Jurnal Hukum Progresif

Vol 7 No 11, November 2024
EISSN : 24490120

ANALISIS HUKUM PIDANA TERHADAP KEJAHATAN SIBER MELALUI PENGIRIMAN DOKUMEN APK (ANDROID PACKAGE KIT) BERBAHAYA: STUDI KASUS PENIPUAN FILE DIGITAL

Izzul Ilmiyani[1], Ahmada Yudhistira Nurilhikam[2]
izzulilmiyani@gmail.com[1], ahmadayudhistira@gmail.com[2]
Universitas Islam Negeri Walisongo Semarang

Abstrak: Penelitian ini membahas penerapan hukum pidana terhadap kejahatan siber melalui modus pengiriman file APK (Android Package Kit) berbahaya dalam kasus penipuan digital yang marak terjadi melalui aplikasi peran instan seperti WhatsApp. Menganalisis efektivitas pasal-pasal yang relevan dalam KUHP, yaitu Pasal 378 dan 492, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam mengatasi kejahatan siber berbasis APK. Metode yang digunakan adalah metode pendekatan yuridis normative dan studi kasus, dengan fokus pada analisis peraturan perundang-undangan yang berlaku di Indonesia serta relevansinya dalam praktik hukum pidana terhadap kejahatan siber. Hasil penelitian menunjukkan bahwa kejahatan siber melalui pengiriman file APK menghadirkan tantangan besar dalam pengumpulan bukti digital dan efektivitas penegakan hukum. Meskipun regulasi telah tersedia, penanganan kasus ini memerlukan dukungan kerja sama antarlembaga dan peningkatan kapasitas teknis aparat hukum untuk menciptakan efek jera pada pelaku dan melindungi masyarakat dari risiko kejahatan siber serupa.
Kata Kunci: Kejahatan Siber, Penipuan, Android Package Kit (APK).

PENDAHULUAN

Kemajuan teknologi informasi telah memberi dampak signifikan dalam berbagai aspek kehidupan, termasuk ekonomi, pendidikan, sosial, dan hukum. Dalam era digital ini, kemudahan komunikasi dan akses informasi telah memicu perkembangan di dunia maya yang dikenal dengan siber, Di sisi lain, perkembangan ini juga memunculkan tantangan baru dalam bentuk kejahatan siber yang semakin kompleks dan sulit ditangani secara konvensional. Salah satu modus kejahatan siber yang marak terjadi adalah penipuan melalui pengiriman dokumen berformat APK (*Android Package*) berbahaya yang sering digunakan untu menyebarkan perangkat lunak berbahaya atau *malware*.

APK berbahaya ini sering kali dikirim melalui platfrom pesan instan atau email dengan kedok sebagai file penting atau menarik bagi korban, seperti dokumen resmi atau aplikasi yang bermanfaat. Ketika korban mengunduh dan menginstal file tersebut, malware di dalamnya dapat mencuri data pribadi, informasi perbankan, atau bahkan mengambil alih perangkat korban. Hal ini menimbulkan kerugian yan cukup besar. Kejahatan adalah sifat alami yang dimiliki oleh manusia. Sifat jahat sudah ada melekat pada manusia sejak dia lahir. Naluri jahat tidak selalu dipengaruhi oleh faktor eksternal, sering kali, dorongan untuk melakukan tindakan yang merugikan berasal dari dalam sendiri. Kejahatan ada di setiap masyarakat tanpa memandang waktu maupun tempat. Perkembangan teknologi dan perubuhan sosial hanya mengubah motif dan bentuk kejahatan, tapi tidak menghilangkannya. Dalam sudut pandang kriminologi, kejahatan penipuan ini tergolong dalam jenis kejahatan yang trus berulang. Kondisi ini menunjukkan bahwa upaya penanganan dan penegakan hukum terhadap pelaku kejahatan penipuan belum efektif. Dengan kata lain, tujuan pemidanaan dalam hukum pidana nasional msih belum berhasil diwujudkan.[1]

Kejahatan dipengaruhi oleh berbagai faktor, seperti kondisi ekonomi, lingkungan pergaulan, serta kesempatan yang tersedia. Faktor-faktor ini, yang ada di Indonesia, telah membawa dampak negatif. Banyak orang di masyarakat yang terlibat dalam tindakan melanggar hukum demi memenuhi kebutuhan hidupnya. Oleh karena itu, diperlukan kajian yang kritis untuk memahami alasan seseorang melakukan kejahatan, yang dapat dianalisis melalui teori-teori kriminologi. Meskipun sifatnya abstrak, teori-teori ini penting untuk memahami mengapa sebagian orang mampu mematuhi norma sosial dan hukum, sementara yang lain melanggarnya. Selain berperan dalam penelitian dan kegiatan akademik, teori-teori ini juga berguna dalam pendidikan masyarakat.[2]

Peningkatan aktivitas transaksi elektronik telah membawa tantangan baru dengan munculnya berbagai bentuk kejahatan siber di ruang kegiatan virtual. Kejahatan siber ini dilakukan oleh individu atau kelompok yang memanfaatkan kelemahan sistem dan rendahnya kesadaran pengguna akan keamanan informasi. Di Indonesia, jenis kejahatan ini dikenal dengan istilah *cybercrime*, dan para pelakunya disebut sebagai *frauder*.[3] *Cybercrime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari duia internasional. Menurut Muladi *Cybercrime* merupakan suatu istilah umum yang pengertiannya mencakup berbagai tindak pidana yang dapat ditemukan dalam KUHP atau perundang-undangan pidana lainnya yang menggunakan teknologi computer sebagai suatu komponen sentral. Cyber crime berupa tindakan sengaja merusak property, masuk tanpa ijin, pencurian hak milik atas kekayaan intelektual, perbuatan cabul,

[1] M Mulyadi and others, 'Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi', *Media Hukum …*, 2.2 (2024), 74–82 <https://ojs.daarulhuda.or.id/index.php/MHI/article/view/296%0Ahttps://ojs.daarulhuda.or.id/index.php/MHI/article/download/296/327>.

[2] Hardianto Djanggih and Nurul Qamar, 'Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)', *Pandecta: Research Law Journal*, 13.1 (2018), 10–23 <https://doi.org/10.15294/pandecta.v13i1.14020>.

[3] Fairus Hasna, Analisis Kejahatan Pishing dengan Modus Link Undangan Pernikahan pada Aplikasi WhatsApp: Prespektif Hukum Pidana Ekonomi."

pemalsuan, pornografi anak dan pencurian.[4]

Cybercrime memiliki beberapa ciri, yaitu: 1. Akses tidak sah (untuk membantu tindakan kriminal); 2. Perubahan atau kerusakan data tanpa izin; 3. Menghambat operasional computer; 4. Mengganggu atau merusak akses komputer. Negara Indonesia marak sekali kasus kasus tentang penipuan menggunakan email, e-banking, dan e-commerce dikaitkan dengan beberapa kasus criminal. Untuk memberantas dan menghukum para pelaku kejahatan siber ini, diterbitkan peraturan siber (*cyber law)* yang terdapat dalam UU ITE No. 19 Tahun 2016 yang dibentuk guna meminimalisir dan menghapuskan kasus tentang peretasan dan kasus siber lainnya. *Cyber law* adalah aspek hukum yang mengatur individu dan entitas yang menggunakan teknologi internet, meliputi hak cipta, pencemaran nama baik, merek dagang, penghinaan, penistaan, peretasan, transaksi elektronik, pengelolaan sumber daya, keamanan pribadi, pembuktian, kehati-hatian, kejahatan IT, penyelidikan, pencurian melalui internet, perlindungan, serta pemanfaatan internet dalam kehidupan sehar-hari.[5]

Selain itu, penipuan online saat ini telah memanfaatkan media sosial sebagai salah satu sarana dalam melancarkan aksinya. Hal tersebut beberapa kali terjadi melalui aplikasi komunikasi seperti Whatsapp, Instagram, Facebook, Telegram, dan masih banyak lagi. Seperti yang terjadi pada beberapa waktu lalu, pada tahun 2023 dilaporkan terdapaat korban penipuan online di WhatsApp yang kerugiannya mencapai Rp 1,4 M. Kronologinya, Silvia seorang pengusaha aksesori kendaraan asal Malang, Jawa Timur kehilangan uang tabungan Rp 1,4 M di rekeningnya setelah membuka link yang undangan nikah palsu yang dikirim via WhatsApp. Setelh link undangan nikah palsu berisi file aplikasi APK penipuan dibuka, uang tabungan korban di bank terkuras Rp 1,4 M. Uang tabungan tersebut raib dalam beberapa kali transaksi yang tidak diketahui korban. Saat file tersebut dibuka, yang muncul ternyata bukan undangan nikah sebagaimana mestinya, melainkan gambar seperti brosur iklan. Setelah beberapa saat, Silvia menerima pemberitahuan bahwa terdapat upaya ilegal untuk mengakses emailnya. Dari pemberitahuan tersebt, Silvia kemudian memindahkan data ke ponsel dan mengganti password emiailnya. Aksi pengurasan rekening terjadi setelah itu, terdapat aktivitas transfer dana dari dua rekening milik Silvia ke tiga nomor rekening tak dikenal. Selain itu, ada jug transaksi aneh tak dikenal via m-Banking layanan perbankan, lalu beberapa transfer dana ke QRIS, dan beberapa aktivitas pembelian pulsa ke sebuah nomor ponsel tak dikenal. Transaksi tak dikenal yang menguras tabungan Rp 1,4 M itu dijalankan aplikasi mobile banking. Namun anehnya, Silvia mengaku tidak pernah mengunuduh aplikasi tersebut dionselnya. Saat dicek di aplikasi, nomor telepon yang digunakan untuk mendaftar mobile banking juga bukan milik Silvi. Diduga penipu mendaftarkan dengan nomornya sendiri yang bukan milik korban, setelah memiliki akses ke rekening korban.[6]

Di Indonesia, Fenomena ini menarik perharian para ahli hukum dan penegak hukum, mengingat dampak buruk yang ditimbulkan dan tantangan dalam menegakkan hukum terhadap kasus kejahatan siber, Undang-undang Infornasi dan Transaksi Elektronik (UU ITE) di Indonesia, bersama dengan aturan hukum pidana lainnya, sebenarnya telah menyediakan dasar hukum untuk menangani kasus seperti ini, Namun kenyataanya, penegak hukum terhadap kejahatan siber terutama yang melibatkan modus operandi baru seperti penipuan melalui file APK berbahaya, masih menghadapi berbagai kendala. Salah satunya adalah keterbatasan dalam deteksi awal dan pembuktian digital yang memadai, mengingatkejahatan ini bersifat lintas negara dan memiliki mekanisme penyebaran yang sulit dilacak.

[4] Hadion Wijoyo et al, *Cyber Crime* (Juli 2024), hlm.9.

[5] D N Ayman and L Nurhadiyanto, 'Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong)', *IKRA-ITH HUMANIORA: Jurnal …*, 8.2 (2024), 373–84.

[6] Kompas.com, "Korban Penipuan File APK Terkuras Rp 1,4 M, Ini Ciriciri Modusnya, Hati-hati," diakses pada 3 November 2024, https://tekno.kompas.com/read/2023/07/07/10150007/korban-penipuan-file-apk-terkuras-rp-1-4-m-ini-ciri-ciri-modusnya-hati-hati?page=all.

METODE

Dalam penelitian ini, metode yang digunakan adalah dengan menggunakan metode pendekatan yuridis normative serta pendekatan kasus. Penelitian hukum normatif merupakan penelitian yang mengutamakan data kepustakaan yaitu penelitian terhadap data sekunder. Data sekunder tersebut dapat berupa bahan hukum primer, sekunder maupun tersier. Penelitian ini meliputi penelitian mengenai ketentuan hukum positif yang berlaku di Indonesia yang berkaitan cyber crime dari sudut pandang hukum pidana. Metode ini fokus pada analisis terhadap peraturan perundang-undangan yang relevan, serta penerapannya dalam praktek hukum. Dalam konteks jurnal tersebut, analisis hukum terhadap kejahatan siber dengan modus pengiriman APK berbahaya melalui WhatsApp akan didasarkan pada hukum positif yang berlaku, seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Perlindungan Data Pribadi

HASIL DAN PEMBAHASAN

1. Definisi Kejahatan Siber melalui APK

Kejahatan siber pada zaman sekarang ini juga mengalami perkembangan. Terutama dalam beberapa kasus terakhir ini, terdapat banyak kasus dari penipuan hadiah dari bank tertentu, kiriman file pdf bertujuan untuk undangan pernikahan, pengumuman, kabar terkini dan sebagainya. Kejahatan siber dapat mengganggu privasi yang dimiliki oleh setiap individu, kelompok, hingga negara. Hal ini sungguh merugikan banyak orang apalagi bagi kalangan tua yang minim akan pemahaman teknologi yamg banyak menjadi korban. Kejadian seperti ini perlu mendapatkan perhatian khusus dari pemerintah, karena motif kejahatannya berbeda dengan kejahatan biasanya. Kejahatan siber ini dilakukan secara diam tapi dapat meraup harta dan privasi seseorang. Dalam pasal 28 ayat 1 UU ITE menyatakan bahwa setiap orang dengan sengaja tanpa hak menyebarkan informasi elektronikdan dokumen-dokumen elektronik yang memiliki muatan penghinaan atau fitnah, dapat dikenakan pidana penjara. Berdasarkan undang-undang yang telah dibuat, kejahatan dalam media sosial sangat ditekan agar tindakan ini dapat membuat para pelaku jera.

Perkembangan teknologi memang banyak memberi kemudahan manusia dalam melakukan berbagai pekerjaan menjadi cepat dan efisien, seperti halnya mudah dalam bertransaksi, berkomunikasi tanpa harus menemui secara langsung dan masih banyak lagi. Namun tantangan dalam perkembangan teknologi ini juga menimbulkan banyak tantangan yaitu para oknum yang menguasai ilmu pengetahuan teknologi menggunakan ilmunya untuk mencari kesempatan. Tindakan yang merugikan seperti penipuan online dan pencurian identitas. Kejahatan siber ini juga terdampak karena hamper seluruh menusia ketergantungan terhadap teknologi. Ketergantungan teknologi ini yang memudahkan manusia menjadi korban kejahatan siber. Berikut macam-macam jenis kejahatan siber yang merugikan masyarakat yaitu:

a) Illigal Acces

Jenis kejahatan ini dilakukan dengan cara meretas computer secara tidak sah atau dengan kata lain tanpa izin dari pemiliknya.

b) Illegal Contents

Motif kejahatan ini dilakukan dengan cara memalsukan data dokumen penting yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum di internet.

c) Data Forgery

Data Forgery adalah modus criminal di dunia maya yang dilakukan dengan memalsukan data dokumen yang penting dengan menyimpan sebagai dokumen digital melalui internet. Jenis kejahatan ini biasanya menargetkan dokumen *e-commerce*, seolah olah ada *"typo"* yang akan menguntungkan pelaku karena korban memberikan data pribadi dan nomor kartu kredit kepada pelaku.

d) Cyber Espionage

Jenis kejahatan yang menggunakan jaringan internet dengan memasuki sistem jaringan computer pihak yang menjadi korban untuk dimata-matai.

e) Cyber Sabotage dan Extortion

Modus kejahatan jenis ini biasanya dilakukan dengan mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program computer, atau sistem jaringan komputer. Ini biasanya dilakukan dengan menggunakan logic bomb, virus, atau program tertentu yang membuat data, program, atau sistem jaringan computer tidak dapat digunakan atau beroperasi secara normal, tetapi telah dikendalikan oleh orang lain.

f) Offense against intellectual property

Metode kejahatan ini adalah menyasar hak kekayaan intelektual orang lain di internet, seperti meniru konten di website orang lain seperti illegal.

g) Infringements of privacy

Jenis kejahatan ini biasanya menargetkan informasi pribadi yang disimpan dalam formulir data pribadi yang disimpan secara computer. Mengetahui informasi ini dapat menyebabkan kerugian materiil maupun immaterial kepada korban, seperti bocornya nomor pin ATM dan lainnya.[7]

Adapun penyebab sering terjadinya kejahatan siber yang meresahkan warga ini dikarenakan beberapa hal yaitu:

a) Internet tak terbatas

Internet memiliki akses yang tak terbatas dan tidak mengenal ruang dan waktu. Akses ini yang menyebabkan kasus kejahatan siber terus berkembang karena tidak adanya batasan internet.

b) Kelalaian

Kelalaian adalah bentuk tindakan yang salah akibat dari kurangnya kehatian-hatian. Kelalaian ini juga menjadi penyebab utama terjadinya kejahatan siber. Hal ini karena kecerobohan atau bisa menjadi cela untuk para pelaku kejahatan siber.

c) Keamanan yang rendah

Sistem keamanan adalah kunci dalam menjaga data kita dari pelaku kejahatan siber. Dengan keamanan yang rendah dapat mempermudah pelakukejahatan dalam melancarkan aksinya.

d) Pelaku yang cerdas dalam teknologi

Pelaku dalam kejahatan siber adalah orang yang ahli atau cerdas dalam teknologi, mereka mempunyai pengetahuan yang luas di bidang teknologi. Pengetahuan yang dimiliki jauh melebihi operator computer biasa.

e) Kurangnya perhatian terhadap kejahatan siber

Masyarakat dan penegak hukum kurang memberikan perhatian khusus terhadap dampak dari kejahatan siber ini, sehingga kejahatan ini akan terus berlanjut dan bertambahnya kejahatan siber yang baru.[8]

f) Fasilitas yang memadai

Fasilitas teknologi dan informasi untuk saat sekarang ini sangat berkembang pesat didalam masyarakat. Setiap masyarakat pada umumnya memiliki smartphone yang selalu ada disetiap orang, akan tetapi tidak semua orang bisa memfaatkan hal ini dengan perilaku yang positif. Banyak dari masyarakat yang salah pemanfaatan dalam perkembangan teknologi dan informasi.[9]

Maraknya kejahatan siber yang semakin meresahkan masyarakat disebabkan oleh sejumlah faktor diatas. Ketidakpedulian dan kurangnya perlindungan menyebabkan kejahatan siber semakin

[7] Varik Farsyak, Fakultas Hukum, and Universitas Bengkulu, 'Kejahatan Siber, Menangulangi, Penegak Hukum, Peran', 6.7 (2024).

[8] Farsyak, Hukum, and Bengkulu.

[9] Zainudin Hasan and others, 'Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online', *Jurnal Multidisiplin Dehasen (MUDE)*, 2.3 (2023), 375–80 <https://doi.org/10.37676/mude.v2i3.4153>.

berkembang pesat. Oleh karena itu, upaya pencegahan yang serius dan peningkatan kesadaran terhadap ancaman siber sangat diperlukan. Langkah Langkah ini termasuk meningkatkan keamanan sistem, edukasi tentang bahaya siber, serta tindakan hukum yang tegas untuk membatasi ruang gerak pelaku dan menekan kasus kejahtan siber di masa depan.

2. Penerapan Hukum Siber di Era Digital di Indonesia

Dalam era digital yang terus berkembang, tindak pidana siber di Indonesia telah menjadi ancaman serius, khususnya di sektor ekonomi yang rentan. Kejahatan siber seperti pencurian data nasabah, penipuan online, perdagangan ilegal, dan serangan terhadap sistem perbankan terus mengalami peningkatan. Fenomena ini berdampak luas, tidak hanya menyebabkan kerugian finansial bagi masyarakat, tetapi juga mengancam keamanan nasional serta menimbulkan risiko signifikan bagi pertumbuhan ekonomi negara.

Penegakan hukum terhadap kejahatan siber menghadapi berbagai tantangan, terutama dalam upaya harmonisasi regulasi yang berkaitan dengan penggunaan internet. Menghadapi ancaman yang semakin kompleks, penegakan hukum perlu diperkuat dan disesuaikan agar dapat menangani berbagai tantangan dalam lingkungan digital yang dinamis dan terus berubah.

Saat ini, praktik penanganan tindak pidana seperti penipuan, perjudian, dan pornografi masih merujuk pada Kitab Undang-Undang Hukum Pidana (KUHP). Namun, dengan perkembangan teknologi informasi dan komunikasi yang pesat, pola transaksi, pembelian, investasi, serta operasi bisnis mengalami perubahan besar. Perubahan ini juga membuka peluang meningkatnya kejahatan siber, termasuk serangan terhadap sektor perbankan, pencurian data, dan perdagangan ilegal. Oleh karena itu, diperlukan langkah-langkah konkret untuk melindungi sistem komputer, jaringan, perangkat elektronik, dan data dari ancaman siber. Upaya ini sangat penting untuk menjawab tantangan baru yang muncul seiring dengan kemajuan teknologi, sehingga sistem hukum perlu terus diperbarui dan disesuaikan dengan kebutuhan zaman yang berkembang cepat.

Keamanan siber bertujuan menjaga kerahasiaan, integritas, dan ketersediaan informasi sensitif, serta melindungi infrastruktur teknologi informasi dari serangan yang berpotensi merusak sistem atau menimbulkan kerugian besar. Di tengah meningkatnya ancaman, kolaborasi antara pemerintah, sektor swasta, dan masyarakat menjadi semakin penting untuk melindungi keamanan dan kedaulatan negara dari berbagai potensi ancaman dan gangguan. Pemerintah Indonesia telah merespons peningkatan ancaman siber dengan mengadopsi kebijakan dan regulasi guna memperkuat keamanan siber serta melindungi infrastruktur informasi kritis. Salah satu langkah nyata adalah pembentukan Badan Siber dan Sandi Negara (BSSN), lembaga yang secara khusus menangani berbagai ancaman di dunia digital. Meski demikian, tantangan yang dihadapi masih besar, sehingga pembaruan regulasi dan peningkatan kemampuan penegakan hukum sangat diperlukan untuk menjaga keamanan nasional dan meminimalkan risiko kejahatan siber yang dapat mengancam stabilitas dan keamanan Indonesia.[10]

Untuk menghadapi tantangan keamanan siber, Pemerintah Indonesia telah mengambil langkah aktif dalam memperkuat infrastruktur digital nasional. Langkah-langkah tersebut mencakup pengembangan kebijakan, peningkatan teknologi keamanan, dan penyuluhan kepada masyarakat mengenai risiko keamanan siber. Salah satu langkah utama yang dilakukan adalah penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi pilar utama dalam sistem hukum keamanan siber di Indonesia.

UU ITE berperan penting dalam menangani berbagai isu terkait transaksi elektronik dan penyebaran informasi secara digital. Selain mengatur aspek hukum transaksi daring, UU ini juga secara rinci mengatur penyebaran informasi di internet, memberikan kerangka untuk melindungi data pribadi warga, dan menetapkan standar dalam menghadapi kejahatan siber yang semakin kompleks.

[10] Jurnal Ilmu Sosial, ‘Al-Dalil’, 2.2 (2024).

Secara garis besar, dasar hukum untuk menangani kejahatan siber di Indonesia berlandaskan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang telah direvisi oleh Undang-Undang Nomor 19 Tahun 2016. UU ITE ini mencakup berbagai transaksi dan aktivitas berbasis elektronik, termasuk pengaturan terkait konten ilegal, penipuan online, pencurian data, dan peretasan. Melalui undang-undang ini, berbagai bentuk pelanggaran siber, mulai dari penyebaran konten terlarang hingga tindakan penipuan dan peretasan, dapat ditangani untuk melindungi masyarakat.[11]

3. Penerapan Hukum terhadap Kejahatan Siber Melalui Pengiriman Dokumen APK (Android Package Kit) melalui Whatsapp

Kejahatan siber dengan modus pengiriman file APK melalui WhatsApp telah menjadi ancaman serius yang merugikan banyak pihak. Untuk menindaklanjuti kasus semacam ini, pemerintah menerapkan ketentuan hukum yang tegas. Salah satu dasar hukum yang digunakan adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 67 dan Pasal 69 dalam undang-undang ini memberikan sanksi kepada siapa pun yang mengakses atau memperoleh data pribadi secara ilegal untuk keuntungan pribadi, termasuk hukuman pidana penjara, denda, dan sanksi tambahan.

Proses penegakan hukum terhadap pelaku kejahatan siber ini mencakup langkah-langkah seperti penangkapan, penahanan, dan penyitaan barang bukti oleh pihak berwenang. Melalui penerapan hukum ini, korban diharapkan dapat memperoleh kembali hak-hak mereka, serta pelaku akan diberikan efek jera untuk mencegah kejadian serupa. Hal ini juga sesuai dengan prinsip viktimologi yang berfokus pada perlindungan hak-hak korban dan pencegahan terjadinya lebih banyak korban di masa depan. Dengan menerapkan ketentuan ini secara efektif, pemerintah dapat memberikan rasa aman kepada masyarakat dan memperkuat upaya perlindungan terhadap data pribadi di era digital.

Modus penipuan melalui klik file aplikasi termasuk jenis penipuan online, yang dikategorikan sebagai tindak pidana dalam Pasal 378 KUHP lama dan Pasal 492 pada KUHP baru sesuai dengan Undang-Undang Nomor 1 Tahun 2023. Selain itu, dasar hukum yang saat ini berlaku untuk menjerat pelaku penipuan diatur dalam Undang-Undang Nomor 19 Tahun 2016, yang merupakan perubahan dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pada Pasal 28 ayat (1).

Pasal 378 KUHP memuat unsur-unsur penipuan, yaitu tindakan membujuk orang lain agar menyerahkan barang, membuat utang, atau menghapuskan piutang. Berdasarkan unsur-unsur ini, penipuan dapat didefinisikan sebagai perbuatan seseorang menggunakan tipu daya, rangkaian kebohongan, nama palsu, atau keadaan palsu untuk mengambil keuntungan pribadi tanpa hak. Rangkaian kebohongan adalah susunan pernyataan-pernyataan palsu yang dibuat sedemikian rupa sehingga tampak seolah-olah benar.[12]

Penegakan hukum terhadap pelaku kejahatan menjadi sangat penting untuk mencegah dan menindaklanjuti tindak pidana. Dalam kasus penipuan online dengan modus APK (Android Package Kit) melalui WhatsApp, penerapan hukum dilakukan melalui tindakan penindakan terhadap pelaku. Setelah penindakan, pelaku akan menjalani proses hukum yang meliputi tahap penyidikan, tuntutan, hingga penjatuhan pidana oleh hakim. Sanksi yang dijatuhkan kepada pelaku dalam kasus ini mengacu pada Pasal 67 dan Pasal 69 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menjadi dasar hukum perlindungan data pribadi di Indonesia.

Tindakan terhadap pelaku kejahatan penipuan online dengan modus APK (Android Package Kit) melalui WhatsApp merupakan salah satu bentuk penerapan hukum. Dalam Pasal 67 dan Pasal

[11] Jurnal Ilmu Sosial, 'AL-BAHST', 2.1 (2024), 8–16.
[12] Artikel Skripsi and others, 'Lex_Administratum Vol_12_No_05_Sept_2024 Universitas Sam Ratulangi_Fakultas Hukum'.

69 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang memberikan sanksi bagi pelaku penipuan online dengan modus APK melalui WhatsApp, akan menjadi tidak efektif jika tidak diterapkan. Oleh karena itu, tindakan seperti penangkapan, penahanan, dan penyitaan barang bukti yang dilakukan oleh kepolisian merupakan wujud konkret penerapan Pasal 67 dan Pasal 69 dari Undang-Undang tersebut.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menetapkan bahwa seseorang yang secara melawan hukum mengumpulkan atau mendapatkan data pribadi untuk keuntungan pribadi dapat dikenakan hukuman pidana penjara, denda, serta pidana tambahan.[13] Menurut analisis penulis, tindakan penegakan hukum, termasuk penangkapan, penahanan, dan penyitaan barang bukti terhadap pelaku kejahatan tersebut, merupakan wujud penerapan hukum sesuai undang-undang ini. Penerapan hukum terhadap pelaku penipuan online dengan modus APK melalui WhatsApp bertujuan untuk memberikan rasa aman kepada korban, mengembalikan hak-hak korban, memberikan efek jera kepada pelaku, mencegah kejahatan serupa, dan membawa manfaat lainnya. Dalam perspektif viktimologi, langkah ini sejalan dengan tujuan viktimologi untuk melindungi hak-hak korban, memberikan perlindungan hukum, dan mencegah timbulnya lebih banyak korban. Jika Pasal 67 dan Pasal 69 dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi tidak diterapkan, maka korban tidak akan mendapatkan perlindungan hukum, dan pelaku tidak akan merasakan efek jera, sehingga potensi kejahatan serupa akan semakin meningkat. Oleh karena itu, penerapan hukum terhadap pelaku penipuan online dengan modus APK melalui WhatsApp merupakan upaya penting dalam menanggulangi kejahatan serta memberikan rasa aman kepada korban.

KESIMPULAN

Kejahatan siber yang dilakukan melalui pengiriman file APK berbahaya termasuk dalam kategori cyber crime, di mana pelaku mengirimkan aplikasi berbahaya yang mengandung malware atau program jahat lainnya. Tujuannya adalah untuk meretas, mencuri data, atau memeras korban. Jenis kejahatan ini semakin meningkat seiring dengan tingginya penggunaan smartphone dan aksesibilitas terhadap aplikasi pihak ketiga yang tidak diawasi secara ketat. Sistem hukum di Indonesia telah memiliki payung hukum untuk mengatur tindak pidana siber melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta beberapa peraturan turunan lainnya. Namun, penegakan hukum terhadap kejahatan siber menghadapi berbagai tantangan, seperti keterbatasan teknis, kurangnya pemahaman digital di kalangan masyarakat dan aparat penegak hukum, serta kurangnya koordinasi antar lembaga terkait. Penipuan melalui pengiriman APK berbahaya di WhatsApp menimbulkan tantangan tersendiri karena sifatnya yang lintas batas, cepat, dan sulit dideteksi. Beberapa kasus menunjukkan bahwa pelaku dapat dengan mudah menyebarkan malware tanpa terdeteksi, sehingga memperlambat proses penegakan hukum. Namun, dengan adanya peningkatan kerja sama antara lembaga keamanan siber dan penyedia platform seperti WhatsApp, langkah-langkah pencegahan serta deteksi dini diharapkan dapat lebih efektif.

DAFTAR PUSTAKA

Artikel Skripsi and others, ‘Lex_Administratum Vol_12_No_05_Sept_2024 Universitas Sam Ratulangi_Fakultas Hukum’.

D N Ayman and L Nurhadiyanto, ‘Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong)’, IKRA-ITH HUMANIORA: Jurnal …, 8.2 (2024), 373–84.

Fairus Hasna, Analisis Kejahatan Pishing dengan Modus Link Undangan Pernikahan pada Aplikasi WhatsApp: Prespektif Hukum Pidana Ekonomi.”

Farsyak, Hukum, and Bengkulu.

[13] Negara Republik, ‘UU Nomor 27 Tahun 2022’, 016999, 2022.

Hadion Wijoyo et al, Cyber Crime (Juli 2024), hlm.9.

Hardianto Djanggih and Nurul Qamar, 'Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cyber Crime)', Pandecta: Research Law Journal, 13.1 (2018), 10–23 <https://doi.org/10.15294/pandecta.v13i1.14020>.

Jurnal Ilmu Sosial, 'AL-BAHST', 2.1 (2024), 8–16.

Jurnal Ilmu Sosial, 'Al-Dalil', 2.2 (2024).

Kompas.com, "Korban Penipuan File APK Terkuras Rp 1,4 M, Ini Ciriciri Modusnya, Hati-hati," diakses pada 3 November 2024, https://tekno.kompas.com/read/2023/07/07/10150007/korban-penipuan-file-apk-terkuras-rp-1-4-m-ini-ciri-ciri-modusnya-hati-hati?page=all.

M Mulyadi and others, 'Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi', Media Hukum …, 2.2 (2024), 74–82 <https://ojs.daarulhuda.or.id/index.php/MHI/article/view/296%0Ahttps://ojs.daarulhuda.or.id/index.php/MHI/article/download/296/327>.

Varik Farsyak, Fakultas Hukum, and Universitas Bengkulu, 'Kejahatan Siber, Menangulangi, Penegak Hukum, Peran', 6.7 (2024).

Zainudin Hasan and others, 'Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online', Jurnal Multidisiplin Dehasen (MUDE), 2.3 (2023), 375–80 <https://doi.org/10.37676/mude.v2i3.4153>.