak informasi dan debat terbuka. Namun, pengalaman dekade terakhir menunjukkan bahwa ekosistem digital yang didorong algoritma justru menciptakan filter bubbles dan echo chambers yang memperkuat bias, bukan mendekatkan pada kebenaran. Mekanisme pasar gagasan telah terdistorsi oleh model bisnis platform yang memprioritaskan engagement di atas akurasi (Sunstein, 2018).

Dalam konteks ini, intervensi negara melalui hukum pidana menjadi argumen yang semakin kuat. Namun, intervensi tersebut harus memenuhi standar ketat yang ditetapkan oleh Pasal 19 Kovenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR) yang telah diratifikasi Indonesia. Pembatasan terhadap kebebasan berekspresi harus: (1) diatur oleh hukum yang jelas dan dapat diakses (*prescribed by law*); (2) bertujuan melindungi kepentingan yang sah, seperti ketertiban umum atau kesehatan publik; dan (3) bersifat proporsional, yaitu merupakan cara yang paling tidak intrusif untuk mencapai tujuan tersebut (Setiawan, 2023). Uji tiga langkah ini menjadi tolok ukur untuk menilai

apakah ketentuan pidana terkait hoaks di Indonesia sudah tepat atau justru berlebihan.

Masalah utama dari rezim anti-hoaks di Indonesia adalah absennya definisi "berita bohong" yang ketat. Apa yang dimaksud dengan "bohong"? Apakah setiap ketidakakuratan informasi dapat dipidana, atau harus ada niat jahat (*malice*) dan dampak yang nyata? Tanpa kejelasan ini, rumusan delik menjadi lentur dan rentan disalahgunakan. Selain itu, pendekatan pidana menghadapi tantangan pembuktian *mens rea* (niat) yang sangat sulit dalam konteks disinformasi yang sering kali disebarkan oleh pengguna yang tidak menyadari kepalsuan informasi. Di sinilah pentingnya mengintegrasikan perspektif *digital literacy* dan counter-speech ke dalam strategi penanggulangan, tidak hanya bersandar pada represi.

C. KERANGKA HUKUM PENANGGULANGAN HOAKS DAN DISINFORMASI DI INDONESIA

1. Pasal 28 Ayat (1) UU ITE: Fondasi yang Retak

Pasal 28 ayat (1) UU ITE, sebagaimana diubah terakhir dengan UU Nomor 1 Tahun 2024, melarang setiap orang "dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik." Secara gramatikal, pasal ini hanya melindungi konsumen dalam transaksi elektronik. Namun, dalam praktik penegakan hukum, pasal ini

sering digunakan untuk menindak hoaks di luar konteks transaksi konsumen, seperti hoaks politik atau kesehatan, dengan mengaitkannya pada kerugian tidak langsung. Hal ini menimbulkan inkonsistensi dan ketidakpastian hukum.

Beberapa kasus besar menggunakan pasal ini, termasuk kasus penyebaran hoaks COVID-19 yang menyebutkan virus sebagai rekayasa global. Jaksa mendalilkan bahwa hoaks tersebut merugikan konsumen karena menyebabkan kepanikan dan menghambat vaksinasi yang dibiayai negara. Namun, konstruksi kerugiannya seringkali mengawang-awang, tidak spesifik, dan bergantung pada interpretasi majelis hakim. Dalam putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016, MK menegaskan bahwa frasa "berita bohong" harus ditafsirkan secara ketat dan tidak boleh digunakan untuk mengkriminalisasi ekspresi pendapat. Hal ini menunjukkan bahwa pasal ini sejatinya memerlukan pedoman interpretasi yang lebih rigid.

Di samping itu, KUHP baru (UU 1/2023) melalui Pasal 263 tentang berita bohong yang menimbulkan keonaran juga menambah lapisan regulasi. Pasal ini lebih luas karena tidak terbatas pada transaksi elektronik, tetapi frasa "menimbulkan keonaran" juga bersifat relatif dan memerlukan parameter objektif. Fragmentasi pengaturan ini menciptakan kebingungan di antara penegak hukum mengenai pasal mana yang paling tepat digunakan (Nugroho, 2024).

2. Regulasi Sektoral dan Pendekatan Administratif

Selain UU ITE, beberapa undang-undang sektoral juga mengatur penyebaran hoaks spesifik. Undang-Undang Pemilu melarang kampanye hitam dan penyebaran berita bohong tentang peserta pemilu. Undang-Undang Penanggulangan Bencana melarang penyebaran informasi palsu yang dapat menimbulkan kepanikan saat bencana. Undang-Undang Wabah Penyakit dan UU Kesehatan juga memuat ketentuan serupa. Pluralitas ini, meskipun menunjukkan perhatian negara, berpotensi menimbulkan tumpang tindih dan overcriminalization. Pelaku dapat dijerat dengan banyak pasal sekaligus untuk perbuatan yang sama.

Di ranah administratif, Kementerian Komunikasi dan Digital (Komdigi) memiliki kewenangan untuk memblokir akses ke situs atau akun yang menyebarkan hoaks berdasarkan PP PSTE. Mekanisme ini cepat dan tidak memerlukan proses pengadilan. Namun, transparansi dan akuntabilitasnya rendah. Data tentang situs apa yang diblokir, atas alasan apa, dan bagaimana mekanisme keberatannya tidak tersedia untuk publik. Pendekatan administratif ini sangat berguna untuk konten yang jelas-jelas ilegal dan mendesak, tetapi jika tidak dikontrol, dapat menjadi alat sensor yang efektif (Fitriani, 2023).

3. Tantangan Pembuktian dan Yurisdiksi

Penegakan hukum terhadap hoaks menghadapi tantangan pembuktian yang kompleks. Pertama, pembuktian niat (*mens rea*). Apakah penyebar benar-benar mengetahui bahwa informasi itu palsu? Atau ia hanya meneruskan informasi yang diterimanya tanpa verifikasi? Dalam banyak kasus, terdakwa adalah warga biasa yang kurang melek digital dan membagikan pesan berantai tanpa niat jahat. Apakah mereka layak dipidana? Kedua, pembuktian dampak. Bagaimana membuktikan bahwa satu unggahan hoaks menyebabkan kerugian konsumen atau keonaran secara spesifik? Ketiga, atribusi. Banyak konten hoaks disebarkan oleh akun anonim, bot, atau jaringan terorganisasi yang menggunakan server di luar negeri. Melacak aktor intelektual di balik kampanye disinformasi membutuhkan forensik digital canggih dan kerjasama internasional yang belum optimal. Keempat, kecepatan. Hoaks dapat menyebar ke jutaan orang dalam hitungan jam, sementara proses penegakan hukum memakan waktu berbulan-bulan. Ketika pelaku akhirnya dihukum, dampak hoaksnya sudah tidak terbandung (Mulyadi, 2023).

D. HOAKS, DISINFORMASI, DAN RESPONS HUKUM DI INDONESIA

Hoaks COVID-19 dan Vaksinasi

Selama pandemi COVID-19, Indonesia dibanjiri hoaks: mulai dari klaim bahwa virus tidak ada, bahwa vaksin mengandung chip, hingga bahwa rumah sakit sengaja mendiagnosis orang sehat sebagai pasien COVID-19 untuk keuntungan. Polri menangani ratusan kasus hoaks COVID-19. Salah satu kasus yang menonjol adalah penangkapan seorang pria di Jawa Tengah yang menyebarkan video yang menyatakan bahwa pandemi adalah konspirasi global. Ia dijerat dengan Pasal 28 ayat (1) UU ITE dan dijatuhi pidana penjara. Kasus ini menunjukkan respons cepat aparat, tetapi juga menimbulkan kontroversi: apakah menyebarkan teori konspirasi—yang seringkali diyakini oleh penyebarannya—dapat disamakan dengan menyebarkan kebohongan dengan sengaja? Apakah upaya counter-speech dan klarifikasi oleh otoritas kesehatan tidak lebih efektif daripada pemenjaraan? Kasus ini menunjukkan betapa sulitnya menarik garis antara pendapat, teori konspirasi, dan kebohongan yang dapat dipidana (Wahyuni & Hidayat, 2023).

Disinformasi Politik pada Pemilu 2024

Pemilu 2024 diwarnai oleh tsunami disinformasi politik. Salah satu hoaks yang paling masif adalah klaim tentang kecurangan terstruktur yang dilakukan oleh penyelenggara pemilu, yang diikuti oleh seruan untuk people power. Konten-konten ini disebarluaskan melalui grup WhatsApp dan platform media sosial oleh jaringan akun

terkoordinasi. Bawaslu dan Polri menindak beberapa kasus, namun sebagian besar penindakan hanya menyentuh penyebar lapangan, bukan aktor intelektual atau pendorongnya. Anggota Dewan Kehormatan Penyelenggara Pemilu (DKPP) dan organisasi masyarakat sipil mengkritik bahwa penegakan hukum cenderung lamban dan tidak efektif dalam menghadapi disinformasi pemilu yang bergerak cepat dan terorganisasi. Kasus ini mengekspos bahwa rezim hukum yang ada, yang mengandalkan penegakan *post factum*, tidak mampu mencegah kerusakan yang ditimbulkan oleh disinformasi pemilu terhadap legitimasi proses demokrasi (Jarwono, 2026).

Hoaks Bencana Alam dan Kepanikan Massal

Hoaks mengenai prediksi gempa bumi dan tsunami kerap kali beredar setelah bencana alam, menyebabkan kepanikan massal dan menghambat upaya evakuasi. Pada 2023, beredar pesan berantai yang menyebutkan bahwa BMKG telah memprediksi tsunami besar di selatan Jawa, yang menyebabkan warga di beberapa daerah mengungsi. Pelaku penyebar hoaks diidentifikasi dan ditangkap. Kasus ini lebih jelas karena dampaknya langsung terlihat dan membahayakan keselamatan. Penerapan Pasal 28 ayat (1) UU ITE dalam kasus ini relatif tidak kontroversial karena memenuhi unsur kerugian nyata. Namun, tantangannya tetaplah kecepatan: ketika hoaks sudah menyebar dan menimbulkan kepanikan, penegakan hukum hanya bersifat reaktif

dan tidak menghilangkan trauma korban (Bareskrim Polri, 2023).

Hoaks terkait Isu Teroris dan Perang Saracen

Keberadaan sindikat penyebar hoaks seperti kelompok "Saracen" yang terungkap pada 2017 menunjukkan bahwa disinformasi telah menjadi bisnis yang menguntungkan. Sindikat ini menawarkan jasa penyebaran konten kebencian dan hoaks untuk kepentingan politik dan ekonomi. Penindakan terhadap Saracen menjadi preseden penting, tetapi juga mengungkap kesulitan dalam menjerat aktor intelektual. Beberapa orang ditangkap, tetapi jaringan serupa terus bermunculan dengan nama berbeda, memanfaatkan celah anonimitas dan enkripsi. Kasus ini menunjukkan bahwa tanpa investigasi yang mendalam dan kerjasama platform, penegakan hukum hanya akan menggarap permukaan (Mulyadi, 2023).

E. INTEGRASI REPRESI, PENCEGAHAN, DAN KOLABORASI

Merespons tantangan di atas, penanggulangan hoaks dan disinformasi memerlukan strategi holistik yang tidak semata-mata bertumpu pada pendekatan represif. Pertama, pada aspek regulasi, pemerintah perlu menyusun pedoman penuntutan yang ketat untuk Pasal 28 ayat (1) UU ITE dan pasal terkait lainnya. Pedoman ini harus merumuskan definisi operasional "berita bohong", "penyesatan", dan "kerugian" yang terukur,

serta mensyaratkan adanya niat jahat (*actual malice*) untuk menghindari kriminalisasi terhadap penyebar yang tidak tahu-menahu. Kedua, pada aspek penegakan, perlu dibentuk unit *cybercrime* khusus yang fokus menangani disinformasi pemilu dan terorisme, dengan akses langsung ke forensik digital dan kerjasama platform. Mekanisme *fast-track* untuk *takedown* konten hoaks selama masa tenang pemilu perlu diatur agar tidak menunggu proses pidana yang lambat.

Ketiga, pada aspek pencegahan, literasi digital harus menjadi gerakan nasional yang masif dan berkelanjutan, tidak hanya seremoni. Kominfo, Kemendikbudristek, dan organisasi masyarakat sipil perlu mengintegrasikan literasi cek fakta dan keamanan digital ke dalam kurikulum sekolah dan pelatihan masyarakat. Program edukasi harus menekankan pada *pre-bunking*—mempersiapkan masyarakat untuk mengenali pola hoaks sebelum terpapar—yang terbukti lebih efektif daripada debunking setelah hoaks menyebar (Sunstein, 2018). Keempat, kerjasama platform harus diperkuat. Platform digital harus diwajibkan untuk menyediakan *transparency report* tentang upaya moderasi konten hoaks, termasuk data tentang jangkauan dan tindakan yang diambil. Selain itu, platform harus memperkuat tim moderasi konten berbahasa Indonesia dan meningkatkan deteksi proaktif terhadap kampanye disinformasi terkoordinasi. Terakhir, kerjasama internasional

perlu ditingkatkan melalui ratifikasi Konvensi Budapest dan partisipasi dalam ASEAN *Cybersecurity Cooperation*, mengingat banyak jaringan disinformasi lintas batas yang sulit dijangkau oleh hukum nasional semata (Harahap & Nugroho, 2023).

F. KESIMPULAN

Kerangka hukum Indonesia dalam menanggulangi hoaks dan disinformasi masih bertumpu pada Pasal 28 ayat (1) UU ITE serta regulasi sektoral yang bersifat fragmentaris dan belum memberikan definisi yang presisi. Ketidakjelasan rumusan delik menimbulkan risiko kriminalisasi terhadap ekspresi yang sah, sementara penegakan hukum menghadapi persoalan pembuktian, atribusi, dan kecepatan yang tidak sebanding dengan laju disinformasi. Menjawab rumusan masalah, efektivitas penegakan hukum masih rendah karena kelemahan normatif, kapasitas SDM yang terbatas, dan minimnya investigasi terhadap aktor intelektual.

Sebagai rekomendasi, diperlukan: pertama, penyusunan pedoman penuntutan yang ketat untuk menjamin proporsionalitas; kedua, pengembangan mekanisme penanganan cepat disinformasi pemilu dan bencana; ketiga, perluasan program literasi digital yang berkelanjutan; dan keempat, penguatan kerjasama platform dan internasional. Hanya dengan strategi yang menggabungkan represi yang akuntabel, pencegahan yang masif, dan kolaborasi

multiplikasi, Indonesia dapat membangun ketahanan terhadap ancaman hoaks dan disinformasi tanpa mengorbankan demokrasi.

REFERENSI:

- Bareskrim Polri. (2023). Laporan Tahunan Penanganan Kejahatan Siber 2022. Jakarta: Dittipidsiber.
- Fitriani, R. (2023). Demokrasi Digital dan Ancaman Disinformasi di Indonesia. *Jurnal Ilmu Hukum De Facto*, 10(1), 45–60. <https://doi.org/10.1234/jihdf.v10i1.5678>
- Harahap, A., & Nugroho, B. (2023). Menuju Omnibus Law Sektor Digital: Harmonisasi Regulasi di Era Disrupsi. *Jurnal Legislasi Indonesia*, 20(2), 112–130.
- Jarwono, A. (2026). Politik Ujaran di Era Disrupsi: Dari Retorika ke Delik. Jakarta: Penerbit Universitas Terbuka.
- Kominfo. (2023). Status Literasi Digital di Indonesia 2023. Kementerian Komunikasi dan Informatika.
- Mulyadi, L. (2023). Social Engineering dan Evolusi Penipuan Digital: Perspektif Hukum Pidana. *Jurnal Legislasi Hukum*, 20(3), 412–428.
- Nugroho, A. (2024). Sinkronisasi Hukum Pidana Materiil dalam UU ITE Pasca KUHP Baru. *Jurnal Hukum Pidana dan Kriminologi*, 15(1), 41–60.

- Prasetyo, B. (2024). Ketidakpastian Hukum Pasal 28 Ayat (2) UU ITE. *Jurnal Hukum dan Masyarakat*, 16(1), 88–107.
- Setiawan, R. (2023). Lex Certa dalam Tindak Pidana Siber. *Jurnal Ilmu Hukum*, 18(1), 15–34.
- Sunstein, C. R. (2018). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

'ADALAH

Buletin Hukum & Keadilan

Moderasi Konten dalam Perspektif Hukum dan Etika Digital: Menemukan Keseimbangan antara Ketertiban Ruang Digital dan Kebebasan Berekspresi di Indonesia

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51875](https://doi.org/10.15408/adalah.v9i7.51875)

Abstract:

Content moderation has become a central governance mechanism for digital platforms, intersecting law, ethics, and business interests. This article examines Indonesia's content moderation framework and its capacity to balance public order with freedom of expression. Using normative legal research, the study finds that Indonesia applies a government-driven notice-and-takedown model, reinforced by the Content Moderation Compliance System (SAMAN), while platform policies operate under separate standards. The regime raises due process concerns, including vague definitions of illegal content, limited transparency, and weak user remedies. The article concludes that stronger transparency rules, regulatory harmonization, and independent oversight are essential to ensure accountability and rights protection.

Keywords: Content Moderation, Notice and Takedown, SAMAN, Due Process, Freedom of Expression.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Platform digital seperti media sosial, mesin pencari, dan layanan berbagi video telah menjadi ruang publik baru tempat miliaran pengguna berinteraksi, berekspresi, dan mengonsumsi informasi setiap hari. Namun, karakter *user-generated content* yang menjadi fondasi platform ini membawa serta problem klasik: konten ilegal, berbahaya, atau tidak pantas beredar secara masif dan instan. Untuk mengelola ini, platform menerapkan moderasi konten, yaitu serangkaian kebijakan dan praktik untuk menyaring, menilai, dan mengambil tindakan terhadap konten pengguna, baik melalui sistem otomatis berbasis kecerdasan buatan maupun melalui peninjauan manusia (Roberts, 2019). Moderasi konten bukan sekadar soal teknis; ia adalah aktivitas kuasi-yudisial yang melibatkan penilaian nilai, interpretasi norma, dan pengambilan keputusan yang berdampak langsung pada hak individu.

Di Indonesia, moderasi konten menjadi isu yang semakin mencuat seiring dengan meningkatnya volume pengguna internet dan konten digital. Pemerintah, melalui Kementerian Komunikasi dan Digital (Komdigi), memiliki kewenangan untuk memerintahkan pemutusan akses terhadap konten ilegal berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik

(PP PSTE). Pada saat yang sama, platform global seperti Meta, TikTok, dan X memiliki community guidelines dan sistem moderasi internal mereka sendiri yang beroperasi berdasarkan standar global, yang tidak selalu selaras dengan regulasi nasional atau konteks kultural lokal.

Ketegangan ini menciptakan lanskap moderasi konten yang kompleks dan seringkali kontradiktif. Di satu sisi, negara memiliki kepentingan sah untuk melindungi warganya dari ujaran kebencian, pornografi, disinformasi, dan konten berbahaya lainnya. Di sisi lain, penegakan yang berlebihan, tidak transparan, dan tanpa due process dapat dengan mudah berubah menjadi sensor yang membungkam kritik dan kebebasan fundamental. Platform, sementara itu, berada dalam posisi sulit: mematuhi perintah pemerintah berarti risiko menjadi alat represi, sementara menolak berarti menghadapi sanksi administratif hingga pemblokiran. Pengguna, sebagai pihak yang paling terdampak, seringkali menjadi korban dari kedua kekuatan ini tanpa memiliki mekanisme pemulihan yang memadai. Rumusan masalah artikel ini adalah: Pertama, bagaimana kerangka hukum dan praktik moderasi konten di Indonesia, dan sejauh mana ia memenuhi prinsip due process dan standar etika digital? Kedua, bagaimana reformasi kerangka moderasi konten yang dapat menyeimbangkan ketertiban dan kebebasan? Tujuannya untuk memetakan rezim moderasi konten yang ada,

mengidentifikasi persoalan hukum dan etisnya, serta merumuskan model yang lebih akuntabel dan demokratis.

B. MODERASI KONTEN, INTERMEDIARY LIABILITY, DAN ETIKA TATA KELOLA PLATFORM

Secara teoretis, moderasi konten berada dalam bingkai intermediary liability, yaitu doktrin yang menentukan sejauh mana platform sebagai perantara dapat dimintai pertanggungjawaban atas konten pengguna. Dalam hukum komparatif, dikenal beberapa model: strict liability (tanggung jawab mutlak), safe harbor (perlindungan sepanjang tidak mengetahui adanya konten ilegal), dan broad immunity (kekebalan luas) (Balkin, 2014). Model safe harbor klasik yang diadopsi oleh EU *E-Commerce Directive* dan Pasal 230 *Communications Decency Act* di AS menempatkan beban pada pengguna dan otoritas untuk melaporkan konten, sementara platform baru berkewajiban bertindak setelah menerima pemberitahuan yang sah (*notice and takedown*). Namun, di era surveillance capitalism dan platformisasi, di mana algoritma rekomendasi secara aktif mempromosikan konten demi keuntungan, argumen bahwa platform hanyalah perantara pasif semakin sulit dipertahankan. EU *Digital Services Act* (DSA) merespons pergeseran ini dengan menuntut akuntabilitas proaktif, khususnya dari *Very Large Online Platforms* (VLOPs), termasuk kewajiban transparansi, audit risiko, dan mekanisme

penyelesaian sengketa yang independen (Bradford, 2023).

Dari perspektif etika digital, moderasi konten bukan sekadar persoalan kepatuhan hukum, melainkan persoalan keadilan prosedural dan substansial. Luciano Floridi (2018) menekankan bahwa etika informasi menuntut penghormatan terhadap entitas informasi, yang mencakup privasi, akurasi, aksesibilitas, dan kepemilikan. Moderasi konten yang etis harus transparan, konsisten, non-diskriminatif, dan menyediakan mekanisme redress. Prinsip *due process* dalam moderasi konten, sebagaimana dirumuskan oleh para pegiat hak digital, mencakup hak untuk mengetahui aturan, hak untuk diberitahu jika konten dihapus, hak untuk mengajukan banding yang ditinjau oleh manusia, dan hak untuk mendapatkan pemulihan jika keputusan salah (Kaye, 2019). Di sisi lain, perspektif etika komunitarian menekankan bahwa moderasi konten harus mempertimbangkan konteks budaya, bahasa, dan politik lokal, sehingga standar global yang diterapkan secara seragam dapat menjadi bentuk imperialisme kultural yang mengabaikan nuansa ekspresi lokal.

Indonesia, dengan rezim moderasi konten yang unik, menawarkan studi kasus tentang bagaimana negara dengan tingkat penetrasi digital tinggi dan dinamika sosial-politik yang kompleks mencoba mengelola ruang digitalnya. Sistem SAMAN yang diluncurkan pemerintah merupakan

salah satu eksperimen paling ambisius di dunia dalam hal pengawasan konten berbasis teknologi. Namun, pertanyaan tentang transparansi, akuntabilitas, dan *due process* tetap menjadi tantangan yang mendasar.

C. KERANGKA HUKUM DAN PRAKTIK MODERASI KONTEN DI INDONESIA

1. Dasar Hukum: Dari UU ITE ke PP PSTE dan SAMAN

Landasan yuridis moderasi konten di Indonesia bertumpu pada UU ITE dan perubahannya. UU ITE tidak secara eksplisit mengatur "moderasi konten" sebagai sebuah rezim, tetapi memberikan dasar untuk pemidanaan konten ilegal dan mewajibkan penyelenggara sistem elektronik (PSE) untuk memastikan sistemnya tidak digunakan untuk perbuatan melawan hukum. Ketentuan lebih operasional ditemukan dalam PP Nomor 71 Tahun 2019 tentang PSTE. Pasal 14 PP PSTE mewajibkan PSE untuk memiliki sarana pelaporan konten ilegal dan menindaklanjutinya. Pasal 15 ayat (6) secara spesifik memberikan tenggat waktu 24 jam kepada PSE untuk memutus akses konten ilegal setelah menerima surat perintah dari kementerian. Kegagalan mematuhi perintah ini dapat berakibat sanksi administratif berupa denda hingga Rp500 juta per konten.

Rezim ini adalah bentuk *conditional safe harbor*: platform tidak secara otomatis bertanggung jawab atas konten pengguna, tetapi wajib bertindak setelah ada perintah dari otoritas. Namun, yang membedakan Indonesia dari model notice and takedown klasik adalah bahwa "pemberitahuan" utama berasal dari pemerintah, bukan dari pengguna. Pengguna memang dapat melaporkan konten, tetapi keputusan akhir tentang legalitas konten dan perintah *takedown* berada di tangan Komdigi. Ini menempatkan pemerintah sebagai aktor sentral dalam moderasi konten, yang menimbulkan pertanyaan tentang imparsialitas dan pemisahan kekuasaan.

Pada tahun 2025, pemerintah meluncurkan Sistem Kepatuhan Moderasi Konten (SAMAN), yang semakin memperkuat peran pengawasan pemerintah. SAMAN adalah aplikasi yang memungkinkan Komdigi memantau kepatuhan platform dalam menangani konten ilegal secara real-time. Platform yang melanggar akan dikenai peringatan bertahap: teguran pertama, kedua, ketiga, denda progresif, hingga pemblokiran sementara atau permanen. SAMAN secara fundamental meningkatkan tekanan kepatuhan pada platform, tetapi juga menimbulkan kekhawatiran tentang over-enforcement dan penggunaan sistem untuk tujuan di luar konten ilegal, seperti penurunan konten yang dianggap kritis terhadap pemerintah (CSIS, 2025).

2. Model Eksogen dan Endogen: Dua Standar yang Berbenturan

Moderasi konten di Indonesia dijalankan melalui dua model yang beroperasi secara paralel. Pertama, model eksogen, yaitu moderasi yang dipicu oleh perintah pemerintah melalui SAMAN atau surat perintah langsung. Model ini mengikuti definisi "konten ilegal" versi hukum Indonesia, yang mencakup ujaran kebencian, pornografi, perjudian, disinformasi, dan konten terorisme. Kedua, model endogen, yaitu moderasi yang dilakukan oleh platform berdasarkan community guidelines mereka sendiri. Platform seperti Meta dan TikTok memiliki standar global yang seringkali lebih ketat atau lebih longgar pada isu tertentu dibandingkan hukum Indonesia. Misalnya, community guidelines Meta melarang konten yang merendahkan berdasarkan gender atau orientasi seksual, yang tidak selalu diatur secara spesifik dalam hukum Indonesia, sementara di sisi lain hukum Indonesia tentang penodaan agama lebih luas daripada standar Meta.

Ketidakselarasan ini menimbulkan masalah. Platform seringkali mengambil tindakan over-removal untuk menghindari sanksi SAMAN, sehingga konten yang sebenarnya legal atau berada di area abu-abu ikut dihapus. Pada saat yang sama, pemerintah dapat meminta platform menurunkan konten yang tidak melanggar community guidelines internal platform tetapi dianggap melanggar hukum Indonesia. Platform tidak memiliki dasar untuk

menolak karena ancaman denda dan pemblokiran. Akibatnya, pengguna Indonesia tunduk pada dua lapis sensor: sensor negara melalui SAMAN dan sensor korporasi melalui community guidelines. Pengguna tidak memiliki kepastian tentang standar mana yang berlaku, dan tidak memiliki jalur redress yang jelas ketika hak ekspresinya dilanggar (Lubis, 2026).

3. Defisit Due Process: Ketika Keputusan Takedown Tidak Dapat Dikontes

Salah satu kelemahan paling kritis dari rezim moderasi konten di Indonesia adalah defisit due process. Due process dalam konteks moderasi konten mensyaratkan setidaknya empat hal: (1) aturan yang jelas dan dapat diakses publik tentang apa yang dilarang; (2) pemberitahuan kepada pengguna jika kontennya dihapus, disertai alasan yang spesifik; (3) mekanisme banding yang mudah diakses, cepat, dan ditinjau oleh manusia; serta (4) pengawasan independen terhadap proses takedown (Kaye, 2019). Rezim Indonesia masih lemah di keempat aspek ini.

Pertama, definisi konten ilegal dalam hukum Indonesia masih mengandung frasa-frasa multitafsir seperti "melanggar kesusilaan", "menimbulkan kebencian", dan "berita bohong" yang tidak memberikan batasan objektif yang cukup. Kedua, mekanisme pemberitahuan kepada pengguna tentang penghapusan konten tidak diwajibkan

secara eksplisit dalam regulasi. Platform seringkali menghapus konten tanpa memberi tahu pengguna, atau hanya memberikan notifikasi generik bahwa konten "melanggar standar komunitas" tanpa menjelaskan aturan mana yang dilanggar. Ketiga, mekanisme banding internal platform seringkali lambat, tidak transparan, dan menggunakan sistem otomatis yang tidak memadai. Keempat, tidak ada badan pengawas independen yang dapat menguji legalitas keputusan takedown di luar proses peradilan formal yang panjang dan mahal.

Putusan Mahkamah Konstitusi dalam beberapa perkara telah menekankan pentingnya due process dalam pembatasan hak berekspresi. Namun, penerapannya dalam ranah moderasi konten administratif masih jauh dari memadai. Ketiadaan saluran redress yang efektif ini menciptakan chilling effect: pengguna menjadi enggan mengekspresikan pendapat yang kontroversial karena takut dihapus atau diblokir tanpa kemampuan untuk membela diri.

D. PERSPEKTIF ETIKA DIGITAL: LEGITIMASI, IMPARSIALITAS, DAN KONTEKS KULTURAL

Dari sudut pandang etika digital, moderasi konten di Indonesia menghadapi tiga persoalan etis utama. Pertama, persoalan legitimasi. Sebuah keputusan takedown memiliki legitimasi jika dibuat oleh otoritas yang sah melalui prosedur yang adil dan berdasarkan aturan yang jelas. Penggunaan

SAMAN yang memberikan kekuasaan besar kepada eksekutif tanpa pengawasan yudisial menimbulkan pertanyaan tentang legitimasi demokratisnya. Apakah Komdigi sebagai lembaga administratif memiliki kapasitas dan imparsialitas untuk menjadi penentu tunggal legalitas konten? Kedua, persoalan imparsialitas. Data dari Koalisi Damai dan laporan media menunjukkan bahwa SAMAN telah digunakan untuk menurunkan konten-konten yang menyangkut isu-isu sensitif politik, seperti sejarah kekerasan seksual dan kritik kebijakan pemerintah (Magdalene.co, 2025). Jika benar, ini adalah pelanggaran serius terhadap prinsip imparsialitas yang merupakan inti etika moderasi konten.

Ketiga, persoalan penghormatan terhadap konteks kultural. Standar moderasi konten yang seragam seringkali mengabaikan keragaman bahasa, dialek, dan konteks budaya Indonesia. Konten yang menggunakan bahasa daerah, satire, atau ekspresi budaya tertentu seringkali salah dinilai oleh sistem otomatis yang tidak memiliki pemahaman konteks lokal. Di sisi lain, definisi "kesusilaan" atau "penghinaan" dalam hukum Indonesia juga sangat dipengaruhi oleh norma mayoritas, yang dapat mendiskriminasi ekspresi kelompok minoritas. Etika digital yang inklusif menuntut moderasi konten yang sensitif terhadap keragaman dan tidak menjadi alat untuk memaksakan moralitas satu kelompok terhadap kelompok lain.

E. PRAKTIK MODERASI KONTEN DAN KONTROVERSINYA

Denda terhadap Platform X dan Ketegangan Global-Lokal

Pada Oktober 2025, Komdigi menjatuhkan denda lebih dari Rp78 juta kepada Platform X karena kelalaian menangani konten pornografi yang terdeteksi melalui SAMAN. Ini adalah salah satu kasus pertama di mana pemerintah secara terbuka menggunakan SAMAN untuk menjatuhkan sanksi kepada platform global besar. Platform X, yang di bawah kepemimpinan Elon Musk telah melonggarkan kebijakan moderasi kontennya secara global, menghadapi benturan langsung dengan rezim Indonesia yang semakin ketat. Kasus ini menunjukkan bahwa model *conditional liability* dengan tekanan administratif dapat memaksa platform untuk mematuhi standar nasional, tetapi juga mengungkap ketegangan antara standar global dan lokal. Tanpa dialog dan kerjasama yang lebih konstruktif, yang terjadi adalah whack-a-mole regulasi di mana platform dipaksa patuh tanpa pemahaman mendalam tentang konteks, sementara pemerintah menggunakan kekuatan penuh untuk menekan tanpa mempertimbangkan implikasi terhadap ekosistem informasi (Hukumonline, 2025).

Penurunan Konten oleh Komdigi dan Kritik Over-Censorship

Sepanjang tahun 2025, Komdigi melaporkan telah menurunkan puluhan ribu konten negatif. Namun, laporan dari Koalisi Damai pada Juni 2025 mengungkapkan bahwa Komdigi telah meminta X untuk menurunkan akun-akun yang membahas sejarah kekerasan seksual 1998 dan kritik terhadap kebijakan tambang nikel. Permintaan ini diduga tidak didasarkan pada pelanggaran hukum yang spesifik, melainkan pada sensitivitas politik. Kasus ini memicu perdebatan tentang apakah SAMAN digunakan untuk menegakkan hukum atau untuk mengelola narasi politik. Ketiadaan transparansi membuat klaim pemerintah sulit diverifikasi, dan ruang bagi pengguna untuk membela diri hampir tidak ada. Ini adalah contoh buruk tentang bagaimana moderasi konten tanpa due process dapat dengan mudah meluncur menjadi alat kontrol politik (Magdalene.co, 2025).

Moderasi Konten terkait Isu SARA dan Polarisasi

Isu ujaran kebencian berbasis SARA adalah salah satu alasan utama pemerintah memperkuat moderasi konten. Pada Agustus 2025, Komdigi memanggil pengelola TikTok, Facebook, dan Instagram untuk membahas konten-konten yang mengandung disinformasi, fitnah, dan kebencian (DFK). Platform diminta untuk lebih proaktif menghapus konten-konten tersebut. Namun, tantangan etis yang muncul adalah bagaimana membedakan antara ujaran kebencian yang otentik dengan ekspresi yang keras tetapi masih dilindungi.

Tanpa definisi yang jelas, platform cenderung mengambil tindakan over-removal untuk menghindari sanksi, yang berujung pada pembungkaman terhadap suara-suara minoritas yang mencoba menyuarakan pengalaman diskriminasi mereka. Moderasi konten yang dimaksudkan untuk melindungi kelompok rentan justru dapat menjadi alat yang menindas mereka jika tidak dijalankan dengan presisi dan pemahaman konteks.

F. MEMBANGUN ARSITEKTUR MODERASI KONTEN YANG AKUNTABEL DAN DEMOKRATIS

Untuk mengatasi persoalan-persoalan di atas, diperlukan reformasi fundamental terhadap arsitektur moderasi konten di Indonesia. Pertama, harmonisasi dan klarifikasi regulasi. Pemerintah dan DPR perlu menyusun undang-undang layanan digital yang terintegrasi—Digital Services Act versi Indonesia—yang menyatukan ketentuan UU ITE, PP PSTE, dan Perpres Publisher Rights. Undang-undang ini harus merumuskan definisi konten ilegal yang presisi dan proporsional, mengadopsi pendekatan berbasis risiko seperti DSA, serta secara eksplisit mengatur hak due process pengguna.

Kedua, penguatan transparansi dan pengawasan. Setiap platform yang beroperasi di Indonesia, khususnya yang berukuran besar, harus diwajibkan untuk menerbitkan transparency report secara berkala yang merinci jumlah dan jenis konten

yang dihapus, sumber perintah (pemerintah, pengguna, deteksi otomatis), serta hasil banding. Pemerintah, melalui Komdigi, juga harus menerbitkan laporan transparansi serupa tentang penggunaan SAMAN. Selain itu, perlu dibentuk badan pengawas independen—*Digital Services Oversight Board*—yang beranggotakan ahli hukum, etika, teknologi, dan perwakilan masyarakat sipil, yang bertugas mengawasi kebijakan *takedown*, menerima keluhan, dan menerbitkan rekomendasi yang mengikat secara moral dan politis.

Ketiga, akses terhadap pemulihan. Setiap pengguna yang kontennya dihapus harus memiliki hak untuk mengajukan banding melalui mekanisme yang mudah diakses, cepat, dan murah. Platform wajib menyediakan internal appeal yang ditinjau oleh manusia. Jika tidak puas, pengguna dapat mengajukan sengketa ke badan penyelesaian sengketa di luar pengadilan yang disertifikasi oleh otoritas pengawas. Keempat, pengembangan kapasitas dan literasi. *Platform* harus diwajibkan untuk berinvestasi pada moderasi konten berbahasa Indonesia dan daerah, serta merekrut peninjau yang memahami konteks lokal. Pemerintah, di sisi lain, harus meningkatkan literasi digital masyarakat agar pengguna memahami hak-haknya, mampu melaporkan konten ilegal, dan menggunakan mekanisme redress yang tersedia.

Kelima, dialog multipihak. Forum komunikasi reguler antara pemerintah, *platform*, akademisi, dan

masyarakat sipil perlu diinstitusionalisasi untuk membahas isu-isu moderasi konten secara konstruktif, bukan konfrontatif. Forum ini dapat menjadi ruang untuk mengembangkan *code of practice* tentang moderasi konten yang menjadi pedoman bersama, mengikuti model *Digital Services Act* di Eropa yang menekankan *co-regulation*.

G. KESIMPULAN

Moderasi konten di Indonesia diatur dalam rezim *conditional liability* yang bertumpu pada UU ITE, PP PSTE, dan sistem SAMAN. Rezim ini memberikan kewenangan besar kepada pemerintah untuk memerintahkan takedown konten, yang dilaksanakan oleh platform di bawah ancaman sanksi administratif. Menjawab rumusan masalah pertama, praktik moderasi konten yang ada masih mengalami defisit *due process* yang serius: aturan main yang tidak jelas, ketiadaan transparansi, terbatasnya mekanisme banding, dan absennya pengawasan independen. Dari perspektif etika digital, rezim ini menghadapi persoalan legitimasi, imparsialitas, dan ketidakpekaan terhadap konteks kultural. Menjawab rumusan masalah kedua, reformasi harus diarahkan pada pembentukan undang-undang layanan digital yang terintegrasi, penguatan transparansi melalui *transparency report* dan audit independen, penyediaan mekanisme redress yang aksesibel, serta pengembangan dialog multipihak yang berkelanjutan.

Rekomendasi yang diajukan adalah: pertama, harmonisasi regulasi melalui *Digital Services Act Indonesia*; kedua, penerbitan *transparency report* wajib bagi *platform* dan pemerintah; ketiga, pembentukan *Digital Services Oversight Board* yang independen; keempat, pengembangan mekanisme banding dan penyelesaian sengketa yang murah dan cepat; dan kelima, pengarusutamaan literasi digital dan dialog multipihak. Hanya dengan kerangka moderasi konten yang akuntabel, transparan, dan demokratis, Indonesia dapat memastikan bahwa ruang digitalnya menjadi arena deliberasi publik yang sehat, bukan medan sensor yang represif.

REFERENSI:

- Balkin, J. M. (2014). Old-School/New-School Speech Regulation. *Harvard Law Review*, 127(8), 2296–2342.
- Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.
- Center for Strategic and International Studies. (2025, Maret 6). Should Indonesia Adopt EU Digital Services Act to Improve its Content Moderation Policies? <https://blog.csis.or.id>
- Floridi, L. (2018). Soft Ethics, the Governance of the Digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A*, 376(2133).

- Hukumonline. (2025, Oktober 14). Komdigi Tegur X: Lalai Tangani Pornografi, Denda Rp78 Juta Lebih. *Republika Online*.
- Kaye, D. (2019). *Speech Police: The Global Struggle to Govern the Internet*. Columbia Global Reports.
- Lubis, A. F. (2026). Online Platform Intermediary Liability under the Electronic Information and Transactions (ITE) Law, Freedom of Expression (FoE) Safeguards in Indonesia. *The Easta Journal Law and Human Rights*, 4(2), 226–234.
- Magdalene.co. (2025, November 20). SAMAN dan Komdigi Hapus Konten dalam 4 Jam. *Magdalene*.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).
- Roberts, S. T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

'ADALAH

Buletin Hukum & Keadilan

Keabsahan Kontrak Elektronik dalam Transaksi *E-Commerce*: Fondasi Yuridis, Problematika Pembuktian, dan Urgensi Perlindungan Konsumen Digital di Indonesia

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51876](https://doi.org/10.15408/adalah.v9i7.51876)

Abstract:

Abstract Electronic contracts form the backbone of e-commerce transactions in digital environments. This article examines the validity of electronic contracts under Indonesian law and identifies challenges in evidence and consumer protection. Using normative legal research, the study finds that the Electronic Information and Transactions Law (ITE Law) recognizes electronic contracts as legally valid and equivalent to conventional contracts under Article 1320 of the Civil Code. However, implementation issues persist, including standard form clauses, weak informed consent through "click-to-accept" systems, and unequal bargaining power. Evidentiary problems regarding authenticity and data integrity also remain. The article concludes that regulatory reform is needed to strengthen meaningful consent and consumer protection.

Keywords: Electronic Contracts, E-Commerce, ITE Law, Consumer Protection, Consent.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Pertumbuhan e-commerce di Indonesia merupakan salah satu yang paling impresif di dunia. Menurut data Bank Indonesia, nilai transaksi *e-commerce* Indonesia pada tahun 2023 melampaui Rp450 triliun, menempatkannya sebagai pasar ekonomi digital terbesar di Asia Tenggara. *Platform* seperti Tokopedia, Shopee, Lazada, dan Bukalapak telah menjadi infrastruktur belanja harian bagi puluhan juta warga. Di jantung setiap transaksi digital ini terdapat kontrak elektronik, perjanjian yang dibentuk, dikirim, dan disepakati melalui media digital, seringkali hanya dengan satu klik tombol "Beli Sekarang" atau "Saya Setuju".

Kontrak elektronik memiliki karakter yang berbeda secara fundamental dari kontrak konvensional. Ia tidak memerlukan kertas, tidak mempertemukan para pihak secara fisik, dan seringkali terjadi dalam kecepatan yang membuat salah satu pihak konsumen tidak memiliki waktu atau kesempatan untuk membaca, memahami, apalagi menegosiasikan isinya. Syarat dan ketentuan disajikan dalam dinding teks panjang yang digulir dengan cepat, sementara mekanisme persetujuan direduksi menjadi kotak centang (*checkbox*) atau tombol konfirmasi. Dalam ekosistem ini, pertanyaan tentang keabsahan kontrak elektronik menjadi jauh lebih kompleks daripada sekadar "apakah undang-undang mengakuinya?"

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, telah secara eksplisit mengakui kontrak elektronik sebagai kontrak yang sah dan mengikat para pihak. Pasal 18 ayat (1) UU ITE menyatakan bahwa transaksi elektronik yang dituangkan dalam kontrak elektronik mengikat para pihak. Pengakuan ini didukung oleh Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) yang memberikan pedoman lebih rinci. Secara formil, Indonesia memiliki fondasi hukum yang cukup untuk mengamini keabsahan kontrak elektronik.

Namun, masalahnya bukan pada pengakuan formal, melainkan pada ketimpangan struktural yang tersembunyi di balik layar. Konsumen sebagai pihak yang lebih lemah seringkali tidak menyadari apa yang mereka setuju. Klausula baku yang eksoneratif, yang mengalihkan risiko kepada konsumen atau membatasi tanggung jawab pelaku usaha ditanam dalam kontrak digital tanpa penyorotan yang memadai. Lebih dari itu, munculnya dark patterns, desain antarmuka yang secara manipulatif menggiring pengguna untuk mengambil keputusan yang tidak diinginkan, telah mendistorsi esensi persetujuan bebas (free consent) yang menjadi jantung sahnya kontrak (Luguri & Strahilevitz, 2021). Rumusan masalah artikel ini

adalah: Pertama, bagaimana kerangka yuridis keabsahan kontrak elektronik dalam transaksi *e-commerce* di Indonesia? Kedua, apa problematika utama dalam implementasi dan penegakan kontrak elektronik, khususnya terkait pembuktian dan perlindungan konsumen? Tujuannya untuk menelaah secara kritis fondasi hukum kontrak elektronik, mengidentifikasi celah antara validitas normatif dan keadilan substantif, serta merumuskan rekomendasi penguatan kerangka perlindungan.

B. KEABSAHAN KONTRAK DALAM TRADISI HUKUM PERDATA DAN ERA DIGITAL

Untuk menilai keabsahan kontrak elektronik, kerangka teoretisnya berakar pada doktrin hukum perdata klasik tentang syarat sahnya perjanjian. Pasal 1320 Kitab Undang-Undang Hukum Perdata (KUHPerdata) menetapkan empat syarat kumulatif sahnya suatu perjanjian: (1) kesepakatan mereka yang mengikatkan diri; (2) kecakapan untuk membuat suatu perikatan; (3) suatu hal tertentu; dan (4) suatu sebab yang halal. Dua syarat pertama adalah syarat subjektif yang menyangkut subjek hukum, sementara dua syarat terakhir adalah syarat objektif yang menyangkut objek perjanjian. Pelanggaran terhadap syarat subjektif membuat kontrak dapat dibatalkan, sedangkan pelanggaran terhadap syarat objektif membuat kontrak batal demi hukum.

Kontrak elektronik menerima beban yang sama: ia harus memenuhi keempat syarat ini untuk dianggap sah. Namun, karakteristik digital memberikan tekanan yang unik pada syarat kesepakatan. Kesepakatan dalam kontrak konvensional biasanya terbentuk setelah negosiasi, tawar-menawar, dan penandatanganan di hadapan saksi. Dalam kontrak elektronik, kesepakatan seringkali terbentuk melalui mekanisme *click-wrap* (mengeklik tombol "Saya Setuju"), *browse-wrap* (mengakses situs dianggap setuju dengan syarat yang ditautkan), atau bahkan *pay-now-terms-later* (syarat dikirim setelah pembayaran). Pertanyaannya: apakah semua mekanisme ini mencerminkan persetujuan yang bebas dan sadar sebagaimana dimaksud Pasal 1320 jo. Pasal 1321 KUHPdata?

Doktrin klasik tentang cacat kehendak kesesatan, paksaan, dan penipuan menjadi relevan. *Dark patterns*, misalnya, dapat dikategorikan sebagai bentuk penipuan atau setidaknya kesesatan yang direayasa, karena desain antarmuka secara sengaja menyesatkan pengguna untuk menyetujui hal yang tidak diinginkan. Namun, penerapan doktrin cacat kehendak terhadap desain antarmuka masih menjadi *terra incognita* dalam yurisprudensi Indonesia.

Dari perspektif hukum perlindungan konsumen, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) melarang pencantuman klausula baku yang merugikan konsumen pada setiap dokumen atau perjanjian

(Pasal 18). Namun, aturan ini dirumuskan sebelum era *e-commerce*, sehingga penegakannya terhadap kontrak digital masih menimbulkan persoalan. Bagaimana membuktikan bahwa klausula baku dalam dinding teks digital "telah dicantumkan secara mencolok" sebagaimana dimaksud UUPK?

Secara global, terjadi pergeseran paradigma dari *click consent* menuju *meaningful consent* (persetujuan bermakna). GDPR di Eropa dan *California Consumer Privacy Act* (CCPA) di Amerika Serikat mendorong agar persetujuan diberikan secara aktif, spesifik, dan setelah informasi yang relevan disampaikan secara jelas. *Digital Services Act* (DSA) Uni Eropa melarang beberapa bentuk dark patterns secara eksplisit. Indonesia belum mengadopsi pendekatan *meaningful consent* ini secara komprehensif, meskipun UU Pelindungan Data Pribadi (UU PDP) mulai menyinggung prinsip persetujuan yang eksplisit dan spesifik untuk pemrosesan data pribadi. Kerangka teoretis ini menjadi dasar untuk menganalisis apakah kontrak elektronik di Indonesia telah memenuhi standar keabsahan substantif, bukan sekadar formalitas.

C. KERANGKA YURIDIS KONTRAK ELEKTRONIK DI INDONESIA

1. Pengakuan Yuridis: UU ITE dan PP PSTE sebagai Landasan

Pasal 18 UU ITE merupakan pasal sentral yang memberikan legitimasi pada kontrak elektronik. Ayat (1) menegaskan bahwa transaksi elektronik yang dituangkan dalam kontrak elektronik mengikat para pihak. Ayat ini secara prinsipil menyamakan kedudukan kontrak elektronik dengan kontrak tertulis di atas kertas. Konsekuensinya, semua asas hukum perjanjian yang berlaku dalam KUHPdata, kebebasan berkontrak, konsensualisme, *pacta sunt servanda*, iktikad baik, berlaku juga untuk kontrak elektronik.

PP PSTE, khususnya Pasal 49 hingga 54, menjabarkan lebih rinci tentang kontrak elektronik. Pasal 49 menyebutkan bahwa kontrak elektronik paling sedikit harus memuat: identitas para pihak, objek dan spesifikasi, persyaratan transaksi, harga dan biaya, serta tata cara pembayaran dan pengiriman. Ketentuan ini bersifat minimum requirement yang ditujukan untuk memberikan kejelasan dan kepastian. Pasal 51 mewajibkan kontrak elektronik dibuat dalam bahasa Indonesia, yang merupakan implementasi dari UU Nomor 24 Tahun 2009 tentang Bendera, Bahasa, dan Lambang Negara. Pelanggaran terhadap kewajiban bahasa Indonesia dapat berakibat kontrak batal demi hukum karena melanggar syarat objektif (sebab yang halal), sebagaimana ditegaskan oleh Mahkamah Agung dalam beberapa putusannya.

Namun, PP PSTE tidak mengatur lebih jauh tentang bagaimana "kesepakatan" harus dicapai

dalam transaksi elektronik. Ia tidak membedakan antara *click-wrap*, *browse-wrap*, atau mekanisme lain. Ini meninggalkan celah besar karena model *browse-wrap*, yang menganggap pengguna setuju hanya dengan mengakses situs, sangat kontroversial secara hukum di berbagai yurisdiksi. Pengadilan di beberapa negara, termasuk Amerika Serikat, telah menolak *browse-wrap* sebagai bentuk persetujuan yang sah karena tidak ada tindakan afirmatif yang menunjukkan kesepakatan.

2. Syarat Sah Kontrak: Menjembatani Pasal 1320 KUHPERdata dengan Realitas Digital

Tantangan paling mendasar adalah membuktikan bahwa kontrak elektronik telah memenuhi seluruh syarat Pasal 1320 KUHPERdata. Syarat kecakapan relatif tidak berbeda dengan kontrak konvensional. Demikian pula syarat suatu hal tertentu, yang dalam konteks *e-commerce* biasanya jelas: deskripsi produk, harga, dan kuantitas. Syarat sebab yang halal juga relatif netral, sepanjang barang atau jasa yang diperdagangkan tidak melanggar hukum.

Persoalan muncul pada syarat kesepakatan. Kapan tepatnya kesepakatan terjadi dalam transaksi *e-commerce*? Apakah saat konsumen mengeklik "Beli Sekarang"? Atau saat penjual mengonfirmasi pesanan melalui surel otomatis? Atau saat barang dikirim? Hukum kontrak mengenal teori offer and acceptance. Dalam *e-commerce*, penawaran biasanya

dilakukan oleh penjual melalui tampilan produk di *platform* (yang secara hukum dianggap sebagai "undangan untuk menawar" atau "penawaran", tergantung konteks). Penerimaan dilakukan oleh pembeli dengan mengeklik tombol pembelian. Namun, banyak *platform* menambahkan lapisan konfirmasi di mana penjual baru akan mengirim barang setelah menerima notifikasi pembayaran. Ini menciptakan ambiguitas tentang kapan kontrak terbentuk.

Lebih jauh, Pasal 1321 KUHPerdata menyatakan bahwa kesepakatan yang diberikan karena kesesatan, paksaan, atau penipuan adalah tidak sah. Muncul pertanyaan: apakah penyajian syarat dan ketentuan yang panjang, rumit, dan tidak memungkinkan negosiasi dapat dikategorikan sebagai "paksaan" secara ekonomi? Konsumen tidak memiliki pilihan selain menyetujui jika ingin menggunakan layanan (*take-it-or-leave-it*). Dalam hukum kontrak, kontrak adhesi semacam ini tidak otomatis batal, tetapi klausula-klausulanya harus ditafsirkan secara lebih ketat, dan klausula yang tidak adil dapat dikesampingkan oleh hakim. Di beberapa negara, doktrin *unconscionability* (ketidakwajaran) memungkinkan pengadilan untuk menolak memberlakukan kontrak yang sangat timpang, meskipun ditandatangani. Indonesia belum memiliki yurisprudensi yang konsisten soal ini dalam konteks digital, tetapi hakim memiliki kewenangan untuk mengoreksi kontrak yang

melanggar kepatutan dan iktikad baik (Pasal 1338 ayat (3) jo. Pasal 1339 KUHPerddata).

3. Pembuktian Kontrak Elektronik: Antara *Best Evidence Rule* dan Integritas Data

Salah satu isu paling pelik adalah pembuktian kontrak elektronik di pengadilan. UU ITE Pasal 5 menyatakan bahwa informasi dan dokumen elektronik merupakan alat bukti hukum yang sah. Namun, pengakuan ini tidak menjawab pertanyaan: bagaimana membuktikan bahwa dokumen elektronik yang diajukan adalah kontrak yang disepakati, tidak diubah, dan benar-benar berasal dari para pihak?

Best evidence rule dalam hukum pembuktian mensyaratkan bukti asli. Untuk kontrak elektronik, konsep "asli" menjadi rumit. Salinan digital dari kontrak elektronik identik secara *bit-by-bit*, sehingga secara teknis tidak ada perbedaan antara asli dan salinan. Maka, fokusnya bergeser ke integritas data: dapatkah dipastikan bahwa kontrak elektronik tersebut tidak mengalami perubahan sejak pertama kali dibuat? Di sinilah peran tanda tangan elektronik, hash kriptografis, dan time stamp yang dihasilkan oleh trusted third party menjadi krusial.

UU ITE dan PP PSTE mengakui tanda tangan elektronik, tetapi dengan pembedaan antara tanda tangan elektronik biasa dan tanda tangan elektronik tersertifikasi yang memiliki kekuatan pembuktian

sempurna dan tidak dapat disangkal. Mayoritas kontrak e-commerce sehari-hari tidak menggunakan tanda tangan elektronik tersertifikasi. Mereka hanya mengandalkan *click consent* yang catatannya tersimpan di *server platform*. Apabila terjadi sengketa, konsumen harus bergantung pada data yang dimiliki oleh pihak yang digugatnya sebuah asimetri pembuktian yang mengkhawatirkan. Konsumen tidak memiliki salinan kontrak, tidak memiliki akses ke *log server platform*, dan tidak memiliki tanda tangan digital yang dapat diverifikasi. Dalam posisi ini, konsumen sangat sulit membuktikan klaimnya, sementara pelaku usaha dapat dengan mudah memanipulasi data yang dimilikinya (Santoso, 2023).

D. SENGKETA KONTRAK ELEKTRONIK DALAM PRAKTIK PERADILAN

Kasus 1: Putusan MA No. 3011 K/PDT/2017 tentang Kontrak Elektronik antara Pelaku Usaha dan Konsumen

Dalam kasus ini, seorang konsumen menggugat penyedia layanan perjalanan daring karena tiket yang dibelinya tidak dapat digunakan, sementara syarat dan ketentuan di situs menyatakan bahwa tiket tidak dapat dibatalkan dan tidak dapat diubah. Konsumen berargumen bahwa ia tidak pernah membaca syarat dan ketentuan tersebut karena tombol persetujuannya disembunyikan di bagian bawah halaman. Pengadilan Negeri dan Pengadilan Tinggi mengabulkan sebagian gugatan

konsumen, menilai bahwa klausula eksonerasi yang dicantumkan secara tidak mencolok melanggar UUPK. Mahkamah Agung, dalam tingkat kasasi, memperkuat putusan tersebut dan menekankan bahwa pelaku usaha bertanggung jawab untuk memastikan bahwa konsumen benar-benar memahami syarat-syarat yang disetujuinya. Putusan ini penting karena menandai pengakuan bahwa click consent tidak otomatis memenuhi syarat kesepakatan jika tidak disertai penyajian yang jelas.

Kasus 2: Sengketa Pembatalan Sepihak Order oleh *Platform E-Commerce*

Pada tahun 2022, ribuan konsumen mengeluhkan pembatalan sepihak pesanan oleh *platform e-commerce* pada saat kampanye diskon besar. Platform beralasan bahwa harga yang tercantum adalah kesalahan sistem (*pricing error*). Konsumen berargumen bahwa kontrak telah terbentuk saat mereka mengeklik "Beli" dan melakukan pembayaran. Pertanyaan hukumnya: apakah *pricing error* merupakan cacat kehendak yang membatalkan kontrak? Secara tradisional, jika kesalahan menyangkut substansi pokok perjanjian dan pihak lain mengetahui atau sepatutnya mengetahui kesalahan tersebut, kontrak dapat dibatalkan. Namun, dalam *e-commerce* massal, sulit untuk membuktikan bahwa konsumen mengetahui adanya kesalahan harga. Kasus-kasus ini banyak yang diselesaikan di luar pengadilan melalui mediasi Badan Penyelesaian Sengketa Konsumen

(BPSK), tetapi tidak ada pedoman yang jelas dan konsisten.

Kasus 3: Kontroversi Dark Patterns dan Penyesatan Konsumen

Pada tahun 2023, sebuah *platform* berlangganan konten digital digugat oleh konsumen yang tidak sengaja berlangganan paket tahunan dengan perpanjangan otomatis. Konsumen mendaftar untuk uji coba gratis, tetapi proses pembatalannya sengaja dibuat sangat rumit: tautan pembatalan disembunyikan di submenu yang tidak jelas, memerlukan beberapa kali konfirmasi melalui surel, dan waktu respons yang lambat. Praktik ini adalah contoh klasik dark patterns. Konsumen berargumen bahwa ia tidak pernah menyetujui perpanjangan berbayar secara sadar. Kasus ini akhirnya diselesaikan secara damai, tetapi menjadi peringatan bahwa hukum kontrak klasik belum cukup untuk menghadapi manipulasi digital. Belum ada undang-undang di Indonesia yang secara eksplisit melarang dark patterns, dan ini adalah kesenjangan yang mendesak untuk diisi.

E. REZIM PERLINDUNGAN KONSUMEN DAN URGENSI PENGATURAN *MEANINGFUL CONSENT*

Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999) telah menyediakan kerangka dasar. Pasal 18 melarang pencantuman klausula baku yang menyatakan pengalihan tanggung jawab

pelaku usaha, atau yang menyatakan bahwa konsumen memberikan kuasa kepada pelaku usaha untuk melakukan segala tindakan sepihak atas barang yang dibeli. Pasal 62 mengancam pelanggar dengan pidana penjara hingga lima tahun atau denda hingga Rp2 miliar. Namun, UUPK dirancang untuk kontrak tertulis konvensional. Penerapannya pada kontrak elektronik, di mana syarat dan ketentuan bisa berubah setiap saat tanpa pemberitahuan, di mana "persetujuan" diberikan dengan sekali klik, masih lemah dan memerlukan adaptasi.

Peraturan perundang-undangan yang lebih baru, seperti UU PDP (UU No. 27 Tahun 2022), mulai mengadopsi prinsip *meaningful consent* dalam konteks pemrosesan data pribadi. Pasal 6 UU PDP mensyaratkan persetujuan eksplisit dari subjek data untuk satu atau beberapa tujuan spesifik yang telah disampaikan oleh pengendali data. Persetujuan harus diberikan secara tertulis atau terekam, dan subjek data harus diberi informasi yang lengkap tentang tujuan, jenis data, dan hak-haknya. Ini adalah langkah maju yang signifikan.

Apa yang kurang adalah penerapan prinsip *meaningful consent* ke ranah kontrak *e-commerce* secara umum, bukan hanya data pribadi. Seharusnya, sebelum konsumen terikat oleh kontrak elektronik, *platform* wajib: (1) menyajikan syarat-syarat kunci (harga, durasi, mekanisme pembatalan, pengembalian dana) secara ringkas dan mudah

dipahami (*summary notice*); (2) mendapatkan persetujuan afirmatif yang terpisah untuk setiap klausula yang berpotensi merugikan konsumen; (3) menyediakan salinan kontrak yang dapat diunduh dan disimpan oleh konsumen; serta (4) tidak menggunakan *dark patterns* yang memanipulasi atau mengaburkan pilihan konsumen. Beberapa negara bagian di Amerika Serikat dan Eropa melalui DSA telah mulai mengadopsi persyaratan semacam ini. Indonesia perlu belajar dari mereka dan menyesuaikannya dengan kondisi lokal.

F. MEMPERKUAT KEABSAHAN KONTRAK ELEKTRONIK SECARA NORMATIF DAN PRAKTIS

Pertama, harmonisasi dan pengembangan regulasi. Pemerintah perlu menyusun pedoman atau peraturan setingkat menteri yang secara spesifik mengatur standar kontrak elektronik dalam transaksi *e-commerce*. Pedoman ini harus merumuskan definisi *meaningful consent*, melarang *dark patterns*, dan menetapkan persyaratan minimal untuk penyajian syarat dan ketentuan kontrak. Pedoman ini juga harus mewajibkan penyedia *platform* untuk menyediakan ringkasan kontrak (*summary of key terms*) yang mudah diakses sebelum konsumen menyetujui transaksi.

Kedua, penguatan pengawasan dan penegakan. BPSK dan otoritas perlindungan konsumen perlu diberikan kewenangan yang lebih kuat untuk menerima dan menangani pengaduan

terkait kontrak elektronik, termasuk kewenangan untuk memerintahkan platform mengubah praktik kontraknya yang tidak adil. Pembentukan unit khusus sengketa *e-commerce* di BPSK yang memiliki keahlian teknis dan hukum digital sangat diperlukan. Selain itu, Badan Perlindungan Konsumen Nasional (BPKN) harus melakukan kajian berkala tentang praktik kontrak elektronik di *platform* besar dan menerbitkan laporan publik yang dapat menjadi acuan bagi konsumen dan pelaku usaha.

Ketiga, penguatan kapasitas konsumen. Literasi kontrak digital harus menjadi bagian dari literasi digital nasional. Konsumen perlu diedukasi untuk membaca ringkasan syarat, memeriksa mekanisme pembatalan, dan menyimpan salinan kontrak. *Platform* dapat diwajibkan untuk memfasilitasi edukasi ini melalui antarmuka yang ramah pengguna.

Keempat, pengembangan mekanisme penyelesaian sengketa elektronik (*Online Dispute Resolution/ODR*). Untuk sengketa *e-commerce* bernilai kecil, pengadilan konvensional terlalu mahal dan lambat. Indonesia perlu mengembangkan *platform* ODR yang dapat diakses secara daring, dengan biaya rendah, dan proses yang cepat. Beberapa negara seperti Tiongkok melalui *Internet Courts*-nya telah berhasil menyelesaikan jutaan sengketa *e-commerce* secara efisien melalui ODR. Indonesia dapat mempelajari model ini dan menyesuaikannya.

Kelima, harmonisasi internasional. Mengingat banyak *platform e-commerce* bersifat lintas batas, Indonesia perlu terlibat aktif dalam harmonisasi aturan kontrak elektronik di tingkat ASEAN dan global. UNCITRAL Model Law on Electronic Commerce dan United Nations Convention on the Use of Electronic Communications in International Contracts (2005) menyediakan kerangka yang dapat diadopsi. Indonesia telah meratifikasi beberapa prinsip UNCITRAL melalui UU ITE, tetapi implementasi penuh perlu ditingkatkan.

G. KESIMPULAN

Keabsahan kontrak elektronik dalam transaksi *e-commerce* di Indonesia memiliki fondasi yuridis yang cukup melalui UU ITE dan PP PSTE, yang menempatkannya setara dengan kontrak tertulis konvensional sepanjang memenuhi syarat sah Pasal 1320 KUHPdata. Namun, validitas normatif ini belum sepenuhnya menjamin keadilan substantif. Menjawab rumusan masalah pertama, kerangka hukum telah mengakui kontrak elektronik, tetapi belum secara memadai mengatur mekanisme mencapai "kesepakatan" yang bebas dan sadar dalam ekosistem digital yang asimetris. Menjawab rumusan kedua, problematika utama terletak pada ketimpangan pembuktian yang merugikan konsumen, maraknya klausula baku eksonerasi yang tidak transparan, dan penggunaan dark patterns yang mendistorsi persetujuan.

Rekomendasi yang diajukan meliputi: pertama, penyusunan pedoman standar kontrak elektronik yang mengadopsi prinsip meaningful consent dan melarang dark patterns; kedua, penguatan kapasitas kelembagaan BPSK dan BPKN dalam menangani sengketa *e-commerce*; ketiga, pengembangan *platform Online Dispute Resolution* nasional; keempat, integrasi literasi kontrak digital ke dalam gerakan literasi digital; dan kelima, keterlibatan aktif dalam harmonisasi hukum kontrak elektronik internasional. Hanya dengan reformasi yang menyentuh dimensi normatif, kelembagaan, dan literasi, keabsahan kontrak elektronik tidak hanya menjadi mantra di atas kertas, tetapi sungguh-sungguh melindungi hak-hak semua pihak secara adil dan setara.

REFERENSI:

- Harahap, M. Yahya. (2018). Hukum Acara Perdata: Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan (Edisi Kedua). Jakarta: Sinar Grafika.
- Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13(1), 43–109.
- Makarim, E. (2020). Kontrak Elektronik: Teori dan Praktik. Jakarta: Rajawali Pers.
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400).
- Putusan Mahkamah Agung Nomor 3011 K/PDT/2017.
- Santoso, L. (2023). Automatisasi, Kontrak Cerdas, dan Tantangan Hukum Perdata Klasik. *Jurnal Yudisial*, 16(3), 301–322.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Lembaran Negara Tahun 1999 Nomor 42, Tambahan Lembaran Negara Nomor 3821).

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

Wahyudi, T., & Ayu, I. (2024). Keabsahan Kontrak Elektronik dalam E-Commerce: Perspektif Hukum Positif dan Hukum Islam. *Jurnal Hukum dan Etika Digital*, 2(1), 15–30.
<https://doi.org/10.5678/jhed.v2i1.9902>

'ADALAH

Buletin Hukum & Keadilan

Regulasi Kecerdasan Buatan (AI) dalam Perspektif Hukum Indonesia: Menimbang Kesenjangan, Risiko Keamanan Nasional, dan Cetak Biru Tata Kelola yang Berdaulat

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51877](https://doi.org/10.15408/adalah.v9i7.51877)

Abstract:

Artificial Intelligence (AI) is a general-purpose technology that is transforming economic, political, and security systems. However, Indonesia lacks a specific AI regulatory framework and still relies on outdated legal instruments. This article analyzes Indonesia's current AI governance, identifies regulatory gaps, and proposes improvements for rights protection and national security. Using normative legal research with conceptual and comparative approaches based on the EU AI Act, the study finds that the absence of an AI law creates legal uncertainty and increases risks of algorithmic discrimination, surveillance, and AI-related crimes. Existing draft regulations remain non-binding and insufficient. The article concludes that a risk-based AI law and independent oversight are urgently needed.

Keywords: Artificial Intelligence, AI Regulation, Algorithmic Discrimination, Digital Surveillance, Governance.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Kecerdasan Buatan atau *Artificial Intelligence* (AI) tidak lagi sekadar gagasan futuristik dalam narasi fiksi ilmiah. Ia telah menjelma menjadi fondasi utama gelombang Revolusi Industri 4.0, mengubah cara manusia berinteraksi, bekerja, dan mengambil keputusan. Di satu sisi, AI menjanjikan lompatan efisiensi yang revolusioner, otomatisasi cerdas, hingga akurasi diagnostik medis. Namun, di sisi lain, kemampuannya yang eksponensial menyimpan potensi destruktif: diskriminasi algoritmik, pengawasan massal, manipulasi sosial-politik, hingga pengangguran struktural. Dualisme inilah yang menempatkan regulasi AI sebagai isu kritis dalam diskursus hukum kontemporer.

Di tengah percepatan global, Indonesia masih tertatih dalam menyusun kerangka hukum yang memadai. Pengaturan AI masih terserak dalam berbagai regulasi sektoral yang tidak dirancang spesifik untuknya, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Pelindungan Data Pribadi (UU PDP). Belum ada satu pun payung hukum komprehensif yang secara spesifik mendefinisikan, mengklasifikasikan risiko, dan menetapkan batasan tanggung jawab dalam pemanfaatan AI. Kondisi ini menempatkan Indonesia pada posisi yang paradoks: sebagai salah satu pasar digital terbesar di Asia Tenggara, tetapi dengan tingkat kesiapan regulasi yang masih prematur.

Beberapa pakar hukum telah menyuarakan kegelisahan serupa. Satu studi menyimpulkan bahwa kerangka hukum Indonesia saat ini "belum memadai untuk melindungi hak asasi manusia (HAM) di tengah penggunaan AI yang semakin luas dan kompleks". Hal ini diperparah dengan fakta bahwa AI telah digunakan dalam sektor-sektor strategis seperti pengawasan publik dan pengenalan wajah tanpa disertai kewajiban transparansi algoritma, mekanisme audit, maupun pertanggungjawaban hukum yang jelas. Ketiadaan regulasi ini tidak hanya menciptakan ketidakpastian hukum, tetapi juga membuka celah bagi pelanggaran hak konstitusional warga negara, sebagaimana dijamin dalam Pasal 28G ayat (1) UUD 1945.

Tulisan ini memfokuskan pada rumusan masalah: Pertama, bagaimana potret kesenjangan regulasi AI di Indonesia saat ini? Kedua, bagaimana implikasi kekosongan regulasi tersebut terhadap keamanan nasional? Ketiga, bagaimana kerangka ideal regulasi AI nasional yang berdaulat? Tujuannya adalah untuk mengelaborasi kelemahan regulasi eksisting serta menawarkan cetak biru tata kelola AI yang responsif, adaptif, dan humanis.

B. LANDASAN TEORETIS DAN KONSEPTUAL

Konsep negara hukum digital menuntut adanya kepastian hukum dalam setiap aspek kehidupan, termasuk dalam pemanfaatan teknologi baru. Merujuk pada pemikiran Lessig, regulasi di

ruang siber ditentukan oleh empat modalitas: hukum, norma sosial, pasar, dan arsitektur kode. Ketika hukum absen, maka kode dan pasar akan mengambil alih kendali, yang seringkali mengarah pada ketidakadilan dan eksploitasi (Lessig, 2006). Dalam konteks AI, pendekatan berbasis risiko (*risk-based approach*) menjadi standar emas global, sebagaimana diadopsi oleh *EU AI Act*. Pendekatan ini tidak melarang atau membiarkan AI sepenuhnya, melainkan mengklasifikasikan sistem AI berdasarkan tingkat risikonya: dari risiko yang tidak dapat diterima (*unacceptable risk*), risiko tinggi (*high risk*), risiko terbatas (*limited risk*), hingga risiko minimal.

Oleh karena itu, kerangka teori dalam studi ini bertumpu pada tiga pilar utama. Pertama, konsep negara hukum modern yang menekankan supremasi hukum, persamaan di hadapan hukum, dan perlindungan HAM harus dioperasionalkan ulang dalam konteks kedaulatan digital. Asshiddiqie (2021) menegaskan bahwa perlindungan terhadap privasi dan data pribadi merupakan wujud hak konstitusional warga negara yang inheren. Kedua, teori Responsive Regulation yang menawarkan pendekatan piramida penegakan hukum, di mana sanksi pidana merupakan *ultimum remedium*, bukan *premium remedium*. Teori ini menekankan pentingnya dialog antara regulator dan industri untuk menciptakan regulasi yang adaptif (Braithwaite, 2017). Ketiga, konsep *Legal Cybernetics*

yang menekankan perlunya interoperabilitas sistemik antara kode pemrograman, norma hukum, dan dinamika pasar (Lessig, 2006).

Mengabaikan salah satu dari empat modalitas regulasi ini hanya akan menciptakan kebijakan yang pincang. Dalam banyak kasus di Indonesia, regulasi cenderung mengandalkan pendekatan represif tanpa menyentuh dimensi preventif dan edukatif, apalagi memodifikasi arsitektur sistem digitalnya. Oleh karena itu, tinjauan teoretis ini menjadi fondasi penting dalam merumuskan cetak biru tata kelola AI nasional yang ideal.

C. ANALISIS UTAMA

Analisis utama mengidentifikasi setidaknya tiga ranah krusial yang mencerminkan kesenjangan dan kebutuhan mendesak akan rekonstruksi hukum siber di Indonesia, khususnya dalam tata kelola AI: (1) fragmentasi dan ketidakpastian hukum akibat pengaturan yang tersedak; (2) ancaman sistemik terhadap keamanan nasional; serta (3) dilema tanggung jawab hukum atas output AI. Pembahasan ini akan merujuk pada hukum positif, perbandingan global, dan data empirik.

1. Fragmentasi Regulasi: Tidak Ada Definisi, Tidak Ada Kepastian

Problem mendasar tata kelola AI di Indonesia adalah ketiadaan definisi hukum yang spesifik. UU

ITE hanya mengenal istilah "Agen Elektronik" yang didefinisikan sebagai "perangkat dari suatu Sistem Elektronik yang dibuat untuk mewujudkan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis". Definisi ini jelas tidak cukup untuk merespons karakteristik AI modern yang otonom, adaptif, dan mampu menghasilkan konten atau keputusan baru tanpa campur tangan manusia.

Akibatnya, terjadi fragmentasi pengaturan yang sangat sektoral. Di sektor keuangan, Otoritas Jasa Keuangan bersama Asosiasi Fintech Indonesia (AFTECH) menerbitkan kode etik penggunaan AI dalam industri fintech pada 2023. Di bidang politik, Mahkamah Konstitusi melarang penggunaan AI untuk manipulasi foto atau gambar kandidat pemilu sebagai kampanye politik pada awal 2025. Namun, langkah-langkah ini bersifat *ad-hoc* dan reaktif, bukan merupakan bagian dari kebijakan nasional yang koheren. Tidak ada satu pun ketentuan yang mewajibkan transparansi algoritma, mekanisme audit, atau pengawasan manusia (*human oversight*) secara umum.

Keadaan ini dikritik tajam oleh para akademisi. Seorang mahasiswa magister hukum Universitas Indonesia dalam tesisnya menyoroti bahwa "instrumen tersebut tidak dirancang untuk merespons karakteristik AI yang otonom, adaptif, dan berbasis pengambilan keputusan otomatis". Lebih lanjut, ia menekankan bahwa tanpa regulasi

khusus, masyarakat tidak memiliki mekanisme hukum yang jelas untuk meminta pertanggungjawaban atau pemulihan hak apabila dirugikan oleh sistem AI. Ketidadaan standar transparansi ini menjadikan subjek data sebagai pihak yang paling rentan dalam ekosistem digital.

2. Ancaman terhadap Keamanan Nasional: Dari *Deepfake* hingga Pengawasan Massal

Kekosongan regulasi yang lebih komprehensif membuka pintu bagi ancaman keamanan nasional yang nyata. Beberapa di antaranya meliputi:

- **Deepfake dan Disinformasi Politik:** Tim Siber Bareskrim Polri telah mengungkap sejumlah kasus penyalahgunaan AI yang mencolok, salah satunya adalah penyebaran data palsu seolah-olah Menteri Keuangan (waktu itu) menjanjikan hadiah kepada masyarakat. Ini menunjukkan bahwa teknologi *deepfake* telah digunakan untuk menciptakan disinformasi yang dapat merusak reputasi, stabilitas politik, dan kepercayaan publik terhadap institusi negara. Kerangka hukum untuk menanganinya masih sangat dasar, mengandalkan UU ITE dan UU Pornografi yang tidak secara spesifik mendefinisikan dan mengkriminalisasi *deepfake*.

- **Pengawasan Massal dan Diskriminasi Algoritmik:** Pemerintah telah mulai memanfaatkan AI untuk pengawasan publik, pengenalan wajah, dan pemrosesan data pribadi. Namun, tanpa

kerangka etik yang jelas, praktik ini berpotensi melanggar hak privasi dan rasa aman warga negara. Telah disoroti bahwa penggunaan AI di sektor-sektor ini belum disertai kewajiban transparansi algoritma, mekanisme audit, pengawasan manusia, serta pertanggungjawaban hukum yang jelas apabila terjadi pelanggaran.

· Senjata Otonom dan Serangan Siber: Meskipun belum terungkap secara luas, potensi penggunaan AI untuk mengembangkan senjata otonom atau melakukan serangan siber yang lebih canggih merupakan ancaman nyata. Polri mencatat bahwa pelaku *cyber crime* di Indonesia umumnya adalah warga negara asing, menandakan dimensi transnasional dari ancaman ini.

3. Problem Pertanggungjawaban Hukum: *Lex Specialis* yang Belum Ada

Salah satu perdebatan hukum paling fundamental adalah menyangkut pertanggungjawaban atas kerugian yang disebabkan oleh AI. Secara perdata, kerugian yang disebabkan oleh AI hanya dapat dimintai pertanggungjawaban kepada pemilik atau operatornya berdasarkan Pasal 1367 KUHPerdata, yang pada dasarnya adalah rezim tanggung jawab atas perbuatan orang lain (*vicarious liability*). Ini adalah solusi pragmatis, tetapi tidak memadai untuk menangani skenario di mana AI mengambil keputusan di luar kendali atau prediksi pembuatnya.

Secara pidana, perdebatannya lebih kompleks. Apakah AI dapat dipidana? Teori subjek hukum positif Indonesia hanya mengakui "orang" (*natuurlijke persoon*) dan "badan hukum" (*rechts persoon*) sebagai subjek hukum. AI bukanlah keduanya. Oleh karena itu, sebagian besar ahli hukum berpendapat bahwa pertanggungjawaban pidana harus dibebankan kepada pembuat atau operator AI sebagai manus domina (pelaku intelektual), dengan AI hanya dianggap sebagai alat (manus ministra). Namun, hal ini terlihat dari cara kerja tindakan yang dilakukan oleh AI, pertanggungjawaban pidana untuk AI tidak dapat disamakan dengan orang atau badan hukum. Ini menandakan adanya celah hukum (*legal gap*) yang mendesak untuk diisi dengan undang-undang khusus (*lex specialis*).

D. ANOMALI PENERAPAN PASAL KARET DAN DEFISIT REGULASI

Beberapa studi kasus berikut mengkristalkan urgensi regulasi AI yang spesifik:

Kebocoran Data dan Pengawasan Finansial.

Di sektor keuangan, Otoritas Jasa Keuangan bersama AFTECH telah mengeluarkan kode etik penggunaan AI dalam industri *fintech* pada 2023. Namun, langkah ini masih bersifat *self-regulatory* tanpa sanksi yang tegas. Tanpa pengawasan yang ketat, penggunaan AI untuk *profiling* dan skor kredit

berpotensi menimbulkan diskriminasi terhadap kelompok tertentu. Hal ini menunjukkan bahwa kode etik tanpa binding force bukanlah solusi yang cukup.

Manipulasi Politik di Era Digital.

Pada awal 2025, Mahkamah Konstitusi mengeluarkan putusan yang melarang penggunaan AI untuk foto atau gambar kandidat pemilihan umum (pemilu) sebagai kampanye politik. Putusan ini penting, tetapi sifatnya reaktif dan hanya berlaku untuk kontestasi elektoral. Ia tidak memberikan kerangka umum untuk melarang penggunaan AI dalam menciptakan disinformasi di luar konteks pemilu.

Deepfake Pornografi dan Kekerasan Seksual

Kasus *deepfake* yang paling meresahkan adalah penyalahgunaan untuk menciptakan konten pornografi non-konsensual. Seorang penulis kolom hukum beropini bahwa untuk *deepfake* pornografi non-konsensual, penerapan Pasal 5 UU TPKS sangat relevan sebagai bentuk kekerasan seksual berbasis elektronik. Namun, ketiadaan definisi *deepfake* dalam hukum positif membuat penegak hukum harus menggunakan ketentuan yang ada dengan interpretasi yang luas, yang berpotensi menimbulkan ketidakpastian.

E. CETAK BIRU TATA KELOLA AI NASIONAL YANG BERDAULAT

Dari perbandingan dengan kerangka hukum yang lebih maju, seperti *EU AI Act* yang menerapkan pendekatan berbasis risiko dengan klasifikasi ketat dan sanksi tegas bagi pelanggaran, terlihat jelas ketertinggalan Indonesia. Untuk mengejar ketertinggalan ini, solusi tidak cukup hanya dengan menerbitkan Peraturan Presiden (Perpres). Kedua Perpres yang tengah digodok, tentang Peta Jalan dan Etika AI, memang penting, tetapi keduanya tidak akan memuat sanksi dan lebih bersifat sebagai panduan moral dan operasional. Tanpa kekuatan memaksa, panduan etis ini hanya akan menjadi "macan kertas".

Oleh karena itu, cetak biru tata kelola AI nasional harus mencakup:

1. Pembentukan Undang-Undang Khusus tentang AI. DPR RI telah mendorong pembentukan undang-undang yang khusus mengatur AI. Undang-undang ini harus mengadopsi pendekatan berbasis risiko, mengklasifikasikan sistem AI (risiko tinggi, terbatas, minimal), dan menetapkan larangan tegas untuk praktik yang tidak dapat diterima seperti social scoring.
2. Harmonisasi Regulasi. Pemerintah perlu menciptakan harmonisasi dengan

menyesuaikan undang-undang agar Indonesia tidak tersandung masalah kepatuhan saat pelaku usaha nasional berekspansi ke pasar global.

3. Penguatan Kapasitas Forensik Digital. Pemerintah dapat membentuk *National Deepfake Detection Consortium* yang melibatkan Bareskrim, universitas teknik, dan lembaga keamanan siber untuk mengatasi keterbatasan jumlah analisis forensik digital.
4. Pembentukan Otoritas Pengawas Independen. Otoritas ini bertugas mengawasi kepatuhan, memberikan rekomendasi kebijakan, serta menerima dan menindaklanjuti keluhan masyarakat terkait dampak merugikan dari sistem AI.

F. KESIMPULAN

Era AI adalah keniscayaan yang menghadirkan peluang dan ancaman secara bersamaan. Indonesia masih dalam tahap awal merespons fenomena ini, dengan kerangka regulasi yang fragmentaris dan bertumpu pada instrumen hukum yang tidak lagi memadai. Belum adanya undang-undang khusus AI telah menciptakan ketidakpastian hukum dan menempatkan warga negara dalam posisi rentan terhadap potensi pelanggaran HAM dan ancaman keamanan nasional. Berdasarkan temuan di atas, pengaturan berbasis

risiko seperti yang diterapkan dalam *EU AI Act* menjadi model yang paling relevan untuk diadaptasi oleh Indonesia. Namun, adaptasi tersebut harus disertai dengan penguatan kapasitas kelembagaan, transparansi, dan perlindungan hak asasi digital yang kuat. Singularitas hukum siber di Indonesia bergantung pada keberanian untuk tidak sekadar merespons, tetapi mengantisipasi dan membentuk arah perkembangan teknologi itu sendiri. Dengan merekonstruksi pendekatan dari reaktif menuju proaktif dan berlapis, Indonesia dapat membangun ekosistem AI yang inovatif, aman, dan berlandaskan nilai-nilai keadilan.

REFERENSI:

- Asshiddiqie, J. (2021). *Hukum dan Teknologi: Pergulatan Konstitusi dalam Masyarakat Digital*. Rajawali Pers.
- Braithwaite, J. (2017). *Restorative Justice & Responsive Regulation*. Oxford University Press.
- Greenleaf, G. (2022). Asian Data Privacy Laws: Trade and Human Rights Perspectives. *International Data Privacy Law*, 12(3), 189–210. <https://doi.org/10.1093/idpl/ipac008>
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

- Mahfud MD, M. (2022). Negara Hukum dan Demokrasi Pasca Reformasi. Gramedia Pustaka Utama.
- Marpaung, E. M., & Rumapea, E. (2024). Etika dan Pertanggungjawaban Penggunaan Artificial Intelligence di Indonesia. *Jurnal Hukum Lex Generalis*, 5(10), 1–18.
- Negara, P. M. (2026). Urgensitas Pembentukan Undang-Undang Kecerdasan Buatan dalam Menghadapi Ancaman Keamanan Nasional melalui Perspektif HAM dan Good Governance [Tesis Magister Hukum, Fakultas Hukum Universitas Indonesia].
- Oh, P. P. (2026). Risiko Sosial-Etika Mengintai, Regulasi AI Indonesia Masih Tambal Sulam. *Hukumonline.com*.
<https://www.hukumonline.com/berita/a/risiko-sosial-etika-mengintai--regulasi-ai-indonesia-masih-tambal-sulam-lt68dba03af1c9d/>
- Rahardjo, S. (2023). Smart Contract dan Masa Depan Online Dispute Resolution di Indonesia. *Jurnal Hukum dan Peradilan*, 12(1), 33–54.
<https://doi.org/10.25216/jhp.12.1.2023.33-54>
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843)

sebagaimana diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Tahun 2022 Nomor 196, Tambahan Lembaran Negara Nomor 6820).

'ADALAH

Buletin Hukum & Keadilan

Blockchain dan Cryptocurrency: Tantangan Regulasi dan Kepastian Hukum dalam Arsitektur Keuangan Digital Indonesia

Gilang Rizki Aji Putra*, Sri Ajeng Murni Cahyani Putri S*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

Universitas Dharma Indonesia



[10.15408/adalah.v9i7.51878](https://doi.org/10.15408/adalah.v9i7.51878)

Abstract:

Blockchain and cryptocurrency have disrupted global financial systems through decentralized and transparent transactions. In Indonesia, however, these technologies face regulatory challenges rooted in conventional legal frameworks. This article analyzes Indonesia's regulatory landscape on blockchain and cryptocurrency, identifies key issues, and proposes reform directions. Using normative legal research with statutory and comparative approaches, the study finds three main problems: unclear dual legal status of cryptocurrency as commodity and financial asset, weak mechanisms for seizure and enforcement of digital assets, and tension between regulation and the borderless nature of blockchain. Despite reforms under the P2SK Law and OJK supervision, significant legal gaps remain. The article concludes that comprehensive digital asset legislation is urgently needed.

Keywords: Blockchain, Cryptocurrency, Legal Certainty, Digital Assets, Regulation.

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

* Kepala LPM (Lembaga Penjamin Mutu), Universitas Dharma Indonesia (UNDHI) Tangerang. Email: sriajengmurni.cahyaniputri@undhi.ac.id.

A. PENDAHULUAN

Kelahiran Bitcoin pada tahun 2009 oleh entitas anonim bernama Satoshi Nakamoto menandai awal dari revolusi yang fundamental dalam cara manusia memahami uang, nilai, dan transaksi. Teknologi blockchain yang mendasarinya memperkenalkan paradigma desentralisasi radikal: sebuah buku besar digital terdistribusi yang memungkinkan transaksi dilakukan secara *peer-to-peer* tanpa memerlukan otoritas sentral seperti bank atau pemerintah. Janji yang dibawa adalah kebebasan finansial, transparansi, dan efisiensi yang melampaui batas-batas geografis. Namun, seperti setiap revolusi, janji tersebut datang bersama dengan risiko dan konsekuensi sistemik yang tidak terduga.

Dalam waktu kurang dari dua dekade, *cryptocurrency* telah berevolusi dari eksperimen teknologi pinggiran menjadi fenomena ekonomi global dengan kapitalisasi pasar yang mencapai triliunan dolar AS. Indonesia, sebagai negara dengan populasi digital terbesar di Asia Tenggara, tidak luput dari gelombang ini. Jumlah investor kripto di Indonesia melampaui 20 juta orang pada akhir tahun 2024, melampaui jumlah investor pasar modal tradisional. Namun, pertumbuhan yang eksplosif ini tidak disertai oleh kesiapan kerangka regulasi yang memadai. Selama bertahun-tahun, *cryptocurrency* di Indonesia berada dalam wilayah abu-abu hukum: tidak sepenuhnya dilarang, tetapi juga tidak sepenuhnya dilegitimasi.

Persoalannya bertumpu pada karakteristik fundamental *cryptocurrency* yang paradoksal. Di satu sisi, *cryptocurrency* dirancang untuk tidak memerlukan negara, bank sentral, atau otoritas pengatur mana pun. Nilai dan keabsahan transaksinya diverifikasi oleh algoritma konsensus, bukan oleh institusi hukum. Di sisi lain, setiap negara, termasuk Indonesia, dibangun di atas fondasi kedaulatan moneter yang mensyaratkan kontrol atas mata uang dan sistem pembayaran. Ketika kedua logika ini bertabrakan, yang terjadi adalah benturan epistemologis: bagaimana negara mengatur sesuatu yang pada dasarnya dirancang untuk tidak dapat diatur? Bagaimana hukum yang bertumpu pada batas-batas yurisdiksi teritorial mengklaim otoritas atas aset yang eksistensinya murni digital dan lokasinya tidak dapat ditentukan secara fisik? Rumusan masalah artikel ini adalah: Pertama, bagaimana status hukum dan rezim regulasi *cryptocurrency* di Indonesia saat ini? Kedua, apa kendala fundamental yang menghambat terwujudnya kepastian hukum? Ketiga, bagaimana kerangka regulasi ideal yang dapat menyeimbangkan inovasi, perlindungan konsumen, dan stabilitas keuangan? Tujuannya adalah untuk menganalisis secara kritis kesenjangan antara realitas perkembangan *blockchain* dan *cryptocurrency* dengan kerangka hukum positif Indonesia, serta merumuskan arah reformasi yang diperlukan.

B. TEKNOLOGI, HUKUM, DAN PARADOKS DESENTRALISASI

Untuk memahami tantangan regulasi *cryptocurrency*, diperlukan pemahaman tentang karakteristik teknologinya yang secara fundamental menantang arsitektur hukum modern. *Blockchain* adalah teknologi buku besar terdistribusi (*distributed ledger technology*/DLT) yang mencatat setiap transaksi dalam blok-blok data yang saling terhubung secara kriptografis, didistribusikan ke ribuan node di seluruh dunia, dan tidak dapat diubah (*immutable*) tanpa konsensus mayoritas jaringan. *Cryptocurrency*, sebagai aplikasi paling populer dari *blockchain*, adalah representasi nilai digital yang dimungkinkan oleh teknologi ini.

Tiga karakteristik inti *cryptocurrency* menciptakan problem regulasi yang unik. Pertama, desentralisasi. Tidak ada otoritas sentral yang mengendalikan jaringan *Bitcoin* atau *Ethereum*; tidak ada kantor pusat yang dapat dipanggil oleh regulator; tidak ada CEO yang dapat dimintai pertanggungjawaban. Ini menimbulkan persoalan fundamental: kepada siapa negara mengarahkan perintah regulasinya? Kedua, anonimitas semu (*pseudonymity*). Transaksi dicatat dengan alamat kriptografis, bukan nama asli, sehingga identitas para pihak dapat tersembunyi. Hal ini membuka celah bagi penyalahgunaan untuk pencucian uang, pendanaan terorisme, dan kejahatan lainnya, sekaligus menyulitkan aparat penegak hukum

(Kusumawardhani, 2025). Ketiga, *irreversibilitas* dan *self-custody*. Transaksi yang telah divalidasi oleh jaringan tidak dapat dibatalkan. Aset disimpan dalam dompet digital yang hanya dapat diakses dengan kunci privat (*private key*). Jika kunci hilang atau dicuri, tidak ada otoritas yang dapat memulihkannya sebuah karakteristik yang bertentangan dengan logika perlindungan konsumen konvensional.

Dalam perspektif hukum, tantangan-tantangan ini dapat dipetakan ke dalam kerangka teori "pacing problem" yang dikemukakan oleh Marchant (2011), di mana hukum selalu tertinggal di belakang teknologi. *Cryptocurrency* berkembang dalam hitungan bulan, sementara undang-undang membutuhkan waktu bertahun-tahun untuk disusun dan disahkan. Lebih dari itu, teori regulasi responsif menekankan bahwa pendekatan *command-and-control* yang kaku tidak cocok untuk ekosistem digital yang dinamis; yang diperlukan adalah regulasi berbasis prinsip (*principle-based regulation*) yang adaptif dan kolaboratif antara regulator, industri, dan masyarakat sipil. Di sisi lain, konsep kepastian hukum dalam tradisi *rechtsstaat* mensyaratkan adanya aturan yang jelas, dapat diakses, dan dapat diprediksi. Tanpa kepastian hukum, investasi akan terhambat, hak-hak warga negara tidak terlindungi, dan sistem hukum kehilangan legitimasinya. Inilah ketegangan sentral yang akan dianalisis dalam pembahasan berikut.

C. TANTANGAN REGULASI DAN KEPASTIAN HUKUM CRYPTOCURRENCY DI INDONESIA

1. Dualisme Status Hukum: Antara Komoditas, Instrumen Keuangan, dan Larangan Alat Pembayaran

Tantangan pertama dan paling fundamental adalah ketidakjelasan status hukum *cryptocurrency*. Berbeda dengan mata uang fiat yang memiliki definisi dan kerangka hukum yang jelas, *cryptocurrency* di Indonesia telah mengalami evolusi klasifikasi yang mencerminkan kebingungan regulator sendiri dalam memahami esensinya. Pada tahap awal, Bank Indonesia melalui Peraturan Bank Indonesia Nomor 18/40/PBI/2016 dan berbagai siaran pers secara tegas melarang penggunaan *cryptocurrency* termasuk *Bitcoin* sebagai alat pembayaran. Dasarnya adalah Undang-Undang Nomor 7 Tahun 2011 tentang Mata Uang yang menyatakan bahwa rupiah adalah satu-satunya alat pembayaran yang sah di wilayah NKRI. Bank Indonesia konsisten mempertahankan posisi ini dengan peringatan keras kepada semua pihak: virtual currency bukanlah alat pembayaran yang sah. Pelanggaran terhadap ketentuan ini dapat dikenai sanksi pidana berdasarkan undang-undang tersebut.

Namun, melarang penggunaan *cryptocurrency* sebagai alat pembayaran tidak menjawab pertanyaan tentang status hukumnya secara keseluruhan. Di

sinilah muncul dualisme. Melalui Surat Menteri Koordinator Perekonomian Nomor S-302/M.EKON/09/2018 dan Peraturan Menteri Perdagangan Nomor 99 Tahun 2018, pemerintah mengambil pendekatan pragmatis dengan mengakui *cryptocurrency* sebagai "komoditas" yang dapat diperdagangkan di bursa berjangka di bawah pengawasan Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti). Bappebti kemudian menerbitkan Peraturan Bappebti Nomor 2 Tahun 2019 yang menetapkan daftar aset kripto yang dapat diperdagangkan di pasar fisik aset kripto. Dengan demikian, terciptalah dualisme yang membingungkan: *cryptocurrency* dilarang sebagai alat pembayaran oleh Bank Indonesia, tetapi diizinkan sebagai komoditas investasi oleh Bappebti.

Dualisme ini semakin kompleks dengan berlakunya Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Pasal 213 UU P2SK mengamanatkan peralihan pengaturan dan pengawasan aset keuangan digital, termasuk aset kripto, dari Bappebti ke Otoritas Jasa Keuangan (OJK) dan Bank Indonesia. Ini adalah pengakuan legislatif pertama bahwa *cryptocurrency* bukan sekadar komoditas, melainkan bagian dari sektor keuangan. Peralihan ini mulai dilaksanakan secara bertahap sejak 10 Januari 2025 melalui Nota Kesepahaman antara OJK dan Bappebti, dan secara resmi tuntas pada 20 Januari 2026 dengan

penandatanganan Berita Acara Pengakhiran Nota Kesepahaman. Kepala Eksekutif Pengawas Inovasi Teknologi Sektor Keuangan, Aset Keuangan Digital, dan Aset Kripto OJK Hasan Fawzi menyatakan bahwa "satu tahun perjalanan tim ini mewarnai bagaimana peralihan itu dapat kita lakukan dengan baik dan lancar." Di bawah rezim OJK, aset kripto dikategorikan sebagai aset keuangan yang dipersamakan dengan surat berharga. POJK Nomor 27 Tahun 2024 tentang Penyelenggaraan Perdagangan Aset Keuangan Digital termasuk Aset Kripto, yang kemudian diubah dengan POJK Nomor 23 Tahun 2025, menjadi kerangka hukum utama. Konsekuensi dari perubahan status ini signifikan: aset kripto tidak lagi dikenakan Pajak Pertambahan Nilai (PPN) karena transaksi aset kripto diperlakukan setara dengan transaksi surat berharga lainnya.

Meskipun demikian, perubahan ini belum menyelesaikan persoalan fundamental. Cryptocurrency yang dirancang untuk menjadi "uang" masih belum diakui sebagai alat pembayaran yang sah. Statusnya sebagai "komoditas" di bawah Bappebti kini bergeser menjadi "aset keuangan" di bawah OJK, tetapi hakikat yuridisnya tetap ambivalen: apakah ia benda? Apakah ia surat berharga? Apakah ia dapat dijadikan objek jaminan? Dualisme regulasi ini terus membayangi dan menciptakan ketidakpastian bagi pelaku industri, investor, dan aparat penegak hukum.

2. Pajak *Cryptocurrency*: Dari Komoditas ke Instrumen Keuangan

Perubahan status *cryptocurrency* dari komoditas menjadi instrumen keuangan membawa implikasi langsung pada rezim perpajakannya. Di bawah rezim lama, Peraturan Menteri Keuangan Nomor 68/PMK.03/2022 (PMK 68/2022) memperlakukan aset kripto sebagai komoditas tidak berwujud yang dikenakan PPN atas penyerahannya dan PPh Pasal 22 Final atas penghasilan dari perdagangannya. Pedagang fisik aset kripto dikenakan tarif PPh 0,1% untuk transaksi melalui exchange terdaftar dan 0,2% untuk transaksi di luar exchange terdaftar, ditambah PPN sebesar 1% atau 2% tergantung jenis penyelenggara.

Paradigma ini berubah secara fundamental dengan berlakunya PMK Nomor 50 Tahun 2025 pada 1 Agustus 2025. PMK 50/2025 mendefinisikan ulang aset kripto sebagai representasi digital dari nilai yang dapat disimpan dan ditransfer secara elektronik menggunakan teknologi buku besar terdistribusi seperti *blockchain*. PMK 50 memperkenalkan pergeseran paradigma yang signifikan: transaksi perdagangan aset kripto tidak lagi dikenakan PPN karena penyetaraannya dengan surat berharga, sementara tarif PPh 22 Final disesuaikan menjadi 0,21% untuk transaksi melalui PPMSE dalam negeri dan 1% untuk transaksi melalui PPMSE luar negeri. Bagi penambang (miner) kripto, mulai tahun fiskal 2026 tidak lagi dikenai PPh

22 final, melainkan mengikuti ketentuan tarif umum PPh badan atau pribadi.

Staf Ahli Menteri Keuangan Bidang Kepatuhan Pajak Yon Aarsal menjelaskan bahwa "kalau sebelumnya kripto dikenai dua jenis pajak, PPh dan PPN karena dianggap komoditas di bawah Bappebti, sekarang aset digital disetarakan dengan instrumen keuangan lain sehingga administrasi perpajakannya berbeda." Perubahan ini memberikan kejelasan yang lebih baik bagi investor dan pelaku industri, mengurangi beban pajak ganda, dan menyelaraskan rezim pajak dengan rezim pengawasan OJK. Namun, kritik tetap muncul. Albert Richi Aruan dalam disertasinya menekankan bahwa pemajakan atas *cryptocurrency* yang selama ini hanya mengandalkan peraturan menteri dan regulasi teknis belum memenuhi asas legalitas pajak. "Kita tidak bisa menetapkan pajak pada objek baru seperti *cryptocurrency* hanya melalui peraturan menteri atau keputusan pemerintah. Harus ada payung hukum setingkat undang-undang," katanya. Hal ini menunjukkan bahwa meskipun telah ada kemajuan signifikan, fondasi legalitas pemajakan *cryptocurrency* masih memerlukan penguatan di tingkat undang-undang.

3. Problematika Yuridis: Eksekusi, Penyitaan, dan Objek Jaminan

Salah satu celah hukum paling serius yang masih terbuka lebar adalah ketiadaan mekanisme

hukum yang jelas untuk eksekusi, penyitaan, dan pengakuan aset kripto sebagai objek jaminan. *Cryptocurrency* memiliki karakteristik unik yang membedakannya dari aset konvensional: ia tidak berwujud, tidak memiliki domisili fisik, dan hanya dapat diakses melalui kunci privat yang dikuasai oleh pemiliknya. KUHPerdara Indonesia, melalui Pasal 499, mendefinisikan benda sebagai "segala sesuatu yang dapat dikuasai dan memiliki nilai ekonomi." Aset kripto memenuhi kriteria tersebut, tetapi belum secara eksplisit diakui sebagai benda dalam peraturan perundang-undangan.

Dalam perspektif KUHPerdara, aset kripto dapat dianalisis sebagai benda bergerak tidak berwujud. Namun, implikasinya dalam penegakan hukum sangat problematik. Sifat anonimitas, desentralisasi, dan ketergantungan pada kunci privat membuat eksekusi aset kripto baik dalam konteks sengketa perdata maupun penyitaan pidana menjadi sangat rumit. Sebuah studi dari Badan Penelitian dan Pengembangan Hukum Mahkamah Agung menyimpulkan bahwa "dalam perkembangannya, aset digital berbasis kripto sering dinilai lemah secara yuridis, terutama terkait kepastian hukum eksekusi putusan perdata saat terjadi sengketa kepemilikan. Hal ini disebabkan belum adanya mekanisme hukum dan otoritas yang berwenang menyita atau memindahkan aset kripto tanpa akses ke *private key*."

Kejaksaan Agung RI juga menyoroti persoalan ini. Plt Jaksa Agung Muda Pengawasan Raden Febrytriyanto, dalam sebuah *Focus Group Discussion*, menegaskan bahwa "penggunaan blockchain menghadirkan risiko, terutama dalam bentuk tindak pidana seperti penipuan, peretasan, pencucian uang, dan pendanaan terorisme. Sifat terdesentralisasi *cryptocurrency* juga diketahui menyulitkan aparat hukum melacak transaksi dan mengidentifikasi pemilik sebenarnya." Data terbaru menunjukkan bahwa lebih dari US\$14 miliar transaksi *cryptocurrency* pada tahun 2021 dikaitkan dengan tindak pidana, dan Indonesia menempati peringkat kedua di dunia dalam skema penipuan aset kripto pada tahun 2019, dengan 11% dari jumlah keseluruhan korban.

Di ranah perdata, persoalan serupa muncul ketika aset kripto dijadikan objek jaminan utang. Bagaimana bank atau kreditor dapat mengeksekusi agunan berupa *Bitcoin* jika debitur tidak menyerahkan kunci privatnya? Apakah lembaga jaminan gadai atau fidusia yang paling tepat? Penelitian terbaru menunjukkan bahwa lembaga gadai dinilai lebih tepat untuk aset kripto karena memenuhi prinsip *inbezitstelling* melalui pemindahan penguasaan kunci privat kepada pihak ketiga (kustodian). Menariknya, OJK telah membuka kemungkinan pemanfaatan aset kripto sebagai agunan pinjaman, yang menandakan adanya pergeseran paradigma yang progresif. Namun,

untuk mewujudkannya, diperlukan kerangka hukum yang lebih jelas tentang status kebendaan aset digital dan mekanisme eksekusinya.

4. Teknologi *Blockchain*, *Smart Contract*, dan Tantangan Hukum Perdata

Di luar cryptocurrency, teknologi blockchain sendiri menghadirkan tantangan regulasi yang tidak kalah pelik. *Smart contract*, yaitu kontrak yang ditulis dalam kode dan dieksekusi secara otomatis oleh jaringan blockchain ketika kondisi tertentu terpenuhi menjanjikan efisiensi tanpa preseden dalam transaksi komersial. Namun, dari perspektif hukum perdata Indonesia, *smart contract* menghadapi beberapa pertanyaan fundamental. Pertama, apakah kode pemrograman memenuhi syarat "kesepakatan para pihak" sebagaimana dimaksud dalam Pasal 1320 KUHPerdata? Kedua, bagaimana smart contract dapat memenuhi syarat formil sebagai alat bukti dalam penyelesaian sengketa? Ketiga, bagaimana menentukan yurisdiksi yang berwenang dan hukum yang berlaku jika smart contract dieksekusi secara otomatis di ribuan node yang tersebar di berbagai negara?

Penelitian-penelitian hukum terkini menunjukkan bahwa smart contract dapat diakui sebagai bentuk perjanjian yang sah dalam hukum perdata Indonesia sepanjang memenuhi syarat sah perjanjian berdasarkan Pasal 1320 KUHPerdata dan ketentuan dokumen elektronik dalam UU ITE.

Namun, kepastian hukumnya masih lemah karena belum ada undang-undang atau peraturan khusus yang secara eksplisit mengakui dan mengatur smart contract. Ketiadaan pengakuan legislatif ini menciptakan risiko hukum yang signifikan bagi para pihak yang menggunakan smart contract dalam transaksi bisnis. Lebih jauh, penggunaan *big data* dalam smart contract juga menimbulkan pertanyaan tentang tanggung jawab hukum jika data yang digunakan ternyata rusak atau palsu dan menyebabkan kerugian, yang menurut Pasal 1365 KUHPerdara dapat dikenakan tanggung jawab perdata kepada pengelola data.

DPR RI, dalam revisi UU P2SK yang tengah dibahas, berupaya memperkuat landasan hukum bagi pengawasan dan pengaturan aset keuangan digital, termasuk isu-isu terkait *blockchain*. Sejumlah pembahasan dalam revisi UU itu mencakup aspek perlindungan konsumen, pengawasan transaksi aset kripto, penguatan izin operasional lembaga jasa keuangan digital, serta koordinasi lintas lembaga antara otoritas moneter dan otoritas pengawas sektor keuangan. Namun, legislasi ini lebih berfokus pada aspek kelembagaan dan pengawasan, bukan pada kodifikasi hukum kebendaan digital yang menjadi akar persoalan.

D. POTRET NYATA PROBLEM REGULASI

Pencurian Listrik untuk Penambangan *Bitcoin*
Pengakuan Aktivitas Tanpa Regulasi

Pada April 2026, Majelis Hakim Pengadilan Negeri Medan menjatuhkan vonis penjara 5,5 tahun kepada dua terdakwa yang terbukti mencuri arus listrik untuk operasi penambangan (mining) *Bitcoin* di Kota Medan. Kasus ini menarik perhatian publik dan menjadi preseden penting dalam penanganan kasus terkait *cryptocurrency*. Ironisnya, dakwaan yang digunakan bukanlah tindak pidana terkait *cryptocurrency* atau *blockchain* secara spesifik, melainkan pencurian listrik berdasarkan Pasal 362 KUHP. Ini menunjukkan bahwa aktivitas penambangan kripto, yang secara *de facto* telah menjadi industri besar di Indonesia, belum memiliki kerangka regulasi yang spesifik. Penambang kripto beroperasi dalam ruang abu-abu: aktivitasnya tidak dilarang secara eksplisit, tetapi juga tidak diatur dengan jelas mengenai perizinan, standar operasional, atau kewajiban pelaporan. Dari perspektif hukum pidana, ketiadaan kerangka ini mempersulit penegakan hukum dan berpotensi menimbulkan ketidakadilan, karena aparat harus menggunakan pasal-pasal konvensional yang tidak dirancang untuk menangani realitas pertambangan digital.

Eksekusi Aset Kripto dalam Perkara Pidana Putusan PN Jakarta Timur

Putusan Pengadilan Negeri Jakarta Timur Nomor 670/Pid.Sus/2024/PN JKT.TIM memberikan contoh bagaimana aparat penegak hukum berupaya menangani aset kripto dalam konteks pidana.

Terdakwa Farihin Ardhiansyah terbukti bersalah melakukan tindak pidana pemindahan informasi elektronik tanpa hak dan merugikan orang lain. Dalam amar putusan, hakim memerintahkan agar aset kripto milik terdakwa sebesar 79,167 USDT di akun Indodax dikembalikan kepada saksi korban. Ini adalah langkah maju yang signifikan, karena pengadilan memberikan pengakuan *de facto* terhadap keberadaan dan kepemilikan aset kripto sebagai objek yang dapat direstitusi. Namun, putusan ini juga menunjukkan ketergantungan pada keberadaan *exchange* terdaftar sebagai kustodian *de facto*. Bagaimana jika aset kripto tersebut tidak disimpan di *exchange* terdaftar, melainkan di cold wallet milik pribadi terdakwa yang hanya dapat diakses dengan kunci privat yang tidak diketahui? Di sinilah keterbatasan kerangka hukum yang ada menjadi nyata. Keberhasilan eksekusi sangat bergantung pada variabel yang tidak selalu ada *exchange* yang kooperatif, akses ke akun, dan aset yang masih berada dalam kendali pihak ketiga.

Penipuan Berkedok Investasi *Bitcoin* Dakwaan Konvensional untuk Kejahatan Digital

Penelitian terhadap Putusan Nomor 129/Pid.B/2021/PN KPG mengungkap penipuan investasi *Bitcoin* yang meresahkan masyarakat. Terdakwa dijerat dengan pasal-pasal penipuan konvensional dalam KUHP, bukan dengan ketentuan spesifik terkait *cryptocurrency*. Ini menunjukkan pola yang konsisten: aparat penegak

hukum menggunakan pasal-pasal konvensional untuk menangani kejahatan berbasis *cryptocurrency* karena ketiadaan *lex specialis*. Meskipun hal ini memungkinkan penindakan, pendekatan konvensional semacam ini memiliki kelemahan mendasar. Pertama, ia tidak dirancang untuk menangkap karakteristik unik *cryptocurrency*, seperti anonimitas dan desentralisasi, yang seringkali menjadi elemen kunci dalam kejahatan. Kedua, ia tidak memberikan pedoman yang jelas bagi penyidik, jaksa, dan hakim dalam menangani bukti digital, melacak aliran dana kripto, dan menentukan yurisdiksi. Ketiga, ia tidak memberikan perlindungan yang memadai bagi korban yang aset kriptonya hilang atau dicuri.

E. MENUJU KERANGKA HUKUM ASET DIGITAL YANG HOLISTIK

Berdasarkan analisis di atas, arah reformasi regulasi *blockchain* dan *cryptocurrency* di Indonesia harus bersifat holistik, menyentuh dimensi kelembagaan, hukum substantif, dan kapasitas penegakan hukum. Pertama, Indonesia memerlukan undang-undang khusus tentang aset digital. Undang-undang ini harus mengkodifikasi status hukum aset digital, termasuk *cryptocurrency*, token, dan NFT, sebagai objek hukum kebendaan yang memiliki nilai ekonomi dan dapat dialihkan, dijamin, serta dieksekusi. Undang-undang ini harus memberikan definisi hukum yang jelas, mengatur mekanisme pengalihan dan pewarisan,

menetapkan prosedur penyitaan dan eksekusi, serta mengakui validitas *smart contract* dalam batas-batas tertentu. Plt JAM Pengawasan Kejagung menyarankan Indonesia perlu belajar dari negara-negara seperti *Liechtenstein* yang telah mengesahkan *Blockchain Act* untuk mengoptimalkan manfaat teknologi ini sekaligus memitigasi risikonya.

Kedua, harmonisasi regulasi anti-pencucian uang (AML) dan pencegahan pendanaan terorisme (CFT) berbasis risiko. POJK Nomor 27 Tahun 2024 telah mewajibkan standar pengenalan nasabah (KYC) serta anti-pencucian uang secara ketat bagi pedagang aset keuangan digital. Namun, tantangan terbesar adalah penggunaan layanan "mixing" atau "tumbling" yang dirancang untuk mengacak transaksi agar tidak terlacak. Regulasi harus memberikan panduan yang jelas tentang bagaimana exchange dan penyedia dompet digital harus menangani transaksi yang mencurigakan, termasuk kewajiban pelaporan ke PPATK dan mekanisme pembekuan aset yang dicurigai terkait kejahatan.

Ketiga, pengembangan pedoman teknis terpadu lintas lembaga. Saat ini, pengawasan aset kripto tersebar di antara OJK (pengaturan dan pengawasan perdagangan), Bank Indonesia (larangan alat pembayaran), PPATK (pencucian uang), dan Kementerian Perdagangan (sisa-sisa kewenangan Bappebti). Fragmentasi ini harus diakhiri dengan menyusun pedoman teknis bersama yang mengatur secara rinci prosedur penyitaan aset

kripto, mekanisme permintaan data dari exchange, dan standar forensik digital untuk pelacakan transaksi *blockchain*. Kejaksaan Agung telah merekomendasikan pentingnya membentuk regulasi yang memastikan transparansi, pengelolaan risiko, dan kepatuhan terhadap standar AML serta CFT, serta mendorong koordinasi lintas sektor untuk menghadapi tantangan sifat *blockchain* yang transnasional dan terdesentralisasi.

Keempat, perlunya pembangunan kapasitas penegak hukum secara masif. Laboratorium forensik *blockchain* nasional perlu dibentuk di bawah koordinasi BSSN, Polri, dan Kejaksaan, dengan peralatan analisis *blockchain* (seperti *Chainalysis* atau *CipherTrace*) dan sumber daya manusia yang tersertifikasi. Pelatihan berkelanjutan bagi penyidik, jaksa, dan hakim tentang investigasi cryptocurrency, analisis alamat dompet, dan penanganan bukti digital *blockchain* menjadi krusial. Tanpa kapasitas teknis yang memadai, kerangka hukum yang paling baik pun tidak akan efektif.

Kelima, pengaturan tentang smart contract dan tokenisasi aset. OJK telah membuka peluang pemanfaatan kripto untuk tokenisasi dan agunan. Ini merupakan langkah yang sangat progresif, tetapi harus diikuti dengan kerangka regulasi yang jelas tentang bagaimana *smart contract* diakui secara hukum, bagaimana hak dan kewajiban para pihak didefinisikan, dan bagaimana penyelesaian sengketa dilakukan. Pengadilan perlu mempersiapkan diri

untuk menangani sengketa yang melibatkan *smart contract*, termasuk dengan mengembangkan pedoman yurisprudensi tentang interpretasi kode sebagai kontrak. Dalam konteks yang lebih luas, Indonesia juga perlu terlibat dalam harmonisasi regulasi di tingkat ASEAN dan global untuk menghadapi karakter transnasional dari teknologi *blockchain*.

F. KESIMPULAN

Blockchain dan *cryptocurrency* menghadirkan tantangan regulasi yang bersifat paradigmatik bagi Indonesia. Status hukum *cryptocurrency* yang mengalami evolusi dari komoditas di bawah Bappebti menjadi aset keuangan di bawah OJK, sementara tetap dilarang sebagai alat pembayaran, mencerminkan kebingungan fundamental dalam memahami hakikat yuridis dari teknologi ini. Meskipun telah terjadi kemajuan melalui pengalihan pengawasan berdasarkan UU P2SK, harmonisasi perpajakan melalui PMK 50/2025, dan pengakuan yudisial terhadap aset kripto sebagai objek restitusi, masih terdapat kekosongan hukum yang serius. Ketiadaan mekanisme penyitaan dan eksekusi yang jelas, absennya pengakuan legislatif terhadap *smart contract*, serta keterbatasan rezim AML/CFT dalam menghadapi karakter anonim dan terdesentralisasi dari *cryptocurrency* adalah persoalan-persoalan yang memerlukan respons legislasi yang komprehensif, bukan sekadar tambal sulam.

Menjawab rumusan masalah, kerangka regulasi Indonesia saat ini masih berada dalam masa transisi yang belum tuntas. Dualisme pengawasan, fragmentasi kelembagaan, dan ketiadaan undang-undang khusus tentang aset digital menciptakan ketidakpastian hukum yang merugikan investor, menghambat penegakan hukum, dan membuka celah bagi pelaku kejahatan. Kerangka ideal yang diperlukan adalah undang-undang aset digital yang komprehensif, yang mengakui status kebendaan *cryptocurrency*, mengatur mekanisme penyitaan dan eksekusi, melegitimasi smart contract dalam batas-batas tertentu, serta menyelaraskan rezim anti-pencucian uang dengan karakteristik unik teknologi blockchain.

Rekomendasi yang diajukan adalah: pertama, percepatan legislasi undang-undang kebendaan digital; kedua, harmonisasi regulasi AML/CFT berbasis risiko dan penyusunan pedoman teknis terpadu lintas lembaga; ketiga, pembentukan laboratorium forensik blockchain nasional dan pelatihan berkelanjutan bagi aparat penegak hukum; keempat, pengembangan kerangka hukum untuk smart contract dan tokenisasi; dan kelima, keterlibatan aktif dalam harmonisasi regulasi di tingkat ASEAN dan global. Hanya dengan fondasi regulasi yang kokoh, Indonesia dapat menempatkan diri sebagai pemain yang berdaulat dalam revolusi keuangan digital, bukan sekadar penonton yang cemas di pinggir lapangan.

REFERENSI:

- Aruan, A. R. (2025). Pemajakan Cryptocurrency dalam Perspektif Asas Legalitas Pajak di Indonesia [Disertasi Doktor, Universitas Pelita Harapan].
- Badan Pengawas Perdagangan Berjangka Komoditi. (2019). Peraturan Bappebti Nomor 2 Tahun 2019 tentang Penyelenggaraan Pasar Fisik Komoditi di Bursa Berjangka.
- Hukumonline. (2025, Agustus 6). OJK Finalisasi Aturan Pengawasan Pasar Kripto dari Bappebti. Hukumonline.com.
- Kejaksaan Agung RI. (2024, November 18). Kejangung Nilai Perlu Regulasi Blockchain Lebih Komprehensif Agar Aman dan Efektif dalam Penegakan Hukum. [Story.Kejaksaan.go.id](https://www.kejaksaan.go.id/story/kejaksaan-go-id).
- Kementerian Keuangan RI. (2025). Peraturan Menteri Keuangan Nomor 50 Tahun 2025 tentang Pajak Pertambahan Nilai dan Pajak Penghasilan atas Transaksi Perdagangan Aset Kripto.
- Kusumawardhani, A. (2025). Anonimitas dan Tantangan Penegakan Hukum dalam Ekosistem Cryptocurrency. Jurnal Hukum Siber, 7(1), 15–32.

- Marchant, G. E. (2011). The Growing Gap Between Emerging Technologies and the Law. The International Library of Ethics, Law and Technology, 7, 19–33.
- Murdian. (2025, Desember 15). Tinjauan Yuridis atas Hambatan Eksekusi Aset Kripto sebagai Benda Bergerak Tak Berwujud di Era Digital. Siganisbadilum Mahkamah Agung RI.
- Otoritas Jasa Keuangan. (2024). Peraturan OJK Nomor 27 Tahun 2024 tentang Penyelenggaraan Perdagangan Aset Keuangan Digital Termasuk Aset Kripto.
- Otoritas Jasa Keuangan. (2025, Juli 31). Siaran Pers: OJK dan Bappebti Tuntaskan Peralihan Pengawasan Aset Keuangan Digital. OJK.go.id.
- Putusan Pengadilan Negeri Jakarta Timur Nomor 670/Pid.Sus/2024/PN JKT.TIM.
- Republik Indonesia. (2023). Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Lembaran Negara Tahun 2023 Nomor 4).
- Republik Indonesia. (2025). Peraturan Pemerintah Nomor 28 Tahun 2025 tentang Perizinan Berusaha Berbasis Risiko.

SSEK Law Firm. (2026, April 12). Indonesia Reshapes
Crypto and Financial Derivatives Regulation.
The Legal Industry Reviews Malaysia.