Jurnal Hukum dan HAM Wara Sains
Vol. 5, No. 01, Februari 2026, pp. 220-236

Pertanggungjawaban Pidana Terhadap Pelaku Cyber Fraud Berbasis Rekayasa Sosial Dalam Sistem Hukum Indonesia

Andreas Bintang Raja Sihombing[1], Ariel Alexander[2], Boy Gabriel Yohanes Simarmata[3], Dinda Aurelia Rosi Nasution[4], Dyo Ganda Siadari[5], Keisha Zahra Wibowo[6], Michelle Evelyn Marpaung[7], Najla Azrijal Chosaf[8], Patrisia Tanwijaya[9], Yuni Priskila Ginting[10]

[1] Universitas Pelita Harapan dan 01051230159@student.uph.edu
[2] Universitas Pelita Harapan dan 01051230110@student.uph.edu
[3] Universitas Pelita Harapan dan 01051230108@student.uph.edu
[4] Universitas Pelita Harapan dan 01051230116@student.uph.edu
[5] Universitas Pelita Harapan dan 01051230129@student.uph.edu
[6] Universitas Pelita Harapan dan 01051230121@student.uph.edu
[7] Universitas Pelita Harapan dan 01051230100@student.uph.edu
[8] Universitas Pelita Harapan dan 01051230133@student.uph.edu
[9] Universitas Pelita Harapan dan 01051230113@student.uph.edu
[10] Universitas Pelita Harapan dan yuni.ginting@uph.edu

Article Info

Article history:

Received Feb, 2026
Revised Feb, 2026
Accepted Feb, 2026

Kata Kunci:

Cyber Fraud, Rekayasa Sosial, Pertanggungjawaban Pidana, UU ITE, Perlindungan Data Pribadi

Keywords:

Cyber Fraud, Social Engineering, Criminal Liability, ITE Law, Personal Data Protection

ABSTRAK

Perkembangan teknologi digital telah meningkatkan intensitas kejahatan siber berbasis rekayasa sosial yang memanfaatkan manipulasi psikologis untuk memperoleh akses ilegal terhadap data pribadi dan aset digital korban. Cyber fraud tidak hanya menimbulkan kerugian finansial yang signifikan, tetapi juga berpotensi merusak kepercayaan publik terhadap sistem elektronik dan ekosistem ekonomi digital. Penelitian ini bertujuan untuk menganalisis pertanggungjawaban pidana terhadap pelaku cyber fraud berbasis rekayasa sosial dalam sistem hukum Indonesia melalui kajian terhadap penerapan Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana yang baru. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan studi kasus. Hasil penelitian menunjukkan bahwa perbuatan pelaku cyber fraud berbasis rekayasa sosial telah memenuhi unsur actus reus, mens rea, serta kemampuan bertanggung jawab, sehingga pelaku dapat dimintai pertanggungjawaban pidana secara penuh. Sistem hukum Indonesia pada prinsipnya telah memiliki dasar normatif yang cukup komprehensif dalam menanggulangi kejahatan tersebut. Namun, efektivitas penegakan hukum masih bergantung pada peningkatan kapasitas forensik digital, optimalisasi koordinasi antar lembaga penegak hukum, serta penguatan kebijakan preventif melalui literasi digital masyarakat.

ABSTRACT

Digital technology has increased the intensity of cybercrime based on social engineering, which utilizes psychological manipulation to obtain illegal access to victims' personal data and digital assets. Cyber fraud not only causes significant financial losses but also has the potential to undermine public trust in electronic systems and the digital economic ecosystem. This study aims to analyze the criminal liability of perpetrators of social engineering–based cyber fraud within the Indonesian legal system by examining the implementation of the Law

on Information and Electronic Transactions, the Law on Personal Data Protection, and the newly enacted Criminal Code. The research method employed is normative legal research using statutory, conceptual, and case study approaches. The results indicate that the acts committed by perpetrators of social engineering–based cyber fraud fulfill the elements of actus reus, mens rea, and criminal responsibility, thereby enabling the imposition of full criminal liability. In principle, the Indonesian legal system has established a sufficiently comprehensive normative framework to address such crimes. However, the effectiveness of law enforcement remains dependent on the enhancement of digital forensic capabilities, the optimization of inter-agency coordination, and the strengthening of preventive policies through public digital literacy.

Corresponding Author:

Name: Andreas Bintang Raja Sihombing
Institution: Universitas Pelita Harapan
Email: 01051230159@student.uph.edu

1. PENDAHULUAN

Transformasi digital telah mengubah secara fundamental pola interaksi sosial, sistem kerja, serta mekanisme transaksi ekonomi masyarakat modern. Perkembangan teknologi informasi dan komunikasi tidak hanya mempercepat arus pertukaran data secara global, tetapi juga membentuk ekosistem ekonomi digital yang semakin kompleks, terintegrasi, dan saling bergantung. Berbagai sektor strategis, seperti perbankan, perdagangan elektronik, layanan publik, pendidikan, dan kesehatan, kini semakin mengandalkan sistem elektronik dan jaringan internet sebagai sarana utama operasionalnya. Kondisi ini mendorong peningkatan efisiensi, aksesibilitas, serta produktivitas masyarakat secara signifikan (Novrianto, 2025). Di Indonesia, pertumbuhan ekonomi digital menunjukkan tren yang progresif. Berdasarkan data Kementerian Komunikasi dan Informatika, nilai transaksi ekonomi digital terus mengalami peningkatan setiap tahun seiring dengan meningkatnya penetrasi internet dan penggunaan perangkat digital. Namun, perkembangan tersebut tidak terlepas dari berbagai risiko, khususnya dalam bentuk kejahatan siber yang semakin kompleks, terorganisir, dan bersifat lintas yurisdiksi. Salah satu bentuk kejahatan siber yang mengalami peningkatan signifikan adalah *cyber fraud* berbasis rekayasa sosial (*social engineering*).

Cyber fraud berbasis rekayasa sosial merupakan bentuk kejahatan yang tidak hanya menyerang sistem teknologi informasi, tetapi juga mengeksploitasi aspek psikologis manusia sebagai titik lemah utama. Pelaku memanfaatkan manipulasi kepercayaan, rasa takut, tekanan emosional, maupun urgensi palsu untuk mempengaruhi korban agar secara sukarela menyerahkan data pribadi, kredensial akses, maupun aset digital. Pola kejahatan ini menjadikan korban tidak menyadari bahwa dirinya sedang berada dalam situasi penipuan hingga mengalami kerugian secara material maupun immaterial. Meningkatnya kasus cyber fraud menunjukkan bahwa perkembangan teknologi tidak selalu diimbangi dengan tingkat literasi digital masyarakat yang memadai. Rendahnya pemahaman mengenai keamanan siber, perlindungan data pribadi, serta mekanisme transaksi elektronik menjadi faktor yang memperbesar risiko viktimisasi. Selain itu, karakteristik kejahatan siber yang bersifat anonim, cepat, dan lintas batas negara turut menyulitkan proses

penegakan hukum dan pembuktian di tingkat peradilan. Perkembangan teknologi digital menuntut sistem hukum nasional untuk terus beradaptasi secara responsif dan progresif. Sistem hukum tidak hanya dituntut mampu memberikan perlindungan yang efektif bagi korban, tetapi juga harus menjamin bahwa pelaku cyber fraud dapat dimintai pertanggungjawaban pidana secara adil, proporsional, dan berbasis pada prinsip kepastian hukum. Penguatan regulasi, peningkatan kapasitas aparat penegak hukum di bidang forensik digital, serta integrasi kebijakan preventif melalui literasi digital masyarakat menjadi prasyarat utama dalam membangun sistem perlindungan hukum yang komprehensif di era digital.

Fenomena cyber fraud berbasis rekayasa sosial menunjukkan bahwa ancaman keamanan digital tidak lagi didominasi oleh serangan teknis tingkat tinggi, melainkan oleh strategi manipulasi manusia yang relatif sederhana namun sangat efektif. Pelaku tidak perlu menembus sistem enkripsi yang rumit; cukup dengan meniru identitas institusi resmi, menciptakan skenario darurat, atau menyamar sebagai pihak terpercaya, korban dapat secara sukarela menyerahkan data rahasia mereka (Cahyono, 2025). Kondisi ini memperlihatkan bahwa keamanan digital bukan hanya persoalan teknologi, tetapi juga persoalan literasi, psikologi, dan kesadaran hukum masyarakat. Banyak pengguna layanan digital yang masih menganggap ancaman siber sebagai risiko abstrak yang jauh dari kehidupan sehari-hari, padahal transaksi digital telah menjadi bagian rutin dari aktivitas ekonomi masyarakat. Ketidakseimbangan antara kecepatan inovasi teknologi dan kemampuan masyarakat memahami risiko digital menciptakan celah yang dimanfaatkan pelaku kejahatan. Akibatnya, cyber fraud berbasis rekayasa sosial berkembang menjadi salah satu bentuk kriminalitas modern yang paling sulit diberantas karena memadukan aspek teknologi, psikologi, dan ekonomi dalam satu rangkaian perbuatan.

Peningkatan kejahatan siber menunjukkan tren yang mengkhawatirkan dalam beberapa tahun terakhir. Berbagai laporan keamanan digital internasional dan nasional mencatat bahwa phishing dan rekayasa sosial termasuk jenis serangan siber yang paling sering terjadi dengan jumlah korban yang terus meningkat setiap tahun. Kerugian finansial akibat penipuan digital mencapai triliunan rupiah secara global, sementara di Indonesia sendiri ribuan laporan penipuan online diterima aparat penegak hukum setiap tahunnya (Hasanudin et al., 2026). Data dari lembaga keamanan siber nasional menunjukkan bahwa serangan phishing menempati peringkat tertinggi dalam kategori ancaman digital yang dilaporkan masyarakat. Selain kerugian finansial langsung, dampak lanjutan berupa hilangnya kepercayaan publik terhadap sistem transaksi digital juga memiliki konsekuensi ekonomi yang besar. Kejahatan siber tidak hanya merugikan individu korban, tetapi juga mengganggu stabilitas ekosistem ekonomi digital nasional. Angka-angka ini menegaskan bahwa cyber fraud berbasis rekayasa sosial bukan fenomena insidental, melainkan masalah struktural yang memerlukan pendekatan hukum yang sistematis dan komprehensif.

Regulasi mengenai kejahatan siber di Indonesia telah mengalami perkembangan yang signifikan sebagai respons terhadap dinamika dan kompleksitas era digital. Undang-Undang Informasi dan Transaksi Elektronik sebagaimana telah diperbarui melalui Undang-Undang Nomor 1 Tahun 2024 memberikan dasar hukum yang komprehensif terhadap berbagai bentuk pelanggaran di ruang siber, termasuk akses ilegal, manipulasi data elektronik, serta penyalahgunaan sistem elektronik. Regulasi ini berfungsi sebagai instrumen utama dalam mengkriminalisasi perbuatan yang mengganggu keamanan dan keandalan sistem informasi digital.Undang-Undang Perlindungan Data Pribadi memperkuat rezim perlindungan hukum terhadap informasi personal yang dalam praktiknya sering menjadi objek utama dalam kejahatan berbasis rekayasa sosial (Dian

Putri Yasinta & Ernawati, 2025). Kehadiran undang-undang ini menegaskan tanggung jawab negara dalam menjamin hak privasi dan keamanan data warga negara di tengah meningkatnya aktivitas digital. Di sisi lain, Kitab Undang-Undang Hukum Pidana yang baru juga memperluas dan memodernisasi konsep pertanggungjawaban pidana, sehingga lebih relevan dalam menjangkau karakteristik kejahatan berbasis teknologi informasi.

Kombinasi berbagai instrumen hukum tersebut menunjukkan bahwa negara telah mengakui cyber fraud sebagai bentuk kriminalitas serius yang berpotensi mengancam stabilitas ekonomi, keamanan data, serta kepercayaan publik terhadap sistem digital, sehingga memerlukan penanganan dan sanksi yang tegas (Kurniawan, 2025). Secara normatif, sistem hukum Indonesia telah menyediakan kerangka regulasi yang relatif memadai dalam menanggulangi kejahatan siber. Tantangan utama tidak semata-mata terletak pada keberadaan norma hukum, melainkan pada efektivitas penerapannya dalam praktik penegakan hukum. Aparat penegak hukum dihadapkan pada kesulitan dalam menilai dan membuktikan unsur-unsur pertanggungjawaban pidana, khususnya terkait dengan pembuktian unsur kesalahan (mens rea), niat jahat, kemampuan bertanggung jawab, serta hubungan kausal antara perbuatan pelaku dan kerugian yang dialami korban. Kompleksitas karakter kejahatan digital yang bersifat anonim, lintas yurisdiksi, dan berbasis teknologi tinggi semakin memperumit proses pembuktian dan penegakan hukum di tingkat peradilan.

Relevansi penelitian ini semakin menguat ketika dikaitkan dengan studi kasus konkret Donny Alven alias DA, yang menunjukkan bagaimana cyber fraud berbasis rekayasa sosial dapat berlangsung secara sistematis, terencana, dan menimbulkan kerugian dalam skala yang sangat besar. Dalam kasus tersebut, pelaku menyebarkan tautan phishing yang meniru tampilan layanan dompet digital kripto dengan tujuan memperoleh akses ilegal terhadap identitas dan kata sandi korban. Setelah berhasil menguasai akun korban, pelaku memindahkan aset kripto dan mengonversinya menjadi keuntungan finansial pribadi. Pola perbuatan ini memperlihatkan bahwa kejahatan tidak dilakukan secara spontan, melainkan melalui perencanaan yang matang, penguasaan teknologi informasi, serta strategi manipulasi psikologis yang terstruktur terhadap korban (Yulianto, 2025). Pelaku secara sadar memanfaatkan kepercayaan dan ketidaktahuan korban terhadap sistem keamanan digital untuk mencapai tujuan kriminalnya. Hal tersebut menunjukkan adanya integrasi antara kecanggihan teknis dan kecerdasan manipulatif sebagai karakter utama kejahatan berbasis rekayasa sosial.

Dari perspektif hukum pidana, tindakan pelaku tidak hanya memenuhi unsur akses ilegal dan pemindahan data elektronik tanpa hak sebagaimana diatur dalam peraturan perundang-undangan, tetapi juga mencerminkan adanya niat curang (fraudulent intent) yang terstruktur serta kesadaran penuh atas akibat hukum dan kerugian yang ditimbulkan. Unsur kesengajaan, perencanaan, dan penguasaan terhadap sarana kejahatan memperkuat posisi pelaku sebagai subjek yang dapat dimintai pertanggungjawaban pidana secara penuh. Kasus Donny Alven juga menggambarkan karakteristik kejahatan digital modern yang bersifat lintas platform, lintas yurisdiksi, serta memanfaatkan perkembangan teknologi finansial yang bergerak lebih cepat dibandingkan dengan adaptasi regulasi dan mekanisme pengawasan. Kompleksitas tersebut tidak hanya menyulitkan proses pelacakan pelaku dan pemulihan aset korban, tetapi juga menimbulkan tantangan dalam pembuktian hukum di persidangan. Kondisi ini menuntut adanya analisis pertanggungjawaban pidana yang tidak berhenti pada pendekatan konvensional, tetapi mampu menjembatani teori hukum pidana klasik dengan realitas kejahatan siber kontemporer. Pendekatan

yang adaptif dan kontekstual diperlukan agar penegakan hukum tetap relevan, efektif, serta mampu memberikan kepastian hukum, keadilan, dan perlindungan optimal bagi korban di era digital.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam pertanggungjawaban pidana terhadap pelaku cyber fraud berbasis rekayasa sosial dalam sistem hukum Indonesia, dengan menitikberatkan pada penerapan unsur perbuatan pidana, unsur kesalahan, kemampuan bertanggung jawab, serta ketiadaan alasan pembenar dan pemaaf. Analisis ini dilakukan untuk menilai sejauh mana ketentuan hukum positif mampu mengakomodasi karakteristik kejahatan siber yang semakin kompleks dan dinamis.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan yuridis doktrinal yang berfokus pada analisis norma hukum positif yang mengatur pertanggungjawaban pidana terhadap pelaku cyber fraud berbasis rekayasa sosial (J. W. Creswell & Creswell, 2023). Pendekatan ini dipilih karena objek utama penelitian adalah konstruksi pertanggungjawaban pidana dalam sistem hukum Indonesia sebagaimana diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana yang baru. Penelitian hukum normatif memandang hukum sebagai suatu sistem norma yang tersusun secara sistematis dan hierarkis. Oleh karena itu, analisis dalam penelitian ini diarahkan pada pengkajian asas-asas hukum, teori-teori hukum pidana, serta ketentuan peraturan perundang-undangan yang relevan dengan kejahatan siber berbasis rekayasa sosial. Pendekatan yang digunakan meliputi pendekatan perundang-undangan, pendekatan konseptual, dan pendekatan kasus.

Pendekatan perundang-undangan digunakan untuk mengkaji struktur dan substansi norma hukum yang berlaku, pendekatan konseptual untuk menganalisis doktrin dan konsep pertanggungjawaban pidana, sedangkan pendekatan kasus digunakan untuk mengkaji penerapan norma hukum dalam praktik melalui analisis kasus Donny Alven sebagai representasi konkret kejahatan cyber fraud berbasis rekayasa sosial. Sumber bahan hukum dalam penelitian ini terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, khususnya Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana yang baru, serta instrumen hukum terkait tindak pidana pencucian uang (J. W. Creswell & Creswell, 2018). Bahan hukum sekunder diperoleh dari literatur ilmiah berupa jurnal hukum, buku teks, hasil penelitian, dan pendapat para ahli yang membahas hukum pidana siber dan pertanggungjawaban pidana. Adapun bahan hukum tersier berupa kamus hukum, ensiklopedia, dan indeks hukum digunakan untuk memperjelas terminologi dan konsep yang digunakan dalam penelitian (J. Creswell, 2016).

3. HASIL DAN PEMBAHASAN

3.1 Tindak Pidana Cyber Fraud Berbasis Rekayasa Sosial dalam Perspektif Hukum Pidana Indonesia

Cyber fraud berbasis rekayasa sosial merupakan bentuk evolusi kejahatan penipuan yang mengalami transformasi seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Jika dalam penipuan konvensional interaksi antara pelaku dan korban umumnya

berlangsung secara langsung dan bersifat fisik, maka dalam cyber fraud ruang digital berfungsi sebagai medium utama terjadinya kejahatan. Peralihan medium ini tidak hanya mengubah pola operasional pelaku, tetapi juga memperluas jangkauan, kecepatan, dan dampak kejahatan terhadap masyarakat.

Dalam konteks tersebut, rekayasa sosial tidak sekadar berperan sebagai teknik pendukung, melainkan menjadi inti dari modus operandi kejahatan itu sendiri (Wahyudi BR, 2025). Melalui rekayasa sosial, pelaku secara sistematis mengeksploitasi faktor-faktor psikologis manusia, seperti rasa percaya, kepanikan, rasa ingin tahu, tekanan emosional, maupun urgensi palsu, untuk memanipulasi korban agar secara sukarela menyerahkan informasi sensitif, kredensial akses, atau aset digital. Strategi ini menjadikan korban tidak menyadari bahwa dirinya sedang berada dalam situasi penipuan hingga mengalami kerugian. Dari perspektif hukum pidana, fenomena cyber fraud berbasis rekayasa sosial menimbulkan persoalan konseptual yang signifikan, khususnya terkait dengan konstruksi perbuatan pidana. Objek kejahatan tidak lagi terbatas pada benda berwujud, melainkan mencakup data elektronik, identitas digital, serta kepercayaan dalam sistem informasi. Perubahan karakter objek ini menuntut penyesuaian dalam cara memahami dan menafsirkan unsur-unsur delik, terutama dalam kaitannya dengan penipuan, akses ilegal, dan manipulasi data.

Suatu perbuatan dapat dikualifikasikan sebagai tindak pidana apabila memenuhi unsur actus reus (perbuatan lahiriah) dan mens rea (sikap batin pelaku). Pada cyber fraud berbasis rekayasa sosial, actus reus tidak selalu berbentuk perusakan sistem secara teknis, melainkan tindakan manipulatif yang menyebabkan korban menyerahkan akses secara sukarela. Secara formal, pelaku tidak "memaksa" sistem elektronik, tetapi memanipulasi manusia sebagai gerbang akses terhadap sistem tersebut. Hal ini menunjukkan bahwa locus delicti kejahatan tidak semata-mata berada pada perangkat teknologi, melainkan pada interaksi psikologis antara pelaku dan korban (Maharani & Rapik, 2024). Dalam perspektif hukum pidana Indonesia, perbuatan semacam ini tetap memenuhi unsur perbuatan melawan hukum karena tujuan akhirnya adalah memperoleh keuntungan secara tidak sah melalui tipu muslihat. Dengan demikian, rekayasa sosial dapat dipahami sebagai bentuk penipuan digital yang memperluas konsep klasik "tipu daya" ke dalam ruang siber.

Unsur mens rea dalam cyber fraud berbasis rekayasa sosial umumnya berbentuk kesengajaan (dolus) yang kuat dan terstruktur. Pelaku mengetahui bahwa informasi yang diperoleh bersifat rahasia, menyadari bahwa korban bertindak berdasarkan manipulasi, serta menghendaki akibat berupa peralihan kekayaan secara ilegal. Dalam konstruksi hukum pidana, kesengajaan semacam ini termasuk dolus directus, yaitu niat langsung untuk mencapai hasil tertentu (Ismail, 2026). Bahkan dalam banyak kasus, pelaku menunjukkan perencanaan matang, penggunaan identitas palsu, serta pengelolaan hasil kejahatan yang sistematis. Fakta ini menegaskan bahwa cyber fraud bukan sekadar pelanggaran administratif atau kesalahan teknis, melainkan kejahatan ekonomi yang memiliki intensi kriminal tinggi. Oleh karena itu, pendekatan hukum pidana terhadap cyber fraud harus memperlakukan pelaku sebagai subjek dengan kapasitas kesalahan penuh, bukan sekadar pelaku pelanggaran teknologi.

Objek perlindungan hukum dalam cyber fraud berbasis rekayasa sosial juga mengalami perluasan. Dalam hukum pidana klasik, objek yang dilindungi umumnya berupa harta benda fisik. Namun dalam konteks digital, objek yang diserang mencakup data elektronik, identitas digital, dan kepercayaan dalam sistem transaksi elektronik. Kepercayaan menjadi elemen penting karena ekosistem digital bergantung pada asumsi bahwa identitas dan komunikasi elektronik bersifat

autentik. Ketika pelaku memalsukan identitas institusi atau menciptakan tampilan digital yang meniru sistem resmi, ia tidak hanya menyerang individu korban, tetapi juga merusak integritas sistem digital secara keseluruhan. Oleh karena itu, cyber fraud harus dipahami sebagai kejahatan yang berdampak kolektif terhadap stabilitas ekonomi digital dan rasa aman masyarakat.

Dari perspektif asas legalitas muncul pertanyaan apakah hukum pidana Indonesia cukup fleksibel untuk menjangkau bentuk kejahatan digital yang terus berkembang. Asas legalitas menuntut bahwa tidak ada perbuatan yang dapat dipidana tanpa dasar hukum yang jelas. Namun hukum pidana juga harus mampu beradaptasi melalui interpretasi sistematis dan teleologis agar tidak tertinggal oleh perkembangan teknologi. Undang-Undang ITE hadir sebagai respons terhadap kebutuhan ini dengan memperluas definisi data elektronik, akses ilegal, dan manipulasi sistem. Rekayasa sosial, meskipun tidak selalu disebut secara eksplisit, secara substansial termasuk dalam kategori perbuatan yang dilarang karena menghasilkan akses tanpa hak dan perolehan keuntungan ilegal. Dengan demikian, konstruksi hukum pidana terhadap cyber fraud dapat dibangun melalui penafsiran yang menghubungkan norma klasik penipuan dengan norma modern akses elektronik.

Hubungan antara cyber fraud dan penipuan konvensional menunjukkan kontinuitas sekaligus transformasi konsep hukum pidana. Penipuan klasik mensyaratkan adanya tipu muslihat yang menyebabkan korban menyerahkan harta. Dalam cyber fraud, tipu muslihat tetap menjadi elemen inti, tetapi medium dan objeknya berubah. Korban tidak menyerahkan uang secara langsung, melainkan data akses yang kemudian dikonversi menjadi nilai ekonomi oleh pelaku. Perubahan medium ini tidak menghilangkan sifat kriminal perbuatan, melainkan menuntut adaptasi cara pembuktian. Bukti elektronik, jejak digital, dan log sistem menjadi bagian penting dalam konstruksi pembuktian pidana. Hal ini menegaskan bahwa hukum pidana modern harus mampu mengintegrasikan ilmu forensik digital sebagai bagian dari sistem peradilan (Tuju et al., 2025). Cyber fraud berbasis rekayasa sosial memiliki dimensi lintas yurisdiksi yang menantang konsep kedaulatan hukum tradisional. Pelaku, korban, server, dan platform dapat berada di negara yang berbeda. Dalam konteks ini, konstruksi tindak pidana tidak hanya bersifat nasional, tetapi juga terkait dengan kerja sama internasional. Hukum pidana Indonesia harus ditempatkan dalam kerangka hukum siber global yang menuntut harmonisasi regulasi. Tanpa kerja sama lintas negara, penegakan hukum terhadap cyber fraud akan selalu menghadapi keterbatasan jurisdiksi.

Aspek lain yang penting adalah karakter non-kekerasan dari cyber fraud yang sering kali menimbulkan persepsi bahwa kejahatan ini kurang serius dibanding kejahatan fisik. Padahal dampak ekonominya dapat jauh lebih besar. Kerugian finansial, trauma psikologis korban, dan hilangnya kepercayaan terhadap sistem digital menunjukkan bahwa cyber fraud memiliki dimensi sosial yang luas. Oleh karena itu, konstruksi tindak pidana harus mempertimbangkan dampak sosial sebagai bagian dari justifikasi kriminalisasi. Penghukuman terhadap pelaku cyber fraud tidak hanya bertujuan retributif, tetapi juga preventif dan edukatif. Hukuman harus mampu menciptakan efek jera serta memperkuat kepercayaan masyarakat terhadap sistem hukum. Jika pelaku cyber fraud diperlakukan ringan, masyarakat akan memandang ruang digital sebagai wilayah tanpa hukum. Oleh karena itu, konstruksi hukum pidana harus menempatkan cyber fraud sebagai kejahatan serius yang setara dengan kejahatan ekonomi lainnya.

Pendekatan hukum pidana terhadap cyber fraud berbasis rekayasa sosial tidak dapat berdiri sendiri sebagai instrumen represif semata, melainkan harus dipahami sebagai bagian dari strategi perlindungan masyarakat yang lebih luas. Kejahatan digital berkembang lebih cepat daripada respons regulasi, sehingga hukum pidana perlu berfungsi adaptif tanpa kehilangan kepastian

normatifnya. Dalam konteks ini, konstruksi pertanggungjawaban pidana harus mempertimbangkan dimensi teknologi, psikologi korban, serta dampak sosial ekonomi yang ditimbulkan. Hukum tidak hanya berfungsi menghukum pelaku, tetapi juga menjaga stabilitas ekosistem digital agar tetap dipercaya publik. Oleh karena itu, penguatan kerangka hukum pidana terhadap cyber fraud harus dilihat melalui beberapa aspek penting berikut (Febriani Wardojo, 2025):

1. Penguatan konsep perlindungan data dan identitas digital sebagai objek hukum pidana.

Perkembangan teknologi telah mengubah data pribadi menjadi aset ekonomi yang bernilai tinggi, sehingga perlindungannya tidak lagi sekadar isu administratif, melainkan isu pidana. Identitas digital seseorang dapat digunakan untuk mengakses keuangan, layanan publik, hingga reputasi sosial, sehingga penyalahgunaannya memiliki konsekuensi luas. Dalam cyber fraud berbasis rekayasa sosial, pelaku secara langsung menyerang identitas digital korban sebagai pintu masuk ke aset ekonomi. Oleh karena itu, hukum pidana harus menempatkan data dan identitas digital sebagai objek perlindungan yang setara dengan harta benda fisik. Pendekatan ini memperluas paradigma hukum pidana dari perlindungan properti konvensional menuju perlindungan aset informasi.

2. Integrasi antara pendekatan teknologi dan pertanggungjawaban pidana.

Cyber fraud menunjukkan bahwa batas antara kejahatan teknis dan manipulasi psikologis semakin kabur. Penegakan hukum tidak cukup hanya memahami norma pidana, tetapi juga harus didukung pemahaman teknologi forensik digital. Pembuktian dalam perkara cyber fraud bergantung pada jejak elektronik, log sistem, dan rekonstruksi aktivitas digital pelaku. Tanpa integrasi keahlian teknologi, konstruksi pertanggungjawaban pidana menjadi lemah dalam praktik peradilan. Oleh karena itu, sistem hukum harus memperkuat kapasitas aparat penegak hukum dalam bidang teknologi agar prinsip keadilan substantif dapat terwujud.

3. Perluasan perspektif pencegahan sebagai bagian dari tujuan pemidanaan.

Cyber fraud tidak dapat diberantas hanya melalui penghukuman setelah kejahatan terjadi. Pencegahan harus menjadi bagian integral dari konstruksi hukum pidana melalui edukasi publik, literasi digital, dan penguatan keamanan sistem elektronik. Masyarakat yang sadar risiko digital menjadi lapisan pertahanan pertama terhadap rekayasa sosial. Dalam perspektif ini, hukum pidana berfungsi sebagai instrumen deterrence sekaligus sarana pembelajaran sosial. Pendekatan preventif memperkuat legitimasi hukum karena masyarakat melihat hukum tidak hanya menghukum, tetapi juga melindungi.

Secara keseluruhan konstruksi tindak pidana cyber fraud berbasis rekayasa sosial dalam hukum pidana Indonesia menunjukkan bahwa sistem hukum tidak lagi dapat bertumpu pada paradigma perlindungan benda fisik semata, melainkan harus bergerak menuju paradigma perlindungan informasi, identitas, dan kepercayaan digital sebagai aset hukum yang bernilai strategis. Perubahan ini menandai pergeseran fundamental dalam cara hukum memahami kerugian, karena kerusakan dalam ruang digital sering kali tidak terlihat secara fisik tetapi menghasilkan dampak ekonomi dan sosial yang nyata. Dalam konteks tersebut, actus reus tidak lagi terbatas pada tindakan material seperti pengambilan benda atau perusakan fisik, melainkan mencakup manipulasi psikologis yang secara langsung mendorong korban menyerahkan akses terhadap

sistem elektroniknya. Perluasan makna perbuatan ini tetap berada dalam kerangka hukum pidana karena akibat yang ditimbulkan bersifat konkret, terukur, dan menimbulkan kerugian nyata. Mens rea dalam cyber fraud menunjukkan intensi kriminal yang terencana, sadar, dan berorientasi pada keuntungan ekonomi, sehingga memenuhi standar kesalahan tinggi yang menjadi dasar pertanggungjawaban pidana. Pelaku tidak hanya mengetahui sifat melawan hukum dari perbuatannya, tetapi juga secara aktif menghendaki akibat tersebut terjadi. Objek perlindungan hukum pun berkembang dari konsep kepemilikan tradisional menuju perlindungan data elektronik dan sistem kepercayaan digital yang menjadi fondasi transaksi modern. Kepercayaan publik terhadap sistem elektronik merupakan prasyarat utama keberlangsungan ekonomi digital, sehingga setiap serangan terhadapnya memiliki dimensi sosial yang luas.

4.2 Pertanggungjawaban Pidana Pelaku Cyber Fraud Berdasarkan UU ITE, UU PDP, dan KUHP Baru

Pertanggungjawaban pidana terhadap pelaku cyber fraud berbasis rekayasa sosial dalam sistem hukum Indonesia didasarkan pada integrasi berbagai instrumen hukum, khususnya Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, serta Kitab Undang-Undang Hukum Pidana yang baru. Ketiga regulasi tersebut membentuk kerangka normatif yang saling melengkapi dalam menanggulangi kejahatan digital yang semakin kompleks. Pertanggungjawaban pidana terhadap pelaku cyber fraud berbasis rekayasa sosial dalam sistem hukum Indonesia harus dianalisis melalui kerangka teori pertanggungjawaban pidana klasik yang menekankan tiga unsur utama, yaitu adanya perbuatan pidana, kesalahan, dan kemampuan bertanggung jawab. Prinsip ini merupakan fondasi universal dalam hukum pidana yang tetap relevan meskipun objek kejahatan telah bergeser dari benda fisik ke sistem digital (Gabriel Regina Christian & Gousta Feriza, 2026). Cyber fraud tidak menciptakan kategori kejahatan yang sepenuhnya baru, melainkan memperluas medan operasional penipuan ke dalam ruang elektronik yang diatur secara khusus oleh undang-undang. Dalam konteks ini, pertanggungjawaban pidana tidak dapat dilepaskan dari asas legalitas sebagaimana diadopsi dalam KUHP baru yang menegaskan bahwa setiap perbuatan hanya dapat dipidana jika telah dirumuskan sebelumnya dalam undang-undang. Kejahatan rekayasa sosial memenuhi asas ini karena perbuatannya masuk dalam kategori akses ilegal, manipulasi data, dan penipuan elektronik yang telah diatur secara eksplisit dalam UU ITE dan UU Perlindungan Data Pribadi. Dengan demikian, konstruksi pertanggungjawaban pidana pelaku cyber fraud berdiri di atas kombinasi norma umum KUHP dan norma khusus hukum siber, yang membentuk sistem pertanggungjawaban yang bersifat komplementer dan saling menguatkan.

Unsur perbuatan pidana dalam cyber fraud secara langsung berkaitan dengan larangan akses tanpa hak terhadap sistem elektronik sebagaimana diatur dalam Pasal 30 ayat (1) dan ayat (2) UU ITE. Pasal tersebut melarang setiap orang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain untuk memperoleh informasi elektronik. Dalam praktik cyber fraud berbasis rekayasa sosial, akses ilegal memang sering diperoleh melalui manipulasi psikologis, namun hukum tidak membedakan apakah akses diperoleh dengan peretasan teknis atau tipu daya sosial (Alamsyah et al., 2025). Yang menjadi fokus adalah ketiadaan hak untuk memasuki sistem elektronik tersebut. Ketika pelaku memperoleh data login korban melalui phishing, secara hukum ia telah melakukan akses tanpa hak meskipun korban menyerahkan data secara sukarela akibat manipulasi. Prinsip ini penting karena menunjukkan bahwa persetujuan korban yang

diperoleh melalui tipu daya tidak menghapus sifat melawan hukum perbuatan pelaku. Dengan demikian, unsur actus reus telah terpenuhi karena terjadi pelanggaran langsung terhadap integritas sistem elektronik yang dilindungi undang-undang.

Cyber fraud juga memenuhi unsur manipulasi dan pemindahan data elektronik sebagaimana diatur dalam Pasal 32 ayat (1) dan ayat (2) UU ITE. Pasal ini melarang setiap orang dengan sengaja mengubah, menambah, mengurangi, merusak, memindahkan, atau menyembunyikan informasi elektronik milik orang lain tanpa hak. Ketika pelaku memindahkan aset digital korban, tindakan tersebut secara langsung masuk dalam kategori pemindahan data elektronik tanpa hak. Hukum memandang data digital sebagai representasi nilai ekonomi yang memiliki konsekuensi hukum setara dengan harta benda. Oleh karena itu, cyber fraud bukan sekadar pelanggaran sistem, tetapi serangan terhadap kepemilikan ekonomi korban. Ancaman pidana dalam Pasal 48 ayat (1) dan ayat (2) UU ITE menegaskan bahwa perbuatan ini diperlakukan sebagai tindak pidana serius dengan sanksi penjara dan denda tinggi. Hal ini menunjukkan bahwa pembentuk undang-undang telah mengakui bobot kerugian digital sebagai kerugian hukum yang nyata. Dimensi kesalahan pelaku cyber fraud secara tegas menunjukkan bentuk kesengajaan (dolus) sebagaimana menjadi syarat utama pertanggungjawaban pidana dalam KUHP baru. Kesengajaan ini tidak bersifat implisit, melainkan terwujud dalam perencanaan, pelaksanaan, dan pengelolaan hasil kejahatan. Pelaku mengetahui bahwa data yang diperoleh bersifat rahasia dan dilindungi hukum, namun tetap menghendaki akibat berupa peralihan kekayaan. Dalam teori hukum pidana, kondisi ini dikategorikan sebagai dolus directus karena pelaku secara sadar menargetkan hasil tertentu (Sofiana et al., 2025). Tidak terdapat unsur kelalaian atau ketidak sengajaan dalam rekayasa sosial yang dirancang secara sistematis. Bahkan, skema cyber fraud menunjukkan tingkat kalkulasi rasional yang tinggi, yang memperkuat kesimpulan bahwa pelaku bertindak dengan intensi kriminal penuh. Unsur kesalahan terpenuhi secara sempurna dan membuka ruang pertanggungjawaban pidana maksimal.

Perlindungan data pribadi sebagai objek hukum memperluas cakupan pertanggungjawaban pidana melalui UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 67 UU PDP secara tegas mengkriminalisasi perolehan dan penggunaan data pribadi tanpa persetujuan yang sah. Dalam cyber fraud berbasis rekayasa sosial, pengumpulan ID, kata sandi, dan informasi identitas digital korban merupakan inti dari kejahatan. Pelanggaran ini bukan sekadar alat untuk penipuan, tetapi merupakan tindak pidana mandiri terhadap hak privasi. Hukum menempatkan data pribadi sebagai hak fundamental individu yang harus dilindungi. Dengan demikian, pelaku cyber fraud tidak hanya bertanggung jawab atas kerugian finansial, tetapi juga atas pelanggaran hak personal korban. Pendekatan ini memperlihatkan bahwa pertanggungjawaban pidana memiliki dimensi perlindungan hak asasi.

KUHP baru memberikan kerangka umum yang memperkuat konstruksi pertanggungjawaban pidana melalui konsep kemampuan bertanggung jawab sebagaimana tercermin dalam ketentuan mengenai alasan pemaaf. Seseorang tidak dapat dipidana apabila tidak mampu memahami sifat perbuatannya atau tidak mampu mengendalikan kehendaknya. Dalam cyber fraud, pelaku umumnya memiliki kecakapan teknologi, kesadaran penuh, dan kontrol rasional atas tindakannya (Swalar, 2022). Penggunaan perangkat digital canggih menunjukkan kapasitas intelektual yang tinggi. Tidak terdapat indikasi gangguan mental yang dapat menghapus kesalahan. Pelaku memenuhi syarat sebagai subjek hukum yang cakap bertanggung jawab. Konsekuensinya, seluruh unsur pertanggungjawaban pidana terpenuhi secara kumulatif.

Pertanggungjawaban pidana terhadap pelaku cyber fraud juga harus dianalisis dari sudut pandang sistem pembuktian dan struktur pertanggungjawaban modern yang tidak hanya berfokus pada pelaku sebagai individu, tetapi juga pada jaringan kejahatan yang memungkinkan tindak pidana tersebut terjadi. Cyber fraud jarang dilakukan secara terisolasi; sering kali melibatkan infrastruktur digital, platform komunikasi, dan aliran transaksi keuangan yang kompleks. Oleh karena itu, hukum pidana harus membaca pertanggungjawaban tidak hanya sebagai reaksi terhadap satu perbuatan, tetapi sebagai mekanisme pengendalian risiko sosial yang lebih luas. Pendekatan ini menuntut integrasi antara hukum pidana materiil, hukum acara pidana, dan kebijakan keamanan siber nasional. Dalam konteks ini, efektivitas pertanggungjawaban pidana ditentukan oleh kemampuan sistem hukum untuk menyesuaikan diri dengan karakter kejahatan digital yang dinamis. Penguatan kerangka pertanggungjawaban pidana terhadap cyber fraud dapat dianalisis melalui beberapa dimensi berikut (Novrianto, 2025):

1. Dimensi pembuktian digital dalam pertanggungjawaban pidana.

Pembuktian dalam perkara cyber fraud bergantung pada bukti elektronik yang memiliki karakter berbeda dari alat bukti konvensional. Jejak digital berupa log akses, metadata, rekaman transaksi, dan forensik perangkat menjadi dasar utama pembuktian kesalahan pelaku. Tanpa kemampuan membaca dan memverifikasi bukti digital, pertanggungjawaban pidana akan melemah di ruang persidangan. Oleh karena itu, hukum acara pidana harus berkembang seiring teknologi agar standar pembuktian tetap memenuhi prinsip due process of law. Integritas rantai barang bukti digital menjadi kunci untuk memastikan keadilan substantif. Dimensi ini menunjukkan bahwa pertanggungjawaban pidana cyber fraud tidak hanya soal norma, tetapi juga kapasitas teknis penegakan hukum.

2. Pertanggungjawaban pidana sebagai perlindungan kepercayaan publik.

Cyber fraud tidak hanya merugikan korban individual, tetapi merusak kepercayaan kolektif terhadap sistem digital. Kepercayaan merupakan fondasi utama ekonomi elektronik dan transaksi daring. Ketika masyarakat merasa sistem digital tidak aman, partisipasi ekonomi digital akan menurun. Oleh karena itu, pertanggungjawaban pidana memiliki fungsi simbolik untuk menegaskan bahwa negara melindungi ruang digital. Hukuman terhadap pelaku berfungsi sebagai deklarasi normatif bahwa manipulasi digital adalah pelanggaran serius. Dimensi ini memperlihatkan bahwa hukum pidana berperan menjaga stabilitas sosial.

3. Keterkaitan antara cyber fraud dan kejahatan ekonomi modern.

Cyber fraud harus diposisikan sebagai bagian dari kejahatan ekonomi modern yang setara dengan korupsi dan pencucian uang. Kejahatan ini memanfaatkan sistem finansial digital untuk memperoleh keuntungan besar dalam waktu singkat. Dampaknya tidak hanya individual, tetapi sistemik terhadap ekosistem ekonomi. Oleh karena itu, pendekatan hukum pidana terhadap cyber fraud harus seketat penanganan kejahatan ekonomi lainnya. Perampasan aset, pembekuan rekening, dan pelacakan transaksi menjadi bagian integral pertanggungjawaban pidana. Pendekatan ini memastikan bahwa pelaku tidak menikmati hasil kejahatan.

4. Fungsi preventif dalam konstruksi pertanggungjawaban pidana.

Pertanggungjawaban pidana tidak boleh dipahami semata sebagai reaksi setelah kejahatan terjadi. Hukum pidana modern menempatkan pencegahan sebagai tujuan utama. Penghukuman pelaku cyber fraud harus menciptakan efek jera yang nyata bagi masyarakat. Efek ini penting karena kejahatan digital mudah ditiru oleh pelaku lain. Semakin jelas konsekuensi hukumnya, semakin kuat fungsi deterrence hukum pidana. Dengan demikian, pertanggungjawaban pidana berperan sebagai alat kontrol sosial.

5. Adaptasi hukum pidana terhadap evolusi teknologi.

Cyber fraud menunjukkan bahwa teknologi selalu bergerak lebih cepat daripada regulasi. Oleh karena itu, hukum pidana harus bersifat adaptif tanpa melanggar asas legalitas. Penafsiran progresif diperlukan agar norma tetap relevan terhadap modus baru. Namun adaptasi tidak boleh berubah menjadi kriminalisasi berlebihan. Keseimbangan antara kepastian hukum dan fleksibilitas interpretasi menjadi kunci. Pertanggungjawaban pidana harus berkembang seiring perubahan teknologi.

Ancaman pidana dalam UU ITE memperlihatkan pendekatan retributif dan preventif yang kuat. Pasal 46 dan Pasal 48 UU ITE memberikan ancaman penjara hingga sembilan tahun dan denda miliaran rupiah. Besarnya sanksi mencerminkan pengakuan negara bahwa cyber fraud merupakan kejahatan ekonomi serius. Hukuman ini tidak hanya bertujuan menghukum pelaku, tetapi juga menciptakan efek jera kolektif. Dalam teori tujuan pemidanaan modern, deterrence memiliki fungsi penting dalam kejahatan berbasis teknologi yang mudah direplikasi. Jika pelaku diperlakukan ringan, ruang digital akan dipersepsikan sebagai wilayah tanpa hukum. Oleh karena itu, sanksi berat menjadi instrumen perlindungan sosial. Dimensi tambahan pertanggungjawaban pidana muncul ketika hasil cyber fraud dikonversi menjadi aset riil melalui tindak pidana pencucian uang. Dalam situasi ini, pelaku dapat dijerat UU TPPU karena menikmati hasil kejahatan. Prinsip follow the money memastikan bahwa keuntungan ilegal tidak dapat dinikmati pelaku. Perampasan aset menjadi bagian integral dari keadilan pidana modern. Tanpa mekanisme ini, penghukuman kehilangan efektivitasnya. Hukum pidana modern tidak hanya menghukum badan pelaku, tetapi juga menargetkan kekayaan hasil kejahatan.

Secara keseluruhan pertanggungjawaban pidana pelaku cyber fraud dalam sistem hukum Indonesia menunjukkan integrasi kuat antara norma teknologi dan teori hukum pidana klasik. UU ITE melindungi sistem elektronik, UU PDP melindungi data pribadi, dan KUHP baru memberikan fondasi pertanggungjawaban umum. Ketiganya membentuk sistem yang komprehensif untuk menghadapi kejahatan digital. Tantangan utama bukan pada ketiadaan hukum, melainkan pada efektivitas penerapan dan kapasitas penegakan hukum. Cyber fraud bukan kejahatan ringan, melainkan ancaman terhadap kepercayaan sosial. Oleh karena itu, penegakan pertanggungjawaban pidana harus konsisten sebagai bentuk perlindungan masyarakat digital.

4.3 Analisis Kasus Donny Alven dan Implikasi Penegakan Hukum terhadap Kejahatan Rekayasa Sosial

Kasus Donny Alven merupakan representasi konkret dari perkembangan cyber fraud berbasis rekayasa sosial yang telah berevolusi menjadi bentuk kejahatan ekonomi digital yang sistematis, terorganisir, dan berdampak luas terhadap keamanan transaksi elektronik. Modus operandi yang digunakan pelaku memperlihatkan adanya integrasi antara manipulasi psikologis

terhadap korban dan pemanfaatan teknologi digital untuk memperoleh akses tanpa hak terhadap aset kripto. Pola ini menunjukkan bahwa kejahatan tidak dilakukan secara insidental, melainkan melalui perencanaan yang matang dan penguasaan terhadap mekanisme sistem elektronik. Dalam perspektif hukum pidana, kasus ini tidak dapat dipandang sebagai penipuan konvensional semata, melainkan sebagai rangkaian perbuatan yang memenuhi unsur akses ilegal, manipulasi data elektronik, penguasaan aset digital tanpa hak, serta potensi keterkaitan dengan tindak pidana pencucian uang. Skema phishing yang digunakan pelaku menjadi instrumen utama dalam membangun kepercayaan palsu dan menyesatkan korban agar secara sukarela menyerahkan informasi sensitif dan akses terhadap akun digitalnya. Kasus ini menunjukkan bahwa titik lemah utama dalam sistem keamanan digital tidak selalu terletak pada aspek teknologis, melainkan pada faktor manusia sebagai pengguna sistem (Cahyono, 2025). Rendahnya kesadaran keamanan digital, keterbatasan literasi teknologi, serta kerentanan psikologis korban menjadi celah yang dimanfaatkan secara sistematis oleh pelaku. Dalam konteks ini, rekayasa sosial dapat dipahami sebagai bentuk peretasan berbasis psikologi yang secara substantif memiliki tingkat bahaya dan konsekuensi hukum yang setara dengan peretasan teknis.

Kasus Donny Alven memperlihatkan bagaimana batas antara manipulasi sosial dan pelanggaran sistem elektronik semakin kabur dalam praktik kejahatan siber modern. Kondisi ini menuntut pendekatan hukum pidana yang lebih adaptif dan komprehensif, agar mampu menjangkau seluruh dimensi kejahatan, baik yang bersifat teknologis maupun psikologis. Oleh karena itu, analisis terhadap kasus ini menjadi penting untuk menilai sejauh mana sistem hukum pidana Indonesia mampu merespons, mengkualifikasi, dan menegakkan pertanggungjawaban pidana terhadap bentuk-bentuk cyber fraud yang semakin kompleks dan multidimensional. Dari sudut pandang actus reus perbuatan pelaku secara jelas memenuhi unsur akses tanpa hak sebagaimana diatur dalam Pasal 30 ayat (1) dan ayat (2) UU ITE. Pelaku tidak sekadar membuat tautan palsu, tetapi secara aktif memperoleh kendali atas akun digital korban melalui data autentikasi yang diperoleh dengan tipu daya. Hukum tidak mensyaratkan bahwa akses ilegal harus dilakukan dengan perusakan sistem; cukup dengan memasuki sistem tanpa hak yang sah, unsur pidana telah terpenuhi. Fakta bahwa korban menyerahkan data karena manipulasi tidak menghapus sifat melawan hukum perbuatan pelaku. Dalam doktrin hukum pidana, persetujuan yang diperoleh melalui tipu daya dianggap cacat secara hukum (Hasanudin et al., 2026). Oleh karena itu, tindakan pelaku tetap dikualifikasikan sebagai akses ilegal. Selain itu, pemindahan aset kripto korban ke akun pelaku memenuhi unsur Pasal 32 ayat (1) dan ayat (2) UU ITE mengenai pemindahan data elektronik tanpa hak. Dengan demikian, dari sisi perbuatan lahiriah, struktur tindak pidana telah terpenuhi secara kumulatif.

Unsur *mens rea* dalam kasus ini memperlihatkan bentuk kesengajaan tingkat tinggi yang mencerminkan niat curang yang terstruktur, sistematis, dan berkelanjutan. Pelaku tidak hanya mengetahui bahwa tindakannya bertentangan dengan hukum, tetapi secara sadar merancang dan memelihara skema phishing sebagai sarana memperoleh keuntungan ekonomi secara ilegal dalam jangka waktu yang panjang. Dalam doktrin hukum pidana, kondisi ini dapat dikategorikan sebagai *dolus directus*, yaitu kesengajaan langsung di mana pelaku secara eksplisit menghendaki akibat yang ditimbulkan dari perbuatannya. Pelaku memahami sepenuhnya bahwa akses terhadap akun korban tidak sah, bahwa data yang diperoleh bersifat rahasia, dan bahwa pemindahan aset digital akan menimbulkan kerugian nyata bagi pihak lain (Dian Putri Yasinta & Ernawati, 2025). Tidak terdapat unsur kelalaian (*culpa*), kesalahan teknis, atau tindakan impulsif yang tidak direncanakan. Justru

yang terlihat adalah adanya pola kriminal yang stabil dan konsisten selama bertahun-tahun, yang menunjukkan bahwa pelaku bertindak dengan kalkulasi rasional. Dalam teori pertanggungjawaban pidana, keberlanjutan tindakan semacam ini memperkuat tingkat kesalahan subjektif karena menunjukkan persistensi niat jahat. Pelaku menyadari risiko hukum namun tetap memilih melanjutkan perbuatannya, yang berarti terdapat penerimaan sadar terhadap konsekuensi pidana. Oleh karena itu, dari sudut pandang kesalahan, unsur kesengajaan dalam kasus ini berada pada tingkat maksimal yang membenarkan penerapan pertanggungjawaban pidana penuh.

Kemampuan bertanggung jawab pelaku juga tidak menimbulkan keraguan dalam perspektif KUHP baru yang menekankan pentingnya kecakapan mental dan rasionalitas pelaku sebagai syarat pemidanaan. Pelaku memiliki kapasitas intelektual tinggi yang tercermin dari kemampuannya memahami teknologi digital, merancang skema kejahatan, serta mengelola hasil kejahatan secara sistematis. Tidak terdapat indikasi gangguan mental, tekanan eksternal, atau kondisi yang dapat menghapus kesalahan berdasarkan konsep alasan pemaaf dalam hukum pidana. Sebaliknya, kecakapan teknis pelaku justru memperlihatkan tingkat kontrol yang tinggi atas tindakannya. Dalam teori hukum pidana modern, seseorang dianggap mampu bertanggung jawab apabila ia dapat memahami sifat perbuatannya dan mengendalikan kehendaknya sesuai norma hukum. Kedua unsur ini terpenuhi secara jelas dalam kasus ini. Pelaku bertindak sebagai subjek hukum yang sadar, bebas, dan rasional, sehingga tidak ada dasar untuk mengurangi atau menghapus pertanggungjawaban pidananya. Konsekuensinya, seluruh unsur kemampuan bertanggung jawab terpenuhi secara utuh, memperkuat legitimasi penghukuman.

Kasus ini juga mengandung dimensi pelanggaran perlindungan data pribadi yang memperluas spektrum pertanggungjawaban pidana. Pasal 67 UU Perlindungan Data Pribadi secara tegas melarang pengumpulan dan penggunaan data pribadi tanpa persetujuan sah dari pemilik data. Dalam skema cyber fraud berbasis rekayasa sosial, pengambilan ID dan kata sandi korban merupakan inti dari kejahatan itu sendiri. Tindakan tersebut tidak hanya menjadi alat untuk memperoleh keuntungan ekonomi, tetapi merupakan pelanggaran langsung terhadap hak privasi individu yang dilindungi hukum. Hukum modern menempatkan data pribadi sebagai bagian dari hak fundamental yang memiliki nilai hukum dan sosial tinggi. Oleh karena itu, pelanggaran terhadap data pribadi tidak dapat dipandang sebagai efek samping dari penipuan, melainkan sebagai tindak pidana mandiri yang menambah bobot pertanggungjawaban pelaku (Kurniawan, 2025). Cyber fraud dalam kasus ini memiliki karakter ganda: sebagai penipuan ekonomi dan sebagai pelanggaran terhadap identitas digital korban. Konsekuensi hukum dari dualitas ini adalah peningkatan tingkat keseriusan tindak pidana dan penguatan dasar pemidanaan terhadap pelaku.

Ancaman pidana dalam Pasal 46 dan Pasal 48 UU ITE memperlihatkan keseriusan negara dalam menangani kejahatan digital. Sanksi penjara hingga sembilan tahun dan denda miliaran rupiah mencerminkan pengakuan bahwa cyber fraud adalah kejahatan ekonomi berat. Besarnya sanksi memiliki fungsi deterrence yang penting. Jika hukuman ringan dijatuhkan, kejahatan serupa akan mudah direplikasi. Ruang digital akan dipersepsikan sebagai wilayah tanpa konsekuensi hukum. Oleh karena itu, penghukuman tegas menjadi kebutuhan struktural dalam penegakan hukum siber. Implikasi penting dari kasus ini adalah kebutuhan integrasi forensik digital dalam sistem pembuktian pidana. Bukti elektronik menjadi pusat pembuktian, sehingga aparat penegak hukum harus memiliki kapasitas teknis tinggi. Tanpa keahlian digital forensik, rantai pembuktian dapat dipatahkan di pengadilan. Penegakan hukum terhadap cyber fraud bukan hanya persoalan

norma, tetapi juga infrastruktur teknologi penegakan hukum. Investasi negara dalam kapasitas forensik menjadi bagian dari kebijakan hukum pidana.

Kasus Donny juga menunjukkan pentingnya pendekatan *follow the money* sebagai strategi inti dalam penegakan hukum terhadap cyber fraud, khususnya melalui penerapan Undang-Undang Tindak Pidana Pencucian Uang. Kejahatan digital modern tidak berhenti pada perolehan keuntungan ilegal, tetapi berlanjut pada upaya menyamarkan asal-usul harta hasil kejahatan agar tampak sah secara ekonomi. Ketika aset kripto hasil penipuan dikonversi menjadi properti, kendaraan mewah, atau instrumen keuangan lain, pelaku berupaya memutus jejak kriminal dari sumber kekayaan tersebut. Dalam kerangka hukum pidana modern, kondisi ini tidak dapat dibiarkan karena akan menciptakan insentif ekonomi bagi kejahatan. Tanpa mekanisme perampasan aset, hukuman penjara semata tidak cukup menciptakan efek jera, karena pelaku masih dapat menikmati hasil kejahatan setelah menjalani masa pidana. Oleh karena itu, perampasan aset bukan sekadar sanksi tambahan, melainkan bagian integral dari konstruksi pertanggungjawaban pidana yang bertujuan memutus motivasi ekonomi di balik kejahatan. Prinsip *crime should not pay* menjadi landasan moral dan hukum bahwa pelaku tidak boleh memperoleh keuntungan dari tindak pidananya. Dalam konteks keadilan restoratif, perampasan aset juga berfungsi memulihkan kerugian korban dan mengembalikan keseimbangan sosial yang terganggu akibat kejahatan. Dengan demikian, pendekatan *follow the money* memperkuat dimensi keadilan substantif dalam sistem hukum pidana.

Dimensi lain yang muncul dari kasus ini adalah kerusakan kepercayaan publik terhadap sistem kripto dan transaksi digital sebagai fondasi ekonomi modern. Cyber fraud tidak hanya menciptakan korban individual, tetapi juga menimbulkan ketakutan kolektif yang berdampak pada perilaku masyarakat dalam menggunakan teknologi keuangan. Ketika masyarakat merasa ruang digital tidak aman, partisipasi dalam ekonomi digital akan menurun, yang pada akhirnya menghambat inovasi dan pertumbuhan ekonomi nasional. Dalam perspektif sosiologi hukum, kepercayaan publik merupakan modal sosial yang sangat penting bagi stabilitas sistem hukum dan ekonomi. Oleh karena itu, penegakan hukum terhadap pelaku cyber fraud memiliki fungsi simbolik sebagai pernyataan bahwa negara hadir melindungi ruang digital (Yulianto, 2025). Penghukuman pelaku menjadi deklarasi normatif bahwa manipulasi elektronik adalah pelanggaran serius terhadap tatanan sosial. Negara harus menunjukkan bahwa ruang siber bukan wilayah tanpa hukum, melainkan ruang yang tunduk pada aturan dan perlindungan hukum yang sama kuatnya dengan dunia fisik. Dengan demikian, proses peradilan pidana memiliki dimensi legitimasi sosial yang melampaui kepentingan individual korban.

Kasus ini juga menyoroti perlunya literasi digital sebagai kebijakan preventif yang tidak terpisahkan dari penegakan hukum pidana. Pendekatan represif melalui penghukuman pelaku memang penting, tetapi tidak cukup untuk menekan angka cyber fraud yang terus berkembang. Masyarakat harus dibekali kemampuan mengenali pola rekayasa sosial, memahami risiko digital, dan melindungi data pribadinya secara mandiri. Edukasi publik berfungsi sebagai lapisan pertahanan pertama yang dapat mengurangi peluang keberhasilan pelaku kejahatan. Dalam perspektif kriminologi modern, pencegahan sosial memiliki peran setara dengan penghukuman karena mampu menurunkan peluang kejahatan sebelum terjadi. Literasi digital juga memperkuat hubungan antara masyarakat dan sistem hukum, karena warga menjadi aktor aktif dalam perlindungan diri. Negara memiliki tanggung jawab tidak hanya menghukum pelaku, tetapi juga membangun masyarakat yang tahan terhadap manipulasi digital. Dengan demikian, strategi

penanggulangan cyber fraud harus memadukan pendekatan hukum pidana, kebijakan pendidikan, dan penguatan kesadaran sosial secara berkelanjutan.

Secara keseluruhan kasus Donny Alven memperlihatkan bahwa hukum pidana Indonesia pada tingkat normatif sebenarnya telah memiliki instrumen yang relatif memadai untuk menjerat pelaku cyber fraud, namun efektivitasnya sangat bergantung pada kapasitas penegakan hukum di lapangan. Kombinasi UU ITE, UU Perlindungan Data Pribadi, dan rezim Tindak Pidana Pencucian Uang membentuk kerangka hukum yang komprehensif, yang secara teoritis mampu menjangkau dimensi akses ilegal, penyalahgunaan data, hingga perampasan hasil kejahatan. Persoalan utama tidak lagi terletak pada kekosongan norma, melainkan pada implementasi teknis, koordinasi antar lembaga penegak hukum, serta kemampuan adaptasi terhadap teknologi yang berkembang sangat cepat. Penegakan hukum cyber membutuhkan sinergi antara aparat kepolisian, kejaksaan, otoritas keuangan, dan lembaga pengawas digital agar respons terhadap kejahatan bersifat terpadu, bukan sektoral. Selain itu, investasi pada forensik digital, pelatihan sumber daya manusia, dan pembaruan prosedur pembuktian menjadi prasyarat agar norma hukum dapat bekerja secara efektif. Cyber fraud dapat dikatakan sebagai kejahatan masa depan yang sudah hadir dalam realitas hari ini, sehingga sistem hukum tidak memiliki pilihan selain terus berevolusi mengikuti dinamika teknologi.

4. KESIMPULAN

Cyber fraud berbasis rekayasa sosial merupakan bentuk kejahatan digital yang telah memenuhi konstruksi tindak pidana dalam hukum pidana Indonesia, baik dari aspek unsur perbuatan, unsur kesalahan, maupun kemampuan bertanggung jawab. Perbuatan pelaku secara nyata menunjukkan adanya kesengajaan, perencanaan, serta pemanfaatan teknologi informasi untuk memperoleh keuntungan secara melawan hukum. Kerangka hukum nasional yang meliputi Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, Kitab Undang-Undang Hukum Pidana yang baru, serta rezim Tindak Pidana Pencucian Uang telah menyediakan dasar normatif yang relatif komprehensif untuk menjerat pelaku cyber fraud. Regulasi tersebut memungkinkan penerapan sanksi pidana, perampasan aset hasil kejahatan, serta perlindungan terhadap hak-hak korban secara terpadu. Kasus Donny Alven menunjukkan bahwa rekayasa sosial bukan sekadar bentuk manipulasi teknis, melainkan merupakan kejahatan ekonomi digital yang terstruktur dan sistematis, yang menyerang data pribadi, aset digital, serta kepercayaan publik terhadap sistem elektronik. Pertanggungjawaban pidana dalam kasus ini tidak hanya berfungsi sebagai sarana penghukuman terhadap pelaku, tetapi juga sebagai instrumen untuk menjaga legitimasi ruang digital sebagai wilayah yang tunduk pada hukum dan prinsip keadilan. Namun demikian, tantangan utama dalam penanggulangan cyber fraud masih terletak pada efektivitas implementasi regulasi, keterbatasan kapasitas teknis aparat penegak hukum, serta kemampuan sistem hukum untuk beradaptasi dengan dinamika perkembangan teknologi. Cyber fraud perlu diposisikan sebagai kejahatan serius dalam ekosistem ekonomi digital yang menuntut penegakan hukum yang tegas, konsisten, dan progresif.

DAFTAR PUSTAKA

Alamsyah, A., Santoso, E., & Pranadita, N. (2025). Kajian Terhadap Kejahatan Carding Sebagai Bentuk Cybercrime Di Indonesia. *Iustitia Omnibus: Jurnal Ilmu Hukum*, *6*(2), 60–68. https://jurnal-pasca.unla.ac.id/iustitiaomnibus/article/view/189

Cahyono, S. T. (2025). Rikonstruksi Hukum Pidana Terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia. *DJH Dame Journal Hukum*, *1*(1), 1–23.

Creswell, J. (2016). Research design Research design. *Research in Social Science: Interdisciplinary Perspectives*, *September*, 68–84. https://www.researchgate.net/publication/308915548%0Afile:///E:/Documents/dosen/buku Metodologi/[John_W._Creswell]_Research_Design_Qualitative,_Q(Bookos.org).pdf

Creswell, J. W., & Creswell, J. D. (2018). Mixed Methods Procedures. In *Research Defign: Qualitative, Quantitative, and Mixed M ethods Approaches*.

Creswell, J. W., & Creswell, J. D. (2023). Research Design : Qualitative, Quantitative, and A Mixed-Method Approach. In *SAGE Publication*. https://doi.org/10.4324/9780429469237-3

Dian Putri Yasinta, & Ernawati. (2025). Analisis Pertanggungjawaban Pidana Terhadap Penipuan Online Melalui Aplikasi Telegram dalam Perspektif Hukum Pidana. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, *4*(3), 15696–15705. https://doi.org/10.31004/jerkin.v4i3.4295

Febriani Wardojo, M. (2025). Konstruksi Hukum Pidana Dalam Penanggulangan Kejahatan Siber Berbasis Teknologi Deepfake di Indonesia. *Legal Standing*, *9*(5), 1169–1183. https://news.detik.com/berita/d-3567290/polling-58-masyarakat-puas-kinerja-kpk,

Gabriel Regina Christian, & Gousta Feriza. (2026). Penerapan Asas Lex Specialis dalam Kasus Penipuan Berbasis Manipulasi Bukti Transfer Digital. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, *4*(3), 15923–15930. https://doi.org/10.31004/jerkin.v4i3.4527

Hasanudin, T. A., Pamulang, U., Perbankan, U., & Pribadi, U. P. D. (2026). Perlindungan Nasabah dan Tanggung Jawab Bank dalam Penanggulangan Kejahatan Digital Berbasis Social Engineering: Analisis Hukum Perbankan Indonesia. *Indonesia of Journal Business Law*, *5*(1), 99–115. https://doi.org/10.47709/ijbl.v5i1.7476

Ismail, M. N. (2026). Pengaruh Teknologi Ai Terhadap Evolusi Modus Kejahatan Siber Di Indonesia Tahun 2024 – 2025 Dan Implikasinya Terhadap Penegakan Hukum The Impact Of Artificial Intelligence Technology On The Evolution Of Cybercrime Modus Operandi In Indonesia (2024 – 2025. *Jurnal Intelek dan Cendikiawan Nusantara*, *2*(6), 12647–12665.

Kurniawan, M. (2025). Pertanggungjawaban Pidana Dalam Kasus Cyberbullying : Analisis Efektivitas Penegakan UU ITE Terhadap Pelaku Remaja. *Bhayangkara Law Review*, *2*(2), 80–89.

Maharani, P., & Rapik, M. (2024). Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia Puan. *PAMPAS: Journal Of Criminal Law*, *5*(2), 242–252.

Novrianto, M. (2025). Kebijakan Hukum Pidana Terhadap Cyber Crime Berbasis Artificial Intelligence di Indonesia. *Jurnal Kepastian Hukum & Keadilan*, *7*(2).

Sofiana, N., Purnomo, M., & Rosita, D. (2025). Analisis Yuridis Tindak Pidana Love Scamming Sebagai Kejahatan Siber. *Semarang Law Review (SLR)*, *6*(2), 282–298. https://www.hukumonline.com/klinik/mitra/si-pokrol-lt4b457ff0c3e1b/renata-christha-auli--sh-

Swalar, T. K. (2022). Kejahatan Penipuan dengan Modus Investasi Ilegal dalam Prespektif Kriminologi. *Jurnal Riset Ilmiah*, *1*(01), 15–18. https://doi.org/10.62335/sinergi.v2i6.1409

Tuju, M. C., Ramadani, S., & Nasution, C. (2025). Penegakan Hukum Terhadap Tindak Pidana Cyber dalam Kasus Penipuan Jual Beli Online dalam Perspektif Kriminologi. *Penegakan Hukum Terhadap Tindak Pidana Cyber dalam Kasus Penipuan Jual Beli Online dalam Perspektif Kriminologi*, *5*, 1763–1776.

Wahyudi BR. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *INNOVATIVE: Journal Of Social Science Research*, *5*, 3436–3451.

Yulianto, H. P. (2025). Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Cyber. *Mizan: Jurnal Ilmu Hukum*, *14*(2), 167–186.