PERLINDUNGAN HUKUM NASABAH TERHADAP SERANGAN CYBER PADA PLATFORM PERDAGANGAN ASET DIGITAL (STUDI KASUS INDODAX)[1]

Oleh :
Peter Andre Mokorimban [2]
Dientje Rumimpunu [3]
Renny Nansy S. Koloay [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui langkah-langkah mitigasi yang dilakukan oleh Indodax telah sesuai dengan prinsip perlindungan konsumen dalam kasus serangan *cyber* dan untuk mengetahui bagaimana perlindungan hukum bagi nasabah platform perdagangan aset digital, seperti Indodax, dalam menghadapi risiko serangan *cyber* berdasarkan peraturan yang berlaku di Indonesia. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Penelitian ini menemukan bahwa regulasi normatif Indonesia (UUPK, UU ITE yang terakhir diubah, UU Perlindungan Data Pribadi, dan ketentuan BAPPEBTI/OJK) telah menyediakan kerangka hukum yang relevan untuk melindungi nasabah platform perdagangan aset digital, namun implementasi dan efektivitas pengawasan praktik keamanan sistem masih belum memadai berdasarkan analisis kasus Indodax dan praktik mitigasinya. 2. Implikasi kebijakan yang muncul dari temuan ini adalah perlunya penguatan penegakan (sanksi administratif dan audit independen), peningkatan kapasitas teknis aparat penegak hukum dan regulator, serta mekanisme penyelesaian sengketa yang lebih cepat dan khusus untuk insiden siber pada aset digital agar pemulihan hak nasabah dapat terjadi lebih efektif. Selain itu, harmonisasi kewenangan pengawasan (Bappebti/OJK/Kemenkominfo/BNPT/BSSN) dan mekanisme koordinasi insiden lintas lembaga perlu di atur lebih jelas untuk mengatasi persoalan yurisdiksi dan respons cepat terhadap serangan *cyber*.

Kata Kunci : *perlindungan hukum, nasabah, serangan cyber, platform perdagangan aset digital, kasus indodax)*

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi yang begitu pesat di era digital telah mendorong terjadinya transformasi yang membawa pengaruh luas terhadap berbagai aspek kehidupan masyarakat secara menyeluruh. Kemajuan tersebut tidak hanya menghadirkan berbagai inovasi dan kemudahan dalam aktivitas sehari-hari, tetapi juga melahirkan sistem serta pola interaksi baru yang lebih efektif, efisien, dan terintegrasi. Teknologi kini tidak lagi dipandang sekadar sebagai alat bantu, melainkan telah menjadi elemen penting yang menunjang produktivitas, memperluas akses layanan, serta meningkatkan kualitas kinerja dalam berbagai aktivitas manusia. Namun demikian, di balik berbagai manfaat yang ditawarkan, perkembangan teknologi juga memunculkan tantangan berupa meningkatnya risiko penyalahgunaan teknologi, kejahatan *cyber*, pelanggaran data pribadi, serta penyebaran informasi yang tidak akurat. Kejahatan yang berkembang seiring dengan kemajuan teknologi adalah kejahatan *cyber* yang memanfaatkan sistem dan jaringan digital sebagai sarana untuk melakukan tindakan kriminal.

Kejahatan *cyber* merupakan bentuk-bentuk kejahatan yang timbul karenapemanfaatan teknologi internet *Cybercrime* sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, Karakteristik unik dari kejahatan didunia maya tersebut antara lain ruang lingkup kejahatan, sifat kejahatan, pelaku kejahatan, modus kejahatan.[5]

Penggunaan mata uang dengan memanfaatkan teknologi informasi ini juga saat ini telah berkembang di masyarakat. Mata uang tersebut yang biasanya di sebut mata uang digital, kini telah dapat dimanfaatkan oleh masyarakat di berbagai negara, termasuk negara Indonesia. terdapat berbagai jenis mata uang digital yang umum digunakan di kalangan masyarakat, di antaranya seperti *Bitcoin* (BTC) adalah Mata uang digital, *Ethereum* (ETH) adalah platform *blockchain* untuk kontrak pintar dan aplikasi, *Tether* (USDT) adalah *stablecoin* yang di patok 1:1 terhadap dolar, serta berbagai aset kripto lainnya yang diperdagangkan melalui platform perdagangan aset digital seperti Indodax.

Indodax (PT Indodax Nasional Indonesia) adalah perusahaan marketplace dan *exchange* aset kripto terbesar di Indonesia yang mempertemukan penjual dan pembeli mata uang digital. Platform ini menyediakan layanan jual-beli, *trading*, serta

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 220711010629
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Eliasta Ketaren, "*Cybercrime, Cyber Space, dan Cyber Law*," *Jurnal TIMES*, Vol. V, No. 2, 2016, hlm. 36.

pengelolaan berbagai kripto seperti (*Bitcoin, Ethereum*) dan lebih dari 160 aset kripto lainnya di seluruh dunia selama 24 jam. Melalui Indodax masyarakat dapat membeli mata uang kripto yang terdapat pada bursa perdagangannya dengan menggunakan mata uang Rupiah. Platform *exchange* tersebut didirikan pada tahun 2014.[6] Indodax memiIiki Iebih dari 10 juta pengguna dan voIume perdagangan Iebih dari 3 miIiar per buIan. Ini teIah Iama diakui sebagai pIatform yang teIah menduduki peringkat pasar terbaik dunia untuk aset kripto berdasarkan IaIu Iintas situs menurut ICO AnaIytics. Keberadaan Indodax sebagai salah satu platform *exchange* terbesar di Indonesia menunjukkan bahwa perkembangan industri aset kripto di tanah air mengalami pertumbuhan yang sangat pesat. Dengan jumlah pengguna yang mencapai jutaan serta volume perdagangan yang tinggi setiap bulannya, Indodax tidak hanya berperan sebagai sarana transaksi, tetapi juga sebagai indikator meningkatnya minat masyarakat terhadap investasi dan perdagangan aset digital.

Sebagai platform digital yang terhubung secara global, Indodax tidak terlepas dari potensi risiko serangan *cyber* maupun kejahatan digital lainnya, sehingga diperlukan sistem keamanan yang kuat serta perlindungan hukum yang memadai guna menjamin keamanan dan kepastian hukum bagi para nasabah dalam melakukan transaksi aset kripto. salah satu kasus besar kejahatan *cyber* yang terjadi di Indonesia adalah peretasan sistem pada platform perdagangan aset kripto terbesar di Indonesia, yaitu Indodax, pada tahun 2024. Peristiwa ini terjadi pada 11 September 2024 ketika platform perdagangan kripto PT Indodax Nasional Indonesia (Indodax) mengalami serangan peretasan yang mengakibatkan kerugian perusahaan hingga sekitar Rp300 miliar. Dalam kasus Indodax, peretasan yang terjadi tidak hanya melibatkan kerugian finansial bagi pengguna, tetapi juga merusak kepercayaan masyarakat terhadap platform kripto dan sektor keuangan digital secara umum. Keamanan sistem informasi menjadi sangat penting dalam transaksi digital, terutama yang melibatkan aset kripto, yang nilainya dapat berfluktuasi dengan cepat dan dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, penting untuk memahami bahwa *cybercrime* bukan hanya masalah hukum yang berkaitan dengan pelaku, tetapi juga menyangkut perlindungan terhadap integritas sistem ekonomi digital dan data pribadi yang dimiliki oleh masyarakat.[7]

Indonesia memiliki peraturan yang mengatur mengenai kejahatan *cyber*, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Sebagaimana telah di ubah terakhir kali melalui undang-undang nomor 1 Tahun 2024 (perubahan kedua). Selain Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, perlindungan hukum terhadap nasabah platform perdagangan aset digital juga didukung oleh berbagai regulasi lainnya. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan jaminan hak kepada konsumen untuk memperoleh kenyamanan, keamanan, keselamatan, serta hak untuk mendapatkan kompensasi atau ganti rugi atas kerugian yang diderita akibat penggunaan barang dan/atau jasa. Selanjutnya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mewajibkan setiap penyelenggara sistem elektronik untuk menjaga kerahasiaan, keamanan, dan integritas data pribadi pengguna serta bertanggung jawab atas setiap pelanggaran yang mengakibatkan kebocoran data. Di samping itu, Peraturan BAPPEBTI Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka mengatur bahwa penyelenggara platform perdagangan aset kripto wajib menerapkan sistem keamanan yang andal serta manajemen risiko yang memadai guna melindungi dana dan data pelanggan. Ketiga regulasi tersebut menunjukkan bahwa secara normatif negara telah menyediakan kerangka hukum yang cukup untuk melindungi nasabah platform perdagangan aset digital dari berbagai risiko, termasuk serangan *cyber* dan penyalahgunaan data pribadi. penerapan hukum tersebut dalam kasus peretasan Indodax dinilai masih kurang efektif. Kejahatan *cyber* yang semakin kompleks dan terus berkembang sering kali tidak dapat dijangkau oleh hukum yang ada, baik karena kurangnya pemahaman teknis maupun kurangnya penegakan hukum yang tegas.[8]

---

[6] Ulasan Indodax Platform Crypto Paling Populer," *Tradingan.com*, https://tradingan.com/broker/indodax. Diakses 10/1/26.

[7] Rafi Septia Budianto Pansariadi and Noenik Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (2023): 287–98.

[8] Mohammad Fajri and Bagya Agung Prabowo, "Perlindungan Hukum Investor Dari Aspek Gharar, Dharar, Dan Qimar Dalam Transaksi Cryptocurrency Sebagai Al-Tsaman Dan Al-Mutsaman," in *Prosiding Seminar Hukum Aktual Fakultas Hukum Universitas Islam Indonesia*, 2024, 226–43.

Peretasan yang terjadi pada platform Indodax tersebut, terlihat bahwa perkembangan teknologi digital tidak hanya menghadirkan peluang ekonomi, tetapi juga membuka celah terjadinya risiko hukum yang kompleks. Kerugian finansial yang ditimbulkan serta terganggunya kepercayaan masyarakat menunjukkan bahwa keamanan sistem informasi dalam perdagangan aset digital merupakan aspek yang tidak dapat diabaikan. Dalam Hal ini perlindungan terhadap nasabah sebagai pengguna jasa platform menjadi isu yang sangat penting untuk dikaji secara mendalam, terutama dari sudut pandang hukum positif di Indonesia. Keberadaan berbagai regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi pada dasarnya telah memberikan landasan normatif dalam menanggulangi kejahatan *cyber*. Namun demikian, efektivitas penerapan peraturan tersebut dalam memberikan perlindungan hukum kepada nasabah platform perdagangan aset digital masih menimbulkan pertanyaan. Hal ini dikarenakan karakteristik kejahatan *cyber* yang bersifat lintas batas, cepat berkembang, dan memanfaatkan celah teknologi yang sering kali lebih maju dibandingkan dengan perangkat hukum yang tersedia.

B. Rumusan Masalah

1. Bagaimana langkah-langkah pencegahan (mitigasi) yang dilakukan oleh Indodax telah sesuai dengan prinsip perlindungan konsumen dalam kasus serangan *cyber*?
2. Bagaimana perlindungan hukum bagi nasabah platform perdagangan aset digital, seperti Indodax, dalam menghadapi risiko serangan *cyber* berdasarkan peraturan yang berlaku di Indonesia?

C. Metode Penelitian

Jenis penelitian yang digunakan dalam penulisan ini adalah pendekatan Yuridis Normatif.

PEMBAHASAN

A. Langkah-langkah Pencegahan (Mitigasi) Yang Dilakukan Oleh Indodax Telah Sesuai Dengan Prinsip Perlindungan Konsumen Dalam Kasus Serangan Cyber

1. Sistem keamanan platform

a. Kedudukan Sistem Keamanan Platform

Sistem keamanan platform merupakan unsur yang sangat menentukan dalam penyelenggaraan perdagangan aset digital karena seluruh proses transaksi, penyimpanan aset, dan pengelolaan akun pengguna bergantung pada keandalan sistem elektronik. Dalam konteks platform perdagangan aset digital seperti Indodax, keamanan bukan hanya persoalan teknis informasi, melainkan bagian dari kewajiban hukum pelaku usaha untuk menjamin bahwa jasa yang diberikan aman, dapat dipercaya, dan tidak merugikan konsumen. Dengan demikian, sistem keamanan platform harus dipahami sebagai instrumen perlindungan hukum yang menghubungkan kepentingan pelaku usaha, pengguna layanan, dan otoritas pengawas.

b. Keamanan Data dan Akun Pengguna

Keamanan data dan akun pengguna merupakan jantung dari perlindungan konsumen dalam perdagangan aset digital. Dalam praktiknya, akun pengguna adalah pintu utama menuju saldo rupiah, aset kripto, histori transaksi, dan data pribadi yang tersimpan pada sistem. Karena itu, kegagalan menjaga keamanan akun dapat berakibat langsung pada hilangnya aset dan terganggunya hak pengguna sebagai konsumen jasa digital. Dalam kerangka hukum, perlindungan akun tidak bisa dibebankan semata kepada pengguna melalui imbauan untuk menjaga password, melainkan harus dipikul pula oleh platform sebagai pihak yang menguasai sistem. Penerapan keamanan data menurut UU PDP mensyaratkan adanya tindakan preventif sejak awal proses pemrosesan data. Artinya, platform harus memastikan bahwa data pribadi hanya diproses untuk tujuan yang sah, dibatasi aksesnya, dan dijaga dari penyalahgunaan. Apabila terjadi kebocoran data, maka platform harus mampu menunjukkan bahwa langkah-langkah pengamanan yang memadai telah dilaksanakan sebelumnya. Dalam konteks Indodax, keamanan akun pengguna harus meliputi sistem login yang kuat, verifikasi berlapis, proteksi terhadap phishing, pembatasan login dari perangkat yang tidak dikenal, serta notifikasi aktivitas yang tidak biasa.[9]

c. Penerapan Keamanan Data Menurut UU PDP dan BAPPEBTI

Penerapan keamanan data dalam platform aset digital harus dibaca secara kumulatif antara UU PDP dan BAPPEBTI. UU PDP mengatur kewajiban umum pengendali data untuk menjaga keamanan data pribadi, sedangkan BAPPEBTI mengatur standar teknis pengamanan dalam perdagangan aset kripto.

[9] Riantika Pratiwi, Dkk, "Tinjauan Yuridis Perlindungan Data Pribadi Dalam Transaksi E-Commerce", Pagaruyuang Law Journal, Vol. 7, No. 2, Januari 2024, hlm.16.

Keduanya membentuk rezim hukum yang saling melengkapi. UU PDP menekankan tanggung jawab atas data pribadi, sementara BAPPEBTI menekankan mekanisme operasional untuk menjamin keamanan transaksi dan penyimpanan aset. Dalam konteks platform seperti Indodax, data pribadi pengguna yang harus dilindungi mencakup identitas, nomor kontak, informasi verifikasi, dan data akses akun. Jika data tersebut bocor, maka kerugian yang timbul tidak hanya berupa pelanggaran privasi, tetapi juga potensi kehilangan aset digital. Oleh karena itu, penerapan keamanan harus bersifat holistik, mulai dari pengumpulan data, penyimpanan, pemrosesan, distribusi internal, hingga penghentian akses. Platform wajib memiliki kontrol akses internal yang ketat, enkripsi data sensitif, sistem deteksi anomali, dan mekanisme respons insiden yang jelas.[10] BAPPEBTI memperkuat kewajiban ini melalui keharusan audit sistem dan pengawasan internal.

2. Upaya Mitigasi Risiko

a. Upaya mitigasi risiko dalam perdagangan aset digital

Upaya mitigasi risiko dalam perdagangan aset digital merupakan bagian penting dari sistem perlindungan hukum bagi pengguna layanan. Dalam praktiknya, risiko yang paling menonjol adalah peretasan akun, kebocoran data pribadi, dan kehilangan aset digital akibat akses tidak sah terhadap sistem platform. Karena itu, mitigasi tidak dapat dipahami hanya sebagai respons setelah insiden terjadi, melainkan harus ditempatkan sebagai kewajiban preventif yang melekat pada penyelenggara platform sejak awal operasional. Pada platform seperti Indodax, kebutuhan mitigasi menjadi semakin penting karena seluruh transaksi bergantung pada sistem elektronik yang tersambung dengan data identitas, otentikasi, dan aset bernilai ekonomi tinggi.

b. Pencegahan Peretasan

Pencegahan peretasan adalah tujuan paling mendasar dari sistem keamanan elektronik. Dalam konteks perdagangan aset digital, peretasan biasanya diarahkan pada pengambilalihan akun, pencurian kredensial login, penyusupan ke server, atau manipulasi transaksi. Oleh sebab itu, langkah mitigasi harus dibangun secara berlapis melalui autentikasi ganda, enkripsi data, pemantauan anomali, pengamanan akses internal, dan pembatasan hak akses pada sistem inti. Tanpa pengamanan berlapis, platform akan rentan menjadi sasaran serangan yang dapat menimbulkan kerugian masif dalam waktu singkat.[11]

Pada platform seperti Indodax, pencegahan peretasan seharusnya mencakup audit keamanan berkala, pengujian penetrasi, pemisahan jaringan sistem, serta verifikasi login yang lebih kuat. Langkah-langkah ini sejalan dengan praktik perlindungan siber yang dianjurkan dalam berbagai pedoman keamanan industri digital. Secara akademik, pendekatan ini mendukung prinsip perlindungan preventif karena risiko dicegah sebelum menimbulkan kerugian. Dengan demikian, pencegahan peretasan menjadi indikator utama apakah sistem elektronik telah memenuhi standar keamanan yang diharapkan oleh hukum dan praktik tata kelola yang baik.

c. Pencegahan kebocoran data

kebocoran data merupakan risiko yang sangat serius dalam perdagangan aset digital karena data pengguna biasanya mencakup nama, email, nomor telepon, identitas verifikasi, histori transaksi, hingga informasi akses akun. Ketika data tersebut bocor, dampaknya bukan hanya pelanggaran privasi, tetapi juga potensi serangan lanjutan berupa phishing, social engineering, dan pengambilalihan akun. Oleh sebab itu, mitigasi terhadap kebocoran data harus ditempatkan sebagai prioritas utama dalam desain sistem elektronik.

d. Pencegahan Kehilangan Aset

Kehilangan aset merupakan akibat paling langsung dari serangan *cyber* terhadap platform perdagangan kripto. Karena aset digital tersimpan dalam bentuk elektronik, peretasan terhadap akun atau server dapat menyebabkan perpindahan aset secara cepat dan sering kali sulit dipulihkan. Oleh sebab itu, sistem keamanan elektronik harus dirancang tidak hanya untuk menjaga data, tetapi juga untuk melindungi aset dari pengalihan yang tidak sah. Penyedia layanan

[10] Suparman, Raden Agus. "Hukum Siber Indonesia: Panduan Lengkap UU ITE & UU PDP (Terbaru)." Aguspajak.com. 17 Februari 2026. Diakses 24 Juni 2026.

[11] Dimas Andi, "Marak Kebocoran, Begini Taktik Perusahaan Kripto Lindungi Data Pengguna," Bisnis.com, 24 Mei 2023, https://market.bisnis.com/read/20230524/94/1658674/marak-kebocoran-begini-taktik-perusahaan-kripto-lindungi-data-pengguna, diakses 24 Juni 2026.

bertanggung jawab untuk mengembangkan keamanan yang berkelanjutan. Sementara itu, pengguna juga perlu waspada dan *aware* untuk ikut membantu melindungi data dan akun mereka.[12]

3. Transparansi informasi dan risiko nasabah

Transparansi informasi merupakan salah satu inti dari perlindungan konsumen karena hubungan antara pelaku usaha dan konsumen umumnya ditandai oleh ketimpangan pengetahuan. Pelaku usaha mengetahui secara penuh sifat layanan, manfaat, biaya, dan risiko yang melekat pada produk atau jasa, sedangkan konsumen sering kali hanya menerima informasi dalam bentuk promosi, ringkasan syarat dan ketentuan, atau penjelasan umum yang terbatas. Dalam situasi demikian, transparansi berfungsi sebagai mekanisme untuk mengurangi asimetri informasi dan memastikan konsumen dapat mengambil keputusan secara sadar dan bertanggung jawab. Secara historis, prinsip transparansi informasi selalu menyertai perkembangan perlindungan konsumen secara umum. Patut diketahui bahwa sistem perlindungan Konsumen tumbuh seiring dengan berkembangnya pola perekonomian yang makin lama makin pesat.[13]

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan dasar normatif yang tegas mengenai hak konsumen atas informasi. Pasal 4 huruf c menegaskan bahwa konsumen berhak atas "informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa". Ketentuan ini menunjukkan bahwa informasi merupakan hak dasar konsumen, bukan sekadar pelengkap dalam proses transaksi. Kewajiban tersebut diperkuat oleh Pasal 7 huruf b UUPK yang mewajibkan pelaku usaha untuk memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa. Dengan demikian, hukum positif meletakkan beban keterbukaan pada pelaku usaha, bukan pada konsumen. Dalam perspektif ini, penyampaian informasi risiko kepada nasabah adalah perintah normatif yang harus dipenuhi sebagai bagian dari kepatuhan terhadap UUPK. Aturan yang diberlakukan pada UUPK tidak memberikan perlakuan yang berbeda kepada masing-masing pelaku menyelenggarakan usaha kegiatan yang usahanya, sepanjang para pelaku usaha tersebut menjalankannya secara benar dan memberikan informasi yang cukup, relevan, dan dapat dipertanggungjawabkan, serta menyesatkan mempergunakan konsumen atau yang memakai tidak akan atau memanfaatkan barang dan/atau jasa yang ditawarkan kepada konsumen.[14]

4. Keseuaian dengan prinsip perlindungan konsumen

Prinsip perlindungan konsumen dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen bertumpu pada gagasan bahwa konsumen harus ditempatkan sebagai pihak yang wajib dilindungi dari kerugian akibat ketidakseimbangan posisi tawar dengan pelaku usaha. Dalam hubungan jasa digital maupun transaksi berbasis platform, konsumen pada umumnya tidak memiliki kontrol penuh atas sistem, prosedur internal, maupun risiko teknis yang melekat pada layanan. Karena itu, kesesuaian suatu kebijakan atau tindakan pelaku usaha dengan prinsip perlindungan konsumen harus diuji melalui sejauh mana pelaku usaha menjamin keamanan, kenyamanan, kepastian hukum, dan tanggung jawab atas risiko yang timbul. Dalam praktiknya, banyak konsumen yang belum memiliki pemahaman yang memadai mengenai hak dan kewajibannya sehingga berada pada posisi yang lebih lemah dibandingkan pelaku usaha. Faktor utama yang menjadi kelemahan dari konsumen adalah tingkat kesadaran konsumen akan hak-haknya sebagai konsumen. Oleh karena itu Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, berarti agar supaya menjadi suatu landasan hukum yang kuat bagi masyarkat agar dapat melakukan upaya pembinaan dan pendidikan konsumen.[15]

B. Perlindungan Hukum Bagi Nasabah Platform Perdagangan Aset Digital, Seperti Indodax, Dalam Menghadapi Risiko Serangan Cyber Berdasarkan Peraturan Yang Berlaku Di Indonesia.

Perlindungan hukum terhadap nasabah diatur dalam undang undang Nomor 8 tahun 1999 tentang perlindungan konsumen dan menetapkan

---

[12] Husen Miftahudin, "Cegah Peretasan, Simak Tips Aman Jaga Data Aset Kripto," Medcom.id, 24 Desember 2021, tersedia pada https://www.medcom.id/ekonomi/keuangan/nbwMGpxK-cegah-peretasan-simak-tips-aman-jaga-data-aset-kripto, diakses 24 Juni 2026.

[13] Dwi Edi Wibowo, "How Consumers in Indonesia are Protected Fairly?" *Indonesian Journal of Advocacy and Legal Services*, Volume 2 No. 1, 2020, hlm. 58.

[14] Herry F. Tuwaidan, "Pelanggaran Tindak Pidana oleh Pelaku Usaha terhadap Kewajiban Memberikan Informasi yang Benar tentang Barang Dikaitkan dengan Perlindungan Konsumen," Lex Et Societatis, Vol. VI, No. 8, Oktober 2018, hlm. 59

[15] Onang Bambungan, "Perlindungan Hukum terhadap Konsumen atas Kenyamanan, Keamanan dan Keselamatan dalam Mengkonsumsi Barang atau Jasa," Lex Administratum, Vol. XI, No. 4, 2023, hlm. 2.

hak serta kewajiban pelaku usaha. undang-undang ini bertujuan untuk memberikan kepastian hukum dan perlindungan kepada konsumen dalam bertransaksi, serta menciptakan keseimbangan antara hak dan kewajiban konsumen dan pelaku usaha. Ini juga bertujuan untuk mendorong pelaku usaha agar bertanggung jawab dalam menyediakan barang dan jasa yang aman dan berkualitas. Kepastian hukum inilah yang menjadi dasar dalam memberikan perlindungan kepada para pihak yang melakukan atau terlibat dalam suatu tindakan hukum. Berkaitan dengan transaksi jual beli melalui media elektronik termasuk jual beli aset kripto dan bitcoin, Pasal 28 Ayat (1) dan Pasal 45A Ayat (1) Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah menjelaskan bahwa pihak-pihak yang terbukti menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang memuat berita bohong atau informasi yang menyesatkan sehingga menyebabkan konsumen mengalami kerugian dalam transaksi yang dilakukannya dapat diancam dengan pidana penjara enam tahun dan/atau denda satu miliar rupiah.

Jual Beli Aset Digital Dengan Penggunaan *Cryptocurrency* Bitcoin yang telah dilakukan oleh member Pada Platform Trading Indodax Indonesia tidak didasarkan pada perjanjian antara pembeli dan penjual. Pada Platform Trading Indodax Indonesia pembeli dan penjual Beli Aset Digital Dengan Penggunaan *Cryptocurrency* Bitcoin tidak mengikat dirinya pada suatu perjanjian sama seperti transaksi jual beli yang dilakukan masyarakat pada pasar tradisional. Menurut Oscar Dermawan, Platform Trading Indodax Indonesia bertindak sebagai penyedia tempat jual beli aset digital *Cryptocurrency* salah satunya jenisnya Bitcoin kepada para member dan jika terjadi kerugian atau kendala dalam transaksi yang telah dilakukan, pihak PT. Indodax Nasional Indonesia tidak dapat dimintai pertanggung jawaban atas kerugian tersebut.[16] Hal ini terjadi karena mekanisme proteksi terhadap risiko harga *Cryptocurrency* dalam sistem hukun Indonesia dilakukan dengan mengalihkan resiko kepada investor yang mengharapkan keuntungan dari perubahan harga yang terjadi.

Penegakan hukum dalam kasus peretasan platform kripto Indodax mencerminkan kelemahan struktural dan fungsional dalam sistem hukum pidana siber di Indonesia. Salah satu kelemahan utama adalah kurangnya kapasitas teknis dari aparat penegak hukum, termasuk kepolisian dan kejaksaan, dalam memahami dan menangani kasus-kasus yang melibatkan teknologi tinggi seperti peretasan sistem digital dan pencurian data kripto.[17]

Jika platform gagal menyediakan sistem elektronik yang aman sehingga menimbulkan kerugian material bagi nasabah (berupa hilangnya saldo atau pembekuan akun), hal ini memenuhi unsur-unsur:

a. Wanprestasi (Pasal 1238 KUHPerdata): Kegagalan memenuhi kewajiban prestasi dalam menyediakan layanan perdagangan yang aman.
b. Perbuatan Melawan Hukum (Pasal 1365 KUHPerdata): Pelanggaran terhadap kewajiban hukum positif yang diatur dalam Pasal 15 UU ITE terkait kewajiban menyelenggarakan sistem elektronik secara andal dan bertanggung jawab.

Pihak Penyelenggara Sistem dan Transaksi Elektronik (PSTE) yang dalam hal ini adalah setiap orang yang membuat dan mengelola suatu sistem elektronik, baik itu masyarakat, badan usaha maupun lembaga pemerintah. PSTE merupakan pihak yang memiliki peran dasar dalam menjaga data-data pribadi sistem yang dijalankan agar terhindar dari kebocoran data seperti dalam kasus Bjorka atau serangan siber pada umumnya. Dengan kata lain, PSTE memiliki tanggung jawab dalam hal memelihara, menjaga dan melindungi semua data-data pribadi pengguna atau pelanggan sistem elektroniknya tersebut, kecuali jika kesalahan tersebarnya data, karena unsur kelalaian dan kesalahan yang dibuat oleh pengguna atau pelanggan terkait. Hal ini dinyatakan dalam (Pemerintah Pusat 2019) bahwa setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.

Pengelola sistem atau PSTE memiliki tugas dalam melindungi data yang dikelolanya dengan memberikan keamanan dari risiko gangguan siber selain itu juga memberikan pengawasan standar sistem pengoperasian siber sehingga tidak adanya akses ilegal yang terjadi oleh karena itu pihak

[16] Wawancara dengan Oscar Dermawan, Selaku CEO pada PT. Indodax Nasional Indonesia, Pada tanggal 25 Oktober 2024 Pukul 16:20 WIB.

[17] Irfa Khunainah, Soesi Idayanti, and Kanti Rahayu, Pembuktian Kepemilikan Aset Investasi Dengan Trading Kripto Indonesia (Penerbit NEM, 2024), https://books.google.com/books?hl=id&lr=&id=nQUCEQAAQBAJ&oi=fnd&pg=PR1&dq=Lemahnya+Penegakan+Hukum,+Kasus+Peretasan,+Platform+Kripto+Indodax&ots=GzYhbC_gG9&sig=nLiIV9NS3yBkEpnZ2KB4E8UQcp8.

pengelola sistem harus memberikan sebuah sistem yang aman dan akuntabel. Oleh karena itu, apabila kedepannya terdapat kesalahan teknis atau kebocoran data, pihak pengelola sistem wajib mengonfirmasi dan memberitahu tanggung jawab pihak pengelola sistem dalam menyelesaikan masalah kepada pemilik data dan juga menteri bahkan mengonfirmasi kepada masyarakat apabila memang diperlukan.[18]

Kerugian akibat serangan *cyber* pada praktiknya dapat muncul dalam beberapa bentuk. Pertama, kerugian berupa kehilangan akses terhadap akun dan aset digital. Dalam kondisi tertentu, nasabah tidak dapat login, menarik aset, atau mengalihkan kepemilikan aset karena sistem dinonaktifkan demi mitigasi insiden. Kedua, kerugian berupa pengalihan aset tanpa izin, yakni ketika pelaku memperoleh akses ilegal ke dompet digital atau sistem penyimpanan aset. Ketiga, kerugian berupa kebocoran data pribadi, yang dapat membuka peluang penipuan lanjutan, penyalahgunaan identitas, atau social engineering terhadap nasabah. Keempat, kerugian akibat menurunnya tingkat kepercayaan publik, yang secara ekonomi dapat menimbulkan dampak sistemik pada aktivitas perdagangan aset digital. Secara teoritis, kerugian tersebut menunjukkan bahwa aset digital bukan hanya objek ekonomi, melainkan juga objek perlindungan hukum. Karena itu, negara melalui hukum positif berkewajiban memastikan bahwa risiko dari aktivitas digital tidak sepenuhnya dipindahkan kepada konsumen. Dalam kerangka hukum perlindungan konsumen, pelaku usaha wajib menjamin keamanan layanan yang ditawarkan, sedangkan konsumen berhak memperoleh perlindungan dari kerugian yang timbul akibat penggunaan jasa yang tidak aman.[19]

UU Pelindungan Data Pribadi menegaskan bahwa pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Artinya, ketika terjadi kebocoran data akibat serangan *cyber*, maka aspek yang dilanggar bukan hanya kepentingan ekonomis nasabah, tetapi juga hak konstitusional atas rasa aman, perlindungan diri pribadi, dan martabat hukum sebagai subjek data.

a. Bentuk Perlindungan Preventif

   Perlindungan preventif adalah bentuk perlindungan hukum yang bertujuan mencegah timbulnya kerugian sebelum sengketa terjadi. Dalam konteks platform perdagangan aset digital, perlindungan preventif diwujudkan melalui kewajiban penyelenggara platform untuk menyediakan sistem yang aman, menerapkan manajemen risiko, melakukan verifikasi pengguna, menjaga kerahasiaan data, serta menjalankan audit keamanan secara berkala.

   Perlindungan preventif juga mencakup kewajiban memberikan informasi yang benar dan jujur kepada nasabah. Dalam praktik, platform wajib menyampaikan secara transparan risiko transaksi, risiko penyimpanan aset, kebijakan keamanan, dan prosedur pengaduan apabila terjadi gangguan sistem. Keterbukaan informasi sangat penting karena konsumen digital berada dalam posisi asimetris terhadap pengetahuan teknis yang dimiliki pelaku usaha.[20]

b. Bentuk Perlindungan Represif

   Jika kerugian telah terjadi, maka perlindungan hukum beralih ke bentuk represif. Perlindungan represif merupakan perlindungan melalui penegakan hukum dan pemulihan hak setelah terjadi pelanggaran. Dalam konteks serangan *cyber*, bentuk perlindungan represif dapat berupa gugatan ganti rugi, penyelesaian sengketa konsumen, sanksi administratif, maupun proses pidana terhadap pelaku serangan. [21]

Dari sudut hukum perdata, nasabah dapat menuntut penggantian kerugian apabila dapat dibuktikan bahwa platform tidak memenuhi kewajiban penyelenggaraan jasa secara aman. Pasal 19 UUPK menegaskan bahwa ganti rugi dapat berupa pengembalian uang, penggantian barang dan/atau jasa yang sejenis, atau perawatan kesehatan dan pemberian santunan sesuai kerugian yang diderita. Dalam konteks aset digital, bentuk ganti rugi yang paling relevan adalah pengembalian nilai aset, kompensasi atas kerugian transaksi, atau pemulihan saldo jika masih memungkinkan secara teknis.[22]

---

[18] Apryan Anggara Pratama, "Hacker Bjorka: Pihak yang Berperan dalam Pencegahan Kebocoran Data", Jurnal Hukum Magnum Opus, Vol. 6, No. 1, Februari 2023, hlm. 21.

[19] Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

[20] Op.Cit

[21] Dian Erika Nugraheny dan Ihsanuddin, "Perubahan Kedua UU ITE Resmi Berlaku, Diteken Jokowi 2 Januari Jadi UU 1 Tahun 2024," *Kompas TV*, 4 Januari 2024, diakses 20 Juni 2026, https://www.kompas.tv/nasional/474440/perubahan-kedua-uu-ite-resmi-berlaku-diteken-jokowi-2-januari-jadi-uu-1-tahun-2024

[22] Martika Melisa Awon, "Pertanggungjawaban Pelaku Usaha Terhadap Konsumen yang Dirugikan," Lex Privatum, Vol. VI, No. 5, Juli 2018, hlm. 36

Dari sudut administratif, otoritas pengawas dapat menjatuhkan sanksi apabila platform tidak memenuhi standar keamanan atau tidak melaksanakan kewajiban pelaporan insiden secara benar. Dari sudut pidana, serangan *cyber* dapat diproses berdasarkan ketentuan pidana dalam UU ITE dan UU Pelindungan Data Pribadi, terutama jika terdapat akses tanpa hak, manipulasi sistem, atau penyalahgunaan data pribadi. Namun demikian, perlu dibedakan antara pertanggungjawaban pelaku serangan dan pertanggungjawaban platform sebagai penyelenggara layanan. Keduanya dapat berjalan paralel, karena pelaku serangan dipidana, sedangkan platform tetap dapat dimintai tanggung jawab perdata atau administratif apabila kelalaian pengamanan terbukti.[23]

Ganti rugi menurut UUPK merupakan instrumen penting dalam memberi pemulihan kepada konsumen yang dirugikan. Pasal 19 ayat (1) UUPK menentukan bahwa pelaku usaha bertanggung jawab memberikan ganti rugi atas kerusakan, pencemaran, dan/atau kerugian konsumen akibat mengkonsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan. Norma ini bersifat imperatif, artinya kewajiban ganti rugi tidak bergantung pada itikad baik semata, melainkan pada adanya akibat kerugian yang timbul dalam hubungan konsumsi. Lebih lanjut, Pasal 19 ayat (2) UUPK menyebutkan bahwa ganti rugi dapat berupa pengembalian uang, penggantian barang dan/atau jasa yang sejenis atau setara nilainya, atau perawatan kesehatan dan/atau pemberian santunan sesuai ketentuan peraturan perundang-undangan. Dalam kasus serangan *cyber* pada platform aset digital, pengembalian uang dapat dimaknai sebagai pengembalian nilai aset yang hilang atau kompensasi setara kerugian yang dialami nasabah. Jika aset belum berpindah ke pihak yang tidak berhak, maka pemulihan rekening atau rekonsiliasi saldo dapat menjadi bentuk restitusi yang lebih tepat. Namun demikian, penerapan Pasal 19 UUPK dalam ruang digital menghadapi persoalan pembuktian. Nasabah harus membuktikan adanya hubungan kausal antara kelalaian platform dan kerugian yang diderita. Karena itu, dokumen transaksi, riwayat akses, notifikasi keamanan, dan hasil audit insiden menjadi sangat penting. Dalam praktik akademik, tanggung jawab pelaku usaha atas kerugian konsumen sering dikaitkan dengan prinsip tanggung jawab berbasis kesalahan yang diperluas oleh kewajiban kehati-hatian dalam penyediaan jasa.[24]

Selain UUPK, UU Pelindungan Data Pribadi membuka ruang tanggung jawab apabila kebocoran data pribadi terjadi akibat pemrosesan data yang tidak aman. UU PDP tidak hanya mengatur hak subjek data pribadi, tetapi juga meletakkan kewajiban pada pengendali data untuk memastikan keamanan pemrosesan data. Dengan demikian, apabila serangan *cyber* menyebabkan data pribadi nasabah bocor dan kemudian digunakan untuk tindakan lain yang merugikan, maka dapat timbul tanggung jawab hukum berdasarkan rezim perlindungan data pribadi.

Selain UUPK, UU Pelindungan Data Pribadi membuka ruang tanggung jawab apabila kebocoran data pribadi terjadi akibat pemrosesan data yang tidak aman. UU PDP tidak hanya mengatur hak subjek data pribadi, tetapi juga meletakkan kewajiban pada pengendali data untuk memastikan keamanan pemrosesan data. Dengan demikian, apabila serangan *cyber* menyebabkan data pribadi nasabah bocor dan kemudian digunakan untuk tindakan lain yang merugikan, maka dapat timbul tanggung jawab hukum berdasarkan rezim perlindungan data pribadi.[25]

UU ITE sebagaimana diubah dengan UU Nomor 1 Tahun 2024 juga penting karena menjadi dasar pengaturan perbuatan yang dilakukan melalui sistem elektronik. Dalam perspektif perlindungan nasabah, UU ITE berfungsi sebagai payung bagi penanganan akses ilegal, manipulasi data, gangguan sistem, serta tindakan melawan hukum lain yang dilakukan dalam ruang siber. Walaupun UU ITE lebih menonjol dalam ranah pidana dan penyelenggaraan sistem elektronik, keberadaannya mendukung argumentasi bahwa platform wajib memastikan sistemnya aman dan tidak membuka peluang bagi terjadinya serangan.

Pengawasan dalam perdagangan aset digital merupakan unsur yang sangat penting karena karakter aset kripto dan platform perdagangannya memiliki tingkat risiko yang tinggi, baik dari sisi keamanan sistem, perlindungan konsumen, maupun stabilitas transaksi. Dalam kerangka hukum Indonesia, pengawasan tidak hanya dimaknai sebagai kegiatan administratif, melainkan sebagai instrumen negara untuk memastikan bahwa penyelenggaraan perdagangan aset digital berjalan sesuai ketentuan, transparan,

[23] Loc.Cit.

[24] Windi Eka Oktaviani, "Tanggung Jawab Pelaku Usaha Terhadap Kerugian Konsumen Dalam Perspektif Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," Reformasi Hukum, Vol. XIX, No. 2, Juli–Desember 2016, hlm. 227.

[25] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

aman, dan dapat dipertanggungjawabkan. Oleh karena itu, keberadaan pengawasan berfungsi menjaga keseimbangan antara kepentingan pelaku usaha, kepentingan nasabah, dan kepentingan negara dalam menciptakan kepastian hukum.[26]

Pengawasan terhadap perdagangan aset digital berfungsi memastikan bahwa platform yang menyelenggarakan jual beli aset kripto memenuhi standar keamanan tertentu sebelum dan selama beroperasi. BAPPEBTI sebagai lembaga pengawas memiliki posisi strategis untuk menilai apakah penyelenggara perdagangan aset digital telah menjalankan kewajibannya sesuai ketentuan teknis yang berlaku. Dengan demikian, pengawasan bukan hanya sarana kontrol, melainkan juga mekanisme untuk menempatkan tanggung jawab hukum pada pelaku usaha yang mengelola aset dan data nasabah. Pengawasan juga harus dipahami sebagai bentuk kehadiran negara dalam melindungi kepentingan publik di ruang ekonomi digital. Karena aset digital diperdagangkan melalui sistem elektronik, maka risiko yang timbul tidak hanya menyangkut kerugian finansial, tetapi juga potensi kebocoran data pribadi, manipulasi transaksi, dan hilangnya kepercayaan masyarakat terhadap ekosistem perdagangan digital. Oleh sebab itu, regulasi BAPPEBTI harus dianalisis bukan semata sebagai aturan teknis perdagangan, melainkan sebagai bagian dari sistem perlindungan hukum yang meliputi perlindungan konsumen, pelindungan data pribadi, dan keamanan sistem elektronik.

PENUTUP

A. Kesimpulan

1. Penelitian ini menemukan bahwa regulasi normatif Indonesia (UUPK, UU ITE yang terakhir diubah, UU Perlindungan Data Pribadi, dan ketentuan BAPPEBTI/OJK) telah menyediakan kerangka hukum yang relevan untuk melindungi nasabah platform perdagangan aset digital, namun implementasi dan efektivitas pengawasan praktik keamanan sistem masih belum memadai berdasarkan analisis kasus Indodax dan praktik mitigasinya. Temuan menunjukkan adanya kesenjangan antara kewajiban hukum penyelenggara (seperti kewajiban sistem andal, transparansi risiko, dan kewajiban pelaporan insiden) dan praktik operasional nyata yang memperlihatkan kelemahan teknis, koordinasi antar-lembaga yang kurang optimal, serta tantangan pembuktian kausalitas kerugian bagi nasabah.
   Secara teoritis, hasil penelitian mempertegas bahwa prinsip perlindungan konsumen termasuk asas keamanan, transparansi, dan kepastian hukum masih relevan dan perlu dikontekstualisasikan dalam ranah ekonomi digital; penelitian ini menegaskan perlunya sintesis antara rezim perlindungan konsumen, hukum data pribadi, dan aturan sektor khusus agar kepastian hukum lebih kohesif. Secara praktis, penelitian menunjukkan bahwa penyelenggara platform harus meningkatkan praktik keamanan (sertifikasi ISO, proporsi cold storage, mekanisme deteksi anomali, dan prosedur respons insiden) serta memperbaiki cara penyampaiian informasi risiko agar memenuhi kewajiban keterbukaan dan mengurangi asimetri informasi terhadap nasabah.
2. Implikasi kebijakan yang muncul dari temuan ini adalah perlunya penguatan penegakan (sanksi administratif dan audit independen), peningkatan kapasitas teknis aparat penegak hukum dan regulator, serta mekanisme penyelesaian sengketa yang lebih cepat dan khusus untuk insiden siber pada aset digital agar pemulihan hak nasabah dapat terjadi lebih efektif. Selain itu, harmonisasi kewenangan pengawasan (BAPPEBTI/OJK/KEMENKOMINFO/BNPT / BSSN) dan mekanisme koordinasi insiden lintas lembaga perlu di atur lebih jelas untuk mengatasi persoalan yurisdiksi dan respons cepat terhadap serangan *cyber*.

B. Saran

1. Bagi praktisi dan penyelenggara platform aset digital, hasil penelitian ini menegaskan pentingnya penguatan keamanan siber melalui audit berkala, deteksi dini, dan respons insiden yang cepat. Selain itu, syarat dan ketentuan layanan perlu dibuat lebih jelas, terutama mengenai tanggung jawab penyelenggara, risiko serangan siber, dan mekanisme pengaduan agar perlindungan hukum bagi nasabah lebih pasti.
2. Bagi regulator dan pemangku kepentingan, diperlukan koordinasi pengawasan yang lebih efektif antar-lembaga untuk mencegah tumpang tindih kewenangan dan mempercepat penanganan insiden. Pemerintah juga perlu menetapkan standar keamanan minimum bagi platform aset digital, termasuk kewajiban transparansi perlindungan data,

[26] Badan Pengawas Perdagangan Berjangka Komoditi, Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka, Peraturan Bappebti Nomor 8 Tahun 2021.

pelaporan insiden, dan evaluasi kepatuhan secara berkala.

DAFTAR PUSTAKA

Buku

Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd Edition (Sebastopol: O'Reilly Media, 2017).

Ary Putra Ananda, "*Perlindungan Hukum Terhadap Pengguna Grabcar Sebagai Transportasi Berbasis Aplikasi Online Medan Menurut Hukum Positif Indonesia* (Studi Kasus : Grab Indonesia PT. Aria Ruth Deory)" (Doctoral dissertation, Universitas Medan Area, 2017).

Bahan Ajar Kriminologi, Universitas Sam Ratulangi Fakultas Hukum

CST Kansil," in *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia* (Jakarta: Balai Pustaka, 1980).

Ida Bagus Rachmadi Supancana, *Kerangka Hukum Dan Kebijakan Investasi Langsung Di Indonesia* (Jakarta: Ghalia Indonesia, 2006).

Irfa Khunainah, Soesi Idayanti, and Kanti Rahayu, Pembuktian Kepemilikan Aset Investasi Dengan Trading Kripto Indonesia (Penerbit NEM, 2024).

M. Fajri, *Cybercrime dan Permasalahannya*, (Jakarta:, 2008).

Pedro Franco, Understanding Bitcoin : *Cryptography, Engineering, and Economics* (UK: TJ International Ltd, Great Britian UK, 2015).

Rafi Septia Budianto Pansariadi and Noenik Soekorini, "*Tindak Pidana Cyber Crime Dan Penegakan Hukumnya*," *Binamulia Hukum* 12, no. 2 (2023).

Satjipto Rahardjo, "*Ilmu Hukum*," (Bandung,PT. Citra Aditya Bakti, 2000).

Soerjono Soekanto, 2008, *Faktor Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Rajawali Pers.

Sugiyono, *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif dan R&D* (Bandung: Alfabeta, 2013).

Supiyati Supiyati, "*Penerapan Pasal 27 Ayat 3 Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terhadap Tindak Pidana Pencemaran NAMA Baik Melalui Internet Sebagai Cybercrime Di Hubungkan Dengan Kebebasan Berekspresi,*" *Pamulang Law Review* 2, no. 1 (2020).

Peraturan Perundang-Undangan

Undang-Undang Negara Republik Indonesia Tahun 1945.

Undang-undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 25 Tahun 2007 Tentang Penanaman Modal.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Peraturan BAPPEBTI Nomor 5 Tahun 2019 tentang Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka.

Peraturan Bappebti Nomor 8 Tahun 2021 Tentang Badan Pengawas Perdagangan Berjangka Komoditi, Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto (Crypto Asset) di Bursa Berjangka.

Jurnal

Ahmadi Miru, *Hukum Perlindungan Konsumen*, (Jakarta: Rajawali Pers, 2011).

Apryan Anggara Pratama, "*Hacker Bjorka: Pihak yang Berperan dalam Pencegahan Kebocoran Data*", Jurnal Hukum Magnum Opus, Vol. 6, No. 1, Februari 2023.

Chris Brummer, *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*, (New York: Oxford University Press, 2019).

Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran, dan Teknologi Informasi: Regulasi dan Konvergensi*, (Bandung: Refika Aditama, 2010).

Dewa Ayu Fera Nitha dan I Ketut Westra, "*Investasi Cryptocurrency Berdasarkan Peraturan Bappebti No. 5 Tahun 2019,"* Jurnal Magister Hukum Udayana (Udayana Master Law Journal) Vol.9 No. 4 (2020),

Dwi Edi Wibowo, "*How Consumers in Indonesia are Protected Fairly*?" *Indonesian Journal of Advocacy and Legal Services*, Vol. 2 No. 1, 2020.

Edmon Makari, "*Informasi Hukum untuk Sistem Ketahanan Nasional Terhadap Penyelenggaraan Sistem dan Komunikasi Elektronik Global*", Jurnal Ketahanan Nasional, 2014.

Edmon Makarim, *Kompilasi Hukum Telematika*, (Jakarta: Rajawali Pers, 2013.

Eliasta Ketaren, "C*ybercrime*, *Cyber Space, dan Cyber Law*," *Jurnal TIMES*, Vol. V, No. 2, 2016.

Eri Yanti Nasution dkk., "*Perkembangan Transaksi Bisnis E-Commerce terhadap Pertumbuhan Ekonomi di Indonesia*," *Jurnal Ekonomi & Ekonomi Syariah*, Vol. 3, No. 2, Juni 2020.

Eugenia Macchiavello, "The European Union Framework on Crypto-Assets: MiCA and Beyond", *European Company and Financial Law Review*, Vol. 19, No. 1, (2022).

Giancarlo Giudici, Alistair Milne, dan Dmitri Vinogradov, "*Cryptocurrencies: Market Analysis and Perspectives*," Journal of Industrial and Business Economics Vol. 47 No. 1 (2020)

Gregory, Thomas HA, 2005 "*Ketenaran Cybercrime di Indonesia*", Makalah STIMIK Perbanas 2005 yang dipublikasikan diakses pada 19 Desember 2008

Hermansyah, Mustamam Mustamam, and Panca Sarjana Putra, "*Peran Cyber Crime Ditreskrimsus Kepolisian Daerah Sumatera Utara Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Judi Online (studi Di Kepolisian Daerah Sumatera Utara*)," *Jurnal Meta Hukum* 2, no. 3 (November 30, 2023).

Herry F. Tuwaidan, "*Pelanggaran Tindak Pidana oleh Pelaku Usaha terhadap Kewajiban Memberikan Informasi yang Benar tentang Barang Dikaitkan dengan Perlindungan Konsumen*," Lex Et Societatis, Vol. VI, No. 8, Oktober 2018.

Hidayat Rizky Nurul. *Perlindungan Hukum Bagi konsumen investasi online*. Jurnal hukum udayan Vol. 42. No. 2 (2023).

Japan Virtual and Crypto assets Exchange Association (JVCEA), "Self-Regulatory Rules on Security Guidelines", (2020).

Kelvin F.K. Low dan Ernie G.S. Teo, "Bitcoins and Other Cryptocurrencies as Property?", *Law, Innovation and Technology*, Vol. 9, No. 2, (2017).

Kholik, Dkk. 2026. "*Konstitusionalitas Penerapan Sanksi Pidana Terhadap Kebijakan Publik Yang Berimplikasi Pidana*." Interdisciplinary Explorations in Research Journal 4(1).

M.E. Fuady, *Cybercrime Fenomena Kejahatan Melalui Internet di Indonesia*, *Jurnal Mediator*, Vol.6, No.2, 2005.

Martika Melisa Awon, "*Pertanggungjawaban Pelaku Usaha Terhadap Konsumen yang Dirugikan*," Lex Privatum, Vol. VI, No. 5, Juli 2018.

Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, (Jakarta: Kencana Prenada Media Group, 2013).

Matthias Lehmann, "National and EU Regulatory Approaches to Crypto-Assets", *Journal of International Economic Law*, Vol. 24, No. 3, (2021).

Miko A. Suharto dan Maria N. Apriyani, *Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional*, *Risalah Hukum, Volume 17, No. 2*, (2021).

Monetary Authority of Singapore, "Technology Risk Management Guidelines", (2021).

Muhammad Deivito Dunggio (dalam hasil wawancara), '*Bussines Development Spokesperson Indodax – Indonesia Digital Asset Exchange*', Bali, 30 November 2018.

Muhammad Said Honggowongso dan Munawar Kholil, "*Legalitas Bitcoin Dalam Transaksi E-Commerce Sebagai Pengganti Uang Rupiah*", Jurnal Privat Law: Surakarta, Vol. 9 No. 3 (2021).

Muhidin, M. Strategi *Perlindungan Konsumen Dalam Transaksi E-Commerce*: Perlunya Reformasi Regulasi dan Edukasi Publik. *PAMARENDA: Public Administration and Government Journal*, *5*.1, (2025).

Nunuk Sulisrudatin, *Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit,* Jurnal Ilmiah Hukum Dirgantara, 2 Volume 9 No. 1, September 2018.

Oktaviani Jannah, *Perlindungan Hukum Bagi Nasabah Pialang Perdagangan Berjangka Dalam Hal Terjadinya Wanprestasi Yang Dilakukan Oleh Pihak Pialang Perdagangan Berjangka*, Jurnal Hukum dan Keadilan, Vol. 8 , No. 2, 2018.

Onang Bambungan, "*Perlindungan Hukum terhadap Konsumen atas Kenyamanan, Keamanan dan Keselamatan dalam Mengkonsumsi Barang atau Jasa*," Lex Administratum, Vol. XI, No. 4, 2023.

Pande Putu Rino Atmaja dan Made Aditya Pramana Putra, "*Pertanggungjawaban Perdata atas Kehilangan Aset Kripto Akibat Kegagalan Sistem Exchange*," Kertha Desa: Journal Ilmu Hukum, Vol. 14, No. 4, 2026.

Pasaribu, Z. A., & Siregar, O. M. 2022. *Pengaruh Consumer Trust dan E-Payment Terhadap Brand Trust pada Pengguna Tokopedia bagi Mahasiswa di Kota Medan*. *Journal Of Social Research*, 1(6).

Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi*, (Jakarta: Kencana, 2017).

Regulation (EU) 2022/2554 of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector (DORA).

Riantika Pratiwi, Dkk, "*Tinjauan Yuridis Perlindungan Data Pribadi Dalam Transaksi E-Commerce*", Pagaruyuang Law Journal, Vol. 7, No. 2, Januari 2024.

Rizka Asy Syifa, "*Analisis Yuridis Perlindungan Konsumen dalam Perdagangan Aset Kripto Pasca Peralihan Pengawasan dari BAPPEBTI ke OJK Tahun 2025*".

Setiono. *Rule of Law* (*Supremasi Hukum*). Surakarta. Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret. 2004.

Sidi Ahyar Wiraguna, *Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia*, *Jurnal Sosial Politik, Pemerintahan dan Hukum, Vol. 3, No. 3,* (2024).

Soichiro Uno, "Cryptocurrency Regulation in Japan: The Mt. Gox and Coincheck Aftermath", *Asian Journal of Law and Economics*, Vol. 11, No. 2, (2020).

Sunaryati Hartono, *Kapita Selekta Perbandingan Hukum*, (Bandung: Citra Aditya Bakti, 1991).

Sutan Remy Sjahdeini, *Kejahatan Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009).

Syifa, Dkk. 2025. "*Pengaruh Kelas Sosial Terhadap Akses Lembaga Keuangan Syariah (Tinjauan Teori Stratifikasi dalam Perspektif Islam)*." Falah: Jurnal Hukum Ekonomi Syariah 9(2).

Wawancara dengan Oscar Dermawan, Selaku CEO pada PT. Indodax Nasional Indonesia, Pada tanggal 25 Oktober 2024 Pukul 16:20 WIB.

Windi Eka Oktaviani, "*Tanggung Jawab Pelaku Usaha Terhadap Kerugian Konsumen Dalam Perspektif Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*," Reformasi Hukum, Vol. XIX, No. 2, Juli–Desember 2016.

Internet

Badan Pengawas Perdagangan Berjangka Komoditi (Bappebti). Siaran Pers: Bappebti Terbitkan Empat Peraturan Aset Kripto dan Emas Digital. Jakarta, 18 Februari 2019.

BP Lawyers. Newsletter November 2022. Jakarta: BP Lawyers, November 2022. Diakses 24 Juni 2026.

Dian Erika Nugraheny dan Ihsanuddin, "Perubahan Kedua UU ITE Resmi Berlaku, Diteken Jokowi 2 Januari Jadi UU 1 Tahun 2024," *Kompas TV*, 4 Januari 2024, diakses 20 Juni 2026, https://www.kompas.tv/nasional/474440/perubahan-kedua-uu-ite-resmi-berlaku-diteken-jokowi-2-januari-jadi-uu-1-tahun-2024

Dimas Andi, "Marak Kebocoran, Begini Taktik Perusahaan Kripto Lindungi Data Pengguna," Bisnis.com, 24 Mei 2023, https://market.bisnis.com/read/20230524/94/1658674/marak-kebocoran-begini-taktik-perusahaan-kripto-lindungi-data-pengguna, diakses 24 Juni 2026.

Faris Hadinata, "*Pengaruh Teknologi Informasi terhadap Gaya Hidup Masyarakat Modern*," *Telkom University*, 26 September 2024, https://bit.telkomuniversity.ac.id/pengaruh-teknologiinformasi-terhadap-gaya-hidup-masyarakat-modern/, di akses pada 23 Febuari 2026

Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)*, Paris: FATF, June 2019 (Updated 2021), tersedia di https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html, diakses pada 23 Februari 2026.

Husen Miftahudin, "Cegah Peretasan, Simak Tips Aman Jaga Data Aset Kripto," Medcom.id, 24 Desember 2021, https://www.medcom.id/ekonomi/keuangan/nbwMGpxK-cegah-peretasan-simak-tips-aman-jaga-data-aset-kripto, diakses 24 Juni 2026.

INDODAX Help Center, "Apa itu Aset Digital?", diakses pada 18 Mei 2026. (help.indodax.com)

Kaspersky, "Bagaimana Cara Memperkuat Keamanan Mata Uang Kripto Anda?", Kaspersky Resource Center, https://id.kaspersky.com/resource-center/preemptive-safety/strengthen-cryptocurrency-security, diakses 24 Juni 2026.

Suparman, Raden Agus. "Hukum Siber Indonesia: Panduan Lengkap UU ITE & UU PDP (Terbaru)." Aguspajak.com. 17 Februari 2026. Diakses 24 Juni 2026.

Tim Redaksi *Gemasi.id*, "Trading Crypto Legal Bappebti 2026: 10 Platform Resmi + Tips Anti Rugi untuk Pemula," *Gemasi.id*, 24 Januari 2026, https://gemasi.id/trading-

crypto-legal-bappebti-2026-10-platform-resmi-tips-anti-rugi-untuk-pemula/ (diakses 23 Februari 2026).

Ulasan Indodax Platform Crypto Paling Populer," *Tradingan.com*, https://tradingan.com/broker/indodax, diakses pada 2 Febuari 2026.

Sumber Lain

FSA *Guidelines for Administrative Processes* (Japan).

New York Codes, Rules and Regulations, part 200: Virtual *Currencies* (United states).

*Payment Services Act 2019 (*Singapore*).*