

**PERTANGGUNGJAWABAN PIDANA ATAS KEJAHATAN
MANIPULASI ALGORITMA PADA PLATFORM TIKTOK
DALAM PERSPEKTIF HUKUM PIDANA INDONESIA**



Oleh :

MUH. IKSAN NUR KHALISH

040 2022 0376

SKRIPSI

Diajukan sebagai Tugas Akhir dalam rangka Penyelesaian Studi
Pada Program Studi Ilmu Hukum

**FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2026**

HALAMAN JUDUL

**PERTANGGUNGJAWABAN PIDANA ATAS KEJAHATAN
MANIPULASI ALGORITMA PADA PLATFORM TIKTOK
DALAM PERSPEKTIF HUKUM PIDANA INDONESIA**

SKRIPSI

**Skripsi ini diajukan untuk memenuhi salah satu persyaratan guna
memperoleh gelar Sarjana Hukum pada Fakultas Hukum Program Studi
Ilmu Hukum di Universitas Muslim Indonesia**

Oleh :

**MUH. IKSAN NUR KHALISH
040 2022 0376**

**FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2026**

PERSETUJUAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa:

Nama mahasiswa : Muh. Iksan Nur Khalish

NIM : 04020220376

Bagian : Hukum Pidana

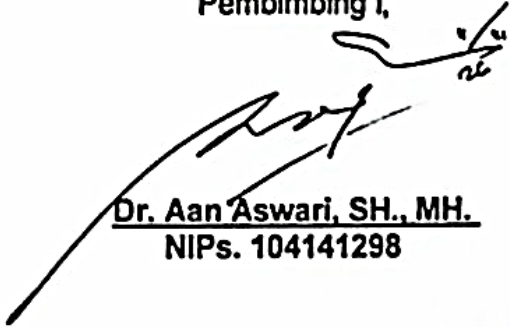
Judul Skripsi : Pertanggungjawaban Pidana Atas Kejahatan
Manipulasi Algoritma Pada Platform TikTok
Dalam Perspektif Hukum Pidana Indonesia

Dasar Penetapan : SK Nomor : 0260/H.05/FH-UMIX/2025

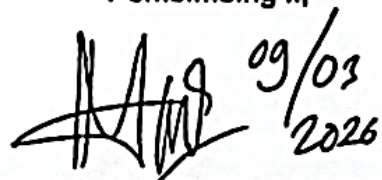
Telah diperiksa dan disetujui untuk diajukan dalam Ujian Skripsi.

Makassar,2026

Pembimbing I,


Dr. Aan Aswari, SH., MH.
NIPs. 104141298

Pembimbing II,


Dr. H. Mursyid M, SH.,MH.
NIPs. 104141299

Mengetahui,
Ketua Bagian Hukum Pidana


Dr. H. Azwad Rachmat Hambali, SH.,MH.
NIPs. 104101114

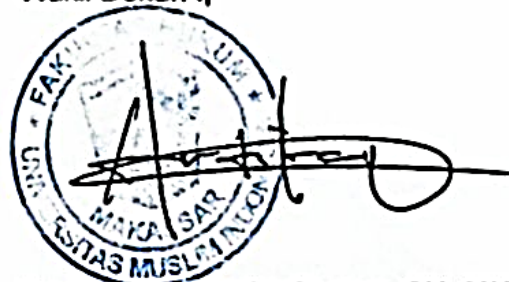
PERSETUJUAN UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama Mahasiswa : Muh. Iksan Nur Khaifh
Nim : 040 2022 0376
Bagian : Hukum Pidana
Judul Skripsi/Penelitian : Pertanggungjawaban Pidana Atas Kejahatan
Manipulasi Algoritma Pada Platform TikTok
Dalam Perspektif Hukum Pidana Indonesia

**Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir
program studi**

Dikeluarkan di : Makassar
Pada Tanggal : 2026
A.n Dekan
Wakil Dekan I,



Dr. Andika Prawira Buana, SH., MH.
NIPs. 104151319

PENGESAHAN SKRIPSI

**PERTANGGUNGJAWABAN PIDANA ATAS KEJAHATAN
MANIPULASI ALGORITMA PADA PLATFORM TIKTOK
DALAM PERSPEKTIF HUKUM PIDANA INDONESIA**

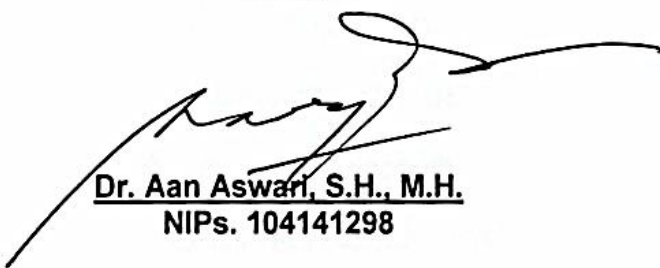
Disusun dan diajukan oleh :

MUH. IKSAN NUR KHALISH
04020220376

Telah dipertahankan dihadapan Panitia Ujian Skripsi pada Program Studi
Sarjana Ilmu Hukum Fakultas Hukum Universitas Muslim Indonesia
Pada Rabu, 1 April 2026
dan dinyatakan diterima

Panitia Ujian

Ketua,



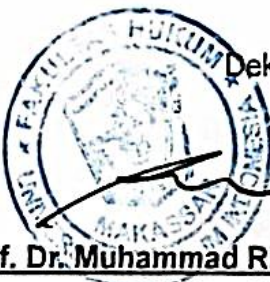
Dr. Aan Aswari, S.H., M.H.
NIPs. 104141298

Anggota,



Dr. H. Mursyid M, S.H., MH.
NIPS.104141299

Dekan,



Prof. Dr. Muhammad Rinaldy Bima, S.H., M.H
NIPs: 104101110

HALAMAN PENGESAHAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama Mahasiswa : Muh. Iksan Nur Khalish
Nim : 040 2022 0376
Bagian : Hukum Pidana
Judul Skripsi/Penelitian : Pertanggungjawaban Pidana Atas
Kejahatan Manipulasi Algoritma Pada
Platform TikTok Dalam Perspektif Hukum
Pidana Indonesia

Telah dipertahankan dan diterima dihadapan Majelis Ujian Skripsi Pada
Rabu, 1 April 2026 dan dinyatakan LULUS oleh:

Dr. Aan Aswari, SH., MH.

(Pembimbing Ketua)

Dr. H. Mursyid M, SH., MH.

(Pembimbing Anggota)

Dr. Nasrullah Arsyad, SH., MH.

(Penguji I)

Rizki Ramadani, SH., MH.

(Pembimbing II)



PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : Muh. Iksan Nur Khalish
NIM : 040 2022 0376
Bagian : Hukum Pidana
Program Studi : Ilmu Hukum
Judul Skripsi/Penelitian : **Pertanggungjawaban Pidana Atas
Kejahatan Manipulasi Algoritma Pada
Platform TikTok Dalam Perspektif Hukum
Pidana Indonesia**

Menyatakan dengan sebenarnya bahwa skripsi saya ini benar merupakan hasil karya sendiri, bukan merupakan hasil plagiasi terhadap karya ilmiah orang lain. Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa Sebagian atau keseluruhan dari skripsi merupakan hasil plagiasi, maka saya bersedia menerima sanksi karena perbuatan tersebut.

Makassar,2026

Yang Menyatakan,



MUH. IKSAN NUR KHALISH

KATA PENGANTAR



Assalamualaikum Warahmatullahi Wabarakatuh

Puji dan Syukur kehadiran Allah SWT, karena dengan rahmat, Taufiq dan inayah-Nya sehingga penyusunan skripsi ini dengan judul **“Pertanggungjawaban Pidana Atas Kejahatan Manipulasi Algoritma Pada Platform TIKTOK Dalam Perspektif Hukum Pidana Indonesia”** dapat dirampungkan sesuai dengan waktu yang direncanakan. Tak lupa penulis kirimkan salawat dan salam kepada Nabi Muhammad SAW sebagai teladan bagi seluruh ummat manusia.

Disadari bahwa skripsi ini kurang sempurna, hal ini disebabkan karena keterbatasan kemampuan yang ada pada penulis. Oleh karena itu, kritik, saran, dan koreksi untuk perbaikan dan penyempurnaannya sangat penulis harapkan.

Pada kesempatan kali ini, perkenankanlah penulis menyampaikan rasa terima kasih diiringi do'a kepada Allah SWT., kepada kedua orang tua penulis Ayahanda **Abdul Waris** terima kasih telah mengusahakan semuanya, cinta, kasih, dan pengorbanan tak terhitung hingga penulis sampai pada proses ini, serta kepada Ibunda **Surya Insani Aspan** terima kasih atas dukungan yang diberikan dan menjadi sumber kekuatan, motivasi, serta keteguhan bagi penulis dalam menyelesaikan seluruh tahapan studi, Juga terima kasih kepada kakak-kakak dari penulis yaitu **Jihan Annisa Mujaddidah** dan **Fauzan Mufadhdhal** yang telah memberi

support dan membantu dalam kelancaran penulisan skripsi ini.

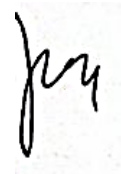
Selanjutnya penulis juga ucapkan terima kasih yang tak terhingga kepada:

1. **Bapak Prof. Dr. H. Hambali Thalib, SH., MH.**, selaku Rektor Universitas Muslim Indonesia;
2. **Bapak Prof. Dr. Muhammad Rinaldy Bima, SH., MH.**, selaku Dekan Fakultas Hukum Universitas Muslim Indonesia;
3. **Bapak Dr. H. Azwad Rachmat Hambali, SH., MH.**, selaku Ketua Bagian Hukum Pidana Fakultas Hukum Universitas Muslim Indonesia; yang telah memberikan izin, kesempatan dan fasilitas kepada penulis selama mengikuti pendidikan Program Sarjana;
4. **Bapak Dr. Aan Aswari, SH., MH.**, dan **Bapak Dr. H. Mursyid M, SH., MH.**, selaku Ketua dan Anggota Pembimbing yang memberikan bimbingan dengan penuh keseriusan, kecermatan dan kebijakan dalam memberi petunjuk-petunjuk perihal prinsip penulisan karya ilmiah kepada penulis;
5. **Bapak Dr. H. Nasrullah Arsyad, SH., MH.**, dan **Bapak Rizki Ramadani, S.H., M.H.**, selaku penilai yang memberikan masukan dan saran pada ujian Seminar Proposal sampai Ujian Skripsi;
6. Terkhusus kepada saudara seperjuangan **teman-teman MABES** yang senantiasa saling support dan membantu satu sama lain dalam penulisan Skripsi ini;

Tidak lupa juga kepada sahabat-sahabat yang tak sempat penulis sebut satu persatu dalam tulisan ini. penulis ucapkan terima kasih atas bantuan dan kebersamaannya.

Akhirnya penulis mengharap semoga dengan hadirnya Skripsi ini dapat bermanfaat bagi pengembangan ilmu dan teknologi. Semoga Allah SWT senasntiasa memberkati dan merahmati segala aktivitas keseharian sebagai suatu ibadah disisi-Nya. Amin.

Makassar,2026

A handwritten signature in black ink, appearing to be 'Muh. Iksan Nur Khalish', written in a cursive style.

MUH. IKSAN NUR KHALISH

ABSTRAK

Muh. Iksan Nur Khalish, 04020220376, “Tanggung Jawab Pidana Atas Kejahatan Manipulasi Algoritma Pada Platform TIKTOK Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik”. Dibawah bimbingan Bapak Aan Aswari selaku Ketua Pembimbing dan Bapak Mursyid selaku Anggota Pembimbing.

Penelitian ini bertujuan untuk mengetahui bagaimana karakteristik perbuatan manipulasi algoritma yang dapat dikualifikasikan sebagai tindak pidana dan bagaimana bentuk pertanggungjawaban secara pidana atas perbuatan manipulasi algoritma pada platform TIKTOK yang didasarkan pada perspektif hukum pidana yang berlaku di Indonesia.

Penelitian ini menggunakan metode penelitian normatif yang dilakukan dengan cara meneliti dan melakukan pengkajian atas berbagai bahan hukum atau referensi yang ada melalui studi kepustakaan yang menitikberatkan hukum sebagai sistem norma dalam merumuskan dan menjawab persoalan hukum secara konseptual.

Hasil Penelitian ini mengindikasikan bahwa manipulasi algoritma memiliki karakteristik sebagai perbuatan yang dilakukan secara sengaja, memanfaatkan sistem elektronik secara tidak sah, mengganggu integritas logika pemrosesan sistem, menghasilkan informasi elektronik yang menyesatkan, serta menimbulkan kerugian. Meskipun sejumlah ketentuan dalam berbagai regulasi dapat digunakan untuk menjerat praktik tersebut melalui penafsiran terhadap delik sistem elektronik, penipuan, dan perbuatan curang, pengaturannya masih bersifat tidak langsung dan fragmentaris. Serta, penelitian ini mengerucut bahwa Pertanggungjawaban pidana atas perbuatan manipulasi algoritma pada platform TikTok secara teoritis dapat dimintai pada individu atau korporasi, namun paling dimungkinkan dimintai kepada individu, karena ruang digital dikatakan serupa dengan ruang konvensional, yang mana letak perbedaannya hanya pada dimensi terjadinya perbuatannya saja. Sehingga bila berbicara pertanggungjawaban pidana, maka dimintai kepada pelaku yang melakukan suatu kejahatan tadi, yang mana dalam konteks ruang digital. maka pertanggungjawabannya dimintai kepada individu yang menjalankan perbuatan manipulasi.

Berdasarkan temuan tersebut, penelitian ini menitikberatkan bahwa diperlukan pembaruan hukum yang mengarah pada penguatan pengaturan secara normatif, serta perumusan delik yang lebih adaptif terhadap kejahatan berbasis teknologi, guna menjamin perlindungan kepentingan hukum masyarakat di ruang digital.

Kata Kunci : Pertanggungjawaban Pidana, Manipulasi Algoritma, Platform Tiktok, Hukum Pidana

DAFTAR ISI

HALAMAN SAMPUL	i
PERSETUJUAN PEMBIMBING	ii
PERNYATAAN ORISINALITAS PENELITIAN	iv
KATA PENGANTAR	vi
ABSTRAK	ix
DAFTAR ISI	x
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah	1
B. Rumusan Masalah	8
C. Tujuan Penelitian	9
D. Manfaat Penelitian	9
BAB II TINJAUAN PUSTAKA	11
A. Tinjauan Umum Tentang Pertanggungjawaban Pidana	11
B. Tinjauan Umum Tentang <i>Cybercrime</i>	14
C. Manipulasi, Algoritma, dan Hubungan Pemanfaatannya	19
D. Akomodir Regulasi Terhadap Manipulasi Algoritma	25
1. Regulasi dalam perspektif KUHP	28
2. Regulasi dalam perspektif berbagai Undang-Undang ..	30
3. Peraturan Pemerintah Nomor 71 Tahun 2019	32
4. Perspektif Perjanjian Internasional OECD	34
BAB III METODE PENELITIAN	37
A. Tipe Penelitian	37
B. Pendekatan Penelitian	37
C. Jenis dan Sumber Bahan Hukum	38
D. Teknik Pengumpulan Bahan Hukum	39
E. Analisis Bahan Hukum	40
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	41
A. Karakteristik Perbuatan Manipulasi Algoritma Pada Platform TikTok yang Dapat Dikualifikasikan Sebagai Tindak Pidana	41

B. Pertanggungjawaban Pidana atas Manipulasi Algoritma pada Platform TikTok dalam Hukum Pidana Positif Indonesia.....	60
BAB V PENUTUP	72
A. Kesimpulan.....	72
B. Saran.....	73
DAFTAR PUSTAKA	75

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan media sosial yang pesat telah membawa perubahan signifikan dalam pola komunikasi, interaksi sosial, dan aktivitas ekonomi masyarakat, khususnya yang terjadi pada platform digital saat ini. Namun, perkembangannya tidak selalu membawa dampak positif, dimana kehadirannya terkadang sengaja dieksploitasi oleh oknum untuk melakukan praktik yang mengarah pada sebuah kejahatan yang dikategorikan sebagai kejahatan ruang digital yang dikenal dengan *cyber crime*.

Cyber crime (kejahatan di dunia maya) merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai kejahatan dunia maya (*cyber - space/virtual - space offence*), dimensi baru dari *hi - tech crime*, dimensi baru dari *transnational crime*, dan dimensi baru dari *white collar crime*.¹ Kejahatan dalam ruang ini memiliki tantangan sendiri dalam penegakannya, karena diperlukan kepastian, termasuk mengenai alat bukti kejahatan, lokasi terjadinya kejahatan, dan identitas korban dari tindak pidana tersebut. Sebaliknya, dalam kejahatan berbasis komputer, semua elemen

¹Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cybercrime Di Indonesia*, ed. Gideon Soerja, edisi 1. Malang: Media Nusa Creative, hlm. 2–3.

tersebut bersifat virtual dan tidak terbatas oleh waktu maupun tempat.² Fenomena tersebut dijumpai diberbagai platform digital yang memiliki pengaruh besar dalam aktivitas sosial di dunia maya, salah satu platformnya adalah TikTok, platform media sosial ini telah menjadi wadah utama untuk interaksi sosial, hiburan, dan distribusi konten kreatif. Platform TikTok memanfaatkan algoritma sebagai instrument yang dirancang untuk mengoptimalkan rekomendasi konten berdasarkan preferensi pengguna melalui mekanisme machine learning dan data *driven analytics*, memainkan peran sentral dalam menentukan visibilitas dan viralitas konten.

Namun, dalam pemanfaatan algoritma tidak selamanya digunakan sesuai dengan ketentuan yang ada, seringkali instrument algoritma ini dieksploitasi untuk melakukan sesuatu yang memberikan keuntungan bagi oknum yang mengeksploitasinya dengan efek merugikan orang lain sebagai pengguna atau dengan kata lain tindakan sengaja mengakali sistem rekomendasi atau distribusi konten agar suatu konten, akun, atau produk memperoleh visibilitas dan popularitas yang tidak sesuai dengan kondisi sebenarnya. Praktik ini antara lain dilakukan melalui pembelian pengikut dan tanda suka palsu, penggunaan bot untuk meningkatkan jumlah tayangan, pembuatan ulasan fiktif, serta *click fraud* terhadap iklan pesaing. Hal ini membuat algoritmik telah muncul sebagai ancaman signifikan terhadap integritas ekosistem digital. Praktik ini tidak hanya mengganggu ekuitas

²*Ibid.*, hlm.4.

kompetitif antar pengguna, tetapi juga berpotensi menimbulkan dampak sosial, ekonomi, dan psikologis, termasuk penyebaran misinformasi, eksploitasi data pribadi, dan distorsi pasar konten.

Fenomena tersebut menyebabkan berbagai ketimpangan di berbagai penjuruk norma-norma kehidupan yang mengakibatkan tercederainya aspek yang dewasa ini menjadi ruang aktivitas masyarakat. Sejalan dengan fenomena yang terjadi dimana suatu perbuatan yang mengarah pada menghasilkan sesuatu dengan cara yang tidak benar dan efeknya merugikan orang lain, perbuatan tersebut memiliki relevansi dengan peringatan dari norma agama melalui Firman Allah SWT yang dijelaskan dalam

QS. An-Nisa {4}: 29

يٰۤاَيُّهَا الَّذِيْنَ ءَامَنُوْا لَا تَأْكُلُوْا اَمْوَالَكُم بَيْنَكُمۡ
بِالْبَاطِلِ اِلَّا اَنْ تَكُوْنَ تِجَارَةً عَنْ تَرَاضٍ مِّنْكُمْ وَلَا نَقْتُلُوْا
اَنْفُسَكُمْ اِنَّ اللّٰهَ كَانَ بِكُمْ رَحِيْمًا ﴿٢٩﴾

Terjemahan:

Wahai orang-orang yang beriman, janganlah kamu memakan harta sesamamu dengan cara yang batil (tidak benar), kecuali berupa perniagaan atas dasar suka sama suka di antara kamu. Janganlah kamu membunuh dirimu. Sesungguhnya Allah adalah Maha Penyayang kepadamu.

Demikianlah dijelaskan melalui Firman Allah SWT yang menjadi peringatan untuk tidak melakukan hal-hal yang dapat mengakibatkan kerugian pada orang lain untuk menguntungkan diri sendiri yang

disimpulkan telah melanggar berbagai norma kehidupan yang ada utamanya norma agama.

Fenomena manipulasi algoritma di Indonesia telah muncul dalam berbagai sektor, terutama dalam ekosistem platform digital dan media sosial. Penelitian Universitas Gadjah Mada menunjukkan bahwa praktik manipulasi algoritma pada platform *social-commerce* berpotensi menimbulkan penyalahgunaan posisi dominan dan diskriminasi terhadap pelaku usaha lain. Hal ini sejalan dengan temuan KPPU, yang mengungkap adanya dugaan “monopoli algoritma” pada sejumlah platform e-commerce, seperti platform yang memprioritaskan mitra logistik tertentu. Kondisi tersebut menunjukkan bahwa algoritma kerap dimanfaatkan secara strategis untuk kepentingan korporasi sehingga menciptakan ketidakadilan dalam persaingan usaha.³

Dalam konteks sosial-politik, algoritma juga digunakan untuk mengatur persebaran informasi secara selektif dan masif, yang berpotensi membentuk opini publik sesuai dengan kepentingan kelompok tertentu. Praktik ini mengancam integritas demokrasi digital karena dapat menyesatkan persepsi masyarakat.

Selain itu, Otoritas Jasa Keuangan (OJK) menyoroti risiko dari kurangnya transparansi algoritma di sektor keuangan, yang dapat menimbulkan bias, ketidakadilan, dan penyalahgunaan data pribadi.

³Sulistyarini. *Manipulasi Algoritma Oleh Platform Bisnis Social-Commerce di Era Ekonomi Digital dalam Perspektif Hukum Persaingan Usaha Di Indonesia*. Tesis, Universitas Gadjah Mada, 2025.

Fakta-fakta tersebut memperlihatkan bahwa meskipun UU ITE telah mengatur aspek keamanan sistem elektronik, regulasi yang ada masih belum mampu mengantisipasi kompleksitas risiko dan kejahatan manipulasi algoritma dalam praktik digital modern.⁴

Dalam konteks hukum pidana, perbuatan tersebut perlu dikaji karena berkaitan dengan penyalahgunaan sistem elektronik yang memiliki dampak luas terhadap keadilan digital. Secara normatif, aspek hukum juga telah memiliki landasan yang sering dikaitkan dalam menghadapi kondisi seperti hal tersebut yang diatur secara implisit melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan kerangka regulasi utama di Indonesia untuk mengatur transaksi elektronik dan kejahatan siber. UU ITE, yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016 serta Undang-Undang Nomor 1 Tahun 2024, menetapkan tanggung jawab pidana bagi pelaku kejahatan yang melibatkan akses ilegal, penyebaran informasi yang merugikan, atau gangguan terhadap sistem informasi.⁵ Dimana hanya lebih fokus pada kejahatan konvensional seperti hacking (Pasal 30), penipuan elektronik (Pasal 35), atau penyebaran hoaks (Pasal 28). Namun, belum mengakomodir modus kejahatan digital baru yang disebut dengan manipulasi

⁴Muhamad Ibrahim. "Jurus OJK Mengatasi Bias Algoritma yang Jadi "Penghalang" Akses Pembiayaan." Infobanknews, 17 Oktober 2025. <https://share.google/QhQEHeWtDLrHROJA>

⁵Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. LN 2024 (1), TLN (6905): 21 hlm.; jdih.setneg.go.id

algoritma dan terjadi pada platform digital. Contohnya, manipulasi algoritma pada platform TikTok yang kerap dilakukan dengan praktik seperti, influencer yang membeli puluhan ribu pengikut dan like palsu untuk meningkatkan viralitas dengan cara yang tidak benar, toko daring yang membayar pihak tertentu untuk memberikan ulasan bintang lima, atau konten kreator yang menggunakan bot agar videonya lebih sering direkomendasikan.

Hal ini menciptakan celah regulasi, di mana praktik manipulasi algoritma yang dapat diklasifikasikan sebagai bentuk cyber manipulation atau algorithmic fraud belum sepenuhnya diakomodasi, sehingga menimbulkan tantangan dalam penegakan hukum dan penentuan tanggung jawab pidana.

Tidak hanya belum diakomodir oleh regulasi yang ada dan mengatur tentang kejahatan dalam ruang digital, tetapi juga telah menyalahi dan mengesampingkan berbagai ketentuan yang telah disebutkan didalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, dimana PP Nomor 71 Tahun 2019 mewajibkan Penyelenggara Sistem Elektronik (PSE) menyelenggarakan sistem elektronik secara andal, aman, dan bertanggung jawab sebagaimana ditegaskan dalam Pasal 3 ayat (1) dan (2), serta menjamin keutuhan dan keautentikan informasi elektronik sesuai Pasal 4 huruf a dan b, dengan tanggung jawab penuh

atas pengoperasian sistem sebagaimana diatur dalam Pasal 5 ayat (1).⁶

Dalam konteks platform TikTok, algoritma rekomendasi dan distribusi konten merupakan bagian dari sistem elektronik yang tunduk pada ketentuan tersebut. Oleh karena itu, manipulasi algoritma yang dilakukan untuk mendistorsi distribusi konten, menguntungkan pihak tertentu, atau menyesatkan pengguna dapat dikualifikasikan sebagai pelanggaran kewajiban hukum PSE untuk menyelenggarakan sistem elektronik secara bertanggung jawab, yang selanjutnya dapat dijadikan dasar konstruksi perbuatan melawan hukum dalam kerangka UU ITE.

Sementara itu, dari sudut pandang hukum, absennya ketentuan spesifik dalam UU ITE mengakibatkan ketidakpastian yuridis, di mana penuntutan sering kali bergantung pada interpretasi analogi terhadap pasal-pasal terkait, seperti akses tanpa hak atau penyebaran informasi yang menimbulkan kerugian. Akibatnya, fenomena ini tidak hanya mengancam kepercayaan pengguna terhadap platform digital tetapi juga menuntut reformasi hukum untuk mengintegrasikan aspek algoritmik ke dalam kerangka pidana, guna memastikan perlindungan terhadap hak digital dan keseimbangan ekosistem informasi.⁷

Atas fenomena itulah diperlukannya sebuah pengkajian akan praktik manipulasi algoritma pada platform TikTok yang menimbulkan

⁶Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. LN.2019/NO.185, TLN NO.6400, JDIH.SETNEG.GO.ID : 57 HLM.

⁷Safitri, Masna Nuros. *Kebijakan Hukum Pidana Penyebaran Hoaks melalui Manipulasi Algoritma Media Sosial dalam UU ITE*. Tesis, Universitas Gadjah Mada, 2025.

persoalan yuridis signifikan terhadap prinsip kejujuran, keadilan, dan kepastian hukum dalam penyelenggaraan sistem elektronik. Karena praktik semacam itu tidak hanya mendistorsi mekanisme distribusi konten dan menyesatkan pengguna, tetapi juga berpotensi melanggar ketentuan peraturan perundang-undangan, khususnya yang berkaitan dengan penipuan, perlindungan konsumen, persaingan usaha tidak sehat, dan penyalahgunaan sistem elektronik.

Oleh karena itu, penelitian ini menjadi relevan dan urgen untuk mengkaji secara normatif bentuk, kualifikasi hukum, serta pertanggungjawaban hukum para pelaku manipulasi algoritma di TikTok, sekaligus menelaah batas tanggung jawab hukum platform sebagai penyelenggara sistem elektronik. Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi terhadap pengembangan doktrin hukum dan perumusan kebijakan yang lebih adaptif guna menjamin tata kelola platform digital yang berkeadilan, transparan, dan akuntabel di Indonesia.

B. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimanakah karakteristik perbuatan manipulasi algoritma pada platform tiktok yang dapat dikualifikasikan sebagai tindak pidana?

2. Bagaimanakah hukum pidana positif Indonesia dalam menjangkau pertanggungjawaban pidana atas manipulasi algoritma pada platform TikTok?

C. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan menguraikan bagaimana karakteristik perbuatan manipulasi algoritma yang dapat dikualifikasikan sebagai tindak pidana
2. Untuk mengetahui dan menentukan bagaimana bentuk pertanggungjawaban pidana atas manipulasi algoritma pada platform tiktok

D. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini diharapkan berkontribusi dalam pengembangan ilmu hukum, khususnya dalam bidang hukum siber dan teknologi informasi, melalui perumusan konseptual mengenai manipulasi algoritma. Lebih lanjut, penelitian ini dapat menjadi dasar dalam memperjelas batasan normatif antara perilaku optimasi konten yang sah dan praktik manipulasi algoritma yang bersifat curang dan menyesatkan, sehingga dapat menjadi rujukan dalam membangun konstruksi hukum yang lebih presisi.

Selain itu, penelitian ini diharapkan mampu memperkuat dasar teoretis bagi pengembangan doktrin pertanggungjawaban hukum

terhadap pelaku manipulasi algoritma maupun penyelenggara sistem elektronik, serta mendorong integrasi prinsip keadilan, transparansi, dan akuntabilitas algoritmik dalam kerangka hukum nasional. Dengan demikian, hasil penelitian ini dapat menjadi pijakan akademik bagi kajian lanjutan dan pembentukan regulasi yang lebih adaptif terhadap dinamika teknologi digital.

2. Manfaat Praktis

Hasil penelitian ini diproyeksikan menjadi acuan ilmiah bagi aparat penegak hukum, kalangan akademisi, serta masyarakat dalam mengkaji dan memahami penerapan norma-norma hukum pidana dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terhadap fenomena manipulasi algoritma di platform digital. Selain itu, penelitian ini juga memberikan gambaran yuridis mengenai implikasi penerapan ketentuan tersebut dalam sistem hukum pidana nasional.

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Pertanggungjawaban Pidana

1. Definisi Pertanggungjawaban Pidana

Menurut Moeljatno, pertanggungjawaban pidana atau *criminal liability* merupakan kemampuan seseorang untuk menanggung akibat hukum atas perbuatan pidana yang telah dilakukannya karena terdapat unsur kesalahan dalam diri pelaku. Artinya, seseorang hanya dapat dijatuhi pidana apabila ia benar-benar telah melakukan perbuatan yang dilarang oleh undang-undang (*perbuatan pidana*) dan memiliki kesalahan atas perbuatan tersebut.

Dengan demikian, prinsip dasar yang dianut dalam hukum pidana adalah *geen straf zonder schuld* atau “tidak ada pidana tanpa kesalahan”, yang menegaskan bahwa pemidanaan hanya dapat dijatuhkan kepada orang yang bersalah secara hukum maupun moral atas perbuatannya.⁸

Lebih lanjut menurut Eddy O.S. Hiariej menyatakan bahwa pertanggungjawaban pidana merupakan akibat hukum yang dibebankan kepada seseorang yang melakukan perbuatan pidana (*strafbaar feit*) disertai dengan adanya unsur kesalahan (*schuld*). Unsur kesalahan menjadi aspek fundamental dalam pertanggungjawaban

⁸Moeljatno. (2008). *ASAS-ASAS HUKUM PIDANA*, Revisi. Jakarta: Rineka Cipta, hlm. 165–77.

pidana, karena tanpa adanya kesalahan, tidak dimungkinkan penjatuhan pidana terhadap pelaku, sejalan dengan asas *geen straf zonder schuld* atau “tidak ada pidana tanpa kesalahan.” Dengan demikian, meskipun suatu perbuatan telah memenuhi unsur delik dan bersifat melawan hukum, pelaku tidak dapat dipidana apabila tidak terbukti memiliki kesalahan atau kemampuan untuk bertanggung jawab.⁹

2. Unsur Pertanggungjawaban Pidana

Dalam hal dimintai pertanggungjawaban pidana, Andi Hamzah menuturkan bahwa seseorang hanya dapat dimintai pertanggungjawaban pidana bila memenuhi unsur-unsur sebagai berikut :

- a. Adanya perbuatan atau tindak pidana (perbuatan atau tindakan yang dilarang atau diancam pidana oleh undang-undang). Hal ini merupakan unsur objektif, menyangkut perbuatan yang dilarang;
- b. Pelaku mampu bertanggung jawab, artinya seseorang mampu memahami makna perbuatannya dan mengendalikan kehendaknya;
- c. Adanya sebuah kesalahan atau *Schuld*, baik berupa kesengajaan maupun kealpaan yang menyebabkan timbulnya akibat pidana;

⁹Eddy O.S. Hiariej. (2016). *Prinsip-Prinsip Hukum Pidana*, revisi. Yogyakarta: Cahaya Atma Pustaka, hlm. 143–79.

- d. Tidak adanya alasan penghapusan pidana, baik pembelaan terpaksa atau *noodweer*, daya paksa atau *overmacht*, dan suatu perintah jabatan yang sah.

3. Kemampuan Bertanggung Jawab

Menurut Andi Hamzah, kemampuan untuk bertanggung jawab merupakan syarat fundamental dalam penerapan pertanggungjawaban pidana terhadap seseorang. Artinya, pemidanaan hanya dapat dijatuhkan apabila pelaku memiliki kapasitas psikis dan intelektual yang memadai untuk memahami serta mengendalikan perbuatannya.

Seseorang tidak dapat dimintai pertanggungjawaban pidana apabila berada dalam kondisi yang meniadakan kesadaran atau kemampuan tersebut, seperti halnya ketika menderita gangguan jiwa yang menghilangkan kesadaran atas perbuatannya, atau masih berada pada usia yang tergolong belum dewasa sehingga belum mampu memahami akibat hukum dari tindakannya. Kemampuan bertanggung jawab ini pada hakikatnya diukur melalui dua aspek utama, yaitu:

- a. Akal, yang mencerminkan kemampuan seseorang untuk mengetahui serta membedakan antara perbuatan yang benar dan salah menurut hukum maupun norma sosial; dan
- b. Kehendak, yang menunjukkan kemampuan individu untuk menyesuaikan perilakunya dengan ketentuan hukum yang berlaku. Dengan demikian, unsur akal dan kehendak menjadi

indikator utama dalam menilai ada atau tidaknya kemampuan bertanggung jawab yang menjadi dasar sahnya pembedaan.

4. Prinsip – Prinsip Pertanggungjawaban Pidana

Pertanggungjawaban pidana didasarkan pada asas atau prinsip-prinsip sebagai berikut :

- a. Asas Kesalahan (Asas Culpabilitas), artinya seseorang dapat dipidana bila pada dirinya terdapat kesalahan (geen straf zonder Schuld);
- b. Asas Legalitas, ialah asas yang menjelaskan bahwa tidak dapat dipidanya seseorang bila perbuatannya belum diatur oleh undang-undang terlebih dahulu (nullum delictum nulla poena sine praevia lege poenali);
- c. Asas Personalitas, bahwa seseorang hanya bisa dimintai pertanggungjawaban atas perbuatannya sendiri;
- d. Asas Kemampuan Bertanggung Jawab, Hanya orang yang mampu memahami dan mengendalikan perbuatannya yang dapat dimintai pertanggungjawaban pidana.¹⁰

B. Tinjauan Umum Tentang *Cybercrime*

1. Definisi *Cybercrime*

Dalam hukum pidana Indonesia, *cybercrime* diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang

¹⁰ Andi Hamzah. (2012). *Asas-Asas Hukum Pidana*, Revisi. Jakarta: Rineka Cipta, hlm. 130–136.

Nomor 19 Tahun 2016. Kejahatan siber dipahami sebagai perbuatan melawan hukum yang menggunakan sistem elektronik atau jaringan komputer sebagai sarana maupun objek kejahatan. Undang-undang ini mencakup berbagai bentuk tindak pidana yang terjadi di ruang digital. Secara esensial, UU ITE menegaskan bahwa pemanfaatan teknologi informasi harus sejalan dengan norma hukum, agama, kesusilaan, dan ketertiban umum, sehingga *cybercrime* dapat dimaknai sebagai setiap perbuatan melawan hukum.¹¹

2. *Cybercrime* Menurut Ahli

Sesuai dengan pemahamannya akan *cybercrime*, beberapa ahli memeberikan definisi mengenai cybercrime. Menurut Barda Nawawi Arief, Cybercrime dapat didefinisikan sebagai bentuk kejahatan kontemporer yang muncul sebagai konsekuensi dari perkembangan teknologi informasi, di mana komputer dan sistem elektronik berfungsi sebagai alat maupun objek dari aktivitas kriminal.¹²

Sementara itu, Abizar Al Ghiffari berpendapat bahwa Kejahatan siber atau *cybercrime* adalah bentuk kejahatan modern yang memanfaatkan teknologi informasi dan sistem elektronik sebagai sarana maupun sasaran untuk melakukan perbuatan melawan hukum, yang berdampak pada kerugian ekonomi, pelanggaran privasi, serta ancaman terhadap keamanan nasional. Kejahatan ini bersifat lintas

¹¹ “Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik” (Jakarta, 2008), <https://peraturan.go.id/uu-no-11-tahun-2008>.

¹² Barda Nawawi Arief. (2010). *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Modern*, Cetakan pertama. Jakarta: Kencana Prenada Media Group, hlm. 52–56.

batas, anonim, dan kompleks, sehingga menuntut adanya penguatan regulasi, peningkatan kapasitas forensik digital, serta literasi keamanan siber masyarakat agar penegakan hukum dapat berjalan efektif dan adaptif terhadap dinamika digital.¹³

3. Klasifikasi *Cybercrime*

Pengklasifikasian akan jenis atau bentuk kejahatan digital atau *cybercrime* dapat dijabarkan kedalam beberapa jenis sebagai berikut:

a. Kejahatan Phising

Phishing merupakan bentuk kejahatan siber yang dilakukan melalui manipulasi korban, biasanya lewat email atau media sosial, dengan menyebarkan tautan atau situs palsu untuk memperoleh data sensitif seperti nama, kata sandi, PIN, dan OTP yang terkait dengan layanan perbankan maupun transaksi digital.

b. Kejahatan *Ransomware*

Ransomware merupakan perangkat lunak berbahaya yang menginfeksi sistem komputer dan menyandera data pengguna. Pelaku biasanya menuntut pembayaran untuk memulihkan akses, disertai ancaman merusak data apabila permintaan tidak dipenuhi.

¹³ Abizar Al Ghiffari. (2025). "Kejahatan Siber Dan Tantangan Penegakan Hukum Di Indonesia Koordinasi Dengan Penegakan Pidana Ketika Kasus Kebocoran Data Beririsan Dengan Tindak Bukti Lintas Batas , Terutama Ketika Infrastruktur Serangan Seperti Server , Domain , Atau Dompet Di Ranah So" 02, no. 02: 1295–99.

c. Penipuan Online

Penipuan digital kini semakin marak, salah satunya melalui penyalahgunaan foto selfie dan KTP yang digunakan untuk kejahatan identitas. Modus ini sering terjadi dalam proses pendaftaran layanan keuangan daring, seperti dompet digital, PayLater, pinjaman online, atau rekening bank, di mana data pribadi korban dieksploitasi untuk pinjaman ilegal, dijual di pasar gelap, atau digunakan dalam tindak pencucian uang.

d. SIM Swap

SIM swap merupakan bentuk penipuan yang dilakukan dengan mencuri nomor telepon atau kartu SIM korban untuk mengakses rekening banknya. Akibatnya, korban kehilangan kendali atas SIM miliknya, sehingga disarankan untuk memotong atau menghancurkan kartu SIM lama guna mencegah penyalahgunaan.

e. Peretasan Situs dan *Email*

Perusakan situs web dan email merupakan kejahatan siber yang dilakukan melalui peretasan untuk mengubah tampilan atau isi. Tindakan ini dapat menimbulkan perubahan visual, penyisipan iklan tersembunyi, serta risiko pencurian data tanpa sepengetahuan pemilik.

f. *OTP Fraud*

Kode OTP (One Time Password) merupakan elemen penting dalam keamanan transaksi karena berfungsi sebagai kunci akhir untuk mengakses atau menyelesaikan transaksi keuangan. Pencurian atau penipuan OTP menjadi kejahatan yang umum terjadi, biasanya disebabkan oleh malware, aplikasi berbahaya, atau teknik rekayasa sosial melalui telepon, SMS, dan email palsu.

g. Pemalsuan Data atau *Data Forgery*

Pemalsuan data atau dokumen penting secara online merupakan tindak pidana yang kerap menyasar dokumen e-commerce atau toko daring, dan dapat menimbulkan kerugian bagi pengguna maupun masyarakat akibat kesalahan informasi.

h. Kejahatan Konten Ilegal

Divisi Hubungan Internasional Polri menyatakan bahwa kejahatan siber mencakup penyebaran konten terlarang, seperti data palsu, tidak etis, melanggar hukum, atau mengganggu ketertiban umum, termasuk fitnah, pornografi, rahasia negara, dan propaganda anti-pemerintah.

i. “Teroris” Dunia Maya atau *Cyber Terrorism*

Cyber terrorism adalah kejahatan yang merusak atau mengganggu data pada jaringan komputer, di mana pelaku sering memanfaatkan kondisi tersebut dengan menawarkan perbaikan data kepada korban demi imbalan tertentu.

j. Mata-mata atau *Cyber Espionage*

Jenis kejahatan siber ini melibatkan akses rahasia ke sistem komputer korban yang dilakukan untuk mencuri informasi rahasia (seperti data militer, politik, ekonomi, atau teknologi) melalui jaringan komputer dan sistem informasi. untuk mengintai informasi sensitif, sering menargetkan perusahaan pesaing yang menyimpan data penting secara digital. Lebih luas lagi, tujuannya bukan merusak sistem, tapi mendapatkan intelijen secara diam-diam untuk keuntungan politik, militer, atau ekonomi.¹⁴

C. Manipulasi, Algoritma, dan Hubungan Pemanfaatannya

1. Pengertian Manipulasi

Berdasarkan Kamus Besar Bahasa Indonesia (KBBI), Manipulasi adalah Tindakan yang meliputi kegiatan terampil yang dilakukan dengan tangan atau alat mekanis, upaya oleh kelompok maupun individu untuk memengaruhi perilaku, sikap, dan pendapat orang lain tanpa disadari, termasuk di dalamnya teknik yang menargetkan alam bawah sadar dengan mengendalikan keinginan dan gagasan melalui sugesti, sehingga pengaruh yang dihasilkan bersifat halus, bertahap, dan sulit terdeteksi oleh pihak yang dikenai.¹⁵

¹⁴ Zaenal Arifin and Emi Puasa Handayani. (2023). *CYBERCRIME: MENYELISIK PENEGAKAN HUKUM DAN PENANGGULANGANNYA*, ed. Zakiyatur Rosidah. Yogyakarta: DEEPUBLISH DIGITAL, hlm. 21–24.

¹⁵ Badan Pengembangan dan Pembinaan Bahasa. (2025) *Kamus Besar Bahasa Indonesia*, Daring. Jakarta: Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. <https://kbbi.kemdikbud.go.id/entri/manipulasi>.

Sedangkan bila berbicara dalam konteks hukum, maka definisi manipulasi menurut pasal 35 UU ITE ialah Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersebut seolah-olah data yang otentik.¹⁶

Manipulasi atau perdayaan adalah proses rekayasa yang disengaja, di mana seseorang atau kelompok menambah, menyembunyikan, menghilangkan, atau mengaburkan bagian atau seluruh sumber informasi, substansi, kenyataan, fakta, data, atau sejarah. Ini dilakukan melalui sistem perancangan yang bisa diterapkan oleh individu, kelompok, atau kerangka nilai tertentu.¹⁷

Sementara dalam disiplin ilmu psikologis juga memiliki pandangan terhadap manipulasi, bahwasanya , manipulasi adalah salah satu fenomena baru dalam lingkup dalam kekerasan psikologis yang tidak terlihat secara fisik tetapi berdampak negatif pada kesehatan mental seseorang.¹⁸

Tak kalah penting juga dalam disiplin ilmu ekonomi, bahwa manipulasi sebagai tindakan sengaja untuk memengaruhi atau

¹⁶Yurizal,(2018). Op. Cit., hlm. 113.

¹⁷ Muhammad Rinaldy Bima, Andi Masagena, and Rizki Ramadani. (2024). "Urgensi Hukum Tindak Pidana Korupsi Pada Perusahaan Yang Manipulasi Pajak" 1, no. July: 2.

¹⁸ Yosi Refatalina and Nisa Uljannah. (2025). "Pengaruh Kekerasan Psikologis Terhadap Kesehatan Mental Korban Kekerasan Dalam Rumah Tangga (KDRT) Sebuah Studi Psikologis Dan Hukum," *CBJIS: Cross-Border Journal of Islamic Studies* 7, no. 2: 361–69, <https://doi.org/10.37567/cbjis.v7i2.4226>.

mengubah mekanisme ekonomi yang sesuai ketentuan untuk memperoleh keuntungan tertentu atau menyesatkan pihak lain, dapat berupa pengaturan harga, pemalsuan data keuangan, pengendalian pasar atau rekayasa informasi ekonomi agar menciptakan persepsi yang salah terhadap kondisi sebenarnya.¹⁹

2. Karakteristik Manipulasi

Setiap perbuatan manipulatif memiliki karakteristik khusus yang membedakannya dari persuasi biasa. Tindakan ini diketahui atas sejumlah indikator substantif yang menunjukkan adanya unsur kesengajaan, penyesatan, serta tujuan tersembunyi di balik perbuatan tersebut. Dengan demikian, manipulasi dipahami bukan sekadar sebagai upaya memengaruhi, melainkan sebagai tindakan yang terencana mengubah persepsi, informasi, atau keadaan faktual yang berpotensi menimbulkan kerugian atau menyesatkan pihak lain.

Berikut ciri khas dari Tindakan manipulasi :

- a. Tujuan yang terencana dan spesifik, berorientasi pada tujuan terencana dengan strategi sistematis untuk memengaruhi target tertentu;
- b. Kontrol yang terkendali, artinya menuntut kontrol ketat atas variabel untuk memastikan hasil sesuai tujuan;

¹⁹ Rizha Claudilla Putri. (2025). "Dark Patterns Sebagai Bentuk Manipulasi Perilaku Konsumen Digital: Analisis Interdisipliner Terhadap Dampak Psikologis, Hukum, Dan Ekonomi Dari Praktik Desain Manipulatif Dalam Ekosistem E-Commerce Global," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2: 1066–71, <https://doi.org/10.31004/riggs.v4i2.611>.

- c. Validasi dan Verifikasi, Manipulasi menuntut verifikasi agar proses dan hasilnya selaras dengan yang direncanakan;
- d. Dampak yang terukur, menghasilkan perubahan terukur yang dapat diverifikasi untuk menilai efektivitas dan hubungan sebab-akibatnya.²⁰

3. Pengertian Algoritma

Menurut Kamus Besar Bahasa Indonesia (KBBI) daring, algoritma dapat dimaknai sebagai rangkaian langkah yang tersusun secara sistematis dan logis untuk menyelesaikan suatu permasalahan dalam batas tahapan tertentu, leboh lanjut Formulasi tersebut mencerminkan sifat normatif, terukur, dan berorientasi pada kepastian hasil.²¹

Istilah algoritma mengalami perluasan makna dan semakin sering digunakan dalam bidang teknologi informasi, khususnya dalam konteks pemrograman komputer. Dalam perspektif akademis dan hukum teknologi, algoritma pemrograman dapat dipahami sebagai serangkaian instruksi logis dan sistematis yang dirancang untuk menyelesaikan suatu permasalahan melalui mekanisme komputasional, sehingga menghasilkan keluaran atau solusi dalam bentuk program komputer.

²⁰ Mochamad Rizal Ahba Ohorella. (2025, 24 Januari). Apa Itu Manipulasi? Definisi, Jenis, dan Karakteristiknya, *Merdeka.com*. Diakses pada tanggal 21 Oktober 2025.

²¹ KBBI

Rumusan ini menegaskan bahwa algoritma tidak hanya memiliki dimensi teknis, tetapi juga mengandung aspek normatif terkait tanggung jawab, transparansi, dan akuntabilitas dalam penerapannya pada sistem digital.²²

4. Ciri – Ciri Algoritma

Beberapa ciri-ciri atau karakteristik dari algoritma antara lain sebagai berikut:

- a. Presisi, ciri utama algoritma adalah presisi, yakni ketepatan dan kejelasan setiap instruksi agar tidak menimbulkan ambiguitas, mencerminkan asas kepastian dan keandalan procedural;
- b. Menyusun jumlah Langkah atau instruksi, setiap tahapan dalam penyusunan algoritma harus tersusun secara sistematis dari awal hingga akhir, meskipun dalam prosesnya mungkin terdapat variasi data yang diolah;
- c. *Terminate*, dalam penyusunan algoritma pemrograman, diperlukan sifat terminasi, yakni kemampuan algoritma untuk berakhir pada titik tertentu dan tidak berlangsung tanpa batas;
- d. Output yang dihasilkan tepat, ciri terakhir algoritma adalah hasil atau output yang dihasilkan harus akurat dan sesuai dengan tujuan, yang hanya dapat dicapai apabila setiap langkahnya disusun secara logis dan dijalankan dengan konsisten.²³

²²Ilham Fikriansyah. (2023, 11 juli). Algoritma Adalah: Pengertian, Ciri-ciri, dan Berbagai Jenisnya, detikedu. Di akses pada tanggal 21 Oktober 2025.

²³*Ibid*

5. Hubungan Pemanfaatan Manipulasi dan Algoritma

Perkembangan teknologi dan digitalisasi yang semakin pesat menjadikan dua variabel antara tindakan manipulasi melalui algoritma dijadikan instrumen untuk dieksploitasi. Konsekuensi sosial dari manipulasi informasi berbasis kecerdasan buatan bersifat signifikan, terutama dalam memperkuat polarisasi dan menghambat tercapainya pemahaman bersama di antara berbagai sudut pandang. Algoritma kurasi informasi berpotensi menciptakan “ruang gema”, di mana individu secara dominan dihadapkan pada konten yang selaras dengan keyakinan yang telah ada sebelumnya.

Belum lagi digitalisasi telah menjadi elemen penting dalam ruang komunikasi publik, sehingga potensial eksploitasi didalamnya terbuka sangat lebar, apalagi sebagian besar publik telah mampu untuk mengoperasikannya dengan mudah dan sebahagian kecil lainnya hanya terjebak dalam dimensi persuasif yang menenggelamkannya untuk percaya dan mengafirmasi apapun yang tampil, lewat, dan muncul dihadapan layer gawainya.²⁴

Dalam lingkungan digital, muncul fenomena kompleks berupa manipulasi sebuah informasi yang kadang dilakukan dengan orientasi algoritma pengguna melalui pemanfaatan akun otomatis atau bot. Bot media sosial merupakan perangkat lunak yang berfungsi melakukan interaksi secara otomatis, meniru perilaku manusia, serta

²⁴ Ilham Nurfajri et al. (2025). “Dampak Algoritma AI Terhadap Komunikasi Publik: Memahami Manipulasi Informasi Dan Realitas,” *CONVERSE Journal Communication Science* 1, no. 3: 10, <https://doi.org/10.47134/converse.v1i3.3543>.

menyebarkan informasi secara masif dan dalam rentang waktu yang sangat singkat. Dari perspektif hukum dan akademis, penggunaan bot ini menimbulkan implikasi terkait tanggung jawab hukum atas penyebaran informasi, potensi pelanggaran hak publik atas informasi yang akurat, serta perlindungan terhadap integritas wacana publik di ranah digital.

Kecenderungan semacam ini yang mampu menyisipkan sebuah cela untuk mengedepankan frekuensi yang teratas melalui konten dengan tagar yang tinggi dan juga populer. Ini merupakan bentuk manipulasi algoritmik yang memanfaatkan logika media sosial untuk menciptakan popularitas buatan.²⁵

D. Akomodir Regulasi Terhadap Manipulasi Algoritma

Peningkatan penggunaan teknologi informasi dan komunikasi, khususnya melalui media sosial, telah memunculkan berbagai bentuk kejahatan siber (*cybercrime*). Salah satu bentuknya, yakni manipulasi siber, merupakan jenis kejahatan modern yang memanfaatkan kemajuan teknologi digital yang bersifat universal di ranah maya. Dari perspektif hukum dan akademis, kejahatan ini menimbulkan dampak negatif yang tidak bersifat fisik, namun secara substansial merugikan pihak korban, setara dengan perbuatan pidana konvensional lainnya.

Indonesia saat ini masih kekurangan aturan yang jelas dan lengkap untuk menangani penyalahgunaan teknologi, karena beberapa

²⁵ Dzunuwanus Ghulam Manar and Mochammad Jose Akmal. (2021). "MANIPULASI NARASI PUBLIK MELALUI AKUN BOT DALAM AKTIVISME DIGITAL PRO-IKN DI MEDIA SOSIAL X", hlm. 167–86.

regulasi yang ada belum mengatur dan mengakomodir berbagai kejahatan di ruang digital secara komprehensif.

Dalam era transformasi digital, hampir semua aspek kehidupan terkoneksi secara online, menjadikan data sensitif rentan terhadap kejahatan siber yang dapat merugikan finansial, reputasi, dan keamanan nasional. Pelaku, baik itu individu, kelompok, maupun negara dapat mencuri data, meretas sistem, atau merusak infrastruktur kritis yang dilancarkan dengan serangan yang memiliki Tingkat kompleksitas sangat tinggi.²⁶

Dalam upaya menanggulangi kejahatan siber, Indonesia telah menetapkan sejumlah regulasi strategis. Salah satunya adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian direvisi melalui Undang-Undang Nomor 19 Tahun 2016, yang mengatur berbagai aspek aktivitas digital, termasuk transaksi elektronik, penyebaran informasi, serta tindakan kriminal yang terjadi di ranah maya. Selain itu, pemerintah telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai langkah progresif dalam memberikan perlindungan hukum terhadap data pribadi masyarakat. Kedua regulasi tersebut menjadi pilar utama dalam kerangka hukum penanganan kejahatan siber di Indonesia.

²⁶ Natanael Hiskia Mongkau, Herlyanty Y. A. Bawole, and Altje Musa. (2025). "PENEGAKKAN HUKUM TERHADAP PENYALHUNAAN KECERDASAN BUATAN DENGAN CARA MEMANIPULASI WAJAH SESEORANG KE DALAM GAMBAR ATAU VIDEO PORNO" 13, no. 2: 1–23.

Meski regulasi telah tersedia, efektivitas penegakan hukum siber di Indonesia masih menghadapi sejumlah kendala. Aparat penegak hukum mengalami kesulitan dalam mendeteksi dan menangani kasus kejahatan siber yang semakin kompleks, antara lain akibat sinergi antar lembaga penegak hukum dan instansi terkait yang belum berjalan secara optimal.²⁷

Kondisi ini mengakibatkan respons terhadap serangan siber masih tergolong lemah. Dalam konteks tersebut, regulasi diharapkan. Pemerintah, melalui Badan Siber dan Sandi Negara (BSSN), telah mengimplementasikan berbagai kebijakan untuk memperkuat keamanan digital, meliputi peningkatan kapasitas infrastruktur siber, penguatan kerja sama internasional, serta edukasi masyarakat mengenai keamanan digital.

Namun demikian, penerapan UU ITE masih menghadapi sejumlah permasalahan substantif. Salah satu isu utama adalah multitafsir pada beberapa pasal, yang kerap mengakibatkan kriminalisasi pengguna internet yang tidak melakukan kejahatan siber yang serius. UU ITE lebih banyak diterapkan dalam penanganan kasus pencemaran nama baik di media sosial dibandingkan dengan kejahatan siber yang lebih kompleks, seperti peretasan dan pencurian data. Hal ini menunjukkan adanya pergeseran fokus dalam penerapan

²⁷ Muhammad Aabid Tyas Dzaky and Ibrahim Fikma Edrisy(2025). "Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital," *PESHUM: Jurnal Pendidikan, Sosia Dan Humaniora* 4, no. 2: 12, <https://ulilalbabininstitute.id/index.php/PESHUM/article/view/8311/6317>.

regulasi, yang pada akhirnya menandakan bahwa efektivitas UU ITE dalam menghadapi ancaman digital yang lebih serius masih terbatas.²⁸

1. Regulasi dalam perspektif KUHP

Dalam upaya penegakan hukum terhadap berbagai tindak pidana yang terjadi di ranah siber, aparat penegak hukum, khususnya penyidik, kerap melakukan analogi atau penafsiran perbandingan terhadap ketentuan-ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP). Hal ini dilakukan karena sejumlah perbuatan dalam kejahatan siber belum secara eksplisit diatur dalam peraturan perundang-undangan yang bersifat khusus. Akibatnya, pasal-pasal dalam KUHP sering diterapkan secara bersamaan atau kumulatif untuk menjerat pelaku, mengingat suatu tindak pidana siber umumnya melibatkan berbagai bentuk perbuatan sekaligus.

Adapun beberapa ketentuan KUHP yang kerap dijadikan dasar hukum dalam penanganan tindak pidana siber antara lain sebagai berikut:

1. **Pasal 362 KUHP** digunakan dalam perkara *carding*, yakni pencurian data nomor kartu kredit milik orang lain untuk melakukan transaksi elektronik tanpa izin. Meskipun objek yang dicuri bukan benda berwujud, perbuatan tersebut memenuhi unsur *taking* terhadap sesuatu yang bernilai ekonomi :
2. **Pasal 378 KUHP** diterapkan dalam kasus penipuan daring, yaitu pelaku yang secara sengaja menampilkan iklan atau menawarkan produk melalui situs web untuk menarik korban mentransfer sejumlah uang, namun barang yang dijanjikan tidak pernah ada atau tidak dikirimkan;

²⁸ *Ibid*

3. **Pasal 335 KUHP** dapat digunakan dalam perkara pengancaman atau pemerasan yang dilakukan melalui surat elektronik (*e-mail*), di mana pelaku memaksa korban melakukan suatu tindakan dengan ancaman akan menyebarkan informasi atau rahasia pribadi korban;
4. **Pasal 311 KUHP** relevan dalam kasus pencemaran nama baik di dunia maya, misalnya melalui penyebaran surat elektronik atau pesan digital berisi tuduhan palsu yang merugikan reputasi seseorang di hadapan publik;
5. **Pasal 303 KUHP** dapat diterapkan terhadap penyelenggaraan atau partisipasi dalam perjudian daring (*online gambling*), baik yang beroperasi di wilayah hukum Indonesia maupun menggunakan server luar negeri;
6. **Pasal 282 KUHP** digunakan untuk menjerat pelaku penyebaran konten bermuatan pornografi melalui situs web atau platform digital. Kendati demikian, penagakannya menghadapi hambatan yuridis ketika domain atau server situs tersebut terdaftar di negara yang tidak menganggap pornografi sebagai perbuatan terlarang;
7. **Pasal 281, 282, dan 311 KUHP** dapat digunakan secara kumulatif terhadap kasus penyebaran konten pribadi yang bersifat vulgar atau bermuatan pornografi, seperti video pribadi tanpa izin. Pasal 281 KUHP memberikan ancaman pidana berupa penjara paling lama dua tahun delapan bulan atau denda paling banyak lima ratus rupiah;
8. **Pasal 378 dan 262 KUHP** juga dapat dikenakan pada kasus *carding*, di mana pelaku menggunakan data kartu kredit hasil pencurian untuk melakukan transaksi fiktif seolah-olah sah dan legal;
9. **Pasal 406 KUHP** diterapkan dalam tindak pidana perusakan data atau sistem komputer, termasuk peretasan dan *defacing* situs web, yang menyebabkan sistem elektronik pihak lain tidak dapat digunakan;
10. **Pasal 112 sampai dengan Pasal 116 KUHP** digunakan untuk menjerat pelaku yang membocorkan, mengakses, atau memata-matai data dan informasi yang tergolong rahasia negara.²⁹

²⁹ Yurizal, (2018). Op. Cit., hlm. 41-44.

2. Regulasi dalam perspektif berbagai Undang-Undang

Berdasarkan Pasal 1 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang dimaksud dengan *telekomunikasi* adalah setiap pemancaran, pengiriman, dan/atau penerimaan informasi dalam bentuk tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari rumusan tersebut dapat dipahami bahwa Internet beserta seluruh fasilitasnya termasuk dalam kategori sarana telekomunikasi, karena memiliki fungsi sebagai media untuk mengirim dan menerima berbagai bentuk informasi, baik berupa teks, gambar, suara, maupun video, melalui mekanisme berbasis gelombang elektromagnetik.

Dengan demikian, segala bentuk penyalahgunaan Internet yang menimbulkan gangguan terhadap ketertiban umum maupun pelanggaran terhadap hak-hak pribadi individu dapat dikenai sanksi hukum berdasarkan ketentuan dalam Undang-Undang Nomor 36 Tahun 1999 antara lain :

- a. Tindak akses ilegal (*illegal access*), yaitu perbuatan mengakses sistem komputer tanpa hak, sementara waktu ketentuan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang telekomunikasi dapat dijadikan dasar hukum untuk menjerat perbuatan tersebut yang menyatakan :

“Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi :

- akses ke jaringan telekomunikasi;
 - dan/atau - akses ke jasa telekomunikasi;
 - dan/atau - akses ke jaringan telekomunikasi khusus
- b. Tindakan intersepsi ilegal terhadap sistem atau jaringan komputer merupakan bentuk penyadapan tanpa izin yang melanggar hukum, Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.³⁰

Dengan demikian, penegakan hukum terhadap tindak pidana siber di Indonesia masih bergantung pada KUHP dan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Kedua instrumen ini digunakan secara analogis untuk menjerat perbuatan seperti *carding*, penipuan daring, pengancaman, peretasan, serta akses dan intersepsi ilegal terhadap sistem komputer. Dengan demikian, keduanya berperan sebagai dasar hukum sementara sebelum terbentuknya regulasi khusus yang lebih komprehensif di bidang kejahatan siber.

Artinya bahwa, , merupakan upaya menegakkan nilai-nilai hukum yang terkandung dalam norma dan prinsip keadilan terhadap perbuatan melawan hukum berbasis teknologi informasi dan komunikasi. Cybercrime pada hakikatnya mencakup dua dimensi: (1) kejahatan yang memanfaatkan teknologi informasi sebagai sarana, dan (2) kejahatan yang menjadikan sistem teknologi itu sendiri sebagai objek serangan.

³⁰ Yurizal, (2018). Op. Cit., hlm. 45-46.

Didasarkan pada kesengajaan mengubah, memalsukan, atau memanipulasi data, algoritma, maupun sistem informasi. Hal tersebut dipengaruhi atas faktor substansi hukum, aparaturnya penegak hukum, sarana dan prasarana pendukung, partisipasi masyarakat, serta nilai-nilai budaya hukum yang hidup di masyarakat.³¹

3. Peraturan Pemerintah Nomor 71 Tahun 2019

Dalam kerangka hukum Indonesia, setiap pihak yang menyelenggarakan dan mengoperasikan sistem elektronik untuk kepentingan layanan publik dikualifikasikan sebagai Penyelenggara Sistem Elektronik (PSE).³² TikTok dapat dikategorikan sebagai PSE lingkup privat karena menyediakan platform digital yang dapat diakses oleh masyarakat luas untuk mengunggah, mengelola, dan menyebarkan konten video. Tingginya jumlah pengguna TikTok menunjukkan luasnya cakupan pemrosesan data pribadi warga negara Indonesia oleh platform tersebut, yang meliputi antara lain data identitas dasar, informasi perangkat, data lokasi, preferensi pengguna, riwayat interaksi, serta pola perilaku digital.³³

Oleh sebab itu, kajian terhadap tanggung jawab hukum TikTok sebagai Penyelenggara Sistem Elektronik (PSE) lingkup privat menjadi krusial untuk menilai sejauh mana kewajiban hukum yang ditetapkan oleh negara benar-benar diimplementasikan dalam praktik pengelolaan

³¹ Yurizal, (2018). Op. Cit., hlm. 72-73.

³² Kominfo RI, "Daftar PSE Lingkup Privat," 2023

³³ Sinta Dewi, *Hukum Perlindungan Data Pribadi* (Bandung: PT Refika Aditama, 2021), hlm 54.

dan pemrosesan data digital di Indonesia. Salah satu tonggak kerangka hukum yang memberikan ketentuan dalam penyelenggaraan sistem elektronik di Indonesia adalah PP 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Bentuk perlindungan tersebut meliputi pemenuhan hak akses, hak untuk melakukan koreksi, hak atas penghapusan data pribadi, serta kewajiban verifikasi usia anak yang harus dilaksanakan oleh TikTok.³⁴

Ketentuan mengenai Penyelenggara Sistem Elektronik (PSE) tercantum dalam Pasal 1 ayat (4) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, yang menyatakan bahwa PSE adalah setiap orang perseorangan, badan usaha, penyelenggara negara, atau komunitas masyarakat yang menyediakan, mengelola, dan/atau menjalankan sistem elektronik bagi pengguna, baik untuk kepentingan sendiri maupun untuk kepentingan pihak lain. Dengan demikian, PSE dipahami sebagai pihak yang memikul tanggung jawab hukum atas penyelenggaraan dan pengelolaan berbagai layanan digital, seperti aplikasi, situs web, serta platform daring.³⁵

Namun demikian, implementasi perlindungan ini masih menghadapi kendala berupa rendahnya tingkat literasi digital

³⁴ Amelia dan Ema Nurkhaerani. 2025. Perlindungan Hak Pengguna dalam Praktik Pengolahan Data oleh Platform TikTok sebagai Penyelenggara Sistem Elektronik Privat: Analisis dalam Perspektif Hukum Teknologi Informasi. *Media Hukum Indonesia*. Vol. 4. No. 1, hlm: 377. doi; <https://doi.org/10.5281/zenodo.17866096>

³⁵ I Gede Arta, dkk. 2026. Pengaturan Clickwrap Agreement Dalam Sistem Hukum Kontrak Di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*. Vol. 4. No. 1. Hlm 3846. doi; <https://doi.org/10.61104/alz.v4i1.3728>

pengguna dan kurangnya transparansi dalam pengelolaan algoritma, yang pada akhirnya menghambat efektivitas pelaksanaannya. Implementasi akan regulasi ini kurang mempengaruhi upaya progresif yang dilakukan dalam menanggulangi berbagai fenomena yang ada dalam platform digital khususnya Tiktok, sehingga diperlukan adanya reformasi yang adaptif dan signifikan terkait ketentuan yang dapat menangkal perbuatan yang merugikan pengguna platform kembali terjadi.

Konsistensi penerapan regulasi ini tidak hanya berfungsi untuk melindungi hak-hak subjek data, tetapi juga menjadi faktor penentu bagi terbentuknya kepercayaan digital masyarakat di masa depan. menentukan masa depan kepercayaan digital masyarakat. Generasi muda Indonesia yang tumbuh bersama platform digital membutuhkan perlindungan komprehensif agar dapat memanfaatkan inovasi tanpa ancaman privasi.³⁶

4. Perspektif Perjanjian Internasional OECD

Organisation for Economic Co-operation and Development (OECD) merupakan organisasi internasional yang bertujuan mendorong kerja sama antarnegara dalam perumusan kebijakan publik guna meningkatkan pertumbuhan ekonomi, stabilitas, dan kesejahteraan sosial.³⁷ Dalam perkembangannya, OECD juga berperan sebagai rujukan normatif global dalam tata kelola teknologi

³⁶ Amelia dan Ema Nurkhaerani, Op. Cit. hlm. 384

³⁷ Milagsita, Anindya. "OECD Adalah Singkatan dari Apa? Pengertian, Negara Anggota, Tujuan, Kantor." *Detik.com*, 28 Oktober 2024

digital dan kecerdasan buatan melalui penerbitan *OECD Principles on Artificial Intelligence* (2019), yang menekankan nilai kemanusiaan, transparansi, keamanan, dan akuntabilitas algoritma, termasuk dalam konteks platform digital, karena menempatkan kewajiban moral dan normatif pada penyelenggara sistem elektronik untuk mencegah penggunaan algoritma yang bersifat manipulatif, diskriminatif, atau merugikan pengguna.³⁸

OECD Principles on Artificial Intelligence (2019) menegaskan bahwa sistem kecerdasan buatan harus dikembangkan dan dioperasikan secara bertanggung jawab dengan menjunjung nilai kemanusiaan, transparansi, keamanan, serta akuntabilitas. Prinsip *human-centred values and fairness* menempatkan kewajiban normatif agar algoritma tidak digunakan untuk memanipulasi perilaku pengguna, menyebarkan konten berbahaya, atau merugikan hak-hak digital subjek data, yang sejalan dengan semangat perlindungan pengguna dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.³⁹

Prinsip *transparency and explainability* memperkuat tuntutan keterbukaan atas cara kerja sistem elektronik, yang secara implisit

³⁸ Prabu Revolusi dan Radians Krisna Febriandy. 2025. Developing AI Regulations in Indonesia. Jurnal Indonesia: Manajemen Informatika dan Komunikasi. Vol. 6. No. 2. hlm 1039. doi; <https://doi.org/10.63447/jimik.v6i2.1380>

³⁹ Nurul Aprianti dan Gusti Ayu Ratih Damayanti. 2025. Negara Hukum Di Era Algoritma: Algoritma Reformulasi Artificial Intelligence Untuk Menjamin Perlindungan HAM Di Indonesia. Jurnal Hukum Agama Hindu WIDYA KERTA. Vol. 8 No. 2, doi: <https://doi.org/10.53977/wk.v8i2.3312>.

selaras dengan kewajiban Penyelenggara Sistem Elektronik dalam Pasal 3 dan Pasal 14 Peraturan Pemerintah Nomor 71 Tahun 2019 untuk menyelenggarakan sistem yang andal, aman, dan dapat dipertanggungjawabkan.

Sementara itu, prinsip *accountability* memberikan dasar etik dan yuridis bahwa pengembang dan operator algoritma dapat dimintai pertanggungjawaban atas dampak hukum dan sosial dari sistem yang mereka operasikan, sehingga prinsip-prinsip OECD tersebut berfungsi sebagai *soft law* internasional yang memperkuat kerangka normatif nasional dalam menilai dan membatasi praktik manipulasi algoritma di platform digital.⁴⁰

Sejalan dengan pandangan internasional yang menganggap bahwa diperlukannya sebuah tatanan normative yang mampu mendegradasi praktik semacam manipulasi algoritma tersebut.

⁴⁰ Ibid.

BAB III

METODE PENELITIAN

A. Tipe Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif (normative legal research). Metode ini bertujuan untuk menganalisis dan mengkaji peraturan perundang-undangan, doktrin hukum, serta prinsip-prinsip hukum yang berlaku terkait dengan topik penelitian. Penelitian normatif berfokus pada studi kepustakaan (library research) dan analisis yuridis terhadap sumber hukum primer, sekunder, dan tersier..

B. Pendekatan Penelitian

Penelitian ini menggunakan metode normatif yuridis, yang bertujuan untuk menganalisis dan menafsirkan peraturan perundang-undangan, doktrin hukum, dan prinsip-prinsip hukum terkait manipulasi algoritma di platform digital. Pendekatan penelitian ini berfokus pada studi kepustakaan (library research), dengan sumber data mencakup hukum primer, sekunder, dan tersier.

Melalui metode ini, penelitian menekankan kajian yuridis terhadap ketentuan hukum yang berlaku, menilai penerapan UU ITE dalam konteks penerapannya menghadapi kejahatan manipulasi algoritma, serta mengidentifikasi kesenjangan yang terjadi antara hukum dan aspek pertanggungjawaban pidana.

Pendekatan normatif yuridis seperti ini memungkinkan peneliti menyusun analisis yang sistematis, konseptual, dan berbasis hukum, sekaligus memberikan rekomendasi untuk penguatan penegakan hukum siber.

C. Jenis dan Sumber Bahan Hukum

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif (*normative legal research*) dengan pendekatan kualitatif, yaitu melalui analisis data secara deskriptif dan interpretatif, bukan berupa angka atau statistik.

Adapun sumber data yang digunakan dalam penelitian ini antara lain berupa :

1. Bahan Hukum Primer

Bahan hukum primer, ialah data berupa bahan hukum yang bersifat autoritatif adalah sumber hukum yang memiliki kekuatan mengikat karena diterbitkan atau ditetapkan oleh lembaga atau otoritas yang berwenang sesuai dengan kewenangannya. Sumber ini dianggap resmi dan sah untuk dijadikan rujukan dalam penerapan, penafsiran, atau analisis hukum. Data primer dapat berupa peraturan perundang-undangan seperti :

- a. Kitab Undang-Undang Hukum Pidana;
- b. Kitab Undang-Undang Hukum Acara Pidana;
- c. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016;

- d. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
- e. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

2. Bahan Hukum Sekunder

Bahan hukum sekunder adalah sumber yang memberikan penjelasan dan interpretasi terhadap bahan hukum primer, meliputi buku, jurnal, artikel ilmiah, penelitian terdahulu, pendapat ahli, serta dokumen relevan lainnya yang mendukung analisis masalah hukum yang diteliti.

3. Bahan Hukum Tersier

Bahan hukum tersier adalah sumber yang menyediakan pedoman, penjelasan, atau interpretasi tambahan terhadap bahan hukum primer dan sekunder. Sumber ini mencakup kamus umum, kamus hukum, glosarium, maupun terminologi hukum, yang digunakan untuk menelusuri makna, istilah, atau konsep hukum yang relevan dengan objek penelitian.

D. Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum primer, sekunder, dan tersier yang digunakan dalam penelitian ini adalah melalui studi kepustakaan (*library research*).

Teknik ini dilakukan dengan membaca, menelaah, mencatat, dan menganalisis peraturan perundang-undangan, buku hukum, jurnal ilmiah, artikel, literatur digital, dan hasil penelitian terdahulu yang

relevan dengan pokok masalah. Semua bahan hukum tersebut digunakan sebagai dasar analisis yuridis dalam penyusunan penelitian.

E. Analisis Bahan Hukum

Analisis penelitian ini dilakukan dengan menafsirkan ketentuan-ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta dikaitkan dengan teori pertanggungjawaban pidana dan teori kejahatan siber yang relevan.

Pendekatan ini diterapkan untuk menilai kesesuaian norma hukum dengan praktik manipulasi algoritma pada platform digital, sekaligus mengevaluasi penerapan pertanggungjawaban pidana terhadap pelaku berdasarkan ketentuan yang berlaku.

Hasil analisis kemudian disusun secara sistematis, dengan tujuan untuk menjawab rumusan masalah penelitian dan menyusun argumentasi yuridis mengenai penerapan UU ITE dalam menjerat pelaku manipulasi algoritma, serta mengidentifikasi kekuatan, kelemahan, dan potensi celah hukum yang ada dalam praktik penegakan hukum.

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Karakteristik Perbuatan Manipulasi Algoritma Pada Platform TikTok yang Dapat Dikualifikasikan Sebagai Tindak Pidana

Aktifitas dalam ruang digital kini mengalami pergeseran sebagai ruang interaksi sosial yang sekarang menjadi sangat fundamental, sebab segala sesuatu dapat terjadi di ruang digital. Apa yang terjadi di dunia nyata, diproyeksikan juga dapat terjadi di dunia maya, olehnya diperlukan kehati-hatian dan mawas diri Ketika melakukan interaksi dan bertindak dalam ruang digital.

Di Indonesia, eskalasi kejahatan siber semakin nyata seiring meningkatnya ketergantungan masyarakat terhadap teknologi digital dalam kehidupan sehari-hari. Pola kejahatan siber tidak lagi dilakukan secara konvensional, melainkan memanfaatkan algoritma cerdas yang mampu meniru perilaku manusia, merekayasa informasi secara persuasif, serta beroperasi melampaui batas-batas yurisdiksi negara.⁴¹

Dalam rangka menata ruang siber, Indonesia telah membentuk kerangka kebijakan hukum, salah satunya melalui Undang-Undang Informasi dan Transaksi Elektronik UU No. 11 Tahun 2008 sebagaimana telah diubah kedalam UU No. 19 Tahun 2016 serta perubahannya ke dalam UU No. 1 Tahun 2024 yang menetapkan

⁴¹ Sigid Suseno. 2021. "Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia". Jurnal Ilmu Hukum 8 (1): 60-62.

norma, larangan, dan ancaman pidana terhadap beragam perbuatan melawan hukum di bidang teknologi informasi, termasuk perbuatan akses ilegal, pengubahan atau pemalsuan informasi elektronik, serta praktik penipuan yang memanfaatkan sistem elektronik.⁴²

Salah satu fenomena yang hidup dalam platform digital berkaitan dengan perbuatan sekelompok oknum yang selalunya ingin menguntungkan diri sendiri ialah praktik manipulasi algoritma yang tanpa sadar marak terjadi, tetapi dianggap sebagai sesuatu yang wajar saja dalam ruang digital.

Namun, semua itu dianggap lumrah karena secara normatif belum ada ketentuan atau aturan yang secara signifikan menganggap hal tersebut sebagai sebuah perbuatan melawan hukum yang ujungnya dikatakan sebagai suatu tindak pidana. Hal itulah yang menyebabkan manipulasi algoritma dianggap lumrah dan belum ada penegakan secara hukum terkait praktiknya, padahal beberapa ketentuan telah menyebutkan dan memberikan batasan bagaimana berperilaku didalam ruang digital untuk menegakkan integritas dan transparansi dalam bermedia sosial.⁴³

Secara konseptual, manipulasi algoritma dapat dipahami sebagai setiap tindakan yang dilakukan secara sengaja untuk

⁴² Sholahuddin Al Fatih, dkk. 2025. Understanding Regulations Of Online Gambling In Indonesia: Is It Forbidden?. *Jurisdictie*. Vol. 16 No. 1. Hlm 55. doi; <https://doi.org/10.18860/j.v16i1.31101>.

⁴³ Madinah Mokobambang, dkk. 2023. Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum terhadap Kejahatan Digital. *Jurnal Hukum dan Ham Wara Sains*. Vol. 2 No. 6. Hlm 521. doi; <https://doi.org/10.58812/jhhws.v2i6.447>.

memengaruhi, mengeksploitasi, atau mengganggu mekanisme kerja algoritma suatu platform digital guna memperoleh keuntungan tertentu atau menimbulkan dampak tertentu yang bertentangan dengan tujuan sistem tersebut. Dalam konteks TikTok, algoritma berfungsi untuk mengatur distribusi konten, menentukan konten yang muncul dalam fitur *For You Page* (FYP), serta mengelola interaksi pengguna berdasarkan parameter tertentu seperti waktu tonton, tingkat interaksi, dan preferensi pengguna.⁴⁴

Algoritma TikTok secara yuridis dapat diposisikan sebagai bagian dari *sistem elektronik* sebagaimana dimaksud dalam Pasal 1 angka 5 UU ITE, yang mendefinisikan sistem elektronik sebagai serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. Dengan demikian, setiap upaya yang secara sengaja mengganggu atau memanipulasi cara kerja algoritma TikTok pada dasarnya merupakan bentuk intervensi terhadap sistem elektronik.⁴⁵

Dalam praktik, manipulasi algoritma di TikTok dapat dilakukan melalui berbagai modus operandi, antara lain: penggunaan bot untuk meningkatkan jumlah tayangan, *likes*, dan pengikut; pemanfaatan *click*

⁴⁴ Wulandari, Cahya. "Perkembangan Algoritma di Media Sosial: Tiktok Sebagai Pemimpin Tren Konten." *Kumparan*, 24 Oktober 2024.

⁴⁵ Edmon Makarim. 2005. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Depok: RajaGrafindo Persada, hlm. 179-181.

farm atau *engagement farm*; rekayasa metadata seperti *hashtag stuffing* dan *misleading caption*; eksploitasi celah sistem rekomendasi (*algorithm gaming*); serta penggunaan kecerdasan buatan untuk menghasilkan interaksi semu atau konten manipulatif seperti *deepfake*. Modus-modus tersebut menunjukkan bahwa manipulasi algoritma bukanlah fenomena abstrak, melainkan praktik konkret yang memiliki implikasi hukum.⁴⁶

Untuk merumuskan dan menguraikan manipulasi algoritma sebagai sebuah ancaman dan tantangan dalam mencapai integritas ruang digital, maka perlu untuk mengetahui karakteristiknya secara yuridis yang diuraikan sebagai berikut:

1. Dilakukan secara sengaja dan terencana

Manipulasi algoritma pada umumnya tidak terjadi secara kebetulan atau tanpa kesadaran pelaku. Tindakan ini dilakukan secara sadar, terencana, dan bertujuan, misalnya untuk meningkatkan popularitas akun secara artifisial, memengaruhi opini publik, atau memperoleh keuntungan ekonomi dari monetisasi konten. Unsur kesengajaan (*dolus*) ini memenuhi salah satu syarat utama pertanggungjawaban pidana, yakni adanya kehendak dan

⁴⁶ Amran Nur Sahid. 2024. " Peran Media Sosial dalam Memerangi Disinformasi di Indonesia: Tanggung Jawab Hukum dan Etis Penyelenggara Sistem Elektronik. *HARISA: Jurnal Hukum, Syariah, dan Sosial*. Vol. 1 No. 2. doi; <https://ejournal.eddhucenter.com/index.php/harisa/article/view/38>.

pengetahuan dari pelaku atas akibat yang ditimbulkan oleh perbuatannya.⁴⁷

Kesengajaan tersebut dapat dibuktikan melalui penggunaan perangkat lunak otomatis, layanan pihak ketiga penyedia bot, atau skema *click farm* yang secara eksplisit dirancang untuk memanipulasi metrik algoritmik. Dengan demikian, manipulasi algoritma tidak dapat dipandang sebagai kelalaian teknis semata, melainkan sebagai tindakan yang secara sadar diarahkan untuk mengelabui sistem elektronik.⁴⁸

2. Menggunakan sarana sistem elektronik secara tidak sah

Karakteristik berikutnya adalah bahwa manipulasi algoritma dilakukan dengan memanfaatkan sistem elektronik secara tidak sah. Perbuatan ini dapat berupa akses tanpa hak ke fitur tertentu, penyalahgunaan antarmuka pemrograman aplikasi (API), eksploitasi bug atau celah keamanan, serta penggunaan perangkat lunak otomatis yang bertentangan dengan ketentuan penggunaan platform.⁴⁹

Dalam perspektif UU ITE, karakteristik ini relevan dengan Pasal 30 ayat (1) UU ITE yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem

⁴⁷ Loso Judijanto, dkk. 2025. Criminal Law Arrangements in Handling the Spread of Social Media Bot-Based False Information in Indonesia. *ESLHR*. Vol. 3 No. 2. Hlm 110-117. doi: <https://doi.org/10.58812/eslhr.v3i02.469>.

⁴⁸ Devi Rahma Fatmala, dkk. 2024. Penggunaan Akun Bot Media Sosial untuk Mempengaruhi Opini Publik: Sebuah Tinjauan Hukum di Indonesia. *Ajudikasi: Jurnal Ilmu Hukum*. Vol. 4 No. 1. Hlm 55–68. doi: <https://doi.org/10.30656/ajudikasi.v4i1.2210>.

⁴⁹ Lani Zihan Ayustin, Perbuatan Pidana Mengakses Tanpa Hak Ke Sistem Elektronik Orang Lain Menurut Undang-Undang No.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Skripsi, Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, 2022).

elektronik milik orang lain.⁵⁰ Apabila akses tersebut mengakibatkan perubahan atau gangguan terhadap sistem, maka dapat dikenai sanksi pidana sebagaimana diatur dalam Pasal 46 UU ITE. Meskipun norma ini belum secara eksplisit menyebut algoritma, algoritma sebagai bagian dari sistem elektronik dapat dimasukkan ke dalam ruang lingkup perlindungan norma tersebut.⁵¹

3. Mengakibatkan perubahan atau gangguan pada integritas sistem

Manipulasi algoritma pada hakikatnya bertujuan untuk mengubah cara kerja normal sistem rekomendasi TikTok. Akibatnya, terjadi distorsi terhadap hasil distribusi konten, ketidakadilan dalam visibilitas akun, serta rusaknya prinsip keaslian interaksi pengguna. Perubahan ini menunjukkan adanya gangguan terhadap integritas sistem elektronik. Sebagaimana yang telah ditetapkan dan diatur secara eksplisit dalam pasal 3 huruf a dan pasal 4 ayat (1) Peraturan Menkominfo 5 Tahun 2020 yang mengatur kewajiban platform digital termasuk Tiktok, serta menjaga keandalan, keamanan, dan fungsi normal sistem elektronik.⁵²

Karakteristik ini berkaitan dengan Pasal 32 UU ITE yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan

⁵⁰ Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

⁵¹ Camelia Billah Puteri, ANALISIS PUTUSAN HAKIM TERHADAP TINDAK PIDANADALAM MENGAkses SISTEM ELEKTRONIK ORANG LAIN TANPA HAK Studi Putusan Nomor 9/Pid.Sus/2021/PN Pli). (Skripsi, Fakultas Hukum Universitas Malikussaleh, 2025).

⁵² Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

hukum mengubah, menambah, mengurangi, mentransmisikan, merusak, menghilangkan, memindahkan, atau menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik. Selain itu, Pasal 33 UU ITE melarang perbuatan yang mengakibatkan terganggunya sistem elektronik sehingga tidak bekerja sebagaimana mestinya. Meskipun norma ini berfokus pada data dan sistem secara umum, manipulasi algoritma dapat dipandang sebagai bentuk gangguan terhadap logika pemrosesan sistem elektronik.⁵³

4. Menghasilkan informasi elektronik yang menyesatkan atau palsu

Manipulasi algoritma seringkali menciptakan interaksi semu (*fake engagement*) yang menimbulkan persepsi publik seolah-olah suatu konten atau akun memiliki tingkat popularitas dan legitimasi yang tinggi. Dalam konteks ini, informasi elektronik yang ditampilkan kepada pengguna tidak lagi mencerminkan kondisi yang sebenarnya, melainkan hasil rekayasa.⁵⁴

Karakteristik ini relevan dengan Pasal 35 UU ITE yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data yang

⁵³ Maharani Dwi Lestari, dkk. 2025. PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN CYBERCRIME DI INDONESIA. *De Juncto Delicti: Journal Of Law*. Vol. 5 No. 2. Hlm 29. doi; <https://doi.org/10.35706/djd.v5i2.8024>.

⁵⁴ Dean Mulya Armanda, dkk. 2025. Filter Bubble dan Echo Chamber: Pengaruh Algoritma Media Sosial terhadap Pola Konsumsi Informasi Mahasiswa Universitas Lampung. *Jurnal Ilmu Komunikasi dan Sosial Politik*. Vol. 2 No. 4. hlm 1124 doi; <https://doi.org/10.62379/jiksp.v2i4.2669>.

otentik.⁵⁵ Selain itu, apabila manipulasi tersebut menimbulkan kerugian konsumen, maka dapat pula dikaitkan dengan Pasal 28 ayat (1) UU ITE mengenai penyebaran informasi menyesatkan yang merugikan konsumen dalam transaksi elektronik.⁵⁶

5. Menimbulkan kerugian nyata atau potensial

Manipulasi algoritma menimbulkan berbagai bentuk kerugian, baik yang bersifat nyata maupun potensial. Kerugian tersebut dapat berupa kerugian ekonomi bagi kreator lain yang tersisih dari distribusi konten, kerugian pengguna akibat misinformasi, kerugian reputasi platform, serta distorsi pasar digital. Kerugian ini menunjukkan bahwa manipulasi algoritma bukan sekadar pelanggaran etika platform, melainkan perbuatan yang berdampak pada kepentingan hukum yang dilindungi. Dalam hukum pidana, unsur akibat hukum ini penting untuk memenuhi karakter delik materiil, khususnya dalam konteks pasal-pasal UU ITE yang mensyaratkan adanya akibat tertentu.⁵⁷

6. Bertentangan dengan prinsip iktikad baik dan tata Kelola digital

Pasal 3 UU ITE menegaskan bahwa pemanfaatan teknologi informasi harus dilakukan berdasarkan asas kepastian hukum,

⁵⁵ Yolanda Sari KS, dkk. 2022. Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Studi Putusan No. 542/Pid.Sus/2019/PN.Mlg. *Locus: Jurnal Konsep Ilmu Hukum*. Vol. 2 No. 2. hlm 55. doi; <https://doi.org/10.56128/jkih.v2i2.22>.

⁵⁶ Firda Laily Mufid dan Tioma Roniuli Hariandja, 2019. Efektivitas Pasal 28 Ayat (1) UU ITE tentang Penyebaran Berita Bohong (Hoax). *Jurnal Rechtsens*. Vol. 8 No. 2. hlm 181. doi; <https://doi.org/10.36835/rechtsens.v8i2.533>.

⁵⁷ Astried Silvanie, dkk. 2024. Tinjauan Komprehensif tentang Dampak Algoritma Media Sosial. *Madani: Jurnal Ilmiah Multidisiplin*. Vol. 2 No. 8. hlm 191-192. doi; [10.5281/zenodo.13253688](https://doi.org/10.5281/zenodo.13253688).

manfaat, kehati-hatian, itikad baik, dan kebebasan memilih teknologi. Selain itu, Pasal 15 ayat (1) dan ayat (2) UU ITE mewajibkan Penyelenggara Sistem Elektronik untuk menyelenggarakan sistem yang andal, aman, dan bertanggung jawab. Hal ini menegaskan bahwa Manipulasi algoritma bertentangan secara langsung dengan prinsip-prinsip tersebut, sehingga memperkuat sifat melawan hukum secara materiil.⁵⁸

Berdasarkan karakteristik perbuatan manipulasi algoritma sebagaimana telah diuraikan sebelumnya, praktik manipulasi algoritma pada platform TikTok secara normatif dapat dipetakan ke dalam beberapa ketentuan pidana dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah. Pertama, apabila manipulasi dilakukan melalui akses tidak sah ke dalam sistem atau infrastruktur algoritmik TikTok, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana akses tanpa hak sebagaimana dimaksud dalam Pasal 30 jo. Pasal 46 UU ITE.⁵⁹

Kedua, dalam hal manipulasi algoritma dilakukan dengan cara mengubah, merusak, atau memanipulasi parameter pemrosesan data dan distribusi konten sehingga memengaruhi integritas informasi

⁵⁸ Komang Febrinayanti Dantes. 2024. Pengaturan Sistem Elektronik dalam Pengambilan Keputusan Rapat Umum Pemegang Saham (RUPS) Perseroan Terbatas Yang Berkepastian. *Jurnal Komunikasi Hukum* 8 (1): 529. <https://doi.org/10.23887/jkh.v8i1.50941>.

⁵⁹ Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

elektronik, perbuatan tersebut relevan dengan ketentuan Pasal 32 jo. Pasal 48 UU ITE.⁶⁰

Ketiga, apabila manipulasi algoritma menyebabkan terganggunya fungsi normal sistem rekomendasi, distribusi konten, atau layanan platform secara keseluruhan, maka perbuatan tersebut dapat dipertimbangkan sebagai gangguan terhadap sistem elektronik sebagaimana diatur dalam Pasal 33 jo. Pasal 49 UU ITE.⁶¹

Keempat, manipulasi algoritma yang bertujuan menciptakan tampilan popularitas semu, visibilitas konten palsu, atau representasi informasi elektronik seolah-olah autentik dan sah, dapat dikualifikasikan sebagai perbuatan manipulasi informasi elektronik agar dianggap otentik sebagaimana dimaksud dalam Pasal 35 jo. Pasal 51 UU ITE.⁶²

Kelima, apabila dampak manipulasi algoritma tersebut berujung pada penyajian informasi menyesatkan yang menimbulkan kerugian bagi konsumen atau pengguna platform, maka perbuatan tersebut juga beririsan dengan ketentuan Pasal 28 ayat (1) UU ITE.⁶³

Meskipun demikian, penerapan pasal-pasal tersebut terhadap perbuatan manipulasi algoritma pada hakikatnya masih bersifat analogis dan ekstensif, mengingat UU ITE belum secara eksplisit menjadikan algoritma sebagai objek hukum mandiri yang dilindungi.

⁶⁰ Ibid., Pasal 32 ayat (1)-(2) jo. Pasal 46 ayat (1)-(3).

⁶¹ Ibid., Pasal 33 jo. Pasal 49.

⁶² Ibid., Pasal 35 jo. Pasal 51 ayat (1).

⁶³ Ibid., Pasal 28 ayat (1).

Akibatnya, konstruksi pertanggungjawaban pidana terhadap manipulasi algoritma masih harus ditarik melalui penafsiran terhadap konsep sistem elektronik, informasi elektronik, dan dokumen elektronik sebagaimana dirumuskan dalam UU ITE, sehingga menimbulkan keterbatasan normatif dalam menjangkau kompleksitas teknis dan dampak sosial dari praktik manipulasi algoritma di platform digital seperti TikTok.⁶⁴

Sementara itu, dari sudut Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pada dasarnya tidak mengatur secara eksplisit mengenai tindak pidana manipulasi algoritma. Namun demikian, regulasi ini menempatkan penyelenggara sistem elektronik (PSE), termasuk platform digital seperti TikTok, dalam kerangka kewajiban teknis dan tata kelola sistem elektronik yang bersifat preventif dan akuntabel.

PP 71 Tahun 2019 mewajibkan setiap PSE untuk menyelenggarakan sistem elektronik yang andal, aman, dan bertanggung jawab, serta menjamin perlindungan terhadap hak-hak pengguna. Selain itu, PSE juga diwajibkan untuk menyediakan rekam jejak audit (audit trail) atau log sistem guna kepentingan pengawasan dan penegakan hukum, serta bertanggung jawab atas tersedianya fitur-fitur koreksi, pembatalan, dan konfirmasi ulang sebagai bagian

⁶⁴ Budi Suhariyanto. 2014. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: RajaGrafindo Persada, hlm. 70-78.

dari mekanisme pengendalian sistem elektronik, termasuk dalam konteks sistem rekomendasi atau algoritma konten.

Dengan demikian, meskipun PP 71 Tahun 2019 tidak merumuskan delik pidana tersendiri mengenai manipulasi algoritma, regulasi ini memperkuat kewajiban normatif PSE dalam mencegah penyalahgunaan sistem elektronik. Apabila algoritma suatu platform diprogram atau dimanfaatkan secara sengaja untuk tujuan yang melawan hukum, seperti memanipulasi data penggunaan atau informasi publik, dan perbuatan tersebut memenuhi unsur delik dalam Undang-Undang Informasi dan Transaksi Elektronik atau Kitab Undang-Undang Hukum Pidana, maka PSE dan/atau pelaku yang bertanggung jawab secara langsung dapat diminta pertanggungjawaban pidana, sementara PP 71 Tahun 2019 berfungsi sebagai dasar penguatan kewajiban teknis dan administratif dalam rangka pencegahan serta pembuktian penyalahgunaan sistem elektronik.⁶⁵

Dalam perspektif Kitab Undang-Undang Hukum Pidana yang baru sebagaimana diatur dalam Undang-Undang Nomor 1 Tahun 2023, perbuatan manipulasi algoritma di platform TikTok memang belum dirumuskan sebagai delik khusus. Namun demikian, perbuatan tersebut tetap dapat dikualifikasikan sebagai tindak pidana melalui

⁶⁵ Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (LN RI Tahun 2019 Nomor 185, TLN RI Nomor 6400).

pendekatan terhadap delik-delik umum yang telah diperbarui dan diperluas cakupannya dalam KUHP Baru.⁶⁶

Salah satu pasal yang relevan adalah Pasal 492 KUHP Baru tentang penipuan. Pasal ini mengatur bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai tipu muslihat atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang, memberi utang, atau menghapuskan piutang, dapat dipidana karena penipuan.⁶⁷

Dalam konteks manipulasi algoritma TikTok, rekayasa terhadap sistem rekomendasi atau distribusi konten dapat diposisikan sebagai bentuk tipu muslihat digital, misalnya dengan membuat suatu konten tampak populer secara organik padahal sebenarnya direkayasa, memalsukan tingkat keterlibatan (engagement) agar pengiklan bersedia membayar lebih mahal, atau menyajikan metrik performa palsu kepada mitra bisnis. Apabila rekayasa algoritmik tersebut mendorong pihak lain untuk mengambil keputusan ekonomi yang merugikan, seperti memasang iklan atau membayar jasa promosi berdasarkan data yang menyesatkan, maka unsur-unsur penipuan

⁶⁶Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842).

⁶⁷ Ibid., Pasal 492, yang merumuskan delik penipuan sebagai perbuatan menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu, martabat palsu, tipu muslihat, atau rangkaian kebohongan yang menggerakkan orang lain untuk menyerahkan barang, memberi utang, atau menghapuskan piutang.

dalam Pasal 492 KUHP Baru secara substansial dapat dianggap terpenuhi.⁶⁸

Selain penipuan, manipulasi algoritma juga dapat dikaitkan dengan konsep pemalsuan dalam arti fungsional sebagaimana berkembang dalam KUHP Baru. Meskipun KUHP Baru tidak lagi membatasi pemalsuan hanya pada “surat” dalam arti fisik, konsep ini diperluas untuk mencakup data atau informasi yang memiliki nilai pembuktian atau akibat hukum. Dengan demikian, manipulasi algoritma yang menghasilkan metrik interaksi palsu, statistik keterlibatan fiktif, atau representasi digital yang tidak sesuai dengan keadaan yang sebenarnya dapat dipandang sebagai bentuk pemalsuan informasi.⁶⁹

Apabila data atau representasi digital tersebut dipakai seolah-olah benar dan digunakan untuk memperoleh keuntungan atau menimbulkan akibat hukum tertentu, maka perbuatan tersebut secara dogmatis dapat diposisikan sebagai pemalsuan “realitas digital”. Dalam hal ini, objek yang dipalsukan bukan lagi dokumen konvensional, melainkan konstruksi data dan informasi yang membentuk persepsi serta keputusan hukum atau ekonomi pihak lain.⁷⁰

⁶⁸ Muladi dan Barda Nawawi Arief. 2010. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni, hlm. 132-138.

⁶⁹ Wirjono Prodjodikoro. 2012. *Tindak-Tindak Pidana Tertentu di Indonesia*. Bandung: Refika Aditama, hlm. 123-129.

⁷⁰ MOHD. Yusuf DM, dkk. 2022. Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime). *Jurnal Pendidikan dan Konseling*. Vol. 4 No. 6. doi; <https://doi.org/10.31004/jpdk.v4i6.9365>.

Lebih lanjut, manipulasi algoritma juga relevan dengan ketentuan mengenai perbuatan curang dalam kegiatan usaha sebagaimana diatur dalam Pasal 500 sampai dengan Pasal 502 KUHP Baru. Ketentuan ini pada prinsipnya menjerat setiap orang yang melakukan perbuatan curang yang menyesatkan pihak lain dalam hubungan ekonomi atau perdagangan dan menimbulkan kerugian.

Dalam ekosistem platform digital seperti TikTok, manipulasi algoritma dapat digunakan untuk menyesatkan konsumen, mengelabui pengiklan, atau memanipulasi pasar perhatian (*attention economy*) dengan cara mengangkat atau menurunkan visibilitas konten secara tidak wajar demi keuntungan tertentu. Apabila perbuatan tersebut dilakukan secara sistematis dan berdampak pada kerugian ekonomi pihak lain, maka manipulasi algoritma tersebut dapat dikualifikasikan sebagai perbuatan curang dalam kegiatan usaha menurut KUHP Baru.⁷¹

Di samping itu, Pasal 485 KUHP Baru tentang perbuatan melawan hukum yang menimbulkan kerugian juga memberikan dasar normatif untuk menjerat manipulasi algoritma. Pasal ini mengatur bahwa setiap orang yang dengan sengaja melakukan perbuatan melawan hukum yang menimbulkan kerugian bagi orang lain dapat dipidana.

⁷¹ Danny Kinarta dan Wiend Sakti Mieharto. 2025. Tindak Pidana Penipuan Diskon Palsu dalam E-Commerce: Kajian Hukum dan Perlindungan Konsumen di Indonesia. *Humaniorum*. Vol. 3 No. 2. doi; [10.37010/hmr.v3i2.113](https://doi.org/10.37010/hmr.v3i2.113).

Dalam konteks TikTok, manipulasi algoritma yang melanggar hak pengguna atas informasi yang benar, merugikan reputasi atau penghasilan kreator lain, atau menimbulkan kerugian bagi pengiklan dan mitra bisnis dapat diposisikan sebagai delik kerugian umum. Karakteristik utama yang membuat manipulasi algoritma relevan secara pidana dalam kerangka ini adalah adanya unsur kesengajaan, adanya perbuatan melawan hukum berupa rekayasa sistem yang menyesatkan, serta timbulnya akibat berupa kerugian nyata atau potensi kerugian yang dapat dipertanggungjawabkan secara hukum.⁷²

Terakhir, KUHP Baru juga membuka ruang pertanggungjawaban pidana korporasi sebagaimana diatur dalam Pasal 45 sampai dengan Pasal 50. Ketentuan ini menegaskan bahwa badan hukum dapat dimintai pertanggungjawaban pidana atas tindak pidana yang dilakukan oleh pengurus, atas perintah pimpinan, atau untuk kepentingan korporasi.⁷³

Dalam konteks manipulasi algoritma TikTok, apabila rekayasa algoritmik dilakukan oleh pengurus perusahaan, diperintahkan oleh manajemen, atau dimaksudkan untuk meningkatkan keuntungan korporasi, maka pertanggungjawaban pidana tidak hanya dapat

⁷² Faisal Santiago dan Endro Satoto. 2024. Obstacles and Solutions in Law Enforcement Against the Crime of Electronic Data and Information Falsification. *Jurnal Indonesia Sosial Sains*. Vol. 5 No.1. hlm. 18-26. doi; <https://doi.org/10.59141/jiss.v5i1.937>.

⁷³ Joko Sriwido dan M.S. Tumanggor. 2024. Regulation of Corporate Criminal Liability According To Law Number 1 Year 2023 On The Criminal Code. *Krtha Bhayangkara*. Vol. 18 No. 1. hlm. 45-50. doi; <https://doi.org/10.31599/krtha.v18i1.1650>.

dibebankan kepada individu pelaku, tetapi juga kepada korporasi sebagai subjek hukum. Dengan demikian, manipulasi algoritma tidak hanya dipandang sebagai penyimpangan teknis, melainkan sebagai perbuatan yang dapat menimbulkan tanggung jawab pidana korporasi dalam kerangka KUHP Baru.⁷⁴

Berdasarkan uraian diatas, terdapat putusan pengadilan yang telah mengadili sebuah perkara tentang perbuatan manipulatif dalam konteks digital melalui instrumen sistem informasi. Dimana putusan oleh Pengadilan Negeri Jakarta Pusat Nomor 442/Pid.Sus/2024 yang menyatakan terdakwa melakukan manipulasi terhadap informasi dan/atau dokumen elektronik melalui sistem elektronik yang fokus pemeriksaan hakim tidak diarahkan pada bentuk fisik data, melainkan pada proses pengolahan dan perubahan informasi secara digital. Majelis hakim menafsirkan unsur “manipulasi” sebagai suatu perbuatan rekayasa yang dilakukan secara sengaja dan tanpa hak melalui sistem elektronik, dengan tujuan mengubah makna, fungsi, atau dampak informasi elektronik, baik melalui penambahan, pengurangan, penghilangan, pengaburan, maupun pengaturan ulang data. Penafsiran ini menegaskan bahwa pembuktian delik manipulasi tidak mensyaratkan adanya kerusakan sistem secara total, melainkan cukup dibuktikan adanya intervensi terhadap logika kerja atau hasil pemrosesan informasi elektronik. Atas dasar tersebut, hakim

⁷⁴ Ananda Chrisna D. Pandjaitan. 2024. Pembaharuan Hukum Pertanggungjawaban Pidana dalam Tindak Pidana Ekonomi. Yustitia. Vol. 16 No. 2. doi; <https://doi.org/10.62279/yustitia.v16i2.972>.

menerapkan Pasal 32 juncto Pasal 48 UU ITE, yang menempatkan perbuatan manipulatif terhadap hasil kerja sistem elektronik sebagai inti delik.⁷⁵

Majelis hakim menegaskan bahwa manipulasi tidak terbatas pada kerusakan fisik sistem elektronik, melainkan mencakup setiap bentuk rekayasa yang disengaja terhadap informasi elektronik melalui sistem elektronik yang berdampak pada perubahan makna, fungsi, atau konsekuensi dari informasi tersebut. Penafsiran ini menempatkan proses pemrosesan data otomatis sebagai objek perlindungan hukum pidana, sehingga setiap intervensi terhadap logika kerja sistem elektronik dapat dikualifikasikan sebagai perbuatan melawan hukum.

Dalam konteks manipulasi algoritma pada platform TikTok, algoritma rekomendasi berfungsi sebagai sistem elektronik yang secara otomatis mengolah data pengguna untuk menentukan distribusi dan visibilitas konten. Oleh karena itu, setiap intervensi yang disengaja terhadap mekanisme algoritmik, baik melalui pengaturan internal, rekayasa teknis, maupun pemberian sistematis yang mengubah jangkauan, prioritas, atau dampak suatu konten dapat dipahami sebagai bentuk manipulasi informasi elektronik sebagaimana dimaksud dalam UU ITE. Meskipun hukum pidana positif Indonesia belum mengatur manipulasi algoritma secara eksplisit, putusan ini

⁷⁵ Geraldo Juwandi Kamu. 2025. "KAJIAN YURIDIS MEMBANTU MELAKUKAN TINDAK PIDANA MANIPULASI INFORMASI ATAU DOKUMEN ELEKTRONIK (PUTUSAN PN JAKARTA PUSAT No. 442/PID.SUS/2024/PN JKT.PST)". *Lex Privatum* 15 (4).

memberikan dasar yurisprudensial bahwa praktik manipulasi algoritmik dapat dianalisis dan dipertanggungjawabkan secara pidana melalui konstruksi delik manipulasi sistem elektronik. Dengan demikian, putusan tersebut memperkuat argumentasi bahwa kekosongan norma eksplisit mengenai algoritma bukan berarti ketiadaan pertanggungjawaban pidana, melainkan menunjukkan perlunya pembaruan hukum agar pengaturan terhadap penyalahgunaan algoritma oleh platform digital, termasuk TikTok sebagai korporasi, memperoleh kepastian dan kejelasan hukum yang lebih memadai.

Berdasarkan uraian di atas, dijabarkan bahwasanya perbuatan manipulasi algoritma pada platform TikTok memiliki karakteristik berupa tindakan yang dilakukan secara sengaja, memanfaatkan sistem elektronik secara tidak sah, mengganggu integritas algoritma, menghasilkan informasi elektronik yang menyesatkan, serta menimbulkan kerugian nyata maupun potensial. Meskipun sejumlah pasal dalam UU ITE dapat digunakan untuk mengkualifikasikan perbuatan tersebut sebagai tindak pidana, pengaturannya masih bersifat tidak langsung dan belum menjadikan algoritma sebagai objek perlindungan hukum yang berdiri sendiri.

Oleh sebab itu, pada realitas yang ada menunjukkan bahwa terdapat kekosongan norma dalam hukum pidana siber Indonesia terkait manipulasi algoritma. Pertama, algoritma belum diakui sebagai objek hukum tersendiri. Kedua, delik-delik UU ITE masih berorientasi

pada data dan sistem, bukan pada logika pemrosesan. Ketiga, pembuktian unsur kausalitas dan niat jahat dalam manipulasi algoritma sangat kompleks karena melibatkan aspek teknis yang sulit diverifikasi secara forensik. Keempat, belum terdapat rezim akuntabilitas algoritmik dalam hukum pidana Indonesia. Kondisi ini menguatkan bahwa manipulasi algoritma belum sepenuhnya terakomodasi secara memadai dalam rezim hukum pidana siber Indonesia.

B. Pertanggungjawaban Pidana atas Manipulasi Algoritma pada Platform TikTok dalam Hukum Pidana Positif Indonesia

Manipulasi algoritma pada platform TikTok merupakan fenomena hukum yang lahir dari perkembangan teknologi informasi dan sistem pemrosesan data berbasis kecerdasan buatan. Dalam hukum pidana positif Indonesia, perbuatan semacam ini belum diatur secara eksplisit sebagai delik tersendiri. Namun demikian, manipulasi algoritma tidak dapat dipandang berada di luar jangkauan hukum pidana, karena dilakukan melalui sistem elektronik yang berdampak pada kepentingan hukum masyarakat, seperti keadilan distribusi informasi, perlindungan konsumen digital, dan hak atas informasi yang tidak dimanipulasi.

Secara konseptual, hukum pidana Indonesia masih bertumpu pada perbuatan manusia sebagai pusat pertanggungjawaban. Algoritma dipandang sebagai alat atau sarana, bukan sebagai subjek maupun objek hukum pidana yang berdiri sendiri. Akibatnya,

manipulasi algoritma hanya dapat dijangkau secara tidak langsung melalui perbuatan manusia yang mengendalikan, merancang, atau memanfaatkan sistem tersebut.⁷⁶

Kondisi ini menunjukkan bahwa kedudukan manipulasi algoritma dalam sistem hukum pidana positif Indonesia masih bersifat implisit dan fragmentaris. Ia tidak hadir sebagai konsep normatif yang utuh, melainkan tersebar dalam berbagai ketentuan yang mengatur sistem elektronik, penyalahgunaan teknologi, atau perbuatan melawan hukum berbasis digital.

Pertanggungjawaban pidana merupakan konsekuensi yuridis yang dikenakan kepada subjek hukum atas perbuatan yang memenuhi unsur tindak pidana dan dilakukan dengan kesalahan. Dalam hukum pidana Indonesia, pertanggungjawaban pidana berlandaskan asas *geen straf zonder schuld*, yang menegaskan bahwa pemidanaan hanya dapat dijatuhkan apabila terdapat hubungan batin antara pelaku dan perbuatannya. Unsur kesalahan mencakup kesengajaan (*dolus*) maupun kealpaan (*culpa*), sehingga pertanggungjawaban pidana hanya dapat dibebankan apabila perbuatan tersebut dilakukan secara sadar, dapat dipertanggungjawabkan, serta tidak terdapat alasan pembenar atau pemaaf.⁷⁷

⁷⁶ Muhammad Tan Abdul Rahman Haris dan Tantimin. 2022. Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence Di Indonesia. *Jurnal Komunikasi Hukum*. Vol. 8 No. 1, hlm 307-316. Doi: <https://doi.org/10.23887/jkh.v8i1.44408>.

⁷⁷ Amanda Rahmadhani, dkk. 2025. Pertanggungjawaban Pidana. *Jurnal Sahabat ISNU SU*. Vol. 2 No. 1. hlm 74-76. doi; <https://doi.org/10.70826/jsisnu.v2i1>.

Dalam konteks manipulasi algoritma pada platform TikTok, penentuan subjek hukum yang dapat dimintai pertanggungjawaban pidana menjadi isu yang krusial. Subjek hukum tersebut tidak hanya terbatas pada individu, tetapi juga mencakup korporasi sebagai Penyelenggara Sistem Elektronik (PSE). Individu yang berpotensi dimintai pertanggungjawaban antara lain pengembang sistem, operator internal, atau pihak yang dengan kewenangan tertentu melakukan intervensi terhadap logika kerja algoritma.⁷⁸

Hal tersebut sejalan dengan hukum pidana positif Indonesia, dimana subjek hukum pidana tidak hanya terbatas pada orang perseorangan, tetapi juga mencakup korporasi. Perkembangan ini menandai pergeseran dari doktrin klasik *societas delinquere non potest* seiring meningkatnya kompleksitas kejahatan modern, termasuk di bidang teknologi informasi. Pengakuan korporasi sebagai subjek hukum pidana tercermin dalam berbagai peraturan perundang-undangan di luar KUHP, seperti Undang-Undang Informasi dan Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi. Oleh karena itu, dalam konteks platform digital seperti TikTok, baik individu pengendali maupun korporasi sebagai entitas hukum dapat dimintai pertanggungjawaban pidana.⁷⁹

Pengakuan korporasi sebagai subjek hukum pidana diikuti dengan berkembangnya teori pertanggungjawaban pidana korporasi,

⁷⁸ Ibid..

⁷⁹ Ragil Surya Prakasa, dkk. 2023. Sistem Pertanggungjawaban Pidana Korporasi Di Indonesia. *Yustisi*. Vol. 10 No. 3. doi; <https://doi.org/10.32832/yustisi.v10i3.18618>.

antara lain teori identifikasi, yang mengatribusikan perbuatan dan kesalahan pengurus kepada korporasi, serta teori *vicarious liability*, yang memungkinkan pemidanaan atas perbuatan pegawai dalam lingkup tugas dan kepentingan korporasi. Selain itu, dikenal pula pendekatan *strict liability* yang tidak mensyaratkan pembuktian kesalahan, meskipun penerapannya dalam hukum pidana Indonesia masih terbatas. Ketiga teori tersebut menunjukkan karakter pertanggungjawaban pidana korporasi yang adaptif dan relevan dalam menganalisis perbuatan manipulasi algoritma pada platform digital.⁸⁰

Dimana TikTok sebagai platform digital berbentuk korporasi memiliki posisi strategis dalam pengelolaan dan pengendalian sistem algoritmik. Dalam hukum pidana positif Indonesia, korporasi telah diakui sebagai subjek hukum pidana, sehingga secara teoritis dimungkinkan untuk membebaskan pertanggungjawaban pidana atas perbuatan manipulasi algoritma yang dilakukan untuk kepentingan atau atas nama korporasi.⁸¹

Permasalahan muncul ketika harus menentukan relasi pertanggungjawaban antara individu dan korporasi. Kompleksitas sistem algoritmik seringkali menyebabkan kaburnya atribusi perbuatan dan kesalahan, sehingga menyulitkan penegak hukum dalam

⁸⁰ Firsyahrina Maharani Rahim. 2026. "Dilema Pertanggungjawaban Pidana Korporasi: Anatomi Kejahatan Lingkungan dalam Industri Pertambangan Indonesia". *Al-Zayn*. 4 (1) : 4623-4624. <https://doi.org/10.61104/alz.v4i1.3894>.

⁸¹ Septi Dyah Tirtawati dan Pujiyono. 2021. Urgensi Pengaturan Mengenai Pertanggungjawaban Pidana Korporasi Dalam Hukum Pidana Di Indonesia. *Gorontalo Law Review*. Vol. 4 No. 1. doi: <https://doi.org/10.32662/golrev.v4i1.1393>.

menunjuk subjek hukum yang paling tepat untuk dimintai pertanggungjawaban pidana.

Sebab, pertanggungjawaban pidana dalam hukum positif Indonesia pada dasarnya mensyaratkan adanya perbuatan, kesalahan, dan kemampuan bertanggung jawab. Dalam kasus manipulasi algoritma, unsur-unsur tersebut harus dikonstruksikan melalui tindakan manusia yang berada di balik sistem algoritmik, baik berupa perbuatan sengaja maupun kelalaian dalam pengelolaan sistem elektronik.⁸²

Hukum pidana positif Indonesia membuka kemungkinan penerapan pertanggungjawaban pidana korporasi, khususnya apabila manipulasi algoritma dilakukan dalam lingkup kegiatan usaha dan memberikan keuntungan bagi korporasi. Bentuk pertanggungjawaban pidana tersebut dapat diarahkan kepada korporasi, pengurus, atau keduanya, sesuai dengan doktrin pertanggungjawaban pidana korporasi yang berkembang.⁸³

Namun demikian, penerapan pertanggungjawaban pidana atas manipulasi algoritma masih menghadapi kesulitan, terutama dalam pembuktian unsur kesalahan dan hubungan kausal antara manipulasi sistem dengan akibat yang ditimbulkan. Hal ini disebabkan oleh sifat algoritma yang kompleks, tertutup, dan seringkali tidak transparan.

⁸² Shulhan Iqbal Nasution. 2025. Mens Rea: Fondasi Pertanggungjawaban Pidana Dalam Sistem Peradilan Di Indonesia. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah*. 7(1).

⁸³ Kuku Dwi Kurniawan dan Dwi Ratna Indri Hapsari. 2022. Pertanggungjawaban Pidana Korporasi Menurut Vicarious Liability Theory. *Jurnal Hukum Ius Quia Iustum*. Vol. 29 No. 2. doi: <https://doi.org/10.20885/iustum.vol29.iss2.art5>.

Selain itu, hukum pidana positif Indonesia belum menyediakan instrumen normatif yang memadai untuk menilai kesalahan dalam konteks pengambilan keputusan otomatis oleh sistem algoritma. Ketergantungan pada konsep kesengajaan dan kelalaian manusia menyebabkan ruang lingkup pertanggungjawaban pidana menjadi sempit dan sulit diterapkan pada kasus manipulasi algoritma yang bersifat struktural.⁸⁴

Keterbatasan norma ini berimplikasi pada terjadinya kekosongan hukum (legal gap), di mana perbuatan manipulasi algoritma yang merugikan kepentingan publik tidak selalu dapat dijerat secara efektif melalui hukum pidana. Keterbatasan normatif dalam menjangkau manipulasi algoritma berdampak langsung pada efektivitas penegakan hukum. Aparat penegak hukum menghadapi kesulitan dalam menentukan dasar hukum, subjek hukum, serta bentuk pertanggungjawaban pidana yang tepat terhadap perbuatan manipulasi algoritma pada platform TikTok.

Ketiadaan pengaturan eksplisit mengenai manipulasi algoritma sebagai delik tersendiri dalam hukum pidana positif Indonesia menimbulkan implikasi langsung terhadap penerapan asas legalitas, yang menegaskan bahwa suatu perbuatan hanya dapat dipidana apabila telah dirumuskan secara jelas dalam peraturan perundang-

⁸⁴ Anggil Syahra Putri Mecca, dkk. 2025. Pemanfaatan Teknologi Kecerdasan Buatan (Artificial Intelligence) Dalam Sistem Peradilan Pidana di Indonesia. *Sostech Jurnal Sosial dan Teknologi*. Vol. 5 No. 6. doi; <https://doi.org/10.59188/jurnalsostech.v5i6.32207>.

undangan sebelum perbuatan tersebut dilakukan. Oleh karena itu, meskipun manipulasi algoritma berpotensi menimbulkan kerugian sosial yang signifikan, pemidanaan tidak dapat dilakukan secara serta-merta tanpa dasar normatif yang tegas, karena hal tersebut berisiko melanggar prinsip kepastian hukum dan perlindungan terhadap hak subjek hukum.⁸⁵

Kondisi tersebut berpotensi menimbulkan ruang impunitas, di mana perbuatan manipulasi algoritma tidak tersentuh oleh sanksi pidana meskipun menimbulkan kerugian sosial yang signifikan. Hal ini pada akhirnya dapat melemahkan fungsi hukum pidana sebagai sarana perlindungan kepentingan hukum masyarakat di ruang digital.

Akibat kekosongan itu, membuat penegak hukum kerap dihadapkan pada dorongan untuk melakukan perluasan penafsiran terhadap ketentuan pidana yang telah ada, khususnya melalui interpretasi ekstensif atas delik-delik yang berkaitan dengan sistem elektronik, penipuan, atau penyalahgunaan teknologi. Namun secara doktrinal, hukum pidana Indonesia melarang penggunaan analogi untuk menciptakan delik baru, karena analogi bertentangan dengan asas legalitas dan dapat membuka ruang kriminalisasi yang tidak terkendali. Oleh sebab itu, manipulasi algoritma hanya dapat dijangkau sejauh masih berada dalam batas makna wajar norma yang ada, tanpa

⁸⁵ Andi Hamzah. 2022. *Hukum Pidana Indonesia*. Jakarta: Sinar Grafika, hlm 63-66.

menciptakan konstruksi delik baru melalui penafsiran yang melampaui maksud pembentuk undang-undang.⁸⁶

Dari perspektif penegakan hukum, kondisi ini menempatkan hakim dan aparat penegak hukum pada posisi dilematis. Di satu sisi, terdapat tuntutan untuk melindungi kepentingan hukum masyarakat dari dampak manipulasi algoritma yang merugikan, di sisi lain terdapat kewajiban konstitusional untuk menjunjung asas legalitas dan kepastian hukum. Dalam situasi demikian, peran hakim pada dasarnya terbatas pada menemukan hukum (*rechtsvinding*) melalui penafsiran sistematis dan teleologis, bukan menciptakan norma pidana baru. Akibatnya, manipulasi algoritma yang bersifat struktural dan sistemik berpotensi tidak tersentuh hukum pidana, meskipun secara sosiologis memenuhi karakter sebagai perbuatan yang merugikan kepentingan publik.⁸⁷

Dari sudut pandang KUHP baru, konstruksi tindak pidana tetap bertumpu pada pembedaan antara delik formil dan delik materiil. Delik formil menitikberatkan pada larangan atas perbuatan itu sendiri, sehingga tindak pidana dianggap selesai ketika perbuatan dilakukan tanpa mensyaratkan timbulnya akibat tertentu. Sebaliknya, delik materiil mensyaratkan terjadinya akibat yang dilarang sebagai unsur esensial delik, sehingga pembuktian hubungan kausal antara

⁸⁶ Dedi Iskandar, dkk. 2024. Perkembangan Teori dan Penerapan Asas Legalitas dalam Hukum Pidana Indonesia. *JIMMI*. Vol. 1 No. 3. hlm 293-300. doi; <https://doi.org/10.71153/jimmi.v1i3.147>.

⁸⁷ Kritiyadi. 2023. Pergeseran Asas Legalitas Dalam Pembaruan Hukum Pidana Indonesia. *JURDIKUM* 1 (1): 26-30. <https://doi.org/10.59435/jurdikum.v1i1.100>.

perbuatan dan akibat menjadi krusial. Relevansi pembedaan ini dalam konteks manipulasi algoritma terletak pada kesulitan pembuktian kausalitas akibat algoritmik yang bersifat kompleks dan tidak transparan.

Oleh karena itu, pendekatan delik formil dalam hukum pidana positif Indonesia secara teoritis lebih adaptif untuk menjangkau perbuatan manipulasi algoritma, karena fokus pada tindakan intervensi terhadap sistem elektronik sebagai perbuatan yang dilarang, tanpa harus selalu membuktikan akibat sosial atau ekonomi secara langsung. Pendekatan ini sejalan dengan arah pembaruan KUHP yang menekankan perlindungan kepentingan hukum masyarakat terhadap bentuk-bentuk kejahatan modern berbasis teknologi.⁸⁸

Sejalan dengan itu, Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020, yang mensyaratkan pendaftaran sistem elektronik kepada pemerintah Indonesia sebelum beroperasi di wilayah hukum nasional, dimana TikTok sebagai Penyelenggara Sistem Elektronik (PSE) Lingkup Privat memiliki kewenangan penuh dalam pengelolaan sistem dan algoritma yang memengaruhi distribusi informasi kepada pengguna. Kedudukan ini menempatkan TikTok pada posisi strategis sekaligus rentan dimintai pertanggungjawaban hukum apabila pengelolaan algoritma dilakukan secara melawan

⁸⁸ Khaila Aurellia dan Irwan Triadi. 2026. Tinjauan Moralitas Hukum terhadap Overkriminalisasi dalam Regulasi Digital Indonesia. *ALADALAH Jurnal Politik, Sosial, Hukum, dan Humaniora*. Vol. 4 No. 1, hlm 35-36. doi: <https://doi.org/10.59246/aladalah.v4i1.1696>.

hukum dan merugikan kepentingan publik, sehingga kewajiban pendaftaran dan pengawasan PSE berfungsi sebagai instrumen preventif terhadap penyalahgunaan sistem elektronik.⁸⁹

Tindakan ini menegaskan bahwa platform digital tidak hanya beroperasi dalam ranah teknologi, tetapi juga memikul tanggung jawab yuridis untuk memastikan sistem elektroniknya tidak disalahgunakan. Dengan menguasai arsitektur algoritmik dan data pengguna dalam skala, sehingga pertanggungjawaban pidana atas manipulasi algoritma patut dikonstruksikan tidak hanya berdasarkan perbuatan aktif, tetapi juga atas kegagalan korporasi dalam mencegah risiko sistemik dan dampak merugikan yang dapat diperkirakan dari pengelolaan algoritma.⁹⁰

Meskipun belum dirumuskan sebagai delik tersendiri dalam hukum pidana positif Indonesia, perbuatan manipulasi algoritma tetap berada dalam jangkauan pertanggungjawaban pidana sepanjang dapat ditelusuri sebagai hasil intervensi manusia terhadap sistem elektronik yang berpotensi merugikan kepentingan hukum masyarakat. Karena hukum pidana Indonesia masih menempatkan perbuatan manusia sebagai pusat pertanggungjawaban, algoritma diposisikan sebagai sarana yang dikendalikan oleh individu atau korporasi.

⁸⁹ Pricillia Alvionita Yusuf, dkk. 2024. Tanggung Jawab Keamanan Data Oleh Penyelenggara Sistem Elektronik. *Lex Privatum*. Vol. 13 No. 5.

⁹⁰ Shelomita Putri Amelia. 2025. "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna". *STUDIA Jurnal Of Humanities and Education Studies* 1(2): 132-141.

Sehingga korporasi sebagai Penyelenggara Sistem Elektronik dapat dimintai pertanggungjawaban pidana apabila manipulasi algoritma dilakukan dalam lingkup kegiatan usaha dan berada dalam pengendalian strukturalnya, melalui konstruksi teori identifikasi maupun vicarious liability dengan memerhatikan beberapa aspek untuk menyimpulkan bentuk pertanggungjawabannya, apakah hal tersebut dapat dipertanggungjawabkan secara administratif atau lebih dari itu dapat dimintai pertanggungjawaban secara pidana.

Dalam kaitannya dengan uraian diatas, pertanggungjawaban yang paling dimungkinkan ialah kepada individu sebagai pelaku dalam perbuatan manipulasi algoritma, sebab pada perkembangannya apapun yang terjadi dalam ruang digital itu pula yang telah atau sedang terjadi pada ruang konvensional, baik itu subjeknya, medianya, maupun sistemnya semuanya dianggap serupa, tetapi terjadi di dimensi yang berbeda saja. Sehingga, bila berbicara mengenai pertanggungjawabannya, maka yang paling dapat dimintai ialah individunya yang menjalankan suatu sistem yang di eksploitasi.

Dengan demikian, rumusan masalah dapat dijawab bahwa pertanggungjawaban pidana atas manipulasi algoritma TikTok secara teoritis dimungkinkan dalam kerangka hukum pidana positif Indonesia, tetapi dengan memperhatikan pihak-pihak mana yang seharusnya dan diyakini menanggung kesalahan untuk dimintai pertanggungjawaban

baik itu individu, korporasi dalam hal ini pengurus atau pihak sebagai representasi korporasi, maupun keduanya.

Olehnya diperlukan kehati-hatian dalam menentukan siapa yang harus menanggung pertanggungjawaban tersebut untuk menghindari adanya kriminalisasi dalam hal ini, sehingga menghindarinya penegakan hukum yang semena-mena kepada siapapun.

Karena itulah, penelitian ini menegaskan urgensi pembaruan hukum pidana yang mengarah pada penguatan pengaturan sistem elektronik dan algoritma, penajaman pertanggungjawaban pidana korporasi, serta pengembangan pendekatan delik yang lebih adaptif terhadap kejahatan berbasis teknologi, guna menjamin perlindungan kepentingan hukum masyarakat di ruang digital.

BAB V

PENUTUP

A. Kesimpulan

1. Manipulasi algoritma pada platform TikTok merupakan perbuatan melawan hukum yang dilakukan secara sengaja dengan memanfaatkan sistem elektronik secara tidak sah, mengganggu integritas logika pemrosesan algoritmik, serta berpotensi menimbulkan kerugian bagi pengguna dan ekosistem digital. Namun, hukum pidana positif Indonesia belum mengaturnya secara eksplisit, karena berbagai ketentuan yang berelevansi dengan perbuatan ini masih bersifat analogis dan fragmentaris. Hal ini menunjukkan adanya kekosongan norma akibat belum diakuinya algoritma sebagai objek perlindungan hukum pidana tersendiri.
2. Pertanggungjawaban pidana atas perbuatan manipulasi algoritma pada platform TikTok secara teoritis dapat dimintai pada individu atau korporasi, namun paling dimungkinkan dimintai kepada individu, karena ruang digital dikatakan serupa dengan ruang konvensional, yang mana letak perbedaannya hanya pada dimensi terjadinya perbuatannya saja. Sehingga bila berbicara pertanggungjawaban pidana, maka dimintai kepada pelaku yang melakukan suatu kejahatan tadi, yang mana dalam konteks ruang digital, maka pertanggungjawabannya dimintai kepada individu yang menjalankan perbuatan manipulasi.

B. Saran

1. Pembentuk undang-undang perlu melakukan pembaruan dan penguatan kerangka hukum pidana siber dengan merumuskan pengaturan yang secara eksplisit mengakui algoritma sebagai objek hukum yang dilindungi. Pengaturan tersebut sebaiknya mencakup larangan terhadap manipulasi algoritma yang mengganggu integritas, transparansi, dan keadilan sistem digital, serta merumuskan unsur delik yang jelas tanpa bergantung pada penafsiran analogis. Dengan demikian, asas legalitas dan kepastian hukum tetap terjaga, sekaligus memungkinkan penegakan hukum pidana yang lebih efektif terhadap praktik manipulasi algoritma di platform digital.
2. Platform digital seperti TikTok sebagai Penyelenggara Sistem Elektronik Lingkup Privat perlu menerapkan prinsip tata kelola algoritma yang bertanggung jawab, termasuk penerapan prinsip kehati-hatian, itikad baik, transparansi, dan akuntabilitas algoritmik. Hal ini dapat diwujudkan melalui mekanisme pencegahan manipulasi sistem, pengawasan internal yang ketat, pelarangan penggunaan bot dan engagement farm, serta penyediaan mekanisme pengaduan dan koreksi bagi pengguna yang dirugikan. Upaya ini tidak hanya berfungsi sebagai langkah preventif, tetapi juga sebagai bentuk pemenuhan kewajiban hukum PSE.

Penguatan penegakan hukum perlu dilakukan melalui penajaman konsep pertanggungjawaban pidana terhadap individu maupun korporasi dalam perkara manipulasi algoritma, khususnya dengan memperjelas batas peran, kewenangan, dan tingkat pengendalian pelaku terhadap sistem algoritmik yang dimanipulasi. Pertanggungjawaban pidana korporasi harus dirumuskan secara lebih operasional agar dapat menjerat Penyelenggara Sistem Elektronik ketika manipulasi algoritma dilakukan dalam lingkup kegiatan usaha dan untuk kepentingan korporasi, tanpa mengabaikan prinsip kesalahan. Selain itu, peningkatan kapasitas teknis aparat penegak hukum menjadi krusial, terutama dalam bidang forensik digital, audit algoritma, dan pembuktian berbasis sistem elektronik, guna mengatasi kompleksitas dan sifat tertutup algoritma. Dengan demikian, pembuktian unsur kesalahan dan hubungan kausal antara perbuatan dan akibat dapat dilakukan secara lebih akurat, sehingga pemidanaan berlangsung efektif, proporsional, dan tidak berujung pada overkriminalisasi terhadap praktik teknologi yang sah dan inovatif.

DAFTAR PUSTAKA

Al-Qur'an

Q.S. An-Nisa ayat 29

Literatur

Abizar Al Ghiffari. (2025). Kejahatan Siber Dan Tantangan Penegakan Hukum Di Indonesia Koordinasi Dengan Penegakan Pidana Ketika Kasus Kebocoran Data Beririsan Dengan Tindak Bukti Lintas Batas , Terutama Ketika Infrastruktur Serangan Seperti Server , Domain , Atau Dompot Di Ranah So" 02, no. 02: 1295–99.

Amanda Rahmadhani, Ilham Maylandy S Damanik, Ali Rahmadi Batubara, Muhammad Faizil Adib, Naufal Nabil. 2025. "Pertanggungjawaban Pidana." *Jurnal Sahabat ISNU SU* 2 (1): 74-76. doi: <https://doi.org/10.70826/jsisnu.v2i1>.

Amelia dan Ema Nurkhaeni. 2025. "Perlindungan Hak Pengguna dalam Praktik Pengolahan Data oleh Platform TikTok Sebagai Penyelenggara Sistem Eletronik Privat: Analisis Dalam Perspektif Hukum Teknologi Informasi." *Media Hukum Indonesia* 4 (1): 377. doi:<https://doi.org/10.5281/zenodo.17866096>.

Amran Nur Sahid. 2024. "Peran Media Sosial Dalam Memerangi Disinformasi di Indonesia." *HARIS: Jurnal Hukum, Syariah, dan Sosial* 1 (2). doi:<https://ejournal.eddhuhacenter.com/index.php/harisa/article/view/38>.

Ananda Chrisna dan D. Pandjaitan 2024. "Pembaharuan Hukum Pertanggungjawaban Pidana dalam Tindak Pidana Ekonomi." *Yustitia* 16 (2). doi:<https://doi.org/10.62279/yustitia.v16i2.972>.

Andi Hamzah. (2012). *Asas-Asas Hukum Pidana*. Revisi. Jakarta: Rineka Cipta.

Andi Hamzah. 2022. *Hukum Pidana Indonesia*. Jakarta: Sinar Grafika.

Andi Masagena, Muhammad Rinaldy Bima, Rizki Ramadani. (2024). "Urgensi Hukum Tindak Pidana Korupsi Pada Perusahaan Yang Manipulasi Pajak" 1, no. July : 3–4.

Anggil Syahra Putri Mecca, Wahab Aznul Hidayat, Hadi Tuasikal. 2025. "Pemanfaatan Teknologi Kecerdasan Buatan(Artificial Intelligence) Dalam Sistem Peradilan Pidana Di Indonesia." *Sostech: Jurnal*

- Anindya Milagista. "OECD Adalah Singkatan dari Apa? Pengertian, Negara Anggota, Tujuan, Kantor". *Detik.com*. 28 Oktober 2024 . Diakses Januari 13, 2026.
- Astried Silvanie, Rino Subekti, Dwi Sidik Permana, Ari Kurniawan. 2024. "Tinjauan Komprehensif tentang Dampak Algoritma Media Sosial." 2 (8): 191-192. doi:10.5281/zenodo.13253688.
- Barda Nawawi Arief. (2010). *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Modern*. Jakarta: Kencana Prenada Media Group.
- Budi Suhariyanto. 2014. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Raja Grafindo Persada.
- Cahya Wulandari. 2024. "Perkembangan Algoritma di Media Sosial: TikTok Sebagai Pemimpin Tren Konten." *Kumparan*. 24 Oktober. Diakses 12 Januari, 2026.
- Camelia Billah Puteri. 2025. "Analisis Putusan Hakim Terhadap Tindak Pidana dalam Mengakses Sistem Elektronik Orang Lain Tanpa Hak Studi Putusan Nomor 9/Pid.Sus/2021/PN Pli)." Skripsi, Aceh.
- Danny Kinarta dan Wiend Sakti Mieharto. 2025. "Tindak Pidana Penipuan Diskon Palsu dalam E-Commerce: Kajian Hukum dan Perlindungan Konsumen di Indonesia." *Humaniorum* 3 (2). doi:10.37010/hmr.v3i2.113.
- Dzunuwanus Ghulam Manar & Mochammad Jose Akmal. (2021). "Manipulasi Narasi Publik Melalui Akun Bot Dalam Aktivisme Digital Pro-IKN Di Media Sosial X". hal 167–86.
- Dean Mulya Armanda, Dzakia Afaf, Restu Kridahyanto. 2025. "Filter Bubble dan Echo Chamber: Pengaruh Algoritma Media Sosial terhadap Pola Konsumsi Informasi Mahasiswa Universitas Lampung ." *Jurnal Ilmu Komunikasi dan Sosial Politik* 2 (4): 1124. doi: <https://doi.org/10.62379/jiksp.v2i4.2669>.
- Dedi Iskandar, Zulbaidah W.N, Angga Almanda, Iswandi Abdinur, Devi Yanda Putra, Cut Yessi Andriani, Zulhazrul. 2024. "Perkembangan Teori dan Penerapan Asas Legalitas Dalam Hukum Pidana Indonesia." *JIMMI* 1 (3): 293-300. doi:<https://doi.org/10.71153/jimmi.v1i3.147>.

- Devi Rahma Fatmala, Amanda Amelia, Fitri Agustina Trianingsih. 2024. "Penggunaan Akun Bot Media Sosial Untuk Mempengaruhi Opini Publik: Sebuah Tinjauan Hukum di Indonesia." *Ajudikasi: Jurnal Ilmu Hukum* 4 (1): 55-68. doi:<https://doi.org/10.30656/ajudikasi.v4i1.2210>.
- Eddy O.S Hiariej. (2016). *Prinsip-Prinsip Hukum Pidana*. Revisi. Yogyakarta: Cahaya Atma Pustaka.
- Edmon Makarim. 2005. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Depok: RajaGrafindo Persada.
- Faisal Santiago dan Endro Satoto. 2024. "Obstacles and Solutions in Law Enforcement Against the Crime of Electronic Data and Information Falsification." *Jurnal Indonesia Sosial Sains* 5 (1): 18-26. doi:<https://doi.org/10.59141/jjiss.v5i1.937>.
- Firda Laily Mufid dan Tiomi Ronjuli Hariandja. 2019. "Efektivitas Pasal 28 Ayat (1) UU ITE tentang Penyebaran Berita Bohong (Hoax)." *Jurnal Rechtsens* 8 (2): 181. doi:<https://doi.org/10.36835/rechtsens.v8i2.533>.
- Firsyahrina Maharani Rahim. 2026. "Dilema Pertanggungjawaban Pidana Korporasi : Anatomi Kejahatan Lingkungan Dalam Industri Pertambangan." *Al-Zayn* 4 (1): 4623-4624. doi:<https://doi.org/10.61104/alz.v4i1.3894>.
- I Gede Artha. 2026. "Pengaturan Clickwrap Agreement Dalam Sistem Hukum Kontrak Di Indonesia." *Al-Zayn : Jurnal Ilmu Sosial & Hukum* 4 (1): 3846. doi:<https://doi.org/10.61104/alz.v4i1.3728>.
- Geraldo Juwandi Kamu. 2026. KAJIAN YURIDIS MEMBANTU MELAKUKAN TINDAK PIDANA MANIPULASI INFORMASI ATAU DOKUMEN ELEKTRONIK (PUTUSAN PN JAKARTA PUSAT No. 442/PID.SUS/2024/PN JKT.PST)". *Lex Privatum* 15(4).
- Ilham Fikriansyah. (2023). "Algoritma Adalah: Pengertian, Ciri-Ciri, Dan Berbagai Jenisnya". Detikedu. <https://www.detik.com/edu/detikpedia/d-6817970/algoritma-adalah-pengertian-ciri-ciri-dan-berbagai-jenisnya>.
- Ilham Nurfajri, Erlangga Teguh Hadi Pratama, Gilang Septian Tupamahu, Ridwan Saputra, Yusi Erwina. (2025). "Dampak Algoritma AI Terhadap Komunikasi Publik: Memahami Manipulasi Informasi Dan Realitas". *CONVERSE Journal Communication Scienc* 1, no.3:13. <https://doi.org/10.47134/converse.v1i3.3543>

- Joko Sriwidodo dan M.S. Tumanggor. 2024. "Regulation Of Corporate Criminal Liability According To Law Number 1 Year 2023 On The Criminal Code." *Krtha Bhayangkara* 8 (1): 45-50. doi:<https://doi.org/10.31599/krtha.v18i1.1650>.
- Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi. (2021). *Kamus Besar Bahasa Indonesia (Edisi Kelima)*. Jakarta: Badan Pengembangan dan Pembinaan Bahasa.
- Khaila Aurellia dan Irwan Triadi. 2026. "Tinjauan Moralitas Hukum Terhadap Overkriminalisasi dalam Regulasi Digital Indonesia." *ALADALAH: Jurnal Politik, Sosial, Hukum, dan Humaniora* 4 (1): 35-36. doi:<https://doi.org/10.59246/aladalah.v4i1.1696>.
- Komang Febrinayanti Dantes. 2024. "Pengaturan Sistem Elektronik Dalam Pengambilan Keputusan Rapat Umum Pemegang Saham (RUPS) Perseroan Terbatas Yang Berkepastian." *Jurnal Komunikasi Hukum* 8 (1): 529. doi:<https://doi.org/10.23887/jkh.v8i1.50941>.
- Kritayadi. 2023. "Pergeseran Asas Legalitas Dalam Perkembangan Hukum Pidana Indonesia." *JURDIKUM* 1 (1): 26-30. doi:<https://doi.org/10.59435/jurdikum.v1i1.100>.
- Kukuh Dwi Kurniawan dan Dwi Ratna Indri Hapsari. 2022. "Pertanggungjawaban Pidana Korporasi Menurut Vicarious Liability Theory ." *Jurnal Hukum Ius Quia Iustum* 29 (2). doi:<https://doi.org/10.20885/iustum.vol29.iss2.art5>.
- Lani Zihan Austin. 2022. "Perbuatan Pidana Mengakses Tanpa Hak Ke Sistem Elektronik Orang Lain Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik." Skripsi, Medan.
- Loso Judijanto, Irman Putra, Sumarni. 2025. "Criminal Law Agreements in Handling the Spread of Social Media Bot-Based False Information in Indonesia." *ESLHR* 3 (2): 110-117. doi:<https://doi.org/10.58812/eslhr.v3i02.469>.
- Loso Judijanto. (2025). "Hukum Pidana Dan Kejahatan Siber: Menanggulangi Ancaman Kejahatan Digital Di Era Teknologi". 5: 1079–85.
- Maharani Dwi Lestari, Fajar Putra Adiatmoko, Dea Putri Rizkia. 2025. "PERLINDUNGAN HUKUM TERHADAP KORBAN KEJAHATAN CYBERCRIME DI INDONESIA." *De Juncto Delicti: Journal Of Law* 5 (2): 29. doi:<https://doi.org/10.35706/djd.v5i2.8024>.

- Madinah Mokobambang. 2023. "Pemberantasan Tindak Pidana Cyber Di Provinsi Jawa Barat: Peran Hukum dan Tantangan Dalam Penegakan Hukum Terhadap Kejahatan Digital." *Jurnal Hukum dan Ham Wara Sains* 2 (6): 521. doi:<https://doi.org/10.58812/jhhws.v2i6.447>.
- Merdeka.com. (2024). "Apa Itu Manipulasi? Definisi, Jenis, Dan Karakteristiknya Yang Perlu Anda Ketahui". Apa Itu Manipulasi? Definisi, Jenis, dan Karakteristiknya yang Perlu Anda Ketahui.
- Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Revisi. Jakarta: Rineka Cipta.
- Muhammad Aabid Tyas Dzaki & Ibrahim Fikma Edrisy. (2025). "Strategi Pencegahan Kejahatan Siber Di Indonesia: Sinergi Antara UU ITE Dan Kebijakan Keamanan Digital". *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora* 4, no. 2 (2025): 12. <https://ulilalbabinstitute.id/index.php/PESHUM/article/view/8311/6317>.
- Muhammad Tan Abdul Rahman Haris dan Tantimin. 2022. "Analisis Pertanggungjawaban Hukum Pidana Terhadap Pemanfaatan Artificial Intelligence ." *Jurnal Komunikasi Hukum* 8 (1): 307-316. doi:<https://doi.org/10.23887/jkh.v8i1.44408>.
- MOHD. Yusuf Dm, Mona Agustania, Siti Zulaiha. 2022. "Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber(Cyber Crime)." *Jurnal Pendidikan dan Konseling* 4 (6). doi:<https://doi.org/10.31004/jpdk.v4i6.9365>.
- Muladi dan Barda Nawawi Arief. 2010. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni .
- Natanael Hiskia Mongkau, Herlyanty Yuliana A. Bawole, Altje Musa. (2025). "Penegakkan Hukum Terhadap Penyalhgunaan Kecerdasan Buatan Dengan Cara Memanipulasi Wajah Seseorang Ke Dalam Gambar Atau Video Porno". 13, no. 2: 1–23.
- Nurul Aprianti dan Gusti Ayu Ratih Damayanti. 2025. "Negara Hukum Di Era Algoritma: Algoritma Reformulasi Artificial Intelligence Untuk Menjamin Perlindungan Ham Di Indonesia." *Jurnal Hukum Agama Hindu WIDYA KERTA* 8 (2). doi:<https://doi.org/10.53977/wk.v8i2.3312>.
- Prabu Revolusi dan Radians Krisna Febriandy. 2025. "Developing AI Regulations in Indonesia." *Jurnal Indonesia: Manajemen Informatika dan Komunikasi* 6 (2): 1039. doi:<https://doi.org/10.63447/jimik.v6i2.1380>.

- Pricillia Alvionita Yusuf, Donna O. Setiabudhi, Maarthen Y Tampanguma. 2024. "Tanggung Jawab Keamanan Data Oleh Penyelenggara Sistem Elektronik." *Lex Privatum* 13 (5).
- Ragil Surya Prakasa. 2023. "Sistem Pertanggungjawaban Pidana Korporasi Di Indonesia." *Yustisi* 10 (3). doi: <https://doi.org/10.32832/yustisi.v10i3.18618>.
- Rizha Claudilla Putri. (2025). "Dark Patterns Sebagai Bentuk Manipulasi Perilaku Konsumen Digital: Analisis Interdisipliner Terhadap Dampak Psikologis, Hukum, Dan Ekonomi Dari Praktik Desain Manipulatif Dalam Ekosistem E-Commerce Global". *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2: 1066–71. <https://doi.org/10.31004/riggs.v4i2.611>.
- Septi Dyah Tirtawati dan Pujiono. 2021. "Urgensi Pengaturan Mengenai Pertanggungjawaban Pidana Korporasi Dalam Hukum Pidana Di Indonesia." *Gorontalo Law Review* 4 (1). doi:<https://doi.org/10.32662/golrev.v4i1.1393>.
- Shelomita Putri Amelia. 2025. "Tanggung Jawab Hukum Penyelenggara Sistem Elektronik Terhadap Kebocoran Data Pribadi Pengguna." *STUDIA Jurnal Of Humanities and Education Studies* 1 (2): 132-141.
- Sholahuddin Al Fatih. 2025. "Understanding Regulations Of Online Gambling In Indonesia: Is It Forbidden?" *Jurisdictie* 16 (1): 55. doi:<https://doi.org/10.53977/wk.v8i2.3312>.
- Shulhan Iqbal Nasution. 2025. "Mens Rea: Fondasi Pertanggungjawaban Pidana Dalam Sistem Peradilan Di Indonesia." *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekomnomi Syariah* 7 (1). doi:<https://doi.org/10.24252/iqtishaduna.v7i1.61542>.
- Sigid Suseno. 2021. "Penegakan Hukum Terhadap Kejahatan Siber Di Indonesia." *Jurnal Ilmu Hukum* 8 (1): 60-62.
- Sinta Dewi. 2021. *Hukum Perlindungan Data Pribadi* . Bandung: PT. Refika Aditama.
- Wirjono Prodjodikoro. 2012. *Tindak-Tindak Pidana Tertentu di Indonesia*. Bandung: Refika Aditama.
- Yolanda Sari KS, Madiasa Ablisar, Mahmud Mulyadi, Jelly Leviza. 2022. Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce menurut Undand-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik." *Locus: Jurnal*

Konsep Ilmu Hukum 2 (2): 55. doi:<https://doi.org/10.56128/jkih.v2i2.22>.

Yosi Refatalina & Nisa Uljannah. (2025). "Pengaruh Kekerasan Psikologis Terhadap Kesehatan Mental Korban Kekerasan Dalam Rumah Tangga (KDRT) Sebuah Studi Psikologis Dan Hukum". *CBJIS: Cross-Border Journal of Islamic Studies* 7, no. 2 : 361–69. <https://doi.org/10.37567/cbjis.v7i2.4226>.

Yurizal. (2018) *Penegakan Hukum Tindak Pidana Cybercrime Di Indonesia*. Edited by Gideon Soerja. Edisi 1. Malang: Media Nusa Creative.

Zaenal Arifin & Emi Puasahandayani. (2023). *Cybercrime: Menyelisik Penegakan Hukum Dan Penanggulangannya*(Edited by. Zakiyatur Rosidah). Yogyakarta: Deepublish Digital.

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008, Sebagaimana telah diubah ke dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, dimana PP Nomor 71 Tahun 2019 mewajibkan Penyelenggara Sistem Elektronik (PSE)