Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Tanggung Jawab Pelaku Tindak Pidana Penipuan Online pada Sistem Digital

Didik Suprasetya
didiksuprasetya20@gmail.com
Nur Handayati
nur.handayati@unitomo.ac.id
Moh. Taufik
moh.taufik@unutomo.ac.id
Vallencia Nandya Paramita
vallencia@unitomo.ac.id

ABSTRACT

The increasing number of cybercrime cases (especially in Indonesia) has drawn the government's attention to immediately enact laws that can be used to apprehend perpetrators of online crimes. The Indonesian government has included the Cybercrime Law (UU Cyber) in the ITE Law Number 11 of 2008, and hopes that this Law Number 11 of 2008 can address, reduce, and stop perpetrators of online crimes. The purpose of this study is to identify and analyze digital platforms that constitute criminal acts and to determine and analyze whether digital platforms can be held criminally responsible for online fraud that occurs within their systems. This research is normative legal research. The approaches used to address the research questions are the Conceptual Approach and the Statutory Approach. The results indicate that digital platforms can be categorized as a means of committing a crime if there is evidence that the platform is used to commit an unlawful act, or if the platform is negligent in providing an adequate security system. Criminal liability for digital platforms can be imposed through a corporate criminal law approach if negligence or profit is proven from illegal activities such as online fraud.

Keywords: *Responsbility, Perpetrator, Crime, Fraud, Online*

ABSTRAK

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cybercrime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya. Tujuan penelitian ini adalah Untuk mengetahui dan menganalisis platform digital yang termasuk tindak pidana

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

dan Untuk mengetahui dan menganalisis apakah platform digital dapat dimintai pertanggung jawaban pidana, atas terjadinya penipuan online yang terjadi pada system. Tipe penelitian ini adalah penelitian hukum normatif. Pendekatan yang digunakan untuk dapat menjawab permasalahan dalam penelitian ini adalah Pendekatan Konseptual (*Conceptual Approach*) Dan Pendekatan Perundang-Undangan (*Statute Approach*). Hasil penelitian menunjukkan bahwa Platform digital dapat dikategorikan sebagai sarana terjadinya tindak pidana apabila terdapat bukti bahwa platform tersebut digunakan untuk melakukan tindakan melawan hukum, atau jika platform lalai dalam menyediakan sistem keamanan yang memadai. Pertanggungjawaban pidana terhadap platform digital dapat dikenakan melalui pendekatan hukum pidana korporasi apabila terbukti adanya kelalaian atau keuntungan yang diperoleh dari aktivitas ilegal seperti penipuan online.

Kata kunci : *Tanggung Jawab; Pelaku; Tindak Pidana; Penipuan; Online*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dewasa ini sudah mengubah peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi membuat dunia menjadi tanpa batas sehingga mengakibatkan terjadinya dinamika sosial dalam bermasyarakat secara signifikan. Perkembangan teknologi informasi dan komunikasi memberikan banyak manfaat dalam berbagai aspek kehidupan manusia.

Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah "*cybercrime*". Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya mencakup Indonesia, tetapi juga mencakup seluruh dunia. Beberapa kejahatan yang terjadi disebabkan oleh maraknya penggunaan e-mail, e-banking dan e-commerce di Indonesia (Fairuzzen et al., 2024).

Dilihat segi positif dunia maya, telah membentuk trend perkembangan teknologi dunia dengan segala bentuk kreativitas manusia. Selain itu, kehadiran internet saat ini memudahkan seseorang dalam mengakses atau mendapatkan informasi, berinteraksi satu

samalain di media sosial atau jejaring sosial tanpa harus bertatap muka langsung. Perkembangan teknologi yang pesar, akan memunculkan berbagai permasalahan akibat penyalahgunaan teknologi informasi tersebut. Pada sisi lain penggunaan internet yang nyaris tanpa kendali menyebabkan berbagai tindak kejahatan di dunia maya, angka kejahatan online alias cybercrime telah menjadi tren baru di banyak Negara saat ini, termasuk di Indonesia.

Menurut *Organization Of European Comunnity Development* (OECD) *Cybercrime* adalah semua bentuk akses ilegal terhadap suatu data. Semua bentuk tindakan yang dilakukan secara tidak sah menggunakan komputer terutama untuk mengakses, mengirimkan, atau memanipulasi data merupakan suatu tindak kejahatan siber. Beberapa contoh kasus *cybercrime* yang terjadi di Indonesia adalah pencurian data pribadi seseorang karena adanya kebocoran data. Jika terjadi demikian maka pihak perusahaan atau organisasi yang mengalami *cybercrime* akan mengalami kerugian secara finansial serta penurunan tingkat kepercayaan konsumen. Dilihat dari sisi konsumen atau individu yang datanya bocor juga mengalami kerugian karena data pribadinya dapat dimanfaatkan oleh sejumlah oknum untuk tujuan tertentu (Agustin, 2024).

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cybercrime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Keterbatasan pengetahuan dan keterampilan aparat penegak hukum dalam bidang teknologi informasi menjadi kendala utama dalam penegakan hukum terhadap *cybercrime*. Banyak petugas yang tidak memiliki pelatihan khusus untuk menangani kasus-kasus yang melibatkan teknologi canggih, sehingga menghambat proses penyelidikan dan penuntutan (Waliadin, 2024). Ada kebutuhan mendesak untuk merevisi

UU ITE agar lebih relevan dengan perkembangan teknologi dan ancaman baru dalam dunia maya. Rancangan konsep KUHP yang baru juga diharapkan dapat mengakomodasi kejahatan siber yang semakin kompleks dan beragam. Pendidikan dan kesadaran masyarakat tentang risiko kejahatan siber juga menjadi isu penting. Masyarakat perlu dilatih untuk mengenali potensi ancaman dan cara melindungi diri mereka dari serangan *cyber*, sehingga dapat mengurangi jumlah korban kejahatan siber. Secara keseluruhan, isu hukum terkait *cybercrime* di Indonesia memerlukan perhatian serius dari semua pihak, termasuk pemerintah, lembaga penegak hukum, dan masyarakat untuk menciptakan lingkungan digital yang aman dan terlindungi dari ancaman kejahatan siber.

Topik ini sangat penting untuk diteliti karena dampak dari *cybercrime* tidak hanya merugikan individu, tetapi juga mengancam keamanan nasional dan stabilitas ekonomi. Kejahatan siber dapat menyebabkan kerugian finansial yang besar bagi perusahaan dan individu, serta mengganggu layanan publik seperti perbankan dan pemerintahan (Ashady, 2024). Oleh karena itu, penelitian tentang relevansi teknologi dalam penanggulangan kejahatan siber dapat membantu dalam merumuskan strategi yang lebih efektif untuk melindungi masyarakat dari ancaman ini. Dengan memahami dinamika kejahatan siber dan bagaimana teknologi dapat dimanfaatkan untuk pencegahan serta penanganannya, diharapkan dapat tercipta kebijakan yang lebih baik dan peningkatan kapasitas aparat penegak hukum dalam menghadapi tantangan ini. Penelitian ini juga dapat memberikan wawasan tentang kebutuhan pelatihan dan pengembangan infrastruktur yang diperlukan untuk meningkatkan efektivitas dalam menanggulangi kejahatan siber di Indonesia.

2. METODE PENELITIAN

Tipe penelitian ini adalah penelitian hukum normatif. Marzuki (2010), menjelaskan penelitian hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, maupun doktrin-doktrin hukum untuk menjawab permasalahan hukum yang dihadapi. Penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep

baru sebagai perskripsi dalam menyelesaikan masalah yang dihadapi. Penelitian hukum ini juga sering disebut dengan penelitian hukum doktriner karena penelitian hukum ini ditujukan atau dilakukan hanya pada peraturan-peraturan yang tertulis atau bahkan hukum yang lain. Dengan demikian, penelitian normatif mempunyai sifat tertutup artinya hanya terbatas pada hukum positif (peraturan perundang-undangan, yurisprudensi, hukum adat, konvensi ketatanegaraan, Dan lain-lain). Metode yang dipergunakan sesuai dengan ilmu mengenai cara-cara mengetahui hukum positif, yaitu metode penafsiran, analogi, konstruksi, perbandingan dan sejarah.

Pendekatan yang digunakan untuk dapat menjawab permasalahan dalam penelitian ini adalah Pendekatan Konseptual (*Conceptual Approach*) Dan Pendekatan Perundang-Undangan (*Statute Approach*) (Marzuki, 2011). Penelitian dengan pendekatan konseptual (*conceptual approach*) adalah penelitian yang dilakukan dengan melihat konsep-konsep tentang Dampak Perkembangan Teknologi dalam Penanggulangan kejahatan mayantara (*cybercrime*) di Indonesia yang terdapat dalam berbagai literatur. Penelitian dengan pendekatan perundang-undangan (*statute approach*) adalah penelitian dengan yang dilakukan dengan cara menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang ditangani.

3. PEMBAHASAN

Bentuk-Bentuk Platform Digital yang Termasuk Kejahatan Tindak Pidana

Pada kasus putusan Nomor 861/Pdt.G/2023/PN Sby tanggal 08 Maret 2022 antara penggugat (Slamet Supriyanto) dan tergugat (Idris Hasni) terjadi kesepakatan perjanjian jual beli barang yang dituangkan dalam Akta Notariil berdasarkan Akta Nomor : 09, “Akta Perjanjian Jual Beli Barang“ yang dibuat di hadapan turut tergugat (Dyta Ragellya Anggraini, S.H., M.Kn.) Notaris di wilayah Kabupaten Pasuruan. Bahwa Penggugat sebagai pemilik barang berupa pakaian pria dan wanita serta anak-anak dan Tergugat sebagai pihak pembeli, berdasarkan ketentuan yang dituangkan dalam klausul Akta

disebutkan antara Penggugat dan Tergugat telah bersepakat dengan ketentuan-ketentuan dan syarat-syarat sebagai berikut: "Pihak Pertama (Penggugat) setuju untuk menjual dan menyerahkan kepada Pihak Kedua (Tergugat) yang setuju dan sepakat untuk membeli dan menerima penyerahan barang dari pihak pertama (Penggugat)". Kondisi barang-barang yang dijual dengan kualitas baik dan tanpa cacat sedikit pun, adapun harga barang-barang yang diperjual belikan disepakati dan disetujui sebesar Rp. 200.000.000,- (*dua ratus juta rupiah*) yang dilakukan dengan sistem per termin. Setelah sekian lama Penggugat bersabar menunggu dan melakukan upaya yang patut menurut hukum untuk menagih sisa uang pelunasan tersebut terhadap Tergugat, akan tetapi hingga saat ini Tergugat belum sama sekali membayar sisa uang tersebut kepada Penggugat, maka hal ini jelas menunjukkan bahwa Tergugat telah melakukan ingkar janji (wanprestasi) terhadap kewajibannya kepada Penggugat. Oleh karenanya penggugat melalui kuasa hukumnya mengajukan gugatan ini ke Pengadilan Negeri Surabaya dengan dasar gugatan wanprestasi.

Perkembangan teknologi digital telah melahirkan beragam platform digital seperti marketplace, media sosial, dompet digital, hingga aplikasi keuangan. Dalam konteks hukum pidana, platform digital dapat dianggap turut serta dalam tindak pidana apabila terbukti menjadi sarana terjadinya kejahatan, atau lalai dalam pengawasan sistem keamanan yang menyebabkan kerugian pada pengguna.

Misalnya, jika suatu platform tidak menerapkan sistem keamanan data yang memadai dan memungkinkan terjadinya kebocoran data, maka hal ini dapat dikategorikan sebagai kelalaian yang mengakibatkan pelanggaran hukum berdasarkan UU ITE. Selain itu, dalam kasus penipuan online yang terjadi melalui platform e-commerce, platform dapat dikenai pertanggungjawaban apabila terbukti tidak melakukan verifikasi identitas pelaku atau tidak menindaklanjuti laporan dari korban secara memadai.

Bentuk-bentuk Tindak Pidana pada Platform Digital:

1. Tindak Pidana Informasi dan Transaksi Elektronik (ITE)

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Berdasarkan UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang ITE, beberapa bentuk tindak pidana di platform digital antara lain:

a) Pencemaran nama baik dan fitnah (Pasal 27 ayat 3). Misalnya: menyebarkan berita bohong atau menjatuhkan nama baik seseorang lewat media sosial.
b) Penipuan daring (online fraud) (Pasal 28 ayat 1). Misalnya: akun jual beli palsu di marketplace yang tidak mengirim barang setelah menerima pembayaran.
c) Penyebaran hoaks atau berita bohong (Pasal 28 ayat 1 dan 2). Contoh: menyebarkan isu yang menyebabkan keresahan publik melalui WhatsApp atau Facebook.
d) Konten bermuatan asusila atau pornografi digital (Pasal 27 ayat 1)

2. Tindak Pidana Keuangan Digital
   a) Manipulasi pasar dan insider trading di platform investasi atau grup saham digital (melanggar UU No. 8 Tahun 1995 tentang Pasar Modal).
   b) Investasi bodong melalui aplikasi atau website, seperti binary option, robot trading ilegal, atau money game.
   c) Pencucian uang digital (cyber laundering) melalui e-wallet atau platform pembayaran.
3. Tindak Pidana Perdagangan Orang dan Eksploitasi Anak

   Platform seperti media sosial atau aplikasi obrolan kerap disalahgunakan untuk:
   a) Eksploitasi seksual online.
   b) Perekrutan pekerja ilegal atau perdagangan manusia.
4. Tindak Pidana Peretasan dan Akses Ilegal
   a) Mengakses atau membobol sistem elektronik tanpa izin (Pasal 30 UU ITE).
   b) Penyebaran malware atau ransomware melalui tautan digital.

   Contoh Kasus:
   1) Kasus penyebaran hoaks COVID-19 melalui Facebook atau TikTok.
   2) Penipuan di platform jual beli (Shopee, Tokopedia, dll) oleh akun palsu.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

3) Kasus Binomo dan Quotex: aplikasi investasi bodong yang dijerat dengan pasal penipuan dan UU ITE.

Tindak pidana yang terjadi melalui platform digital dapat dijerat menggunakan:

1) UU ITE (utama)
2) KUHP (penipuan, pencemaran, penggelapan)
3) UU Perlindungan Konsumen
4) UU Pornografi
5) UU Tindak Pidana Perdagangan Orang
6) UU Pencucian Uang
7) UU Otoritas Jasa Keuangan, jika menyangkut platform keuangan.

Aspek Sosiologis

1) Rendahnya literasi digital masyarakat membuat mereka rentan menjadi korban.
2) Kurangnya pengawasan platform oleh negara terhadap konten dan aktivitas ilegal.
3) Anonimitas digital sering dimanfaatkan pelaku untuk menghindari jerat hukum.

Platform digital dapat menjadi media tindak pidana, baik karena kelalaian pengelola maupun karena disalahgunakan oleh pengguna. Oleh karena itu, penguatan regulasi, literasi digital, dan pengawasan hukum sangat penting untuk mencegah dan menindak kejahatan di era digital.

Platform Digital Dapat Dimintai Pertanggung Jawaban Pidana atas Terjadinya Penipuan Online yang Terjadi pada System

1. Dasar Hukum Terkait

Beberapa regulasi utama yang menjadi dasar dalam analisis ini:

a) UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)
b) KUHP (Kitab Undang-Undang Hukum Pidana) – terutama Pasal 378 tentang penipuan.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

c) UU No. 8 Tahun 1999 tentang Perlindungan Konsumen
d) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)
e) UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (jika data disalahgunakan)

2. Apakah Platform Digital Dapat Dimintai Pertanggungjawaban Pidana?

Secara umum, jawabannya: Bisa, dengan syarat tertentu.

a. Jika Platform Terbukti Lalai (Kelalaian yang Mengakibatkan Kejahatan) maka Platform digital dapat dimintai pertanggungjawaban pidana secara korporasi apabila:
   1) Tidak menyediakan sistem keamanan yang memadai.
   2) Tidak menindaklanjuti laporan penipuan dari pengguna.
   3) Membiarkan pengguna ilegal (scammer) beroperasi secara bebas dan berulang.
   4) Tidak melakukan verifikasi terhadap akun pengguna atau penjual.

   Contoh*:* Jika sebuah marketplace mengetahui adanya akun penipu tapi tetap membiarkannya bertransaksi, maka platform bisa dianggap lalai secara pidana.

b. Teori Pertanggungjawaban Korporasi

   Menurut doktrin pertanggungjawaban pidana korporasi, badan usaha (seperti platform digital) bisa dimintai pertanggungjawaban jika:
   1) Kejahatan dilakukan oleh orang dalam perusahaan (direksi, staf).
   2) Perusahaan mendapat keuntungan dari kejahatan tersebut.
   3) Perusahaan tidak melakukan pencegahan atau pengawasan yang layak.

c. Bentuk Pertanggungjawaban:
   1) Pidana korporasi: Denda besar atau pembekuan usaha (berdasarkan UU ITE dan PP PSTE).
   2) Pidana individu: Jika direksi atau pengelola platform turut serta atau lalai.

3) Gugatan perdata: Ganti rugi oleh korban (berdasarkan UU Perlindungan Konsumen atau KUHPerdata).

3. Analisis Kasus (Contoh Nyata)
   a) Kasus penipuan online di platform e-commerce seperti Shopee atau Tokopedia: meskipun pelaku utama adalah pengguna/penjual, korban kerap menggugat platform karena tidak adanya sistem verifikasi atau pengamanan yang kuat.
   b) Platform binary option (Binomo, Quotex): banyak yang akhirnya dijerat hukum karena mengizinkan sistem penipuan beroperasi dan bahkan beriklan secara aktif untuk menarik korban.
4. Pertimbangan Sosiologis dan Praktis
   a) Di satu sisi, platform hanya penyedia tempat dan bukan pelaku langsung.
   b) Namun di sisi lain, masyarakat awam melihat platform sebagai pihak yang bertanggung jawab, karena transaksi terjadi dalam sistem yang dikelola oleh platform tersebut.

Pertanggungjawaban pidana platform digital dalam konteks penipuan online masih menjadi perdebatan dalam praktik hukum Indonesia. Secara prinsip, pertanggungjawaban pidana menuntut adanya mens rea (niat jahat) dan actus reus (perbuatan melawan hukum). Dalam banyak kasus, platform digital tidak memiliki niat jahat, tetapi kelalaian dalam sistem keamanan atau pengawasan aktivitas pengguna dapat menjadi dasar tanggung jawab secara hukum.

UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) memang tidak secara eksplisit menyebutkan pertanggungjawaban pidana korporasi digital. Namun, doktrin hukum pidana memungkinkan penerapan corporate criminal liability apabila platform digital memperoleh keuntungan dari aktivitas ilegal tersebut atau lalai dalam melindungi konsumen.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

Relevansi Perkembangan Teknologi terhadap Penanggulangan *Cybercrime*

Teknologi bukan hanya menjadi pemicu kejahatan dunia maya, tetapi juga berperan penting dalam penanggulangannya. Penggunaan teknologi forensik digital, big data, hingga sistem keamanan berbasis Artificial Intelligence (AI) sangat diperlukan dalam mendeteksi dan mengatasi kejahatan siber. Namun, kemajuan teknologi juga menuntut peningkatan kapasitas SDM, baik dari sisi penegak hukum maupun pengguna platform digital itu sendiri.

Masih lemahnya pengetahuan aparat penegak hukum terhadap modus-modus baru cybercrime dan keterbatasan anggaran menjadi hambatan besar dalam penanganan kejahatan siber di Indonesia. Oleh karena itu, diperlukan strategi nasional yang komprehensif yang mencakup regulasi, pelatihan aparat, serta kerjasama internasional untuk membendung eskalasi kejahatan digital lintas batas.

Perlindungan Hukum terhadap Korban Kejahatan Mayantara (*Cybercrime*)

Perlindungan hukum merupakan hak konstitusional warga negara yang dijamin dalam Pasal 28G ayat (1) UUD 1945. Dalam konteks kejahatan siber (cybercrime), korban memerlukan perlindungan hukum baik secara preventif (pencegahan) maupun represif (penegakan hukum). Perlindungan ini bertujuan untuk memulihkan kerugian yang dialami korban serta memberikan rasa aman terhadap penggunaan teknologi informasi.

a. Instrumen Hukum yang Berlaku

1. Undang-Undang Nomor 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE). Memberikan dasar hukum untuk melindungi individu dari berbagai bentuk kejahatan digital seperti pencurian data, penipuan daring, pencemaran nama baik, hingga konten ilegal.

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

2. KUHP dan RKUHP. Dalam hal tertentu, pasal-pasal umum dalam KUHP tetap dapat digunakan untuk menjerat pelaku kejahatan digital jika unsur-unsur pidananya terpenuhi, misalnya terkait penipuan, pemalsuan, dan pencurian.
3. Peraturan OJK dan BI. Dalam kasus kejahatan siber di sektor keuangan digital, perlindungan hukum juga diatur dalam peraturan Otoritas Jasa Keuangan dan Bank Indonesia untuk menjamin keamanan transaksi digital dan perlindungan nasabah.

b. Bentuk Perlindungan Hukum

1. Perlindungan Preventif. Meliputi edukasi digital kepada masyarakat, penguatan kebijakan keamanan data oleh penyedia platform, serta pengembangan sistem keamanan siber nasional.
2. Perlindungan Represif. Meliputi proses hukum terhadap pelaku kejahatan siber oleh aparat penegak hukum, restitusi terhadap korban, serta perbaikan kerugian yang ditimbulkan oleh kejahatan tersebut.
3. Perlindungan melalui Pemulihan (Rehabilitasi). Dalam beberapa kasus tertentu, korban juga membutuhkan bantuan pemulihan, seperti layanan konseling psikologis akibat kejahatan berbasis pencemaran nama baik atau intimidasi daring.

c. Tantangan dalam Perlindungan Hukum

1) Kurangnya pemahaman masyarakat tentang hak-haknya sebagai korban kejahatan digital.
2) Minimnya literasi digital dan sistem pelaporan yang belum maksimal.
3) Ketimpangan antara perkembangan teknologi dengan peraturan hukum yang ada, sehingga tidak semua bentuk kejahatan siber dapat diakomodasi dengan hukum positif saat ini.

Upaya penanggulangan kejahatan mayantara di Indonesia tidak cukup hanya dengan pendekatan penegakan hukum terhadap pelaku. Diperlukan pula strategi yang menyeluruh, salah satunya adalah penguatan perlindungan hukum bagi korban. Dengan pendekatan yang berorientasi pada korban (*victim-oriented*), diharapkan negara dapat

Tersedia di online: http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN: 2580-9113
P-ISSN: 2581-2033
LEX JOURNAL: KAJIAN HUKUM & KEADILAN

memberikan rasa aman bagi masyarakat dalam memanfaatkan teknologi informasi dan komunikasi.

4. PENUTUP

Bentuk-bentuk platform digital yang termasuk kejahatan tindak pidana yaitu : Pencemaran nama baik dan fitnah (Pasal 27 ayat 3). Misalnya: menyebarkan berita bohong atau menjatuhkan nama baik seseorang lewat media sosial. Penipuan daring (online fraud) (Pasal 28 ayat 1). Misalnya: akun jual beli palsu di marketplace yang tidak mengirim barang setelah menerima pembayaran. Penyebaran hoaks atau berita bohong (Pasal 28 ayat 1 dan 2). Contoh: menyebarkan isu yang menyebabkan keresahan publik melalui WhatsApp atau Facebook. Konten bermuatan asusila atau pornografi digital (Pasal 27 ayat 1). Manipulasi pasar dan insider trading di platform investasi atau grup saham digital (melanggar UU No. 8 Tahun 1995 tentang Pasar Modal). Investasi bodong melalui aplikasi atau website, seperti binary option, robot trading ilegal, atau money game. Pencucian uang digital (cyber laundering) melalui e-wallet atau platform pembayaran. Eksploitasi seksual online. Perekrutan pekerja ilegal atau perdagangan manusia. Mengakses atau membobol sistem elektronik tanpa izin (Pasal 30 UU ITE). Penyebaran malware atau ransomware melalui tautan digital.

Platform Digital Dapat Dimintai Pertanggungjawaban Pidana Jika Platform Terbukti Lalai (Kelalaian yang Mengakibatkan Kejahatan) maka Platform digital dapat dimintai pertanggungjawaban pidana secara korporasi apabila: Tidak menyediakan sistem keamanan yang memadai, Tidak menindaklanjuti laporan penipuan dari pengguna, Membiarkan pengguna ilegal (scammer) beroperasi secara bebas dan berulang, Tidak melakukan verifikasi terhadap akun pengguna atau penjual. Bentuk Pertanggungjawaban: Pidana korporasi: Denda besar atau pembekuan usaha (berdasarkan UU ITE dan PP PSTE) dan Pidana individu: Jika direksi atau pengelola platform turut serta atau lalai. Gugatan

perdata: Ganti rugi oleh korban (berdasarkan UU Perlindungan Konsumen atau KUHPerdata).

4. DAFTAR PUSTAKA

Agustin, S. (2024). *Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber*. *1*(6), 500–504.

Ashady, S. J. (2024). *Jurisdische : Jurnal Penelitian Hukum Cybercrime sebagai Kejahatan Dunia Maya dalam Perspektif Hukum dan Masyarakat Jurisdische : Jurnal Penelitian Hukum*. *1*, 34–46.

Marzuki, P. M. (2011). *Penelitian Hukum*. Kencana Prenada Media Group.

Mohamad Revaldy Fairuzzen, Abil Arya Putra, Akmal Reihan, & Lilik Prihatini S.H, M.H. (2024). Perkembangan Hukum dan Kejahatan Siber "Cybercrime" di Indonesia. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *2*(1), 139–153. https://doi.org/10.62976/ijijel.v2i1.372

Waliadin. (2024). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *Jurnal Thengkyang*, *15*(1), 37–48.