PENEGAKAN HUKUM TINDAK PIDANA PENIPUAN ONLINE: STUDI IMPLEMENTASI UNDANG-UNDANG ITE DI INDONESIA[1]

Mohammad Daffa Saifullah[2], Agus Pramono[3]
[2, 3]Program Studi Magister Ilmu Hukum, Program Pascasarjana,
Universitas Wisnuwardhana Malang.
Jalan Danau Sentani No. 99, Madyopuro, Kedungkandang, Kota Malang,
Provinsi Jawa Timur, 65139, Telp. (0341) 713604
[2]daffaSJ13@gmail.com, [3]agus_pramono62@yahoo.co.id.

Abstrak

Meningkatnya prevalensi kejahatan siber, khususnya penipuan online, menimbulkan tantangan signifikan bagi sistem hukum modern. Meskipun sejumlah penelitian telah menyoroti dimensi teknologi dan kriminologi dari kejahatan siber, perhatian ilmiah terhadap kecukupan normatif dan daya laku kerangka hukum yang mengatur penipuan online masih terbatas. Penelitian ini mengisi kesenjangan tersebut dengan menelaah interaksi antara Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam mengatur perbuatan penipuan online. Rumusan Masalah yang diangkat dalam penelitian ini adalah (1) Bagaimana hukum yang mengatur penipuan *online* dan (2) Apa saja kendala yang dihadapi dalam proses penegakan Hukum Tentang Penipuan Online. Metode penelitian yang digunakan pada penelitian ini menggunakan metode yuridis-normatif dengan cara menganalisis beberapa sumber hukum primer dan sekunder meliputi peraturan perundang-undangan, artikel jurnal, hingga berita elektronik. Berdasarkan proses penelitian yang telah dilakukan ditemukan bahwa di Indonesia sendiri sudah ada hukum yang mengatur terkait pelanggaran yang dilakukan oleh seseorang/badan yang terjadi di lingkungan maya/virtual yang tercantum di beberapa peraturan perundang-undangan baik di dalam UU ITE maupun KUHP. Namun pada proses pelaksanaannya masih ditemukan banyak kendala yang harus dihadapi oleh aparat penegak hukum dalam melaksanakan tugasnya terhadap kasus *CyberCrime* ini, salah satunya adanya ambiguitas pilihan pasal (*choice of law problem*).

Kata Kunci: Penipuan Online, Kejahatan Siber, Data Pribadi, UU ITE, KUHP

Abstract

The increasing prevalence of cybercrime, particularly online fraud, poses significant challenges for modern legal systems. Although a number of studies have highlighted the technological and criminological dimensions of

[1] Penelitian Mandiri 2024
[2] Alamat korespondensi: daffaSJ13@gmail.com.
[3] Email: agus_pramono62@yahoo.co.id.

cybercrime, scientific attention to the normative adequacy and effectiveness of the legal framework governing online fraud remains limited. This study fills this gap by examining the interaction between the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE) in regulating online fraud. The research questions addressed in this study are (1) How is online fraud regulated by law and (2) What are the obstacles faced in the process of enforcing the Law on Online Fraud? The research method used in this study is a legal-normative method by analyzing several primary and secondary legal sources, including legislation, journal articles, and electronic news. Based on the research process that has been carried out, it was found that in Indonesia itself, there are already laws that regulate violations committed by individuals/entities in the virtual environment, which are listed in several laws and regulations, both in the ITE Law and the Criminal Code. However, in the implementation process, law enforcement officials still face many obstacles in carrying out their duties in relation to cybercrime cases, one of which is the ambiguity of the choice of law.

Keywords: *Online Fraud, Cybercrime, Personal Data, ITE Law, Criminal Code*

A. Latar Belakang

Munculnya teknologi baru seperti *Metaverse* menghadirkan risiko tambahan terhadap kejahatan siber[4]. Perkembangan teknologi di Indonesia dewasa ini bersamaan dengan semakin meningkatnya penggunaan dan semakin meratanya akses internet dari tahun ke tahun. Pemanfaatan teknologi dan internet sendiri khususnya di negara Indonesia sangat beragam, mulai dari kebutuhan bisnis, pendidikan, hiburan, hingga keperluan komunikasi sehari-hari.[5] Kehadiran dan perkembangan internet yang pesat telah membentuk sebuah fenomena baru. Orang-orang dapat melakukan kegiatan berkomunikasi satu sama lain di dalam sebuah dunia baru yang bersifat maya atau semu. Hal ini mampu memberikan nuansa realitas baru di dunia komunikasi yang berbasis internet dan komputer[6]. Namun seiring dengan semakin pesatnya perkembangan teknologi yang ada, tentu saja selain dapat membawa dampak positif juga membawa dampak buruk tersendiri. Dampak buruk tersebut mengarah kepada tindak kejahatan dengan melakukan penyalahgunaan teknologi yang sering disebut dengan istilah *"CyberCrime"*[7].

CyberCrime adalah setiap tindakan ilegal yang dilakukan dengan

---

[4] Shafik, W., "Predicting future cybercrime trends in the metaverse era. In Forecasting Cyber Crimes in the Age of the Metaverse", *IGI Global*, 2023, (pp. 78–113). https://doi.org/10.4018/9798369302200.ch005.

[5] Hapsari, R.D., "Ancaman CyberCrime di Indonesia ", *Jurnal Konstituen*, 2023.

[6] Puspitasari, I., "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif di Indonesia", *HUMANI (Hukum dan Masyarkat Madani),* 2018.

[7] Lutfiana, Z., Zulfiani, A., "Analisis Pencurian E-Money pada Platform E- Commerce dalam Tindak Pidana Cybercrime yang Dikategorikan sebagai Tindak Pidana Ekonomi", Yustisia, 2024.

menggunakan sistem komputer di ruang siber[8]. Tindak kejahatan siber tersebut meliputi penipuan, perdagangan anak, penyebaran konten pornografi, pencurian kekayaan intelektual, pencurian identitas, pelanggaran privasi, dan lain sebagainya[9].

Beberapa faktor yang menjadi penyebab semakin banyaknya *CyberCrime* adalah (1) kapasitas ukuran data di komputer yang relatif kecil sehingga mempercepat proses pelaku untuk melakukan pencurian data, (2) kelalaian pemilik data dalam menyimpan dan memproteksi data pribadi, (3) komputer yang memiliki kompleksitas tinggi sehingga susah bagi orang awam dalam memberikan proteksi tambahan bagi data pribadinya di komputer, (4) data yang mudah dihapus, sehingga bukti-bukti tindak kejahatan susah untuk dilacak[10].

Cybercrime adalah kejahatan yang dapat dilakukan di lintas negara. Serangan siber pada dasarnya bersifat transnasional, sehingga memerlukan kerja sama internasional untuk membentuk kerangka regulasi yang diakui dan diterima secara universal. Sifat kejahatan siber yang tidak mengenal batas wilayah menantang batas yurisdiksi tradisional, sehingga kolaborasi internasional menjadi sangat penting[11]. Selain itu, *cybercrime* memiliki dampak global. Kejahatan siber memengaruhi kondisi ekonomi, sistem politik-ekonomi, dan kehidupan individu dalam skala global, dengan konsekuensi sosial-ekonomi yang signifikan[12].

Meskipun kejahatan siber telah menjadi objek kajian multidisipliner yang luas, sebagian besar penelitian terdahulu lebih menekankan pada aspek keamanan teknologi dan profil kriminologis pelaku. Hanya sedikit kajian yang menyoroti koherensi normatif dan efektivitas penegakan hukum terkait penipuan online terutama di negara berkembang, di mana infrastruktur hukum masih beradaptasi terhadap kompleksitas tata kelola digital. Ketidaksinkronan normatif ini menimbulkan ketidakpastian penegakan hukum, khususnya ketika ketentuan pidana konvensional seperti dalam KUHP beririsan dengan regulasi khusus seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

Berdasarkan permasalahan dan topik yang akan dibahas selanjutnya di dalam penelitian ini, maka perlu adanya rumusan masalah yang bertujuan untuk memberikan jawaban yang jelas dan tuntas atas apa yang menjadi dasar permasalahan yang akan dibahas dalam penelitian ini. Rumusan

---

[8] Chitadze, N., "Basic principles of information and cyber security. In Analyzing New Forms of Social Disorders in Modern Virtual Environments", *IGI Global*, 2023, (pp. 193–223). https://doi.org/10.4018/978-1-6684-5760-3.ch009.

[9] Dennis, M., A., 2024, "*CyberCrime*", Encyclopedia Britanica.

[10] Khadas, H., M., "The Causes of CyberCrime", *International Journal of Innovative Science and Research Technology*, 2020.

[11] Maskun, Irwansyah, Yunus, A., Safira, A., & Lubis, S. N., "Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It", *Jambe Law Journal*, 4(2), 2021, 131–150 https://doi.org/10.22437/jlj.4.2.131-150.

[12] Abubakari, Y., "The reasons, impacts and limitations of cybercrime policies in anglophone West Africa: A review", *Przestrzen Spoleczna*. (2021). https://www.scopus.com/pages/publications/85121982762?origin=resultslist.

masalah tersebut meliputi: (1) Bagaimana hukum yang mengatur penipuan *online*?; (2) Apa saja kendala yang dihadapi dalam proses penegakan Hukum Tentang Penipuan Online?

Penelitian yang dilakukan dalam penulisan karya ilmiah ini menggunakan metode penelitian yuridis-normatif melalui pendekatan terhadap peraturan perundang-undangan *(statute approach)* yang menjadi sumber hukum primer. Kemudian penelitian akan berfokus pada proses telaah ilmiah secara tekstual terhadap tulisan-tulisan hukum, asas-asas hukum, dan analisis antar peraturan perundang-undangan[13].

Penelitian dengan topik serupa sebelumnya yang telah dilakukan oleh peneliti lain dengan judul "Analisis Hukum Atas Pertanggungjawaban Tindak Pidana Penipuan Arisan Online Menurut Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus No.345/Pid.B/2017.Pn Tpg)" yang dilakukan oleh Ervina Sari Sipahutar berfokus pada penerapan UU ITE terhadap sebuah kasus Penipuan Arisan Online termasuk dengan perlindungan hukum bagi korbannya[14]. Kemudian penelitian lainnya dengan judul "Analisis Dampak Undang-Undang Cybercrime pada Pencegahan Penipuan Transaksi Elektronik di Sektor Perbankan Indonesia" yang dilakukan oleh Dhicky Fanandi Herwanta menjelaskan terkait implementasi UU ITE terhadap kasus penipuan transaksi elektronik pada sektor perbankan yang terjadi di Indonesia[15]. Kemudian berdasarkan penelitian yang telah dilakukan oleh peneliti lain tersebut, kebaharuan yang ada di penelitian ini terletak pada penerapan UU ITE secara umum terhadap tindak pidana kejahatan siber pada umumnya, dan kendala yang dihadapi aparat penegak hukum terhadap bentuk tindak pidana kejahatan baru ini di Indonesia.

B. Pembahasan

1. Hukum yang Mengatur Penipuan *Online*

Kasus terkait tindak kejahatan siber yang diadili pertama kali di Indonesia adalah pada kasus sengketa nama *domain* mustika-ratu.com yang didaftarkan oleh Tjandra Sugiono (selaku terdakwa) di Network Solution di USA pada Oktober 1999 lalu. Pada laman tersebut ternyata didapati bahwa produk yang tercantum adalah produk milik PT Martina Berto yang mana merupakan perusahaan saingan dari PT Mustika Ratu[16]. Kemudian hakim pada saat itu memberikan dakwaan dengan pasal 382 bis KUHP dan pasal 48

---

[13] M. Najibur Rohman, "Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia*", Jurnal Supremasi: Jurnal Ilmiah Ilmu Hukum*, 2021

[14] Ervina Sari Sipahutar, "Analisis Hukum Atas Pertanggungjawaban Tindak Pidana Penipuan Arisan Online Menurut Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus No.345/Pid.B/2017.Pn Tpg)", *Jurnal Normatif*, 2021

[15] Dhicky Fanandi Herwanta , "Analisis Dampak Undang-Undang Cybercrime pada Pencegahan Penipuan Transaksi Elektronik di Sektor Perbankan Indonesia ", *Repositori IBLAM*, 2024

[16] A. Wahyuwijaya dan Y. Risdiana, "Domain Name mustika-ratu Pasal 382 bis KUHP Menjangkau Dunia Maya?", *https://www.hukumonline.com/berita/a/domain-name-mustika-ratupasal-382-bis-kuhp- menjangkau-dunia-maya-hol7940/*, diakses pada 28 Desember 2024.

(1) jo Pasal 19 huruf B UU No. 5 Tahun 1999 Tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat dengan hukuman pidana 4 bulan dan denda sejumlah 30 juta rupiah[17]. Namun karena bukti terkait keuntungan yang diperoleh PT Martina Berto dan kerugian yang dialami oleh PT Mustika Ratu tidak terbukti di pengadilan pada waktu itu, maka hakim memberikan vonis bebas pada terdakwa pada 11 September 2001 lalu[18].

Berkaitan dengan semakin maraknya kegiatan *CyberCrime* yang terjadi di Indonesia, pemerintah bertindak dengan membuat undang-undang yang mengatur terkait pelanggaran yang terjadi di dunia maya yaitu melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diperbarui dan dicabut sebagian dengan beberapa peraturan baru meliputi UU No. 19 Tahun 2016, UU No. 1 Tahun 2023, dan UU No. 1 Tahun 2024.

Sebelum masuk pada pembahasan maka dipaparkan terlebih dahulu empat tipe umum dari *cybercrime* antara lain[19] (1) Komputer sebagai Sasaran: pencurian hak kekayaan intelektual, pencurian informasi pemasaran (misalnya, daftar pelanggan, data harga, atau rencana pemasaran), dan pemerasan berdasarkan informasi yang diperoleh dari berkas komputer (misalnya, informasi medis, riwayat pribadi, atau preferensi seksual); (2) Komputer sebagai alat kejahatan: penggunaan kartu dan rekening mesin teller otomatis (ATM) secara curang, pencurian uang dari rekening akrual, konversi, atau transfer, penipuan kartu kredit, penipuan dari transaksi komputer (transfer saham, penjualan, atau penagihan), dan penipuan telekomunikasi; (3) Penggunaan komputer merupakan hal yang bersifat insidental dalam kejahatan lain: pencucian uang dan transaksi perbankan ilegal, catatan atau buku kejahatan terorganisir, serta perjudian; dan (4) Kejahatan yang terkait dengan prevalensi komputer: pembajakan perangkat lunak/pemalsuan, pelanggaran hak cipta program komputer, peralatan palsu, perdagangan gelap peralatan dan program komputer, serta pencurian peralatan teknologi. Pada kasus tindak kejahatan siber pertama kali di Indonesia adalah masuk kategori cybercrime pertama. Hal ini dikarenakan nama domain masuk dalam ranah hak kekayaan intelektual. Kegiatan yang dilakukan oleh Tjandra Sugiono dalam istilah siber dinamakan *cybersquatting. Cybersquatting* adalah pendaftaran domain secara tidak sah yang meniru merek dagang yang sudah mapan dengan tujuan untuk mendapatkan keuntungan dari reputasi baik pemilik merek dagang yang sah. Praktik ini sering melibatkan pendaftaran domain secara

---

[17] Hukumonline, "Tjandra Sugiono Dituntut Pidana 4 Bulan dan Denda Rp30 Juta", *https://www.hukumonline.com/berita/a/tjandra-sugiono-dituntut-pidana-4-bulan-dan-denda-rp30-juta-hol4275*, diakses pada 28 Desember 2024

[18] Hukumonline, "Dakwaan Tidak Terbukti, Tjandra Sugiono Dibebaskan", *https://www.hukumonline.com/berita/a/dakwaan-tidak-terbukti-tjandra-sugiono-dibebaskan-- hol4451*, diakses pada 28 Desember 2024.

[19] Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A., *Cybercrime classification and characteristics*, Cyber Crime and Cyber Terrorism Investigator's Handbook, (2014). 149–164. https://doi.org/10.1016/B978-0-12-800743-3.00012-8.

tidak jujur untuk kemudian dijual kembali kepada pemilik merek dagang yang sah atau untuk membingungkan pengguna demi keuntungan ilegal[20].

Pasal 23 ayat (3) UU ITE mengatur bahwa setiap orang yang dirugikan karena penggunaan nama domain secara tanpa hak oleh orang lain maka dapat mengajukan gugatan pembatalan nama domain dimaksud[21]. Penggunaan nama domain secara tanpa hak maksudnya adalah pendaftaran dan penggunaan nama domain yang semata-mata ditujukan untuk menghalangi atau menghambat orang lain untuk menggunakan nama domain yang semestinya berhak atas nama domian tersebut, atau pendaftaran dan penggunaan nama domain yang bertujuan untuk mendompleng reputasi orang atau badan usaha lain dengan maksud mencari keuntungan atau merusak reputasi, atau menyesatkan konsumen.

Meskipun Pasal 23 Ayat (3) UU ITE mengakomodir gugatan pembatalan nama domain bagi pihak yang dirugikan, ketentuan ini mengandung lacuna atau kekosongan hukum yang signifikan. Regulasi tersebut gagal menyediakan mekanisme gugatan perdata khusus untuk ganti rugi, baik materiil maupun immateriil, bagi Pemilik Merek yang menjadi korban praktik *cybersquatting*. Akibatnya, meskipun nama domain dapat dibatalkan, kerugian ekonomi dan reputasi yang substansial seringkali tidak dapat dipulihkan.

Berdasarkan pasal 28 ayat (1) UU ITE dikatakan bahwa: siapapun yang secara sengaja menyebarkan informasi/dokumen elektronik yang sifatnya tidak sesuai dengan fakta dan dapat menyebabkan kerugian bagi orang lain, dapat dikenakan hukuman pidana yang dijabarkan dalam pasal 45A ayat (1) dengan hukuman penjara paling lama 6 tahun dan denda paling banyak Rp1.000.000.000[22]. Hal ini juga dapat diterapkan pada *cybersquattor.*

Terkait kerugian yang ditimbulkan dari adanya penyebaran informasi/dokumen elektronik dapat diberikan hukuman baik secara perdata maupun pidana. Apabila melihat dari korban yang mengalami kerugian secara material maupun nonmateriil, maka korban dapat mengajukan gugatan secara perdata sesuai dengan peraturan perundangan yang berlaku[23]. Pada kasus sejenis contoh di atas, penipuan online dalam bentuk *cybersquatting* dapat meminta ganti kerugian menggunakan pasal 1365 KUH Perdata karena apabila menggunakan pasal 23 ayat (3) UU ITE hanya mampu membatalkan nama domainnya saja. Kerugian lain tidak tercover dengan pasal yang ada dalam UU ITE. Unsur perbuatan melawan hukum

---

[20] Mondal, A., Paikaray, J., & Chatterjee, P. S., "Intelligent Legal and Technical Strategies to Mitigate Cybersquatting: Bridging Global Frameworks and Indian Contexts", ESIC 2025 - 5th International Conference on Emerging Systems and Intelligent Computing, Proceedings, 2025. 913–918. https://doi.org/10.1109/ESIC64052.2025.10962791

[21] Pasal 23 ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

[22] Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

[23] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

dalam kasus cybersquatting dapat diukur menggunakan indikator sebagai berikut. (1) Adanya perbuatan melawan hukum, (2) Adanya kesalahan, (3) Adanya unsur kerugian dan (4) Adanya hubungan kausal.

Adanya perbuatan melawan hukum dalam *cybersquatting* memenuhi unsur ini karena: (1) Melanggar Hak Subyektif: Praktik ini merupakan pelanggaran langsung terhadap hak kekayaan intelektual pemilik merek; (2) Melanggar Kewajiban Hukum: Tindakan ini bertentangan dengan asas itikad baik dalam hukum dan semangat undang-undang merek; (3) Bertentangan dengan Kesusilaan: Eksploitasi reputasi dan goodwill entitas lain secara parasitik bertentangan dengan prinsip persaingan usaha sehat dan etika bisnis.

Unsur kesalahan terpenuhi secara inherent melalui sifat *cybersquatting* yang dilakukan dengan itikad buruk (*bad faith*). Bukti itikad buruk dapat berupa niat menjual domain dengan harga tinggi, pola tindakan serupa, atau upaya sengaja menyesatkan konsumen.

Dilihat dari unsur kerugian, *cybersquatting* menyebabkan kerugian ganda yaitu kerugian materiil dan immateriil. Kerugian materiil dapat berupa kehilangan penjualan, biaya hukum dan proses sengketa, serta biaya pemasaran korektif, sedangkan kerugian immateriil dapat berupa tergerusnya ekuitas merek, reputasi, dan kepercayaan konsumen. Pelemahan daya pembeda merek ini merupakan kerugian immateriil signifikan dengan konsekuensi jangka panjang.

Indikator selanjutya adalah adanya hubungan kausal. Hubungan sebab-akibat langsung terbukti yaitu pendaftaran domain dengan itikad buruk langsung mengakibatkan kerugian-kerugian yang ada.

Korban *squatting* juga dapat melakukan penuntutan berdasar pasal 378 KUHP. Pasal ini menjerat pelaku dengan pidana penjara paling lama empat tahun[24]. Dalam pasal 378 KUHP juga disebutkan adanya unsur untuk mementingkan kepentingan pribadi dan pihak tertentu yang tujuannya untuk memberikan sesuatu oleh korban yang telah tertipu agar melakukan kegiatan yang sesuai dengan keinginan pelaku[25].

2. Kendala yang Dihadapi Dalam Proses Penegakan Hukum Tentang Penipuan *Online*

Perlindungan terhadap hak asasi manusia seringkali masih menjadi kendala dalam penegakan UU ITE. Implementasi belum sepenuhnya mempermudah penggunaan, penerapan, dan keabsahan alat bukti elektronik dalam perkara di pengadilan, sehingga dengan perkembangan teknologi ini kepastian dan keadilan hukum yang lebih baik belum diatur dengan jelas[26].

Pengaturan hukum di beberapa peraturan perundang-undangan terkait dengan penipuan online masih menciptakan persoalan terkait dengan aturan

[24] Pasal 378 Kitab Undang-Undang Hukum Pidana

[25] Zabindin, "Analisis Penegakan Hukum Tindak Pidana Penipuan Online di Indonesia", *Jurnal Spektrum Hukum*, 2021.

[26] Audrian, R.P., "Kendala Penerapan Pembuktian Dokumen Elektronik dalam Pemeriksaan di Pengadilan", *Causa: Jurnal Hukum dan Kewarganegaraan*, 2024.

mana yang cocok digunakan untuk menjerat jenis *cybercrime* tersebut. Adanya ambiguitas pilihan pasal (*choice of law problem*) pasal 378 KUHP dengan pasal 28 ayat (1) jo. 45 A (1) UU ITE dapat terjadi dengan melihat perbandingan di kedua pasal tersebut sebagai berikut.

Tabel 1. Perbandingan kedua aturan

Aspek	KUHP Pasal 378	UU ITE Pasal 28(1) jo 45A(1)
Rumusan Delik	"Dengan maksud menguntungkan diri sendiri... dengan nama palsu/keadaan palsu/tipu muslihat/rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang/membuat utang/menghapus piutang"	"Dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik"
Ancaman Pidana	Maksimal 4 tahun	Maksimal 6 tahun dan/atau denda Rp 1 miliar
Elemen Kunci	Tipu muslihat → menggerakkan → penyerahan barang/utang	Berita bohong → kerugian konsumen → dalam transaksi elektronik
Medium	Medium-agnostic (berlaku offline dan online)	Spesifik untuk transaksi elektronik
Unsur Korban	Tidak harus konsumen	Harus konsumen

Sumber: Data sekunder, diolah, 2025

Dilihat dari tabel perbandingan di atas, rumusan delik pasal 378 KUHP bersifat lebih luas dan abstrak. Pasal ini dirancang untuk menangkap inti perbuatan penipuan, terlepas dari medium yang digunakan. Unsur "tipu muslihat" atau "rangkaian kebohongan" dapat dengan mudah diterapkan pada tindakan *cybersquatting*, di mana pelaku membuat situs palsu yang menyerupai entitas bisnis sah untuk menipu korban. Rumusan delik pasal 28(1) jo. 45A(1) UU ITE lebih spesifik dan kontekstual. Pasal ini secara eksplisit mensyaratkan medium "Transaksi Elektronik" dan jenis korban "konsumen". Spesifisitas ini menjadi kekuatan sekaligus kelemahan, karena membatasi penerapannya hanya pada kasus yang melibatkan konsumen dalam transaksi elektronik, dan tidak mencakup, misalnya, penipuan antar badan usaha.

Dilihat di sisi medium kejahatan dan relevansi digital pada pasal 378 KUHP bersifat medium-agnostic. Pasal ini sama efektifnya untuk penipuan yang dilakukan secara tatap muka, melalui telepon, maupun secara online. Fleksibilitas ini memungkinkannya tetap relevan seiring dengan perubahan teknologi. Pada pasal 28 ayat (1) jo. 45A ayat (1) UU ITE bersifat medium-specific. Pasal ini secara khusus dirancang untuk lingkungan digital, sehingga memberikan penegak hukum dasar hukum yang langsung mengakar pada karakteristik transaksi elektronik, seperti kecepatan, lintas batas, dan kesulitan penelusuran.

Dilihat dari segi sanksi, pasal 378 KUHP menerapkan sanksi lebih ringan daripada UU ITE. Hal ini dikarenakan pasal 378 KUHP dulu asal-usulnya dirancang untuk penipuan konvensional, sedangkan sanksi pada UU ITE lebih berat karena dampak penipuan online lebih masif (menjangkau banyak korban) dan kerugian ekonomi serta kepercayaan publik terhadap ekosistem digital. Jaksa dalam hal membuat keputusan penuntutan akan lebih cenderung menerapkan sanksi yang lebih berat sebagai *bargaining power* di persidangan.

Dilihat dari elemen kunci, pasal 378 KUHP terdiri dari (1) Adanya tipu muslihat: pelaku gunakan kebohongan/identitas palsu (misal: situs phising mirip bank resmi); (2) Unsur menggerakkan: korban termotivasi oleh tipu daya untuk bertindak (misal: klik tautan, transfer uang); (3) Penyerahan barang/utang: korban kehilangan aset nyata (uang, data, barang), contoh: *cybersquatting* untuk menipu pemilik merek agar membeli domain dengan harga tinggi, sedangkan pasal UU ITE terdiri dari: (1) Berita bohong berupa konten palsu/menyesatkan (misal: iklan diskon 90% di situs cybersquatting); (2) Kerugian konsumen. Konsumen dirugikan secara ekonomis/psikologis (kehilangan uang, stres); (3) Transaksi elektronik. Kejahatan terjadi di ruang digital (situs, aplikasi, email).

Dilihat dari sisi korban misalnya, pasal 378 KUHP memiliki perlindungannya universal. Korban dapat siapapun yaitu individu, konsumen, atau badan usaha yang terdorong untuk menyerahkan barang atau uang akibat tipu muslihat. Ini membuatnya sangat relevan untuk kasus *cybersquatting* yang menargetkan pemilik merek (badan usaha) untuk memeras uang tebusan domain, sedangkan pasal 28(1) jo. 45A(1) UU ITE ruang lingkup perlindungannya terbatas. Pasal ini secara tegas hanya melindungi konsumen. Oleh karena itu, jika korban *cybersquatting* adalah perusahaan rival yang dirugikan, pasal ini tidak dapat diterapkan, meskipun kerugian terjadi dalam transaksi elektronik.

Kemudian pada pasal 28 Ayat (1) UU ITE juga tidak menjelaskan terkait kegiatan penipuan yang dilakukan ditujukan kepada siapa dan pihak mana yang diuntungkan dari tindak kejahatan. Namun penggunaan pasal tersebut pada umumnya lebih diberatkan kepada adanya kerugian yang ditimbulkan oleh pelaku melalui kegiatan di media elektronik[27]

[27] Rumlus, A., "Tanggung Jawab Hukum Pelaku Tindak Pidana Penipuan Berbasis *Online*", *UNISSULA Institutional Repository*, 2023

C. Penutup

Pengaturan hukum terkait dengan cybercrime berupa penipuan online sudah diatur dalam beberapa peraturan perundang-undangan baik di dalam UU ITE maupun KUHP. Kendala ynag dihadapi oleh penegakan hukum terkait penipuan online adalah adanya ambiguitas pilihan pasal (*choice of law problem*).

DAFTAR PUSTAKA

Buku

Dennis, M., A., 2024, "*CyberCrime*", Encyclopedia Britanica.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A., 2014, "Cybercrime classification and characteristics, Cyber Crime and Cyber Terrorism Investigator's Handbook, 149–164. https://doi.org/10.1016/B978-0-12-800743-3.00012-8.

Artikel Jurnal

Abubakari, Y., "The reasons, impacts and limitations of cybercrime policies in anglophone West Africa: A review", *Przestrzen Spoleczna*. (2021). https://www.scopus.com/pages/publications/85121982762?origin=resultslist

Audrian, R.P., "Kendala Penerapan Pembuktian Dokumen Elektronik dalam Pemeriksaan di Pengadilan", *Causa: Jurnal Hukum dan Kewarganegaraan* , 2024.

Chitadze, N., "Basic principles of information and cyber security. In Analyzing New Forms of Social Disorders in Modern Virtual Environments", *IGI Global*, 2023, (pp. 193–223). https://doi.org/10.4018/978-1-6684-5760-3.ch009.

Dhicky Fanandi Herwanta , "Analisis Dampak Undang-Undang Cybercrime pada Pencegahan Penipuan Transaksi Elektronik di Sektor Perbankan Indonesia ", *Repositori IBLAM*, 2024

Ervina Sari Sipahutar, "Analisis Hukum Atas Pertanggungjawaban Tindak Pidana Penipuan Arisan Online Menurut Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus No.345/Pid.B/2017.Pn Tpg)", *Jurnal Normatif*, 2021

Hapsari, R.D., "Ancaman CyberCrime di Indonesia ", *Jurnal Konstituen*, 2023.

Khadas, H., M., "The Causes of CyberCrime", *International Journal of Innovative Science and Research Technology*, 2020

Lutfiana, Z., Zulfiani, A., "Analisis Pencurian E-Money pada Platform E-Commerce dalam Tindak Pidana Cybercrime yang Dikategorikan sebagai Tindak Pidana Ekonomi", Yustisia, 2024.

M. Najibur Rohman, "Tinjauan Yuridis Normatif Terhadap Regulasi Mata Uang Kripto (Crypto Currency) di Indonesia*", Jurnal Supremasi: Jurnal Ilmiah Ilmu Hukum*, 2021.

Maskun, Irwansyah, Yunus, A., Safira, A., & Lubis, S. N., "Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with It", *Jambe Law Journal*, 4(2), 2021, 131–150 https://doi.org/10.22437/jlj.4.2.131-150.

Mondal, A., Paikaray, J., & Chatterjee, P. S., "Intelligent Legal and Technical

Strategies to Mitigate Cybersquatting: Bridging Global Frameworks and Indian Contexts", ESIC 2025 - 5th International Conference on Emerging Systems and Intelligent Computing, Proceedings, 2025. 913–918. https://doi.org/10.1109/ESIC64052.2025.10962791.

Puspitasari, I., "Pertanggungjawaban Pidana Pelaku Tindak Pidana Penipuan Online Dalam Hukum Positif di Indonesia", *HUMANI (Hukum dan Masyarkat Madani),* 2018.

Shafik, W., "Predicting future cybercrime trends in the metaverse era. In Forecasting Cyber Crimes in the Age of the Metaverse", *IGI Global*, 2023, (pp. 78–113). https://doi.org/10.4018/9798369302200.ch005.

Zabindin, "Analisis Penegakan Hukum Tindak Pidana Penipuan Online di Indonesia", *Jurnal Spektrum Hukum*, 2021.

Internet

A. Wahyuwijaya dan Y. Risdiana, "Domain Name mustika-ratu Pasal 382 bis KUHP Menjangkau Dunia Maya?", *https://www.hukumonline.com/berita/a/domain-name-mustika-ratupasal-382-bis-kuhp- menjangkau-dunia-maya-hol7940/*, diakses pada 28 Desember 2024

Hukumonline, "Dakwaan Tidak Terbukti, Tjandra Sugiono Dibebaskan", *https://www.hukumonline.com/berita/a/dakwaan-tidak-terbukti-tjandra-sugiono-dibebaskan-- hol4451*, diakses pada 28 Desember 2024.

Hukumonline, "Tjandra Sugiono Dituntut Pidana 4 Bulan dan Denda Rp30 Juta", *https://www.hukumonline.com/berita/a/tjandra-sugiono-dituntut-pidana-4-bulan-dan-denda-rp30- juta-hol4275*, diakses pada 28 Desember 2024

Peraturan perundang-undangan

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 6905.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Tambahan Lembaran Negara Republik Indonesia Nomor 4843