

Pertanggungjawaban Hukum Terhadap Tindakan Doxing Dalam Perbuatan Penipuan Dalam Pelunasan Sistem Jasa Titip Online

Nanda Fitri Dian Permatasari ¹, Ahmad Heru Romadhon ²

Universitas Maarif Hasyim Latif, Sidoarjo, Indonesia

nanda_fitri_dian_permatasari@student.umaha.ac.id ¹, heru-romadhon@dosen.umaha.ac.id ²

Informasi Artikel	Abstract
E-ISSN : 3026-6874 Vol: 3 No: 1 Januari 2025 Halaman : 136-142	<i>The act of publishing someone's personal information without the consent of the data owner (Doxing), which is increasingly prevalent in digital interactions, is also part of the buying and selling activities through the online consignment service system (Jastip). The purpose of this study is to analyze the legal liability for doxing committed by the owner of the online consignment service as a form of retribution for fraudulent actions carried out by customers. A normative juridical approach is used to explore this issue, which focuses on understanding and analyzing the existing rules and legal doctrines in Indonesia, centered on relevant legislation such as the Electronic Information and Transactions Law (UU ITE) and the Indonesian Criminal Code (KUHP). The findings of this study conclude that doxing can be subject to legal sanctions under Articles 27A and 27B of the UU ITE, which regulate defamation and the dissemination of unlawful information. Furthermore, in cases of fraud within the online consignment service system, Article 28 paragraph (1) of the UU ITE can provide a more relevant legal foundation, replacing the general provisions of Article 378 of the Indonesian Criminal Code (KUHP). Online consignment service providers are advised to establish clear regulations regarding obligations and sanctions, as well as unilateral cancellation policies or legal actions if customers fail to make payments. Thoughtful resolution methods not only comprehensively resolve the issues but also prevent the emergence of new problems.</i>
Keywords: Personal Data Doxing Fraud	

Abstrak

Tindakan mempublikasi informasi pribadi seseorang tanpa seizin pemilik data pribadi (Doxing) yang marak terjadi dalam interaksi digital termasuk dalam kegiatan jual beli melalui sistem jasa titip online (Jastip). Tujuan dari penelitian ini adalah guna menganalisis pertanggungjawaban hukum atas tindakan doxing yang diperbuat oleh pemilik layanan jasa titip online sebagai bentuk penghakiman atas tindakan penipuan yang dilakukan oleh pelanggan. Pendekatan yuridis normatif digunakan untuk menggali permasalahan ini, yang berfokus pada pemahaman dan analisis aturan dan doktrin-doktrin hukum di Indonesia yang sudah ada dengan berpusat pada peraturan perundang-undangan terkait Undang-undang Informasi dan Transaksi Elektronik dan KUHP. Hasil penelitian ini menyimpulkan bahwa tindakan doxing dapat dikenakan sanksi hukum berdasarkan Pasal 27A dan Pasal 27B UU ITE yang mengatur tentang pencemaran nama baik dan penyebaran informasi yang melanggar hukum. Selain itu, pada kasus penipuan yang terjadi dalam sistem jasa titip online, Pasal 28 ayat (1) UU ITE dapat menjadi landasan hukum yang lebih relevan menggantikan ketentuan umum dalam Pasal 378 KUHP. Penyedia layanan jasa titip online disarankan untuk menetapkan peraturan yang jelas mengenai kewajiban dan sanksi, serta kebijakan pembatalan sepihak atau tindakan hukum jika pelanggan gagal melunasi. Bentuk penyelesaian masalah yang dipertimbangkan secara matang tidak hanya mengakhiri masalah secara menyeluruh, tetapi juga mencegah munculnya permasalahan baru.

Kata Kunci: Data Pribadi, Doxing, Penipuan.

PENDAHULUAN

Perkembangan dalam teknologi informasi dan komunikasi mengalami kemajuan signifikan dalam beberapa dekade terakhir, khususnya sejak terciptanya jaringan internet dan perangkat digital. Kemajuan ini memberikan dampak besar bagi pola hidup masyarakat serta pada bagaimana cara masyarakat berkomunikasi, bertukar informasi, mengakses ilmu pengetahuan dengan mudah serta dapat di akses di mana pun dan kapan pun. Dewasa ini, sebagian besar masyarakat tidak lagi bergantung pada komunikasi konvensional misalnya melalui mengirim surat atau bertemu tatap muka, hal ini dikarenakan sudah tersedianya teknologi yang memungkinkan terlaksananya interaksi tak terbatas seperti layanan pesan singkat dan panggilan seluler. Secara menyeluruh dalam perkembangan kemajuan

teknologi informasi dan komunikasi telah memberikan berbagai macam kemudahan dalam kehidupan masyarakat sekaligus menuntut kesiapan masyarakat untuk beradaptasi dengan teknologi dan memanfaatkannya dengan bijaksana.

Sebagaimana dampak positif yang diperoleh, hal ini tentu tidak terlepas dari dampak negatif yang ditimbulkan. Efek ketergantungan terhadap teknologi, khususnya media sosial dapat memicu masalah kesehatan mental berupa gangguan psikologis yang di sebabkan karena individu menghabiskan banyak waktu di hidupnya hanya untuk mengakses media sosial sebab faktor tingginya rasa ingin tahu serta ketidakmampuan mengontrol diri sehingga keproduktifan aktivitas melemah dalam kehidupan sehari harinya. Kebiasaan kecil yang pada akhirnya dapat memberikan dampak fatal seperti stres, gangguan kecemasan dan perasaan kesepian dikarenakan individu menjadi terlalu bergantung pada validasi dari media sosial.(Wulandari & Netrawati, 2020) Selain itu, dampak negatif perkembangan teknologi dapat pula berupa ancaman keamanan siber serta kejahatan dalam dunia maya berbasis teknologi atau umum di kenal dengan sebutan cybercrime.

Cybercrime atau kejahatan siber adalah pelanggaran yang dilakukan dengan unsur kesengajaan oleh sekelompok orang atau perorangan dengan tujuan merusak reputasi serta menyebabkan kerugian fisik, mental dan materi korban berbasis teknologi modern seperti internet dan forum media sosial.(Nastiti, 2023) Bentuk upaya perlindungan hukum yang diberikan oleh negara dalam ruang lingkup siber tertuang dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Seirama dengan kemajuan teknologi, bentuk modus kejahatan dalam ruang siber semakin beragam, di antaranya adalah Doxing. Doxing merupakan tindakan menyebarkan informasi pribadi yang bukan miliknya kepada publik di ruang lingkup media sosial tanpa persetujuan dari pemilik data dengan tujuan untuk merusak reputasi, memperlakukan, merundung, mengancam untuk menyakiti mental maupun fisik korban.

Kemajuan teknologi telah mengubah segalanya, memberikan kemudahan dalam mengakses informasi dan ilmu pengetahuan tak terbatas melalui mesin penelusur, platform pembelajaran jarak jauh dan media sosial. Tidak hanya itu, di dalam bidang ekonomi kehadiran teknologi memudahkan adanya transaksi digital serta kegiatan jual beli yang dilakukan secara daring (e-commerce). Mempermudah bisnis beroperasi tanpa harus mendirikan toko fisik sehingga dapat mengurangi biaya operasional dan memberikan kesempatan bagi pengusaha mikro kecil dan menengah untuk berkembang. Seluruh pola kehidupan sosial berubah dengan munculnya berbagai komunitas daring dan budaya dalam bersosial media.

Jasa titip (Jastip), adalah layanan di mana seseorang membantu membeli barang atau tiket atas nama orang lain dengan imbalan berupa biaya jasa. Dalam dunia K-pop, jastip menjadi solusi favorit para penggemar untuk mendapatkan tiket konser atau merchandise resmi yang sering kali sulit diakses karena stok terbatas, sistem penjualan cepat habis, atau hanya dijual di tempat dan waktu tertentu, seperti acara konser dan fan meeting. Layanan ini memungkinkan penggemar yang tidak dapat hadir secara langsung karena faktor geografis, pekerjaan, atau keterbatasan waktu untuk tetap memiliki akses ke barang-barang yang mereka inginkan.

Jasa titip dalam lingkup penggemar K-pop umumnya dikelola oleh individu atau kelompok kecil yang sudah memiliki pengalaman dan jaringan kuat untuk mengakses tiket konser, merchandise, atau event tertentu. Mereka sering kali menggunakan akun media sosial seperti Instagram, Twitter, atau platform pesan seperti WhatsApp dan Telegram untuk menawarkan layanan mereka. Pemesan biasanya harus mengikuti syarat dan ketentuan dari penyedia jasa, seperti memberikan uang muka atau membayar penuh di awal. Setelah pemesanan diterima, penyedia jasa akan membeli barang atau tiket sesuai dengan permintaan, kemudian mengatur pengiriman barang atau e-tiket kepada pelanggan. Untuk barang fisik seperti lightstick atau album, pengiriman dilakukan melalui jasa kurir, sementara tiket digital biasanya dikirim melalui email atau aplikasi pesan.

Pelanggan memesan dengan memberikan detail lengkap mengenai barang atau tiket yang diinginkan, termasuk kuantitas, kategori tiket (VIP atau reguler), serta instruksi khusus jika ada. Setelah transaksi disepakati dan pembayaran dilakukan, jastiper akan membeli tiket atau merchandise sesuai

kebutuhan. Barang fisik yang telah dibeli biasanya dikirim menggunakan layanan ekspedisi. Dalam beberapa kasus, terutama untuk tiket konser fisik, pelanggan bisa memilih opsi pengambilan langsung di lokasi konser. Keamanan dan kejelasan pengiriman sangat penting untuk memastikan barang tiba sesuai harapan dan tepat waktu, terutama ketika terkait dengan event yang terikat jadwal.

Menjalankan operasi layanan jasa titip (jastip) tidak selalu bebas risiko. Salah satu risiko utama adalah penipuan yang diperbuat oleh pelanggan, seperti pembatalan sepihak dengan alasan yang tidak jelas, atau kasus pelunasan pembayaran barang dimana pelanggan lari dari tanggung jawab pembayaran pelunasan barang pesannya dengan memutuskan semua kontak yang menghubungkan dirinya dengan pemilik jasa, sehingga menyebabkan kerugian bagi penyedia jasa yang harus menanggung biaya pelunasan pelanggan dan menjualnya kembali. Meskipun barang tetap bisa dijual kembali akan tetapi perolehan tidak ada perolehan keuntungan sama sekali yang didapat melainkan risiko kerugian mengingat sebagian besar barang mengalami harga naik dan turun.

Untuk mengurangi risiko ingkar janji pelunasan, sebagian besar penyedia jasa menerapkan aturan ketat dan sanksi bagi pelanggan yang enggan atau gagal melunasi kewajibannya. Salah satu sanksi yang kerap diterapkan adalah penyebaran informasi pribadi pelaku di media sosial, atau yang dikenal sebagai doxing. Hal ini terjadi ketika pelanggan gagal melunasi pembayaran setelah barang telah dibeli oleh penyedia jasa, sehingga menyebabkan kerugian finansial bagi penyedia jasa. Akibat frustrasi dengan tindakan ingkar janji tersebut, beberapa penyedia jasa mengambil langkah ekstrem dengan mempublikasikan identitas pelanggan di media sosial. Informasi yang sering dibagikan meliputi nama lengkap, nomor telepon, alamat, atau tangkapan layar percakapan, dengan tujuan memberikan tekanan agar pelanggan segera melunasi kewajiban mereka. Dari sudut pandang penyedia jasa, praktik ini dimaksudkan sebagai wujud tekanan agar pelanggan segera melunasi kewajibannya sekaligus sebagai peringatan bagi penyedia jasa titip online lain agar waspada terhadap perbuatan tidak bertanggung jawab yang dilakukan pelanggan tersebut.

METODE

Dalam penyusunan penelitian ini, penulis mengaplikasikan pendekatan yuridis normatif yakni metode penelitian hukum yang berfokus pada penelaahan bahan pustaka. (Mamudji, 1995) Metode ini diterapkan dengan mengkaji berbagai literatur yang relevan dengan topik hukum yang diteliti. Peneliti akan menelaah berbagai sumber hukum untuk menemukan kaidah-kaidah yang dapat digunakan untuk menjawab permasalahan hukum yang dihadapi. Melalui pendekatan yuridis normatif, peneliti mencari kejelasan dan kepastian hukum dengan merujuk kepada regulasi yang berlaku. Ini mencakup analisis mendalam terhadap KUHP, dan Undang-Undang terkait lainnya untuk mendapatkan pemahaman yang menyeluruh tentang kerangka hukum yang relevan.

HASIL DAN PEMBAHASAN

Pengertian Tindakan Penyebaran Data Pribadi (Doxing)

Doxing adalah singkatan dari dropping documents adalah bentuk dari perundungan siber cyberbullying di mana pelaku mengumpulkan dan menyebarkan informasi yang bersifat pribadi milik seseorang, seperti nomor telepon, alamat tempat tinggal, riwayat pendidikan, foto atau tulisan cerita pribadi, serta data sensitif lainnya, tanpa izin. Tujuan dari tindakan ini biasanya untuk menyingkap identitas atau detail pribadi korban ke publik, sehingga membuka potensi terjadinya gangguan atau pelecehan lebih lanjut. Praktik ini melanggar privasi korban dan sering kali mengarah pada intimidasi atau ancaman, baik secara langsung maupun tidak langsung, yang dapat berdampak serius pada kesejahteraan korban di dunia nyata. (Cabreran., M. Carmen Elisa Larrañaga, 2024)

Doxing awalnya muncul sebagai bentuk dari perwujudan aksi pembalasan dendam di komunitas daring pada periode sekitar tahun 1990. Pelaku mengumpulkan dan mempublikasikan data sensitif milik seseorang sebagai cara untuk mempermalukan atau membalas dendam terhadap target tersebut, terutama dalam komunitas peretas. (Putri, 2023) Para pelaku doxing biasanya menggunakan identitas

anonim untuk melindungi diri saat melakukan aksinya. Saat ini, doxing diartikan sebagai tindakan yang dilakukan melibatkan unsur kesengajaan dengan menyebarkan data atau informasi yang bersifat pribadi milik seseorang di media sosial. Istilah doxing telah menjadi cukup menonjol sehingga dimasukkan ke dalam kamus formal, seperti Oxford British and World English Dictionary. Kamus tersebut mendefinisikan doxing sebagai tindakan mencari dan membagikan informasi pribadi atau identitas seseorang di internet, yang biasanya dilakukan dengan niat jahat. (Oxford Reference, n.d.)

Doxing dilakukan dengan berbagai motif, salah satunya adalah keinginan untuk mengungkap kesalahan atau meminta pertanggungjawaban dari seseorang yang dianggap bersalah. Tindakan ini sering digunakan sebagai cara guna mengintimidasi, mengancam, menjatuhkan martabat atau nama baik korban di depan publik hingga menghukum individu yang menjadi targetnya sebagai bentuk wujud main hakim sendiri. Doxing telah menjadi semacam bentuk "main hakim sendiri" di dunia maya, di mana mereka yang tidak setuju dengan tindakan seseorang dapat membalasnya dengan menyebarkan identitas dan informasi pribadi orang tersebut. Akibatnya, korban doxing kerap menerima ejekan terbuka, pelecehan, hingga fitnah di ruang publik, yang dapat merusak reputasi dan memengaruhi kesejahteraannya.

Pelaku pada umumnya menetapkan target terlebih dahulu, kemudian mulai mengumpulkan data pribadi terkait korban. Setelah data berhasil terkumpul, pelaku menyebarkannya melalui media sosial yang nantinya memancing keterlibatan banyak orang sehingga dampak yang ditimbulkan akan semakin meluas. Tidak hanya faktor dari niat jahat pelaku, Doxing juga dapat terjadi karena disebabkan oleh kelalaian pengguna atau pemilik data pribadi dalam mengunggah postingan berisi data pribadinya sendiri secara terbuka di media sosial, sehingga memberikan kemudahan kepada pelaku untuk mengakses lalu menyebarkannya.

Pertanggungjawaban Hukum Tindakan Penyebaran Data Pribadi (Doxing)

Pengertian data pribadi menurut Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi adalah segala sesuatu mengenai informasi tentang data perseorangan berisi keterangan yang nyata dan benar adanya, serta dapat mengidentifikasi pemilik baik secara langsung maupun disertai dengan kombinasi data. (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022) Di Indonesia, peraturan mengenai perlindungan data pribadi telah tertulis dalam Peraturan Menteri Komunikasi dan Informatika (Kominfo) Nomor 20 Tahun 2016 yang mensyaratkan adanya persetujuan tertulis baik secara elektronik maupun manual dari pemilik data pribadi sebelum data pribadi di proses sebarluaskan. Dalam peraturan ini di haruskan pemilik data pribadi memahami tentang bagaimana informasi mereka diperoleh, dikumpulkan, diproses, diarsipkan dan dipublikasikan. Ketentuan lain mengenai perlindungan data pribadi juga tertulis dalam Pasal 26 ayat (2) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan dengan tegas bahwa dalam penggunaan data pribadi seseorang di haruskan adanya konfirmasi dari pemilik data. Apabila hak privasi dari seseorang dilanggar maka dirinya berhak mengajukan gugatan atas kerugian yang telah dialami. (Achmada et al., 2023)

Doxing dapat menimbulkan kerugian fisik, mental maupun materi kepada korban. Mengingat dalam keterkaitannya dengan Hak Privasi dalam Pasal 28G (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945 sebagai Hak Asasi Manusia dan pengertian data pribadi menurut Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, di mana setiap individu berhak mengendalikan penyebaran informasi miliknya pribadi termasuk dengan pemberian persetujuan untuk menggunakannya atau menyebarkanluaskannya, oleh sebab itu dalam penggunaan data pribadi di haruskan adanya konfirmasi dari pemilik data, dengan tujuan menghindari terjadinya risiko penyalahgunaan dan memberikan kepastian dalam penggunaan atau penyebaran data pribadi supaya nantinya tidak akan merugikan pihak mana pun. (Sulthanah, 2023)

Indonesia telah mengatur tindakan pidana doxing melalui berbagai peraturan perundang-undangan yang cukup komprehensif. Doxing diakui sebagai delik dalam hukum pidana Indonesia, yang

diatur dalam Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Ketentuan mengenai doxing diatur dalam Pasal 27A terkait kesengajaan mencemarkan nama baik atau kehormatan orang lain melalui tuduhan yang di sampaikan kepada publik melalui informasi atau dokumen elektronik dapat dipidana penjara paling lama 2 tahun dan/atau denda paling banyak Rp 400 juta. Berikutnya ketentuan mengenai Doxing juga diatur dalam pasal 27B terkait kesengajaan menyebarkan informasi atau dokumen elektronik untuk keuntungan secara melawan hukum melalui memberikan ancaman atau pembukaan rahasia dapat di ancam dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar.(Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2024)

Tindakan doxing dalam kasus jastip sering kali muncul karena rasa marah dan kekecewaan selaku penyedia jasa. Terutama ketika nominal transaksi cukup besar, kerugian yang dialami penyedia jasa bisa sangat signifikan. Dengan mempublikasikan data pribadi pelanggan, penyedia jasa berharap bisa mendapat dukungan moral dari komunitas online, baik dari sesama penyedia jasa maupun pelanggan lainnya yang merasa empati dengan situasi tersebut dan juga pelanggan yang tidak atau enggan melunasi pembayaran tersebut bisa dengan cepat kembali melunasi dan mendapatkan efek jera atas perbuatannya. Namun, meskipun tindakan ini terlihat efektif untuk memberikan tekanan sosial, dampaknya bisa sangat fatal. Publikasi data pribadi dapat menyebabkan pelanggan yang bersangkutan menjadi sasaran pelecehan daring, ancaman fisik, atau bahkan mengancam keamanan dan privasinya. Hal ini juga dapat berujung pada dampak psikologis yang serius bagi pihak yang datanya di publikasikan. Jangan sampai dengan maksud mencari keadilan tapi secara tidak sadar telah membahayakan diri sendiri melalui memilih penyelesaian masalah secara instan dan tidak efektif. Masalah cenderung tidak semakin membaik dan berakhir semakin runyam.

Pertanggungjawaban Hukum Tindakan Penipuan Dalam Pelunasan Sistem Jasa Titip Online

Penipuan adalah perbuatan bohong atau palsu yang dilakukan dengan niat tipu muslihat dengan tujuan untuk menyesatkan dan mencari keuntungan. Penipuan diatur dalam Pasal 378 Kitab Undang-undang Hukum Pidana (KUHP) dengan ancaman pidana penjara paling lama 4 tahun. Menurut Van Hamel, Pidana adalah hukuman berupa penderitaan khusus yang dijatuhkan oleh negara melalui pihak yang berwenang. Hukuman ini diberikan kepada seseorang yang melanggar aturan hukum, untuk menjaga ketertiban umum. Serta menurut Satochid Kartanegara Hukum pidana adalah kumpulan aturan yang dibuat oleh negara, berisi larangan atau perintah tertentu yang harus ditaati. Jika aturan itu dilanggar, negara memiliki hak untuk menuntut pelaku dan menjatuhkan hukuman.(Fardha, 2023)

Dalam tindak pidana terdapat unsur-unsur tertentu yang harus terpenuhi agar seseorang dapat dipidana. Unsur objektif meliputi sesuatu yang terkait dengan keadaan yakni kondisi dimana tindakan yang timbul dari diri pelaku harus dilakukan. Serta unsur subjektif suatu hal yang ada dan berhubungan pada diri pelaku meliputi segala sesuatu yang ada pada hatinya.(P.A.F. Lamintang, 2022) Namun, perkembangan teknologi membuat kasus dalam ranah hukum pidana menjadi lebih kompleks, seperti dalam kasus penipuan yang dilakukan di media sosial, meskipun seluruh unsur pidana tersebut terpenuhi akan tetapi akan tidak cukup jika dibuktikan hanya dengan mengandalkan Pasal 378 KUHP. Hal ini dikarenakan penipuan yang menggunakan media elektronik tidak diatur dalam KUHP.(Aritama, 2022)

Cara-cara penipuan online berbeda dari penipuan konvensional seperti memiliki identitas palsu, mengirimkan informasi palsu, menyamar sebagai orang lain, atau menjalankan skema rumit melalui jaringan tertentu. KUHP juga tidak dapat menghukum korporasi yang terlibat dalam penipuan online karena hanya mengenal subjek hukum individu. Hal ini menyulitkan penegak hukum dalam pembuktian dan yurisdiksi. (Muhammad Kamran, 2021) Untuk mengatasi kelemahan ini, Pasal 28 ayat (1) Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik digunakan untuk menangani penipuan online.(I Gusti Made

Jaya Kesuma, Ida Ayu Putu Widiati, 2020) UU ITE memberikan dasar hukum yang lebih relevan untuk kasus-kasus yang melibatkan transaksi elektronik, termasuk jual beli online. Meskipun UU ITE tidak secara eksplisit membahas dan mengatur tentang penipuan seperti dalam Pasal 378 KUHP, undang-undang ini berfungsi sebagai perlindungan konsumen di dunia digital dan memungkinkan pelaku penipuan online dituntut sesuai hukum.

Dalam konteks hukum, UU ITE menjadi (*lex specialis*) atau aturan khusus yang mengesampingkan Pasal 378 KUHP yang bersifat umum (*lex generalis*). Pasal 378 KUHP tetap relevan untuk penipuan konvensional, sedangkan Pasal 28 ayat (1) Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik lebih cocok untuk kasus penipuan online. Kombinasi kedua aturan ini bertujuan untuk menutupi celah hukum dan memastikan pelaku penipuan tidak lolos dari hukuman. Dengan demikian UU ITE menjadi alat yang tepat untuk menghadapi penipuan di era digital yang semakin canggih.

Solusi Alternatif Penyediaan Peraturan Dan Sanksi Kepada Pelanggan

Penyedia layanan jastip disarankan mencari solusi alternatif guna mengurangi adanya tindakan yang akan dilakukan oleh pelanggan. Salah satu cara efektif adalah dengan menerapkan peraturan yang memuat kewajiban yang harus dilakukan oleh pelanggan dan sanksi kepada pelanggan yang melanggar selain sanksi penyebaran data pribadi. Apabila pelanggan tetap gagal melunasi, jastiper bisa menerapkan kebijakan pembatalan sepihak pada jam tertentu setelah pemesanan apabila pelanggan masih belum mengkonfirmasi lebih lanjut terkait pembayaran, atau di bawahnya kasus ke ranah hukum apabila kerugian yang dialami cukup besar. Terkait pelanggan yang masih di bawah umur disarankan pelanggan hanya dapat membeli barang dengan jumlah barang yang terbatas dan barang dengan harga yang relatif lebih rendah. Perlunya kesepakatan yang jelas sejak awal sangat penting agar hak dan kewajiban kedua belah pihak terlindungi.

Menuntaskan suatu masalah dengan cara membuat masalah lain hanya akan berdampak pada munculnya siklus masalah yang akan terus berkelanjutan serta semakin sulit teratasi. Ketika solusi yang diambil tidak menyelesaikan akar permasalahan, tetapi justru memicu masalah lain, kondisi ini akan menyebabkan masalah-masalah baru bermunculan dan saling tumpang tindih. Dampaknya bukan hanya pada kesulitan dalam mengatasi persoalan utama, tetapi juga pada munculnya masalah sekunder yang semakin mempersulit penyelesaian secara keseluruhan.

Penyelesaian masalah yang berkelanjutan hanya dapat dicapai melalui pemahaman mendalam terhadap akar permasalahan dan penerapan langkah-langkah yang tepat serta adil. Dengan menghindari solusi instan yang merugikan pihak lain atau melanggar aturan, semua pihak dapat bekerja sama untuk mencari solusi yang berimbang dan berkelanjutan.

KESIMPULAN

Doxing adalah bentuk perundungan siber yang melanggar privasi dengan membagikan informasi pribadi tanpa izin untuk tujuan intimidasi atau ancaman yang dapat berdampak serius pada kesejahteraan korban. Indonesia telah mengatur tindakan pidana doxing melalui Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi. Pasal 27A UU ITE dengan ancaman pidana paling lama 2 tahun dan/atau denda paling banyak Rp 400 juta untuk tindakan mencemarkan nama baik, sedangkan Pasal 27B dengan ancaman pidana paling lama 6 tahun dan/atau denda paling banyak Rp 1 miliar untuk perbuatan penyebaran informasi secara melawan hukum dengan tujuan mengancam atau mengambil keuntungan.

Dalam menangani penipuan dalam sistem jasa titip online, diperlukan pendekatan hukum yang sesuai dengan perkembangan peradaban. Dalam Pasal 378 KUHP mengatur penipuan konvensional, oleh karenanya penipuan yang terjadi di dunia digital membutuhkan landasan hukum yang lebih relevan. Hal berikut diatur dalam Pasal 28 ayat (1) UU ITE. UU ITE berperan sebagai aturan khusus yang

mengesampingkan ketentuan umum dalam KUHP, sehingga dapat memberikan solusi yang lebih efektif dalam menanggulangi penipuan online.

REFERENCES

- Achmada, D., Sonatab, ; Depri Liber, Faridc ; Muhammad, Januartid ; Rasti Putri, & Syavira, ; Alyfia. (2023). Legal Protection against Victims of Doxing Crime in Indonesia. *Jurnal Bina Mulia Hukum*, 8(1), 92–105.
- Aritama, R. (2022). Penipuan Dalam Hukum Pidana dan Hukum Perdata. *SENTRI: Jurnal Riset Ilmiah*, 1(3), 728–736.
- Cabreran., M. Carmen Elisa Larrañaga, S. Y. (2024). Bullying/Cyberbullying in Secondary Education: A Comparison Between Secondary Schools in Rural and Urban Contexts. *Child and Adolescent Social Work Journal*, 41(4), 617–631.
- Fardha, K. V. (2023). Perkembangan Teori-Teori Hukum Pidana. *INNOVATIVE: Journal Of Social Science Research*, 3(5), 3982–3991.
- I Gusti Made Jaya Kesuma, Ida Ayu Putu Widiati, I. N. G. S. (2020). Penegakkan Hukum Terhadap Penipuan Melalui Media Elektronik. *Jurnal Preferensi Hukum*, 1(2), 72–77.
- Mamudji, S. S. dan S. (1995). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Raja Grafindo.
- Muhammad Kamran, M. (2021). Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika. *Balobe Law Journal*, 1(1), 41–56.
- Nastiti, F. K. (2023). *Perlindungan Hukum Pidana Terhadap Mahasiswa Universitas Islam Indonesia yang Mengalami Doxing oleh Akun Uiicantikganteng di Platform Instagram*. (Doctoral Dissertation, Universitas Islam Indonesia).
- Oxford Reference. (n.d.). [https://www.oxfordreference.com/display/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-405#:~:text=doxing%5Bfrom%27dox%2C%27abbrev.&text=An online practice of exposing,requires a subscription or purchase](https://www.oxfordreference.com/display/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-405#:~:text=doxing%5Bfrom%27dox%2C%27abbrev.&text=An%20online%20practice%20of%20exposing,requires%20a%20subscription%20or%20purchase).
- P.A.F. Lamintang, F. T. L. (2022). *Dasar-Dasar Hukum Pidana di Indonesia*. Sinar Grafika.
- Putri, C. N. (2023). *KAJIAN KRIMINOLOGI KEJAHATAN PENYEBARAN DATA PRIBADI (DOXING) MELALUI MEDIA SOSIAL*.
- Sulthanah, J. N. S. L. T. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewarganegaraan*, 7(2), 1708–1713.
- Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (2024).
- Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022).
- Wulandari, R., & Netrawati, N. (2020). Analisis tingkat kecanduan media sosial pada remaja. *Jurnal Riset Tindakan Indonesia*, 5(2), 41–46.