E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 10 No 2
2025

EKSISTENSI TINDAK PIDANA PENIPUAN (BEDROG) DALAM PASAL 378 KUHP DI ERA DIGITAL

Yusran Radyamal Al Miski
Universitas Pakuan, Indonesia, almiski.211221@gmail.com

Satria Manggala Putra
Universitas Pakuan, Indonesia, manggalaputra636@gmail.com

Muhammad Iqbal Purwanto
Universitas Pakuan, Indonesia, iqbalpurwanto67@gmail.com

Syadza Luthfiyyah
Universitas Pakuan, Indonesia, syadzaluthfiyyah02@gmail.com

Abstract

The advancement of digital technology has given rise to new and complex modes of fraudulent crime, necessitating an evaluation of the relevance of Article 378 of the Indonesian Criminal Code (KUHP) as a legal basis. This study aims to analyze the compatibility of conventional fraud elements under the KUHP with the characteristics of digital fraud and the challenges in its enforcement. The research employs a normative juridical approach through literature review and case analysis. The findings indicate that while Article 378 KUHP can be applied to digital fraud through broad interpretation, significant challenges remain, including perpetrator anonymity, cross-jurisdictional issues, and the need for digital evidence. Supporting regulations such as the ITE Law and the draft revision of the Criminal Code (RKUHP) play a role in expanding legal protection, yet policy updates are required to address legal gaps. The study concludes that Article 378 KUHP remains relevant but requires adaptation through dynamic interpretation and harmonization with specialized cybercrime regulations.
Keywords: *Article 378 KUHP, Criminal act of fraud, Cybercrime, Digital era, ITE Law.*

Abstrak

Penelitian ini diadakan karena adanya perkembangan teknologi digital telah melahirkan modus kejahatan penipuan baru yang kompleks, menuntut evaluasi relevansi Pasal 378 KUHP sebagai dasar hukum. Penelitian ini bertujuan menganalisis kesesuaian unsur-unsur penipuan konvensional dalam KUHP dengan karakteristik penipuan digital serta tantangan penegakannya. Metode penelitian menggunakan pendekatan yuridis normatif melalui studi literatur dan analisis kasus. Hasil penelitian menunjukkan bahwa meskipun Pasal 378 KUHP dapat diterapkan pada penipuan digital melalui interpretasi luas, terdapat tantangan signifikan seperti anonimitas pelaku, lintas yurisdiksi, dan kebutuhan alat bukti elektronik. Regulasi pendukung seperti UU ITE dan perkembangan RKUHP berperan memperluas perlindungan hukum, namun diperlukan pembaruan kebijakan untuk mengatasi celah hukum. Simpulan penelitian menegaskan bahwa Pasal 378 KUHP masih relevan tetapi memerlukan adaptasi melalui penafsiran dinamis dan harmonisasi dengan peraturan khusus kejahatan siber.
Kata kunci: Era digital, Kejahatan siber, Pasal 378 KUHP, Tindak pidana penipuan, UU ITE.

A. Pendahuluan

Perkembangan teknologi digital yang pesat telah membawa transformasi signifikan dalam berbagai aspek kehidupan, termasuk dalam dunia kejahatan. Salah satu dampaknya adalah munculnya modus cybercrime berbasis penipuan digital yang semakin kompleks dan sulit dilacak. Fenomena ini menimbulkan tantangan baru bagi penegakan hukum, khususnya dalam menerapkan ketentuan-ketentuan hukum pidana konvensional seperti Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP), yang dirumuskan jauh sebelum era digital.

Pasal 378 KUHP mengatur tentang tindak pidana penipuan (bedrog) dengan unsur-unsur klasik seperti adanya tipu muslihat, kebohongan, atau penyalahgunaan kesempatan yang mengakibatkan kerugian korban. Namun, karakteristik penipuan digital seperti anonimitas pelaku, penggunaan teknologi canggih, dan lintas batas yurisdiksi menuntut evaluasi ulang terhadap kesesuaian pasal tersebut sebagai dasar hukum. Selain itu, alat bukti elektronik (*digital evidence*) dan mekanisme penyidikan yang berbeda dari kejahatan konvensional turut mempersulit penanganan kasus.[1]

Beberapa regulasi pendukung, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Rancangan KUHP (RKUHP), telah berupaya memperluas cakupan hukum pidana di ruang digital. Namun, efektivitasnya masih dipertanyakan mengingat dinamika kejahatan siber yang terus berkembang. Oleh karena itu, penelitian ini bertujuan untuk menganalisis relevansi Pasal 378 KUHP dalam konteks penipuan

[1] Sulistyowati, E, *Cyber Law: Tinjauan atas UU ITE dan Implementasinya di Indonesia*, Refika Aditama, Bandung, 2019.

digital, mengidentifikasi tantangan penegakannya, serta mengevaluasi kebutuhan pembaruan kebijakan hukum.

Melalui pendekatan yuridis normatif dan analisis kasus, penelitian ini diharapkan dapat memberikan kontribusi akademis dalam memperkaya diskusi tentang perlindungan hukum terhadap kejahatan digital sekaligus memberikan rekomendasi bagi pembaruan sistem hukum pidana di Indonesia. Temuan penelitian ini juga dapat menjadi bahan pertimbangan bagi legislator, aparat penegak hukum, dan pemangku kepentingan lainnya dalam merespons tantangan kejahatan siber di masa depan.

B. Rumusan Masalah

1. Bagaimana kesesuaian unsur-unsur penipuan konvensional dalam Pasal 378 KUHP dengan karakteristik penipuan digital?
2. Apa saja tantangan penegakan hukum terhadap kejahatan penipuan digital berdasarkan Pasal 378 KUHP?
3. Bagaimana peran regulasi pendukung seperti UU ITE dan RKUHP dalam mengatasi celah hukum penipuan digital?
4. Upaya apa yang diperlukan untuk memperkuat relevansi Pasal 378 KUHP dalam menghadapi perkembangan kejahatan siber?

Rumusan masalah ini akan menjadi panduan dalam menganalisis efektivitas hukum pidana konvensional dalam menjawab tantangan kejahatan digital serta mengevaluasi kebutuhan pembaruan kebijakan hukum.

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, penelitian ini bertujuan untuk:

1. Menganalisis kesesuaian unsur-unsur penipuan konvensional dalam Pasal

378 KUHP dengan karakteristik penipuan digital, termasuk mengkaji apakah ketentuan hukum yang ada masih dapat mencakup modus-modus kejahatan siber yang berkembang.

2. Mengidentifikasi tantangan penegakan hukum terkait penerapan Pasal 378 KUHP pada kasus penipuan digital, seperti masalah anonimitas pelaku, lintas yurisdiksi, kesulitan pembuktian elektronik, serta kendala teknis dan prosedural dalam penyidikan.
3. Menilai peran regulasi pendukung seperti UU ITE dan RKUHP dalam melengkapi dan memperluas perlindungan hukum terhadap penipuan digital, serta mengkaji sejauh mana harmonisasi antara hukum pidana konvensional dan hukum siber.
4. Memberikan rekomendasi kebijakan hukum untuk memperkuat relevansi Pasal 378 KUHP dalam menghadapi kejahatan digital, baik melalui penafsiran dinamis, reformasi hukum, maupun penguatan kerangka regulasi yang lebih adaptif terhadap perkembangan teknologi.

D. Metode Penelitian

Pendekatan Penelitian ini menggunakan pendekatan yuridis normatif dengan analisis kualitatif. Pendekatan ini dipilih karena fokus penelitian adalah mengkaji aspek hukum tertulis (Pasal 378 KUHP, UU ITE, dan RKUHP) serta penerapannya dalam kasus penipuan digital. Jenis Penelitian ini bersifat deskriptif-analitis, yaitu menggambarkan dan menganalisis kesesuaian Pasal 378 KUHP dengan perkembangan penipuan digital serta mengidentifikasi tantangan dan solusi hukum. Teknik Pengumpulan Data, dengan Studi Dokumen (Library Research) dan Analisis Kasus (Case Study). Menggunakan metode penafsiran gramatikal, sistematis,

dan teleologis untuk menilai relevansi Pasal 378 KUHP.

E. Hasil Penelitian dan Pembahasan

Perkembangan teknologi digital telah menciptakan paradoks dalam sistem hukum pidana Indonesia. Di satu sisi, Pasal 378 KUHP yang menjadi dasar hukum penipuan konvensional tetap menunjukkan relevansinya, namun di sisi lain muncul berbagai tantangan implementasi ketika dihadapkan pada karakteristik unik penipuan digital. Penelitian ini mengungkap bahwa secara normatif, unsur-unsur dalam Pasal 378 KUHP masih dapat menjangkau tindak pidana penipuan digital melalui interpretasi ekstensif, khususnya dalam hal unsur tipu muslihat dan kerugian korban.

Temuan penelitian menunjukkan bahwa karakteristik penipuan digital yang meliputi anonimitas pelaku, penggunaan teknologi canggih, dan sifatnya yang lintas batas yurisdiksi menciptakan kompleksitas dalam penegakan hukum. Kasus-kasus yang dianalisis mengungkapkan bahwa aparat penegak hukum seringkali menghadapi kesulitan dalam hal pembuktian, terutama terkait alat bukti elektronik yang memerlukan keahlian khusus. Kondisi ini diperparah oleh belum optimalnya pemahaman para penegak hukum terhadap teknologi digital dan kerangka hukum yang mengaturnya.

Regulasi pendukung seperti UU ITE memang telah memberikan dasar hukum tambahan untuk menjerat pelaku penipuan digital. Namun, penelitian menemukan bahwa masih terdapat tumpang tindih dan inkonsistensi antara ketentuan dalam UU ITE dengan KUHP. RKUHP yang sedang dalam proses penyusunan tampaknya berusaha menjawab tantangan ini dengan memasukkan ketentuan khusus tentang kejahatan siber,

meskipun belum sepenuhnya mengakomodir dinamika perkembangan teknologi.[2]

Pembahasan teoritis mengungkapkan bahwa pendekatan hukum pidana konvensional yang bersifat territorial menghadapi tantangan serius dalam menangani kejahatan digital yang bersifat transnasional. Teori-teori hukum pidana modern menyarankan perlunya pendekatan kolaboratif antar negara dan penguatan kerangka hukum internasional. Selain itu, perkembangan terbaru dalam doktrin hukum menunjukkan pentingnya membangun sistem hukum yang lebih responsif terhadap perubahan teknologi.

Temuan penting lainnya adalah perlunya penguatan kapasitas aparat penegak hukum dalam menghadapi kejahatan digital. Pelatihan khusus tentang digital forensik dan pemahaman mendalam tentang karakteristik kejahatan siber menjadi kebutuhan mendesak. Penelitian ini juga mengidentifikasi perlunya standarisasi dalam penanganan bukti digital dan prosedur penyidikan yang sesuai dengan perkembangan teknologi.

Dari perspektif kebijakan hukum, penelitian ini menyoroti perlunya harmonisasi antara berbagai peraturan perundang-undangan yang mengatur tentang kejahatan digital. Pembaruan terhadap Pasal 378 KUHP perlu mempertimbangkan aspek-aspek khusus penipuan digital tanpa menghilangkan prinsip-prinsip dasar hukum pidana. Pendekatan kebijakan yang berorientasi pada pencegahan (preventif) melalui edukasi masyarakat tentang keamanan digital juga perlu diperkuat.[3]

[2] Indriyanto Seno Adji, "Reformulasi Tindak Pidana Penipuan di Era Digital" dalam *Jurnal Mimbar Hukum*, Vol. 33 No. 1, 2021.

[3] Harahap, M. Yahya, *Pembahasan Permasalahan dan Penerapan KUHAP*, Sinar Grafika, Jakarta, 2020.

1. **Unsur-Unsur Penipuan Konvensional Dalam Pasal 378 KUHP (Kitab Undang-Undang Hukum Pidana) Dirumuskan**

Unsur perbuatan dengan danya perbuatan menipu (bedrog) yang dapat berupa kebohongan, penyembunyian kebenaran, atau akal bulus, Menggerakkan orang untuk menyerahkan barang atau memberikan utang/piutang, atau menghapuskan piutang. Unsur kesalahan yang dilakukan dengan sengaja (*opzettelijk*) untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Unsur akibat yang menimbulkan kerugian bagi korban. [4]

Kesesuaian dengan Penipuan Digital (*cyber fraud*) memiliki karakteristik yang berbeda karena menggunakan teknologi informasi, tetapi secara substansi dapat memenuhi unsur-unsur Pasal 378 KUHP dengan beberapa penyesuaian:

a. Perbuatan Menipu dalam dunia digital: Dalam penipuan digital, kebohongan atau manipulasi dilakukan melalui media elektronik (email palsu, phishing, fake website, scam investasi online, dll.). [5]Contohnya sering terjadi penipuan dengan cara menelpon seolah-olah keluarga teman atau saudara kita kecelakaan dan membutuhkan biaya untuk pengobatan cepat. Unsur (menggerakkan orang) tetap ada, misalnya korban dikelabui untuk mentransfer uang atau memberikan data pribadi dengan alasan yang dibuat-buat oleh pelaku, contohnya “Selamat bapak mendapat hadiah sekian klik link dibawah untuk

[4] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta, 2008, hlm. 112–115.
[5] Andi Hamzah, *Hukum Pidana Siber*, Jakarta, 2021, hlm. 89–92.

melengkapi biodata agar dapat mencairkan hadiah tersebut." Secara tidak langsung korban akan merasa tergiur dengan uang dan masuk dalam jebakan.[6]

b. Kesengajaan dan Unsur Melawan Hukum: Pelaku sengaja menggunakan teknologi untuk menipu (misalnya hacking, social engineering).[7] Tujuan menguntungkan diri sendiri atau orang lain tetap relevan, seperti pencurian dana atau data. Banyak terjadi hal tersebut dilakukan saat kita memperbaiki handphone atau laptop yang rusak, tidak menutup kemungkinan orang akan mencuri data di dalamnya.

c. Kerugian dalam Penipuan Digital: Kerugian tidak hanya berupa barang fisik, tetapi juga aset digital (uang elektronik, *cryptocurrency*, akses akun). Banyak terjadi pembobolan akun media social yang Dimana itu sangat merugikan pihak-pihak tertentu karena media tersebut adalah sumber mata pencaharian mereka atau bisa disebut salah satu aset digital. Sering juga terjadi hilangnya uang digital atau yang biasa di sebut uang elektronik dengan secara tiba-tiba, kemungkinan adanya kerusakan system pada e-wallet yang dipakai.[8]

Kendala Penerapan Pasal 378 KUHP pada Penipuan Digital :

[6] Rizki Ananda, "Perlindungan Hukum terhadap Korban Penipuan Daring Berbasis Fintech" dalam *Jurnal Legislasi Indonesia*, Vol. 18 No. 3, 2021.
[7] Ronny Hanitijo Soemitro, *Tinjauan Hukum Kejahatan Siber*, Bandung, 2022,hlm. 134–136.
[8] Sofyan, Andi, "Penegakan Hukum terhadap Tindak Pidana Penipuan dalam Transaksi Elektronik" dalam *Jurnal Hukum Pidana dan Kriminologi*, Vol. 3 No. 2, 2019.

a. Keterbatasan terminologi: Pasal 378 KUHP tidak secara eksplisit mencakup modus digital. Isi Pasal 378 KUHP: "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau keadaan palsu, atau dengan tipu muslihat, atau rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu, atau memberikan hutang, yang dapat mendatangkan kerugian, diancam dengan pidana penjara paling lama empat tahun."

[9]Pasal ini mengatur tentang penipuan dengan menggunakan modus operandi seperti menyamar menggunakan identitas palsu, memberikan informasi yang salah, atau melakukan tindakan yang membujuk korban untuk menyerahkan harta benda atau memberikan pinjaman. Hukuman bagi pelaku penipuan ini adalah penjara maksimal 4 tahun.

b. Kesulitan pembuktian: Pelaku bisa berada di luar yurisdiksi, dan jejak digital memerlukan ahli IT untuk menggalinya.[10]

c. Perlunya aturan khusus: Indonesia memiliki UU ITE (Pasal 28 ayat (1) jo. Pasal 45) yang lebih spesifik untuk penipuan online. Isi Pasal 28 Ayat (1): "Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan

[9] Kitab Undang-Undang Hukum Pidana, UU No. 1 Tahun 2023, Pasal 378 tentang Penipuan.

[10] Marbun, Rocky, *Hukum Pidana Siber di Indonesia: Teori & Praktik*, Sinar Grafika, Jakarta, 2021.

antargolongan (SARA)." Sanksi Pidana (Pasal 45 Ayat (2)): Dipidana penjara maksimal 6 (enam) tahun dan/atau Denda maksimal Rp1 miliar. Unsur Pidana dengan Sengaja menyebarkan informasi, Tanpa hak (tidak ada izin atau dasar hukum), Bertujuan menimbulkan kebencian/permusuhan SARA.[11]

Contoh Pelanggaran seperti memposting atau mengupload ujaran kebencian di media social, Menyebarkan hoaks yang memicu konflik SARA, Konten provokatif yang menyerang kelompok tertentu.

Perkembangan Terkait UU ITE sering digunakan untuk menjerat ujaran kebencian dan penyebaran hoaks.

Pasal ini juga dikritik karena berpotensi membatasi kebebasan berekspresi, tetapi Mahkamah Konstitusi (MK) telah menegaskan bahwa pembatasan demi menjaga ketertiban umum sah secara konstitusional.[12]

Unsur-unsur Pasal 378 KUHP dapat diterapkan pada penipuan digital jika memenuhi:

a. Ada tindakan penipuan melalui sarana digital.
b. Ada kesengajaan untuk keuntungan tidak sah.
c. Menimbulkan kerugian bagi korban.

Namun, penegakan hukum sering mengacu pada UU ITE atau peraturan khusus (seperti PP tentang Transaksi Elektronik)

[11] "RKUHP dan Kejahatan Digital: Apa yang Berubah?", https://www.hukumonline.com/berita/a/mengulas-pengaturan-kejahatan-digital-dalam-kuhp-baru-lt63b3c9d523eb8/, diakses pada tanggal 15 Maret 2025.

[12] "Panduan Literasi Digital untuk Pencegahan Kejahatan Siber", https://aptika.kominfo.go.id/2023/08/upaya-pencegahan-dan-literasi-pegang-peranan-penting-hadapi-kejahatan-keuangan-digital/, diakses pada tanggal 10 Maret 2025.

karena lebih mengakomodasi karakteristik kejahatan digital.[13]

2. **Penegakan Hukum Terhadap Kejahatan Penipuan Digital Berdasarkan Pasal 378 KUHP (Kitab Undang-Undang Hukum Pidana) Menghadapi Beberapa Tantangan Utama, Terutama Karena Pasal Ini Awalnya Dirancang Untuk Penipuan Konvensional (Bedrog) Dan Belum Sepenuhnya Mengakomodasi Dinamika Kejahatan Digital.**

Pasal 378 KUHP mengatur penipuan tradisional dengan unsur: Adanya perbuatan menipu (*opzettelijke bedrog*). Membujuk korban untuk menyerahkan barang atau uang. Adanya kerugian bagi korban. Namun, kejahatan digital sering kali melibatkan metode yang lebih kompleks (seperti phishing, hacking, atau manipulasi data) yang tidak selalu sesuai dengan definisi klasik "penipuan" dalam KUHP.

Unsur "menipu" dalam penipuan digital sering kali bersifat *virtual* dan melibatkan rekayasa teknologi, sehingga sulit dibuktikan secara langsung.

Pelaku bisa menggunakan identitas palsu, VPN, atau rekening dummy, menyulitkan penelusuran. Transaksi digital (seperti cryptocurrency) sering kali anonim, mempersulit pelacakan aliran dana.

Banyak kasus penipuan digital melibatkan pelaku dari luar negeri, sementara Pasal 378 KUHP hanya berlaku di Indonesia. Proses ekstradisi atau kerja sama internasional sering kali lambat dan rumit.[14]

[13] Arief B. Witarto, "Penegakan Hukum terhadap Kejahatan Siber dalam Perspektif KUHP dan UU ITE" dalam *Jurnal Hukum dan Peradilan*, Vol. 10 No. 2, 2021.

[14] "Tantangan Penegakan Hukum Penipuan Online di Era Digital", https://www.kompasiana.com/muhammadirfan5596/657dfa86de948f19de43a6a2/tantangan-penegakan-

Banyak penyidang (polisi, jaksa, hakim) kurang memahami teknologi digital, sehingga kesulitan mengidentifikasi modus operandi atau mengumpulkan bukti digital. Bukti digital (seperti log server, metadata, atau rekaman digital) memerlukan keahlian khusus untuk diolah dan diajukan di pengadilan.

KUHP tidak secara eksplisit mengatur penipuan berbasis teknologi, sehingga sering kali harus dikombinasikan dengan UU lain seperti: UU ITE (Pasal 28 ayat (1) tentang Penyebaran Berita Bohong), UU Tindak Pidana Perdagangan Orang (jika melibatkan human trafficking scam), UU Perlindungan Konsumen (untuk penipuan e-commerce), Hal ini menyebabkan tumpang tindih hukum dan ketidakpastian dalam penuntutan.[15]

Modus penipuan digital terus berkembang (misalnya deepfake, AI scam, social engineering), sementara hukum pidana konvensional seperti KUHP tidak fleksibel mengikutinya. Proses penyidikan dan persidangan sering terlalu lama, sementara bukti digital bisa dengan mudah dihapus atau dimanipulasi.

Solusi yang diperlukan seperti, Revisi KUHP atau membuat regulasi khusus tentang cyber fraud yang lebih adaptif, peningkatan kapasitas aparat penegak hukum dalam hal digital forensic, Kerja sama internasional untuk penanganan kejahatan lintas negara, Sosialisasi kepada masyarakat untuk meningkatkan kewaspadaan terhadap penipuan digital.[16]

hukum-di-era-digital, diakses pada tanggal 30 Maret 2025.

[15] "Polemik UU ITE dan Penanganan Penipuan Online", https://nasional.kompas.com/read/2022/08/13/01460041/undang-undang-penipuan-online, diakses pada tanggal 2 April 2025.

[16] Wahyudi, Johannes, *Cybercrime & Digital Forensik: Pendekatan Hukum & Teknis*, Refika Aditama, Bandung, 2022.

3. **Peran Regulasi Pendukung Seperti UU ITE (Undang-Undang Informasi Dan Transaksi Elektronik) Dan RKUHP (Rancangan Kitab Undang-Undang Hukum Pidana) Dalam Mengatasi Celah Hukum Penipuan Digital Cukup Signifikan, Meskipun Masih Ada Tantangan Dalam Implementasinya.**

Hasil analisis menunjukan UU ITE (Undang-Undang No. 11/2008 yang diubah menjadi UU No. 19/2016) UU ITE ini menjadi dasar hukum utama untuk mengatasi kejahatan digital, termasuk penipuan online. Contoh beberapa pasal yang menyangkut kejahatan digital:

a. Pasal 28 ayat (1): Mengatur penyebaran informasi palsu yang menyesatkan (hoax) dan penipuan.
b. Pasal 35-36: Mengancam tindakan pencurian data, peretasan, atau manipulasi sistem elektronik.
c. Pasal 45-46: Memuat sanksi pidana bagi pelaku penipuan digital.

Kontribusi dalam penanganan penipuan digital seperti Memberikan payung hukum untuk menjerat pelaku penipuan online (*e-commerce fraud, phishing, scam*). Memungkinkan penyelidikan dan pelacakan transaksi digital dengan bantuan dari pihak kepolisian. Kekurangannya karena Pasal karet pada Pasal 27 ayat 3 tentang pencemaran nama baik yang sering disalahgunakan, mengalihkan fokus dari penipuan yang dilakukan. Proses pembuktian sulit, terutama jika pelaku menggunakan identitas palsu atau server luar negeri untuk mengelabui korban atau penyidik.[17]

[17] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.

RKUHP (yang menggantikan KUHP lama) memperbarui beberapa ketentuan terkait kejahatan digital, termasuk pada:

a. Pasal 478-479 RKUHP: Mengatur penipuan umum, termasuk yang dilakukan secara digital.
b. Pasal 263-264: Memperluas definisi penipuan dengan modus digital.[18]

Kontribusi dalam penanganan penipuan digital seperti, memperjelas unsur-unsur penipuan digital, termasuk manipulasi data dan transaksi elektronik, sanksi yang lebih tegas, termasuk denda besar dan pidana penjara. Kekurangannya karena tumpang tindih dengan UU ITE, berpotensi membingungkan penegak hukum dan implementasi belum maksimal karena masih dalam tahap sosialisasi. Tentang apa yang harus dilakukan untuk memperbaiki, dengan melakukanKoordinasi antarlembaga (Polri, BSSN, Kominfo) perlu diperkuat untuk investigasi penipuan digital. Lalu pembaruan regulasi untuk mencakup perkembangan teknologi seperti deepfake dan cryptocurrency scam. Dan yang paling penting adalah mengedukasi Masyarakat agar lebih waspada terhadap modus penipuan digital.

UU ITE dan RKUHP telah memberikan dasar hukum untuk memerangi penipuan digital, tetapi perlu pembaruan dan penegakan yang lebih efektif untuk menutup celah hukum yang masih ada. Kolaborasi antara pemerintah, penegak hukum, dan masyarakat juga kunci penting dalam mengurangi kasus penipuan online. [19]

[18] Kementerian Hukum dan Hak Asasi Manusia RI Tahun 2022, *Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP): Naskah Akademik*. Jakarta: Kemenkumham RI.

[19] Arief, Barda Nawawi, *Kejahatan Mayantara (Cyber Crime): Perkembangan & Penanggulangannya*, PT RajaGrafindo Persada, Depok, 2020.

4. **Untuk Memperkuat Relevansi Pasal 378 KUHP (Tentang Penipuan) Dalam Menghadapi Perkembangan Kejahatan Siber, Diperlukan Beberapa Upaya, Baik Dari Segi Hukum, Penegakan Hukum, Maupun Teknologi.**

Beberapa langkah yang dapat diambil, Penyesuaian Interpretasi Hukum (Reinterpretasi) seperti memperluas definisi "penipuan" dalam Pasal 378 KUHP agar mencakup modus kejahatan siber, seperti phishing, social engineering, atau manipulasi digital, Lalu memastikan unsur-unsur Pasal 378 (seperti "itikad buruk" dan "kerugian") dapat diterapkan pada kasus digital, misalnya dengan mengakui data sebagai objek yang dapat dicuri/dimanipulasi.

Pembaruan Aturan Pendukung, Mengintegrasikan dengan UU ITE (UU No. 11/2008 yang diubah menjadi UU No. 19/2016) untuk menjembatani kekosongan hukum terkait bukti digital dan transaksi elektronik. Memperkuat payung hukum turunan, seperti Peraturan Pemerintah atau Surat Edaran Mahkamah Agung, untuk memberikan panduan penerapan Pasal 378 dalam kasus siber. [20]

Peningkatan Kapasitas Penegak Hukum, Pelatihan aparat penegak hukum (polisi, jaksa, hakim) dalam menginvestigasi kejahatan siber dan memahami dinamika digital. Pembentukan unit khusus kejahatan siber yang memahami teknik digital forensik untuk mengumpulkan bukti elektronik yang sah di pengadilan.

Kolaborasi dengan Sektor Swasta dan Teknologi, Kerja sama dengan platform digital (perbankan, e-commerce, media sosial) untuk deteksi dini penipuan dan

[20] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 No. 58. Jakarta: Sekretariat Negara.

pelaporan cepat. Pemanfaatan teknologi AI dan big data untuk memantau transaksi mencurigakan atau pola penipuan berbasis siber.

Kesadaran Masyarakat (Awareness), Edukasi publik tentang modus kejahatan siber dan cara melaporkannya ke pihak berwajib. Kampanye literasi digital untuk mengurangi korban penipuan online yang mungkin kurang paham risiko teknologi.[21]

Harmonisasi dengan Hukum Internasional, Kerja sama lintas negara dalam penanganan kejahatan siber transnasional, mengingat banyak penipuan siber melibatkan pelaku dari luar yurisdiksi Indonesia.

Kendalanya adalah pada bukti digital yang seringkali sulit dipertahankan di pengadilan → Perlu standar pembuktian elektronik yang jelas untuk membuktikannya.

Solusinya dengan kecepatan perubahan teknologi → Hukum harus lebih fleksibel melalui legislasi dinamis atau asas analogi. Legislasi Dinamis merujuk pada kemampuan hukum untuk berkembang dan menyesuaikan diri dengan perubahan sosial, teknologi, ekonomi, dan nilai-nilai masyarakat tanpa harus selalu mengandalkan pembentukan undang-undang baru. Konsep ini menekankan pada penafsiran hukum yang fleksibel oleh hakim atau lembaga legislatif untuk memastikan hukum tetap relevan.

Asas analogi adalah metode penafsiran hukum dengan menerapkan ketentuan yang berlaku untuk suatu kasus tertentu ke kasus lain yang memiliki kesamaan esensial (prinsip atau tujuan hukum), meskipun fakta

[21] Artikel: "Penegakan Hukum terhadap Kejahatan Penipuan Digital di Indonesia" dalam Jurnal Hukum dan Peradilan, Vol. 8 No. 2, 2019.

kasusnya tidak identik. Legislasi dinamis dan asas analogi sama-sama alat untuk menghadapi ketertinggalan hukum, tetapi:

a. Legislasi dinamis bersifat progresif (mengembangkan hukum baru).
b. Analogi bersifat interpretatif (memperluas aturan yang ada).

Keduanya penting untuk hukum yang responsif, tetapi perlu dibatasi agar tidak melanggar kepastian hukum. Dengan pendekatan multidimensi ini, Pasal 378 KUHP dapat tetap relevan dalam menjerat pelaku kejahatan siber, meskipun idealnya juga perlu pembaruan KUHP secara menyeluruh (seperti dalam RKUHP) untuk mengakomodasi perkembangan kejahatan modern.[22]

F. Penutup/Kesimpulan

1. Kesimpulan

a. Kesesuaian Pasal 378 KUHP dengan Penipuan Digital, Pasal 378 KUHP yang mengatur penipuan konvensional memiliki unsur-unsur dasar seperti tipu muslihat, penyesatan, dan kerugian korban, yang secara prinsip dapat diterapkan pada penipuan digital. Namun, ketentuan ini tidak secara eksplisit mencakup modus-modus kejahatan siber yang kompleks, seperti phishing, social engineering, atau manipulasi data digital, sehingga menimbulkan ketidakpastian hukum.
b. Tantangan Penegakan Hukum, Anonimitas dan Lintas Yurisdiksi Pelaku penipuan digital sering menggunakan identitas palsu dan beroperasi lintas negara, menyulitkan

[22] Kurniawan, Budi, *Perkembangan Hukum Pidana Siber di Indonesia*, CV Andi Offset, Yogyakarta 2021.

identifikasi dan penangkapan. Pembuktian Elektronik Alat bukti digital (e.g., log transaksi, metadata) memerlukan keahlian khusus dan infrastruktur TI yang memadai, yang belum selalu tersedia di lembaga penegak hukum. Kendala Prosedural Proses penyidikan dan kerja sama internasional (e.g., *mutual legal assistance*) sering lambat dan tidak efektif untuk kejahatan siber yang dinamis.

c. Peran Regulasi Pendukung, UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) Pasal 28 ayat (1) UU ITE telah melengkapi Pasal 378 KUHP dengan mengkhususkan kejahatan siber, tetapi tumpang tindih norma dan ambigu dalam definisi menimbulkan masalah interpretasi. RKUHP Meski belum berlaku, RKUHP mencoba mengakomodasi kejahatan digital dengan memperluas definisi alat bukti dan modus penipuan, tetapi implementasinya perlu diuji. Harmonisasi Hukum Pidana dan Hukum Siber, Terdapat kesenjangan antara hukum pidana konvensional (KUHP) dan kebutuhan hukum siber, terutama dalam hal kecepatan respons, definisi tindak pidana, dan mekanisme pemulihan korban.

d. Agar Pasal 378 KUHP tetap relevan, diperlukan reinterpretasi hukum, pembaruan regulasi pendukung, peningkatan kapasitas penegak hukum, kolaborasi dengan sektor teknologi, dan edukasi masyarakat. Pendekatan multidisiplin ini akan memperkuat kerangka hukum dalam menjawab tantangan kejahatan siber yang terus berkembang.

2. Saran

Reformasi Hukum Substantif, Memperbarui Pasal 378 KUHP atau membuat ketentuan khusus dalam RKUHP yang mencakup modus penipuan digital secara eksplisit (e.g., manipulasi sistem elektronik, penggunaan malware). Menyederhanakan dan mengharmonisasikan UU ITE dengan KUHP untuk menghindari tumpang tindih dan dualisme penafsiran. Penguatan Kapasitas Penegakan Hukum, Membentuk unit khusus kejahatan siber (e.g., *Cyber Crime Unit*) dengan SDM terlatih dan teknologi digital forensics. Meningkatkan kerja sama internasional melalui perjanjian ekstradisi dan pertukaran data elektronik (e.g., dengan Interpol atau *ASEAN Cyber Capacity Program*). Penyempurnaan Alat Bukti dan Prosedur, Mengakui alat bukti digital (e.g., *blockchain, log server*) secara sah dalam KUHAP dan memastikan standar pembuktian yang jelas. Mempercepat proses penyidikan dengan mekanisme preservation request untuk data elektronik sebelum dihapus pelaku. Edukasi dan Perlindungan Korban, Sosialisasi literasi digital untuk mencegah penipuan dan memandu korban dalam pelaporan, Membentuk mekanisme ganti rugi yang cepat bagi korban, termasuk kerja sama dengan *platform digital* (e.g., pembekuan rekening penipu). Penafsiran Dinamis oleh Hakim, Mendorong hakim menggunakan penafsiran progresif (e.g., menganggap *phishing* sebagai "tipu muslihat" dalam Pasal 378 KUHP) melalui putusan-putusan landmark. Pembaruan hukum pidana harus seimbang antara kepastian hukum dan fleksibilitas menghadapi perkembangan teknologi. Kolaborasi antara legislator, penegak hukum, sektor privat, dan masyarakat sipil menjadi kunci untuk menciptakan kerangka hukum yang adaptif terhadap kejahatan digital.

Daftar Pustaka

1. Buku

Andi Hamzah, *Hukum Pidana Siber*, Sinar Grafika, Jakarta, 2021,

Arief, Barda Nawawi, *Kejahatan Mayantara (Cyber Crime): Perkembangan & Penanggulangannya*, PT RajaGrafindo Persada, Depok, 2020.

Harahap, M. Yahya, *Pembahasan Permasalahan dan Penerapan KUHAP*, Sinar Grafika, Jakarta, 2020.

Kurniawan, Budi, *Perkembangan Hukum Pidana Siber di Indonesia*, CV Andi Offset, Yogyakarta 2021.

Marbun, Rocky, *Hukum Pidana Siber di Indonesia: Teori & Praktik*, Sinar Grafika, Jakarta, 2021.

Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2008.

Ronny Hanitijo Soemitro, *Tinjauan Hukum Kejahatan Siber*, Remaja Rosdakarya, Bandung, 2022,

Sulistyowati, E, *Cyber Law: Tinjauan atas UU ITE dan Implementasinya di Indonesia*, Refika Aditama, Bandung, 2019.

Wahyudi, Johannes, *Cybercrime & Digital Forensik: Pendekatan Hukum & Teknis*, Refika Aditama, Bandung, 2022.

2. Artikel Jurnal

Arief B. Witarto, "Penegakan Hukum terhadap Kejahatan Siber dalam Perspektif KUHP dan UU ITE" dalam *Jurnal Hukum dan Peradilan*, Vol. 10 No. 2, 2021.

Indriyanto Seno Adji, "Reformulasi Tindak Pidana Penipuan di Era Digital" dalam *Jurnal Mimbar Hukum*, Vol. 33 No. 1, 2021.

Rizki Ananda, "Perlindungan Hukum terhadap Korban Penipuan Daring Berbasis Fintech" dalam *Jurnal Legislasi Indonesia*, Vol. 18 No. 3, 2021.

Sofyan, Andi, "Penegakan Hukum terhadap Tindak Pidana Penipuan dalam Transaksi Elektronik" dalam *Jurnal Hukum Pidana dan Kriminologi*, Vol. 3 No. 2, 2019.

Artikel: "Penegakan Hukum terhadap Kejahatan Penipuan Digital di Indonesia" dalam Jurnal Hukum dan Peradilan, Vol. 8 No. 2, 2019.

3. Internet

"Polemik UU ITE dan Penanganan Penipuan Online", https://nasional.kompas.com/read/2022/08/13/01460041/undang-undang-penipuan-online, diakses pada tanggal 2 April 2025.

"Tantangan Penegakan Hukum Penipuan Online di Era Digital", https://www.kompasiana.com/muhammadirfan5596/657dfa86de948f19de43a6a2/tantangan-penegakan-

hukum-di-era-digital, diakses pada tanggal 30 Maret 2025.

"RKUHP dan Kejahatan Digital: Apa yang Berubah?", https://www.hukumonline.com/berita/a/mengulas-pengaturan-kejahatan-digital-dalam-kuhp-baru-lt63b3c9d523eb8/, diakses pada tanggal 15 Maret 2025.

"Panduan Literasi Digital untuk Pencegahan Kejahatan Siber", https://aptika.kominfo.go.id/2023/08/upaya-pencegahan-dan-literasi-pegang-peranan-penting-hadapi-kejahatan-keuangan-digital/, diakses pada tanggal 10 Maret 2025.

4. Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana, UU No. 1 Tahun 2023, Pasal 378 tentang Penipuan.

Kementerian Hukum dan Hak Asasi Manusia RI Tahun 2022, *Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP): Naskah Akademik*. Jakarta: Kemenkumham RI.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 No. 58. Jakarta: Sekretariat Negara.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.