

Celah Hukum dan Pertanggungjawaban Pidana atas Manipulasi Algoritma TikTok dalam Hukum Pidana Indonesia

Muhammad Iksan Nur Khalish¹, Aan Aswari², Mursyid Mursyid³

¹²³Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Email Koresponden: iksancank040@gmail.com

Abstrak: Penelitian ini bertujuan untuk menganalisis kualifikasi hukum praktik manipulasi algoritma pada platform digital serta menelaah bentuk pertanggungjawaban pidana terhadap pelakunya dalam perspektif hukum pidana Indonesia. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan yuridis normatif yang menitikberatkan pada kajian terhadap norma hukum, doktrin, serta prinsip-prinsip hukum pidana yang berkaitan dengan kejahatan siber. Data penelitian diperoleh melalui studi kepustakaan terhadap berbagai bahan hukum dan literatur ilmiah yang relevan. Kebaruan penelitian ini terletak pada analisis mengenai manipulasi algoritma sebagai bentuk kejahatan digital yang belum diatur secara eksplisit dalam hukum pidana, khususnya dalam konteks platform media sosial berbasis algoritma. Hasil penelitian menunjukkan bahwa manipulasi algoritma merupakan perbuatan yang dilakukan secara sengaja dengan memanfaatkan sistem elektronik secara tidak sah sehingga dapat mengganggu integritas pemrosesan algoritmik dan menimbulkan kerugian bagi pengguna maupun ekosistem digital. Meskipun demikian, pengaturan hukum yang ada masih bersifat interpretatif karena algoritma belum diakui sebagai objek perlindungan hukum pidana secara khusus. Penelitian ini menyimpulkan bahwa pertanggungjawaban pidana atas manipulasi algoritma secara teoritis dapat dikenakan kepada individu maupun korporasi, namun dalam praktiknya lebih memungkinkan diarahkan kepada individu yang secara langsung melakukan intervensi terhadap sistem algoritmik. Kondisi tersebut menunjukkan perlunya penguatan kerangka regulasi yang lebih adaptif terhadap perkembangan teknologi digital guna memberikan kepastian hukum dalam penanggulangan kejahatan berbasis algoritma.

Kata Kunci: Manipulasi Algoritma; Platform Digital; Kejahatan Siber.

Abstract: *This study aims to analyze the legal qualification of algorithm manipulation practices on digital platforms and examine the form of criminal liability for such acts within the perspective of Indonesian criminal law. This research employs a normative legal research method with a juridical–normative approach focusing on the analysis of legal norms, doctrines, and criminal law principles related to cybercrime. The research data were obtained through library research involving various legal materials and relevant scientific literature. The novelty of this research lies in its examination of algorithm manipulation as a form of digital crime that has not been explicitly regulated in criminal law, particularly within algorithm-based social media platforms. The findings indicate that algorithm manipulation constitutes an intentional act carried out by unlawfully exploiting electronic systems, which can disrupt the integrity of algorithmic processing and potentially cause harm to users and the broader digital ecosystem. However, the existing legal framework remains interpretative because algorithms have not yet been recognized as a distinct object of criminal law*

protection. This study concludes that criminal liability for algorithm manipulation can theoretically be imposed on both individuals and corporations, although in practice it is more feasible to attribute liability to individuals who directly conduct interventions within algorithmic systems. These findings highlight the need for a more adaptive regulatory framework to ensure legal certainty in addressing algorithm-based digital crimes.

Keywords: *Algorithm Manipulation; Digital Platforms; Cybercrime.*

A. PENDAHULUAN

Perkembangan teknologi informasi dan media sosial telah mengubah pola interaksi sosial, ekonomi, dan komunikasi masyarakat secara signifikan [1]. Platform digital tidak hanya menjadi sarana berbagi informasi, tetapi juga menjadi ruang aktivitas ekonomi, distribusi konten, serta pembentukan opini publik. Namun, kemajuan tersebut juga melahirkan berbagai bentuk kejahatan baru di ruang siber (*cyber crime*), yang memanfaatkan teknologi informasi sebagai sarana maupun objek kejahatan. Kejahatan siber memiliki karakteristik yang kompleks karena bersifat lintas batas, anonim, dan berlangsung dalam ruang virtual sehingga menimbulkan tantangan dalam proses pembuktian, identifikasi pelaku, serta penentuan yurisdiksi hukum [2], [3].

Salah satu fenomena yang berkembang dalam ekosistem media sosial adalah manipulasi algoritma pada platform digital, termasuk pada TikTok [4], [5]. Platform ini menggunakan algoritma berbasis *machine learning* untuk menentukan distribusi dan rekomendasi konten kepada pengguna [4]. Namun dalam praktiknya, algoritma tersebut sering dimanfaatkan secara tidak sah melalui pembelian pengikut palsu, penggunaan bot untuk meningkatkan jumlah tayangan, ulasan fiktif, maupun praktik click fraud guna meningkatkan visibilitas konten secara tidak wajar. Praktik manipulasi algoritma tersebut berpotensi menimbulkan distorsi informasi, persaingan usaha tidak sehat, serta kerugian bagi pengguna maupun pelaku usaha lain dalam ekosistem digital [6].

Dalam perspektif hukum Indonesia, regulasi utama yang mengatur aktivitas digital adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahan-perubahannya [7]. Meskipun undang-undang ini telah mengatur berbagai bentuk kejahatan siber seperti akses ilegal, penipuan elektronik, dan penyebaran informasi yang merugikan, ketentuan tersebut belum secara eksplisit

mengatur praktik manipulasi algoritma pada platform digital. Akibatnya, fenomena ini menimbulkan ketidakpastian hukum karena penegakan hukum sering kali bergantung pada interpretasi terhadap pasal-pasal yang ada [4], [8] .

Sejumlah penelitian sebelumnya lebih banyak membahas kejahatan siber dalam konteks umum seperti hacking, penipuan digital, atau penyebaran informasi palsu, sementara kajian mengenai manipulasi algoritma dalam perspektif hukum pidana masih relatif terbatas [9]. Kondisi ini menunjukkan adanya kesenjangan penelitian (*research gap*) terkait kualifikasi hukum dan bentuk pertanggungjawaban pidana atas manipulasi algoritma dalam ekosistem platform digital. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kualifikasi hukum praktik manipulasi algoritma pada platform TikTok serta menelaah bentuk pertanggungjawaban pidana terhadap pelaku dalam perspektif hukum pidana Indonesia [10]. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan doktrin hukum pidana siber serta mendukung pembaruan regulasi yang lebih adaptif terhadap perkembangan teknologi digital.

B. METODE

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan yuridis normatif yang berfokus pada kajian terhadap norma hukum yang berlaku terkait kejahatan manipulasi algoritma pada platform digital [11]. Pendekatan ini digunakan untuk menganalisis ketentuan peraturan perundang-undangan, doktrin hukum, serta prinsip-prinsip hukum pidana yang relevan dalam menilai kualifikasi perbuatan dan bentuk pertanggungjawaban pidana terhadap praktik manipulasi algoritma. Spesifikasi penelitian bersifat deskriptif-analitis, yaitu menggambarkan secara sistematis norma hukum yang mengatur kejahatan siber sekaligus menganalisis penerapannya dalam konteks manipulasi algoritma pada platform digital [12].

Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh melalui studi kepustakaan (*library research*). Data sekunder tersebut terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier [12]. Bahan hukum primer meliputi peraturan perundang-undangan yang memiliki kekuatan mengikat, antara lain Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum

Acara Pidana (KUHAP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [7]. Bahan hukum sekunder mencakup literatur ilmiah berupa buku, jurnal hukum, hasil penelitian terdahulu, serta pendapat para ahli yang relevan dengan kajian hukum pidana siber dan regulasi sistem elektronik. Sementara itu, bahan hukum tersier meliputi kamus hukum, ensiklopedia, serta sumber referensi lain yang membantu menjelaskan istilah dan konsep hukum yang berkaitan dengan objek penelitian [13].

Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan cara menelusuri, membaca, mengkaji, dan mencatat berbagai sumber hukum yang relevan dengan permasalahan penelitian [14]. Seluruh bahan hukum tersebut kemudian diklasifikasikan dan disusun secara sistematis untuk mendukung analisis yuridis terhadap isu hukum yang diteliti.

C. PEMBAHASAN

1. Karakteristik Manipulasi Algoritma pada Platform TikTok sebagai Kualifikasi Tindak Pidana

Transformasi ruang digital telah menjadikan media sosial sebagai arena utama interaksi sosial, produksi informasi, dan aktivitas ekonomi masyarakat. Dalam ekosistem digital tersebut, berbagai praktik penyalahgunaan teknologi turut berkembang seiring meningkatnya ketergantungan masyarakat terhadap platform digital. Salah satu fenomena yang muncul adalah praktik manipulasi algoritma pada platform media sosial, khususnya pada TikTok, yang memanfaatkan sistem rekomendasi berbasis machine learning untuk menentukan distribusi dan visibilitas konten kepada pengguna [9], [15].

Secara konseptual, manipulasi algoritma dapat dipahami sebagai tindakan yang dilakukan secara sengaja untuk memengaruhi atau mengeksploitasi mekanisme kerja algoritma suatu platform digital guna memperoleh keuntungan tertentu atau menciptakan dampak

tertentu yang tidak sesuai dengan tujuan sistem tersebut. Dalam konteks platform digital, algoritma merupakan bagian dari sistem elektronik sebagaimana dimaksud dalam Pasal 1 angka 5 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya. Oleh karena itu, setiap bentuk intervensi yang secara sengaja memengaruhi cara kerja algoritma dapat dikategorikan sebagai bentuk intervensi terhadap sistem elektronik [7], [16].

Dalam praktiknya, manipulasi algoritma pada platform TikTok dapat dilakukan melalui berbagai modus operandi, seperti penggunaan bot untuk meningkatkan jumlah tayangan dan interaksi, praktik *click farm* atau *engagement farm*, rekayasa metadata melalui *hashtag stuffing*, eksploitasi celah sistem rekomendasi (*algorithm gaming*), serta pemanfaatan teknologi kecerdasan buatan untuk menghasilkan interaksi semu [17]. Praktik tersebut menunjukkan bahwa manipulasi algoritma bukan sekadar persoalan etika penggunaan platform, melainkan memiliki implikasi hukum yang nyata.

Dari perspektif hukum pidana siber, manipulasi algoritma memiliki beberapa karakteristik utama yang dapat menjadikannya sebagai perbuatan yang berpotensi dikualifikasikan sebagai tindak pidana. Pertama, perbuatan tersebut dilakukan secara sengaja dan terencana. Unsur kesengajaan (*dolus*) tampak dari adanya tujuan tertentu yang ingin dicapai pelaku, seperti meningkatkan popularitas akun secara artifisial atau memperoleh keuntungan ekonomi dari monetisasi konten [5], [6].

Kedua, manipulasi algoritma dilakukan melalui pemanfaatan sistem elektronik secara tidak sah. Praktik ini dapat berupa penggunaan perangkat lunak otomatis, eksploitasi celah keamanan sistem, maupun penyalahgunaan antarmuka aplikasi yang bertentangan dengan ketentuan penggunaan platform. Karakteristik ini relevan dengan ketentuan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik yang melarang setiap orang mengakses sistem elektronik tanpa hak atau melawan hukum [6], [10].

Ketiga, manipulasi algoritma menimbulkan gangguan terhadap integritas sistem elektronik. Distorsi terhadap sistem rekomendasi menyebabkan distribusi konten tidak lagi mencerminkan interaksi pengguna yang sebenarnya. Kondisi tersebut berkaitan

dengan larangan mengubah atau memanipulasi informasi elektronik sebagaimana diatur dalam Pasal 32 serta larangan mengganggu sistem elektronik dalam Pasal 33 Undang-Undang Informasi dan Transaksi Elektronik [15].

Keempat, manipulasi algoritma menghasilkan informasi elektronik yang menyesatkan. Interaksi semu yang diciptakan melalui praktik manipulasi menimbulkan persepsi publik seolah-olah suatu konten memiliki tingkat popularitas yang tinggi secara organik. Kondisi ini relevan dengan Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik yang melarang manipulasi informasi elektronik agar dianggap sebagai data yang otentik [9].

Kelima, praktik manipulasi algoritma berpotensi menimbulkan kerugian ekonomi maupun sosial. Kerugian tersebut dapat dialami oleh kreator lain yang kehilangan visibilitas konten, konsumen yang menerima informasi menyesatkan, maupun pelaku usaha yang dirugikan dalam kompetisi digital [8].

Selain itu, praktik manipulasi algoritma juga bertentangan dengan asas itikad baik dalam pemanfaatan teknologi informasi sebagaimana diatur dalam Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik. Asas tersebut menegaskan bahwa penggunaan teknologi informasi harus dilandasi prinsip kehati-hatian, kejujuran, serta tanggung jawab dalam menjaga integritas ruang digital [9].

Meskipun manipulasi algoritma belum dirumuskan secara eksplisit sebagai delik tersendiri dalam hukum pidana Indonesia, perbuatan tersebut secara normatif dapat dipetakan ke dalam beberapa ketentuan pidana yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik.

Pertama, manipulasi algoritma yang dilakukan melalui akses tidak sah terhadap sistem elektronik dapat dikualifikasikan sebagai tindak pidana akses ilegal sebagaimana diatur dalam Pasal 30 jo. Pasal 46 Undang-Undang Informasi dan Transaksi Elektronik [18], [19].

Kedua, apabila manipulasi dilakukan dengan cara mengubah atau merusak integritas informasi elektronik yang memengaruhi distribusi konten, maka perbuatan tersebut dapat dikaitkan dengan ketentuan Pasal 32 jo. Pasal 48 Undang-Undang Informasi dan Transaksi Elektronik [18], [19].

Ketiga, apabila manipulasi algoritma menyebabkan sistem elektronik tidak bekerja sebagaimana mestinya, maka perbuatan tersebut dapat dipandang sebagai gangguan terhadap sistem elektronik sebagaimana diatur dalam Pasal 33 jo. Pasal 49 Undang-Undang Informasi dan Transaksi Elektronik [18], [19].

Keempat, manipulasi algoritma yang bertujuan menciptakan representasi informasi elektronik seolah-olah autentik dapat dikualifikasikan sebagai manipulasi data elektronik sebagaimana diatur dalam Pasal 35 jo. Pasal 51 Undang-Undang Informasi dan Transaksi Elektronik [18], [19].

Namun demikian, penerapan pasal-pasal tersebut terhadap manipulasi algoritma pada dasarnya masih bersifat interpretatif karena algoritma belum secara eksplisit diakui sebagai objek perlindungan hukum yang berdiri sendiri dalam sistem hukum pidana Indonesia. Oleh karena itu, konstruksi delik masih bergantung pada penafsiran terhadap konsep sistem elektronik dan informasi elektronik [18], [19].

Dalam konteks regulasi yang lebih luas, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan kerangka normatif mengenai kewajiban Penyelenggara Sistem Elektronik untuk menyelenggarakan sistem yang andal, aman, dan bertanggung jawab. Meskipun tidak memuat ketentuan pidana secara langsung, regulasi ini berfungsi sebagai instrumen pengawasan dan pencegahan terhadap penyalahgunaan sistem elektronik [20].

Dalam praktik peradilan, interpretasi terhadap delik manipulasi sistem elektronik telah berkembang melalui putusan pengadilan. Salah satu contoh adalah Putusan Pengadilan Negeri Jakarta Pusat Nomor 442/Pid.Sus/2024 yang menegaskan bahwa unsur manipulasi dalam sistem elektronik tidak terbatas pada perusakan fisik sistem, tetapi juga mencakup setiap bentuk rekayasa yang mengubah fungsi atau makna informasi elektronik [21].

Majelis hakim dalam perkara tersebut menafsirkan bahwa manipulasi dapat terjadi melalui intervensi terhadap proses pemrosesan data dalam sistem elektronik, sehingga tidak lagi mencerminkan kondisi yang sebenarnya. Penafsiran ini memperluas

pemahaman bahwa objek perlindungan hukum pidana tidak hanya terbatas pada data atau perangkat fisik, tetapi juga mencakup logika pemrosesan informasi dalam sistem elektronik [21].

Dengan demikian, yurisprudensi tersebut memberikan dasar interpretatif bahwa manipulasi algoritma pada platform digital, termasuk pada TikTok, dapat dianalisis sebagai bentuk manipulasi sistem elektronik sepanjang terbukti adanya intervensi terhadap proses pemrosesan informasi yang berdampak pada perubahan fungsi atau makna data elektronik.

2. Pertanggungjawaban Pidana atas Manipulasi Algoritma dalam Hukum Pidana Indonesia

Dalam hukum pidana Indonesia, pertanggungjawaban pidana didasarkan pada asas *geen straf zonder schuld*, yang menegaskan bahwa pemidanaan hanya dapat dijatuhkan apabila terdapat kesalahan dari pelaku. Unsur kesalahan tersebut dapat berupa kesengajaan (*dolus*) maupun kelalaian (*culpa*) [22].

Dalam konteks manipulasi algoritma pada platform TikTok, subjek hukum yang dapat dimintai pertanggungjawaban pidana tidak hanya terbatas pada individu, tetapi juga dapat mencakup korporasi sebagai Penyelenggara Sistem Elektronik. Individu yang berpotensi dimintai pertanggungjawaban antara lain pengembang sistem, operator teknis, maupun pihak yang secara sengaja melakukan intervensi terhadap sistem algoritmik [8], [9].

Selain itu, hukum pidana modern juga mengakui korporasi sebagai subjek hukum pidana. Pengakuan ini tercermin dalam berbagai peraturan perundang-undangan, termasuk Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Dalam kerangka ini, pertanggungjawaban pidana korporasi dapat dianalisis

melalui beberapa teori, antara lain teori identifikasi (*identification theory*) dan *vicarious liability*, yang memungkinkan atribusi kesalahan individu kepada korporasi [4], [6].

Namun demikian, penerapan pertanggungjawaban pidana terhadap manipulasi algoritma menghadapi sejumlah kendala. Kompleksitas sistem algoritmik sering kali menyebabkan kesulitan dalam menentukan hubungan kausal antara perbuatan manipulasi dengan kerugian yang ditimbulkan. Selain itu, sifat algoritma yang tidak transparan (*black box algorithm*) juga menyulitkan proses pembuktian dalam praktik penegakan hukum [6].

Analisis terhadap kerangka hukum yang ada menunjukkan adanya kesenjangan normatif dalam pengaturan manipulasi algoritma dalam hukum pidana Indonesia. Pertama, algoritma belum diakui sebagai objek hukum yang secara khusus dilindungi dalam peraturan perundang-undangan. Kedua, pengaturan dalam Undang-Undang Informasi dan Transaksi Elektronik masih berfokus pada perlindungan data dan sistem elektronik secara umum, sehingga belum mampu menjangkau kompleksitas manipulasi algoritmik [17], [18].

Ketiga, pembuktian unsur kesalahan dan hubungan kausal dalam manipulasi algoritma sangat kompleks karena melibatkan aspek teknis yang sulit diverifikasi secara forensik. Keempat, belum terdapat rezim akuntabilitas algoritmik yang secara komprehensif mengatur tanggung jawab platform digital dalam mengelola sistem rekomendasi berbasis kecerdasan buatan [17].

Kondisi tersebut menunjukkan bahwa manipulasi algoritma merupakan bentuk kejahatan digital yang masih berada dalam wilayah abu-abu (*legal grey area*) dalam hukum pidana Indonesia. Oleh karena itu, diperlukan pembaruan hukum yang mengarah pada penguatan pengaturan sistem elektronik dan algoritma, termasuk pengembangan konsep pertanggungjawaban pidana yang lebih adaptif terhadap kejahatan berbasis teknologi. Reformasi hukum tersebut menjadi penting untuk memastikan perlindungan kepentingan hukum masyarakat sekaligus menjaga integritas ekosistem digital di Indonesia [15].

D. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa manipulasi algoritma pada platform TikTok pada dasarnya merupakan bentuk perbuatan melawan hukum yang dilakukan secara sengaja dengan memanfaatkan sistem elektronik secara tidak sah sehingga berpotensi mengganggu integritas proses pemrosesan algoritmik serta menimbulkan kerugian bagi pengguna maupun ekosistem digital secara lebih luas. Praktik tersebut menunjukkan karakteristik sebagai kejahatan berbasis teknologi yang memanfaatkan celah dalam sistem digital untuk memengaruhi distribusi informasi dan visibilitas konten. Meskipun demikian, dalam kerangka hukum pidana positif di Indonesia, pengaturan mengenai manipulasi algoritma belum dirumuskan secara eksplisit. Ketentuan yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, maupun ketentuan dalam Kitab Undang-Undang Hukum Pidana yang baru masih bersifat analogis dan tersebar pada berbagai norma yang tidak secara khusus menempatkan algoritma sebagai objek perlindungan hukum pidana. Kondisi tersebut menunjukkan adanya kekosongan norma dalam pengaturan hukum pidana terkait perlindungan terhadap integritas algoritma sebagai bagian penting dari sistem elektronik, sehingga diperlukan penguatan kerangka regulasi yang lebih komprehensif guna memberikan kepastian hukum dalam penanggulangan kejahatan digital berbasis manipulasi algoritmik.

Selanjutnya, dalam perspektif pertanggungjawaban pidana, perbuatan manipulasi algoritma secara teoritis memungkinkan dikenakan kepada subjek hukum berupa individu maupun korporasi yang terlibat dalam praktik tersebut. Namun, dalam konteks praktik dan konstruksi pertanggungjawaban pidana, individu merupakan subjek yang paling memungkinkan untuk dimintai pertanggungjawaban. Hal ini didasarkan pada pemahaman bahwa ruang digital pada dasarnya memiliki karakter yang sebanding dengan ruang konvensional, dengan perbedaan utama terletak pada dimensi terjadinya perbuatan yang berlangsung melalui sistem elektronik. Oleh karena itu, ketika suatu perbuatan manipulasi algoritma dilakukan, maka pertanggungjawaban pidana pada

prinsipnya diarahkan kepada pelaku yang secara langsung menjalankan atau mengendalikan tindakan tersebut dalam ruang digital. Dengan demikian, penegakan hukum pidana terhadap manipulasi algoritma perlu diarahkan pada identifikasi pelaku individu yang melakukan intervensi terhadap sistem algoritmik, disertai dengan penguatan kerangka regulasi yang mampu memberikan kepastian mengenai batasan perbuatan yang dikualifikasikan sebagai manipulasi algoritma serta mekanisme pertanggungjawaban pidananya dalam sistem hukum Indonesia.

E. REFERENSI

- [1] F. E. T. Sirait, "Manusia dan teknologi: perilaku interaksi interpersonal sebelum dan sesudah media digital," *Journal of Education, Humaniora and Social Sciences (JEHSS)*, vol. 3, no. 2, 2020.
- [2] Mohamad Revaldy Fairuzzen, Abil Arya Putra, Akmal Reihan, and Lilik Prihatini S.H, M.H, "Perkembangan Hukum dan Kejahatan Siber 'Cybercrime' di Indonesia," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, vol. 2, no. 1, 2024, doi: 10.62976/ijjel.v2i1.372.
- [3] M. R. Habibi and I. Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, vol. 23, no. 2, 2020, doi: 10.15642/alqanun.2020.23.2.400-426.
- [4] A. Suhaemin and M. Muslih, "Karakteristik Cybercrime di Indonesia," *EduLaw : Journal of Islamic Law and Jurisprudence*, vol. 5, no. 2, 2023.
- [5] S. Agustin, "Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber," *Jurnal Penelitian Multidisiplin Bangsa*, vol. 1, no. 6, 2024, doi: 10.59837/jpnmb.v1i6.93.
- [6] S. R. R. Ginting, S. Suparman, and M. Mulyono, "Algoritma Cerdas Tiktok: Mengubah Cara Generasi Z Mengonsumsi Informasi," *Edutik : Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 5, no. 3, 2025, doi: 10.53682/edutik.v5i3.11840.
- [7] I. Z. Lisi, "Tinjauan Hukum Pidana Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik di Indonesia," *Jurnal Risalah Hukum*, vol. 1, no. 1, pp. 18-24, 2020.
- [8] H. Muhammad Salman, A. Syawla Malika, A. Amelia Fahra, B. Marfin, and N. Pia Khoirotun, "Seberapa Besar Algoritma TikTok dalam Mempengaruhi Opini Publik

- tentang Kebijakan Kesehatan di Jakarta Selatan,” *Edu Society: Jurnal Pendidikan, Ilmu Sosial, dan Pengabdian Kepada Masyarakat*, vol. 5, no. 2, 2025.
- [9] H. Prasetyo and A. Nugroho, “Peran dan Tanggung Jawab Platform Digital dalam Upaya Pengawasan dan Perlindungan Konsumen di Indonesia,” *Jurnal Hukum dan Peraturan Indonesia*, vol. 1, no. 2, 2024.
- [10] G. M. L. Putri, “Pengaruh Konten Marketing Affiliate, Algoritma FYP, dan E-WOM pada Media Sosial Tiktok terhadap Keputusan Pembelian Generasi Z (Studi pada Generasi Z di Indonesia),” *Journal of Economic, Bussines and Accounting (COSTING)*, vol. 7, no. 4, 2024, doi: 10.31539/costing.v7i4.10290.
- [11] S. Soekanto and S. Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan*, vol. 1, no. 1. 2019.
- [12] K. Benuf and M. Azhar, “Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer,” *Gema Keadilan*, vol. 7, no. 1, 2020, doi: 10.14710/gk.2020.7504.
- [13] S. S. dan S. Mamuji, “Penelitian Hukum Normatif Suatu Tinjauan Singkat, Raja Grafindo Persada, Jakarta,” *Prosiding: Problematika Hukum ...*, 2018.
- [14] D. Tan, “Metode Penelitian Hukum : Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Metode Penelitian Hukum,” *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, vol. 8, no. 8, 2021.
- [15] G. Dzunuwanus, S. Manar, M. S. Ip, and J. Akmal, “Manipulasi Narasi Publik Melalui Akun Bot Dalam Aktivisme Digital Pro-Ikn di Media Sosial X,” *Journal of Politic and Government Studies*, vol. 14, no. 3, 2025.
- [16] T. J. Holt and A. M. Bossler, *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. 2015. doi: 10.4324/9781315775944.
- [17] Yogiswara Dharma Putra, I Putu Sugi Almantara, I Made Bagus Wahyu Mahendra, and Ida Bagus Paalakaa RNB, “Klasifikasi Pelanggaran UU ITE Pada Tiktok Menggunakan Algoritma Naive Bayes,” *Jurnal Teknologi Informasi dan Komputer*, vol. 10, no. 2, 2024, doi: 10.36002/jutik.v10i2.3021.
- [18] N. Tasya and S. Sunariyo, “Analisis Hukum Manipulasi Identitas Visual oleh Gemini AI di Tiktok: Etika dan Regulasi Siber,” *PESHUM : Jurnal Pendidikan, Sosial dan Humaniora*, vol. 5, no. 1, 2025, doi: 10.56799/peshum.v5i1.13611.
- [19] R. Ayu, A. Dewi, N. Putri, and Firman, “Melihat Peran Buzzer di Aplikasi Tiktok dalam Pemilu 2024 Studi Kasus Buzzer terhadap Pasangan 01 Melihat Pengaruh dalam Ruang Digital,” *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora*, vol. 4, no. 2, 2024, doi: 10.53697/iso.v4i2.1993.

Jurnal Dialogica
Volume I Issue 2 Tahun 2026

- [20] C. Vania, M. Markoni, H. Saragih, and J. Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," *Jurnal Multidisiplin Indonesia*, vol. 2, no. 3, 2023, doi: 10.58344/jmi.v2i3.157.
- [21] Geraldo Juwandi Kamu, "Kajian Yuridis Membantu Melakukan Tindak Pidana Manipulasi Informasi atau Dokumen Elektronik (Putusan PN Jakarta Pusat No. 442/PID.SUS/2024/PN JKT.PST)," *Jurnal Fakultas Hukum unsrat*, vol. Vol. 15 No. 4, 2025.
- [22] A. Azhari, "Pertanggungjawaban Pidana Dalam Persepsi Kajian Islam," *OR! ENT: Journal of Islamic Studies & Culture*, vol. 1, no. 01, 2025.