ASPEK HUKUM PIDANA TERHADAP KEJAHATAN PENCURIAN DATA MELALUI WHATSAPP BERDASARKAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Clarisa Tambing Mangngelo[1], Ivan Zairani Lisi[2], Deny Slamet Pribadi[3]
clarisatm19@gmail.com [1], ivanzairani@fh.unmul.ac.id[2], denypribadi88@gmail.com[3]
Universita Mulawarman

ABSTRAK

Aspek hukum pidana terhadap kejahatan pencurian data pribadi melalui Whatsapp yang ditinjau berdasarkan Undang-Undang Informasi dan Transaksi Elektronik serta mengkaji penegakan hukum terhadap pelaku kasus pencurian data pribadi melalui Whatsapp. penelitian ini menggunakan metode yuridis normatif dengan pendekatan doktrinal, menganalisis bahan hukum primer berupa Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, serta bahan hukum sekunder dan tersier. Hasil penelitian menunjukkan bahwa perbuatan pencurian data melalui WhatsApp seharusnya telah memenuhi unsur-unsur tindak pidana sebagaimana diatur dalam Pasal 30 jo 46 dan Pasal 32 jo 48 UU ITE dengan ancaman pidana maksimal 9 tahun penjara dan denda 3 miliar rupiah, serta Pasal 65 dan 67 UU Perlindungan Data Pribadi dengan ancaman maksimal 5 tahun penjara dan denda 5 miliar rupiah. Namun, dalam praktiknya seluruh 114 dari tahun 2021-2025 kasus masih terhenti pada tahap penyelidikan tanpa ada yang mencapai tahap persidangan. Kasus ini terkendala dalam tahap penyelidikan bukan karena perbuatan tersebut tidak termasuk tindak pidana, melainkan karena kendala teknis dalam pembuktian identitas pelaku.
Kata Kunci: Perlindungan Data Pribadi, Whatsapp, Undang-Undang Ite.

ABSTRACT

Criminal law aspects of personal data theft crimes through WhatsApp as reviewed based on the Electronic Information and Transaction Law and to examine law enforcement against perpetrators of personal data theft cases through WhatsApp. This research uses a normative juridical method with a doctrinal approach, analyzing primary legal materials in the form of Law Number 1 of 2024 concerning Electronic Information and Transactions, as well as secondary and tertiary legal materials. The results of the study show that data theft via WhatsApp has fulfilled the elements of a criminal offense as stipulated in Article 30 jo 46 and Article 32 jo 48 of the ITE Law with a maximum criminal penalty of 9 years imprisonment and a fine of 3 billion rupiah, as well as Articles 65 and 67 of the Personal Data Protection Law with a maximum penalty of 5 years imprisonment and a fine of 5 billion rupiah. However, in practice, all 114 cases from 2021-2025 are still stuck at the investigation stage with none reaching the trial stage. These cases are stalled at the investigation stage not because the acts do not constitute criminal offenses, but due to technical challenges in proving the perpetrators' identities.
Keywords: *Personal Data Theft, Whatsapp, ITE Law.*

PENDAHULUAN

Perkembangan teknologi yang semakin berkembang pesat, dunia menjadi tidak terbatas serta perubahan yang besar dan cepat terjadi di masyarakat, yang tidak selalu mengarah ke hal positif tetapi juga negatif. Perkembangan teknologi mengakibatkan munculnya kejahatan di media sosial yang biasa disebut *cybercrime*, dengan salah satu modusnya yaitu pencurian data pribadi pengguna media sosial, tindakan ilegal bertujuan untuk mendapatkan informasi pribadi seperti PIN, nomor kartu kredit, *User ID*, nomor telepon, nomor rekening dan data pribadi lainnya.

Undang-Undang No 1 Tahun 2024 atas perubahan kedua atas Undang-Undang No 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik merupakan regulasi yang mengatur pengelolaan informasi dan transaksi elektronik di tingkat nasional, bertujuan agar

pengembangan teknologi informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat untuk mencerdaskan kehidupan bangsa, sekaligus memenuhi kebutuhan perkembangan dan kemajuan teknologi informasi yang demikian pesat.

Whatsapp merupakan aplikasi yang digunakan lebih dari 87% penduduk Indonesia untuk kebutuhan pribadi maupun profesional,[1] *Whatsapp* menjadi media penting dalam pertukaran informasi, termasuk data-data pribadi dan rahasia. Namun, kemudahan ini juga membuka cela bagi kejahatan digital, salah satunya adalah pencurian data melalui file *APK* yang disisipkan pada *malwer*. Pencurian data ini termasuk dalam kategori kejahatan siber atau *cybercrime* yang mencakup segala bentuk kejahatan yang menargetkan jaringan komputer dan menggunakan teknologi telekomunikasi.

Modus operandi kejahatan pencurian data ini dimulai Ketika korban menerima pesan *Whatsapp* dari nomor tidak dikenal yang menyertakan file lampirantampat tidak mencurigakan, seperti undangan pernikahan, foto paket kiriman, atau kartu ucapan hari raya, yang sengaja dirancang untuk mendorong korban agar mengunduh dan membukanya. Begitu file tersebut dibuka, *malwer* yang tertanam di dalamnya akan terinstal secara otomatis, memberikan pelaku akses penuh untuk memantau aktivitas ponsel korban, membaca pesan masuk, mengambil kode OTP via SMS, serta mencuri data pribadi sensitive seperti informasi kartu identitas dan nomor rekening. Dengan memanfaatkan data dan kode OTP yang berhasil disadap, pelaku kemudian dapat mengakses rekening bank korban, yang kemudian melakukan transfer dana tanpa sepengetahuan korban, hingga menyalagunakan data pribadi tersebut untuk tindak kejahatan lain seperti pembuatan akun anonym atau trasaksi illegal atas nama korban.

Berdasarkan data Kepolisian Resor Kota Samarinda, dari tahun 2021 hingga 2025 tercatat 114 kasus pencurian data melalui aplikasi *WhatsApp* yang seluruhnya masih dalam tahap penyelidikan dan belum ada yang mencapai tahap persidangan. Kasus-kasus tersebut umumnya melibatkan modus operandi yang menggunakan file APK yang kemudian dapat menembus data-data pribadi korban. Dari total 114 kasus yang tercatat, pada tahun 2021 terdapat 20 kasus, tahun 2022 mengalami peningkatan menjadi 22 kasus, tahun 2023 tercatat 24 kasus, tahun 2024 mencapai 23 kasus, dan hingga awal tahun 2025 (januari-oktober) sudah tercatat 25 kasus baru yang dilaporkan.

Pencurian data pribadi sebagaimana yang telah diatur pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah pada Undang-Undang No. 1 Tahun 2024. Dalam UU ITE, terdapat pasal-pasal yang dapat menjerat pelaku kejahatan siber, seperti Pasal 30 jo 46 dan Pasal 32 jo 48 yang mengatur akses ilegal dan manipulasi data elektronik setiap orang yang dengan sengaja melawan hukum dengan cara apapun mengakses, melakukan transmisi, menghilangkan dan memindahkan sistem elektronik milik orang lain dan informasi elektronik milik orang lain.

Pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data pribadi juga telah mengatur mengenai penyalagunaan data pribadi, pada pasal 65 berbunyi "bahwa setiap orang secara melawan hukum dilarang memperoleh atau mengumpulkan data pribadi, mengungkapkan data pribadi dan juga menggunakan data pribadi yang mengakibatkan kerugian bagi subjek data pribadi". Kemudian pada pasal 67 berbunyi "bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh dan mengumpulkan, mengungkapkan dan menggunakan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri yang mengakibatkan kerugian subjek data pribadi dapat di pidana paling lama 5 tahun dan/atau pidana denda paling banyak Rp. 5 Miliar Rupiah".

---

[1] Wahyuddin, Lutfiah, Gusti, Taufik, dan Alem, Analisis Jaringan Komunikasi Penipuan Daring Melalui Media Sosial Whatsapp Messenger, Jurnal Netnografi Komunikaasi (JKN), Vol. 2, No. 2. 2024, hlm. 75. Diakses pada tanggal 26 September 2025 pukul 00.00 https://netnografiikom.org/index.php/netnografi/article/view/27

Meskipun secara normatif kasus pencurian data pribadi melalui *Whatsapp* telah diatur dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pada faktanya kasus pencurian data pribadi melalui *whatsapp* masih terjadi sampai saat ini hal ini membuktikan penegakan hukum yang masih lemah yaitu minimnya kemampuan aparat untuk menemukan pelaku dari kasus pencurian data pribadi dan kurangnya koordinasi antara instansi terkait. Kondisi ini diperparah oleh keamanan pada *whatsapp* yaitu *end-to-end* tidak mencakup file yang digunakan pelaku, sehingga *malwer* pad file tersebut dapat mengambil alih perangkat korban.

Lambatnya respons penegak hukum, bahkan dalam kasus yang sudah dilaporkan dengan bukti yang jelas, memberikan rasa aman semu bagi para pelaku untuk terus melancarkan aksinya. Dari data yang ada dengan rendahnya tingkat penyelesaian kasus dan jarangnya pelaku yang berhasil ditangkap, sehingga menciptakan persepsi bahwa kejahatan siber memiliki risiko hukum yang rendah namun dengan potensi keuntungan finansial yang tinggi, yang pada akhirnya semakin mendorong maraknya tindak pidana pencurian data melalui platform digital.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara mendalam bagaimana respon penegak hukum terhadap tindakan pencurian data pribadi melalui *WhatsApp* yang dapat dikategorikan sebagai tindak pidana berdasarkan unsur-unsur yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik, sekaligus mengidentifikasi bagaimana hukum pidana dalam penegakan hukum mengatur, melindungi kepentingan kepentingan korban, dan menegakkan keadilan terhadap pelakumelalui segala aspek hukum pidana yang berlaku di Indonesia.

METODE PENELITIAN

Pelaksanaan penelitian ini, penulis menggunakan pendekatan yuridis normatif, serta jenis penelitian dalam penulisan ini adalah Doktrinal. Penelitian ini merupakan suatu proses untuk menemukan suatu aturan hukum untuk menjawab permasalahan hukum yang dihadapi, penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai petunjuk dalam peneyelesaian masalah yang di hadapi.

Bahan hukum yang digunakan terdiri sari bahan hukum primer (peraturan perundang-undangan), bahan hukum sekunder (buku, jurnal, hasil penelitian), dan bahan hukum tersier (kamus hukum dan wawancara). Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yang kemudian dianalisis secara kualitatif untuk mendeskripsikan jawaban atas permasalahan penelitian.

HASIL DAN PEMBAHASAN

Kasus Pencurian Data Pribadi Di Samarinda

Data kasus pencurian data pribadi melalui whatsapp di Kepolisian Resor Kota Samarinda, yang diperoleh pada 30 Oktober 2025.

TAHUN	JUMLAH	PROSES PENEGAKAN
2021	20	LIDIK
2022	22	LIDIK
2023	24	LIDIK
2024	23	LIDIK
2025	25 (JAN-OKT)	LIDIK

Dalam kurun waktu waktu tahun 2021 hingga Oktober tahun 2025, kasus pencurian data pribadi melalui Whatsapp di wilayah hukum Polres Kota Samarinda terus meningkat, tercatat 20 kasus pada tahun 2021, meningkat menjadi 22 kasus pada tahun 2022, kemudian 24 kasus

pada 2023, sedikit mengalami penurunan menjadi 23 kasus pada tahun 2024, dan Kembali meningkat menjadi 25 kasus hanya dalam periode Januari hingga Oktober 2025. Secara kumulatif, total keseluruhan kasus yang berhasil dihimpun dalam rentang waktu tersebut mencapai 114 kasus, suatu angka yang mencerminkan eskalasi kejahatan siber yang perlu mendapatkan perhatian serius dari berbagai pihak.

Dari aspek modus operandi, terdapat perkembangan yang semakin kompleks dan terstruktur dari tahun ke tahun. Pada awalnya, pelaku menggunakan metode yang relatif sederhana seperti pembajakan akun melalui kode *One-Time Password* (OTP) palsu, phishing dengan menggunakan file berbahaya yang disebarkan melalui pesan *whatsapp,* hingga manipulasi psikologis Dimana pelaku menyamar sebagai pihak tertentu untuk memperoleh informasi pribadi korban. Adapun penurunan jumlah laporan pada tahun 2024 tidak mengindikasikan bahawa situasi keamanan digital membaik melainkan menurunnya kepercayaan publik terhadap sistem pelaporan dari progres penanganan kasus sebelumnya.

Temuan yang paling krusial dalam kajian ini adalah dari 114 kasus yang tercatat, tidak satu pun yang berhasil diselesaikan hingga tahap penuntutan maupun persidangan, seluruhnya masih bertahan dalam proses penyelidikan yang berkepanjangan tanpa kepastian hukum yang jelas. Kondisi demikian mengindikasikan adanya disfungsi struktural dan sistematis dalam mekanisme penegakan hukum terhadap kejahatan siber, khususnya di wilayah hukum Polres Kota Samarinda. Hal ini tidak hanya berdampak pada hilangnya hak katas keadilan bagi para korban, tetapi juga secara tidak langsung menciptakan kebebasan bagi pelaku, yang pada akhirnya berpotensi mendorong peningkatan angka kejahatan serupa di masa mendatang.

1. Modus Operandi Pelaku dari Tindak Pencurian Data Pribadi

a) Modus operandi yang paling sering ditemukan adalah skema penipuan melalui iklan online di media sosial yang mengarahkan korban ke permainan berhadiah di *WhatsApp*, di mana pelaku menggunakan identitas palsu dan bahkan mentransfer sejumlah uang kecil pada tahap awal sebagai strategi psikologis untuk membangun kepercayaan korban. Setelah korban terlena, pelaku mendorong korban mengunduh file APK yang mengandung *malware* untuk mengakses data pribadi perangkat korban, dengan eksekusi yang sengaja dilakukan pada akhir pekan ketika layanan perbankan tidak beroperasi, sehingga pelaku memiliki lebih banyak waktu untuk menguras rekening korban sebelum tindakan pencegahan dapat dilakukan
b) Modus operandi kedua yang banyak dilaporkan di Polres Samarinda adalah skema penipuan yang memanfaatkan popularitas platform *e-commerce Shopee*, di mana pelaku menawarkan pekerjaan sampingan berupa pemberian like pada produk-produk tertentu di *Shopee* dengan imbalan komisi, yang kemudian dibuktikan melalui *screenshot* yang dikirimkan korban kepada pelaku melalui *WhatsApp*.

2. Analisis Pertanggungjawaban Hukum

Berdasarkan data dari Polres Samarinda periode 2021 hingga Oktober 2025, dari total 114 kasus pencurian data pribadi melalui *WhatsApp* yang dilaporkan, tidak satu pun yang berhasil diselesaikan hingga tahap penyidikan, penuntutan, maupun persidangan, seluruhnya masih terhenti pada tahap penyelidikan. Kondisi ini sangat bertentangan dengan prinsip kepastian hukum dan ketentuan KUHAP, di mana penyelidikan seharusnya menjadi tahap awal yang segera menentukan kelayakan suatu perkara untuk naik ke tahap penyidikan, bukan berlarut-larut tanpa progres yang jelas.

Para korban pun tidak mendapatkan informasi yang transparan mengenai perkembangan kasusnya, yang secara nyata bertentangan dengan Pasal 109 KUHAP dan Pasal 184 ayat (1) Peraturan Kapolri Nomor 6 Tahun 2019 yang mewajibkan penyidik memberikan informasi perkembangan perkara kepada pelapor, sehingga menimbulkan kerugian materiil maupun psikologis bagi korban sekaligus menurunkan kepercayaan publik terhadap institusi

kepolisian.

Lebih mengkhawatirkan lagi, Polres Samarinda tampak belum menunjukkan respons strategis yang memadai terhadap permasalahan sistemik ini, terlihat dari tidak adanya upaya nyata berupa evaluasi internal, pelatihan khusus kejahatan siber, pengadaan peralatan forensik digital, maupun pembentukan unit *cybercrime* yang lebih profesional meskipun kasus terus meningkat dari tahun ke tahun.

Akumulasi 114 kasus yang tidak terselesaikan seharusnya menjadi peringatan serius bagi pimpinan Polres Samarinda untuk segera melakukan reformasi internal dan meminta dukungan dari Polda Kalimantan Timur maupun Mabes Polri, karena ketiadaan respons yang signifikan ini mencerminkan lemahnya akuntabilitas institusional dan absennya mekanisme kontrol internal yang efektif dalam penanganan kejahatan siber.

Analisis Hukum Pidana Terkait Dengan Pencurian Data Pribadi

1. Undang-Undang Informasi dan Transaksi Elektronik

Pasal 30 mengatur secara tegas bahwa setiap orang yang dengan sengaja dan tanpa hak mengakses computer dan/atau sistem elektronik milik orang lain dapat dipidana penjara antara 6 hingga 8 tahun serta dikenakan denda antara Rp. 600.000.000 hingga Rp.800.000.000, Ketentuan ini mencakup tiga ayat yang masing-masing mengatur unsur-unsur berbeda, dimulai dari akses tanpa izin pemilik pada ayat (1), akses dengan tujuan memperoleh informasi elektronik yang bersifat rahasia, (2), hingga akses dengan cara melanggar, menerobos, atau menjebol sistem pengamanan, (3), mensyaratkan adanya unsur kesengajaan, perbuatan melawan hukum, dan objek berupa computer dan/atau sistem elektronik milik orang lain.

Apabila dikaitkan dengan kasus pencurian data melaui *whatsapp* menggunakan metode pengiriman file *malwer*, seluruh unsur dalam pasal 30 telah terpebuhi. Pelaku terbukti memenuhi unsur subjek hukum sebagai setiap orang yang dapat dimintai pertanggungjawaban pidana, unsur kesengajaan yang tercermin dari serangkain tindkan sistematis mulai dari pembuatan hingga pengiriman file *malwer*, unsur tanpa hak karena tidak adanya izin korban untuk mengakses perangkatnya, serta unsur mengakses sistem elektronik yang dilakukan secara diam-diam melalui *malwer* yang terinstal di perangkat korban tanpa sepengetahuan korban.

Pasal 32 jo pasal 48 ayat (1) mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, merusak, menghilangkan, mentransmisikan, atau memindahkan informasi dan/atau dokumen elektronik milik orang lain dapat diancam pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp.2.000.000.000. dalam konteks pencurian data melalui *whatsapp* menggunakan file *malwer*, seluruh pasal tersebut telah terpenuhi, yakni unsur kesengajaan yang terbukti dari persiapan fie berformat APK sebagai sarana penyadapan, unsur melawan hukum karena pelaku tidak memiliki izin untuk mengakses data korban, usnur dengan cara apapun yang mencakup penggunaan *malwer* sebagai metode akses illegal, serta unsur memindahkan data yang terjadi Ketika *malwer* mengirimkan Salinan data pribadi korban melalui jaringan internet ke perangkat pelaku.

Pada pasal 32 ayat (2) secara khusus melarang tindakan memindahkan atau mentransfer informasi elektronik kepada sistem elektronik orang lain yang tidak berhak, dengan cara apapun. Dalam kasus pencurian data melalui *whatsapp*, unsur ini terpenuhi secara nyata karena *malwer* yang tersisip dalam file mengumpulkan data pribadi korban seperti nomor rekening, PIN, dan dokumen peribadi lainnya, kemudian mentransfernya ke server atau perangkat pelaku yang jelas tidak memiliki hak hukum atas data tersebut. Berdasarkan hal ini, secara yuriidis normatif perbuatan pencurian data melalui *whatsapp* telah memenuhi seluruh unsur tindak pidana sebagaimana telah diatur, sehingga pelaku wajib diproses dan diadili oleh aparat penegak hukum.

2. Undang-Undang Perlindungan Data Pribadi

Pasal 65 dan 67, secara tegas melarang setiap orang untuk secara melawan hukum memperoleh, mengumpulkan, mengungkapkan, maupun menggunakan data pribadi milik orang lain, dengan ancaman pidana penjara hingga 5 tahun dan denda hingga Rp.5.000.000.000. dalam hal ini pencurian data melalui *whatsapp* menggunakan file *malwer*, seluruh unsur pasal tersebut telah terpenuhi karena pelaku terbukti memperoleh dan mengumpulkan data peribadi korban seperti nomor rekening, PIN, dan *password* tanpa persetujuan, kemudian menggunakannya untuk keuntungan pribadi yang mengakibatkan kerugian besar bagi korban. [2]

3. Perbandingan Undang-Undang Informasi dan Transaksi Elektronik dengan Undang-Undang Perlindungan Data Pribadi

Dalam menganalisis aspek hukum pidana terhadap kejahatan pencurian data pribadi melalui *WhatsApp,* terdapat perbedaan mendasar antara Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-Undang Informasi dan Transaksi Elektronik melalui Pasal 30 jo 46 dan Pasal 32 jo 48 memfokuskan pengaturannya pada aspek teknis perbuatan kejahatan siber, yakni akses ilegal terhadap sistem elektronik dengan ancaman pidana penjara hingga 9 tahun, sementara Undang-Undang Perlindungan Data Pribadi melalui Pasal 65 dan 67 lebih menitikberatkan pada perlindungan hak privasi dan data pribadi sebagai hak asasi manusia dengan ancaman denda hingga Rp5.000.000.000.[3]

Mengingat kedua regulasi melindungi objek hukum yang berbeda namun sama-sama dilanggar dalam satu rangkaian kejahatan, pendekatan yang paling tepat adalah penerapan secara kumulatif berdasarkan asas *concursus realis*, sehingga kombinasi pidana penjara yang berat dari Undang-Undang Informasi dan Transaksi Elektronik dengan pidana denda yang besar dari Undang-Undang Perlindungan Data Pribadi dapat menciptakan efek jera yang lebih komprehensif dan optimal.

Namun demikian, efektivitas penerapan kumulatif kedua regulasi tersebut sangat bergantung pada kapasitas aparat penegak hukum di lapangan. Fakta bahwa dari 114 kasus pencurian data pribadi melalui *WhatsApp* yang dilaporkan di Polres Kota Samarinda selama periode 2021 hingga 2025 tidak ada satu pun yang berhasil mencapai tahap persidangan membuktikan bahwa permasalahan utama bukan terletak pada substansi hukum, melainkan pada aspek struktural penegakan hukum, yang meliputi keterbatasan kapasitas teknis penyidik dalam digital forensik, minimnya peralatan investigasi kejahatan siber, serta lemahnya koordinasi antar instansi.

Oleh karena itu, diperlukan reformasi menyeluruh yang mencakup pelatihan khusus digital forensik, pengadaan teknologi investigasi yang canggih, pembentukan unit khusus *cybercrime* di setiap kepolisian daerah, serta penyusunan standar operasional prosedur yang jelas agar sanksi dalam kedua regulasi dapat benar-benar ditegakkan dan memberikan perlindungan hukum yang nyata bagi masyarakat.

Penegakan Hukum yang Dilakukan Kepolisian Terhadap Pelaku Pencurian Data Pribadi Melalui Whatsapp

Penegakan hukum pada dasarnya merupakan serangkaian kegiatan untuk mewujudkan keteraturan sosial melalui penerapan norma-norma hukum, dan dari segi regulasi Indonesia telah memiliki payung hukum yang cukup komprehensif untuk menangani kasus pencurian

[2] Mulyadi, Aulia, Axara dkk, Analsiis Penipuan Online Melalui Media Sosial Dalam Perspekstif Krimonologi, Media Hukum Indonesia, Vol. 2, No. 2, April-Juni 2024, hlm. 74-82.

[3] Risti Dwi Ramasari, Angga Alfiyan, Yuli Sintiya Pratiwi, Perlindungan Hukum Terhadap Data Pengguna Whatsapp Berdasarkan Undang-Undang No 19 Tahun 2016, Jurnal Of Law, Vol. 7, No. 1, April 2024, hlm. 29-39.

data pribadi. Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik secara tegas mengatur larangan akses ilegal terhadap sistem elektronik melalui Pasal 30 dengan ancaman pidana mulai dari 6 tahun penjara dan denda Rp600.000.000 untuk akses ilegal biasa, hingga 8 tahun penjara dan denda Rp800.000.000 jika dilakukan dengan melanggar sistem pengamanan.

Pasal 32 mengatur sanksi atas tindakan memindahkan atau mentransfer informasi elektronik milik orang lain dengan ancaman hingga 9 tahun penjara dan denda Rp3.000.000.000, bahkan Pasal 35 memberikan sanksi terberat yakni 12 tahun penjara dan denda hingga Rp12.000.000.000 untuk kasus manipulasi data yang merugikan orang lain. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui Pasal 65 dan 67 turut memperkuat perlindungan hukum dengan mengancam pidana penjara hingga 5 tahun dan denda hingga Rp5.000.000.000 bagi setiap orang yang secara tidak sah memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi milik orang lain.

Proses penegakan hukum pidana di Indonesia, termasuk kasus kejahatan siber, umumnya mengikuti tahapan sebagai berikut:

1. Tahap Pelaporan (Kepolisian)
    a) Pembuatan Laporan Polisi (LP)
    b) Penyelidikan
    c) Penyidikan
2. Tahap Penuntutan (Kejaksaan)
3. Tahap Persidangan (Peradilan)

Data kasus pencurian data pribadi di wilayah hukum Polres Kota Samarinda mengungkapkan permasalahan yang sangat serius dalam penegakan hukum kejahatan siber di Indonesia. Dari total 114 kasus yang dilaporkan selama periode 2021 hingga Oktober 2025, tidak satu pun yang berhasil ditingkatkan dari tahap penyelidikan ke tahap penyidikan, apalagi penuntutan dan persidangan. Kondisi ini mencerminkan adanya kesenjangan yang sangat lebar antara ketersediaan regulasi yang secara normatif telah memadai, sebagaimana termuat dalam Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dengan implementasinya di lapangan yang sama sekali tidak berjalan efektif.

Sebagaimana ditegaskan oleh para pakar hukum siber seperti Prof. Edmon Makarim dan Dr. Sinta Dewi Rosadi, hambatan utama terletak pada keterbatasan kemampuan teknis penyidik dalam digital forensik, minimnya peralatan investigasi yang memadai, serta lemahnya koordinasi antara aparat penegak hukum dengan platform digital, operator telekomunikasi, dan lembaga keuangan terkait.[4]

Kelemahan struktural dalam penegakan hukum ini bersifat saling berkaitan dan menciptakan siklus negatif yang terus berkelanjutan. Dari aspek teknis, aparat penegak hukum menghadapi kesulitan serius dalam mengidentifikasi pelaku yang memanfaatkan teknologi enkripsi tingkat tinggi, akun anonim sekali pakai, dan operasi lintas wilayah bahkan lintas negara. Dari aspek kelembagaan, unit khusus penanganan kejahatan siber di tingkat Polres masih sangat terbatas baik dari segi personel maupun fasilitas pendukung, sementara prosedur penanganan yang terlalu birokratis memperlambat proses investigasi secara signifikan.

Kondisi ini diperparah oleh fenomena angka gelap kejahatan atau dark number yang tinggi, di mana jumlah kejahatan yang sebenarnya terjadi diperkirakan jauh lebih besar dari yang dilaporkan, mengingat banyak korban yang memilih tidak melapor karena hilangnya

[4] Judijanto, L., Nugroho, B, Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum dan HAM*, Vol 3, No.03, 2025, hlm. 118-124.

kepercayaan terhadap efektivitas sistem penegakan hukum. Ketiadaan efek jera yang nyata pada akhirnya mendorong pelaku untuk semakin berani beroperasi dan menginspirasi munculnya pelaku-pelaku baru yang menganggap kejahatan siber sebagai aktivitas yang relatif aman dari jerat hukum.

Menyikapi kompleksitas permasalahan tersebut, diperlukan reformasi yang bersifat menyeluruh dan terkoordinasi dari berbagai pihak. Pertama, peningkatan kapasitas sumber daya manusia melalui pelatihan khusus dan sertifikasi digital forensik bagi para penyidik, baik melalui lembaga dalam negeri maupun kerja sama internasional. Kedua, pengadaan laboratorium forensik digital yang memadai minimal di tingkat Polda guna mendukung analisis bukti digital yang cepat dan akurat. Ketiga, penguatan koordinasi kelembagaan antara Polri, Kementerian Komunikasi dan Informatika, Otoritas Jasa Keuangan, serta platform digital melalui mekanisme pelaporan yang lebih terintegrasi.

Keempat, pembentukan unit khusus penanganan kejahatan siber di Polres Kota Samarinda yang dilengkapi dengan *Standard Operating Procedure* yang jelas. Kelima, sosialisasi literasi digital secara masif dan sistematis kepada masyarakat sebagai upaya *preventif*. Tanpa langkah-langkah konkret tersebut, angka 114 kasus yang hingga kini tidak terselesaikan akan terus bertambah, yang pada akhirnya semakin mengikis kepercayaan publik terhadap sistem penegakan hukum Indonesia dalam menghadapi kejahatan teknologi informasi yang dampaknya terus meluas di era digital ini.

Hambatan Yang Terjadi Dalam Penegakan Hukum

Penegakan hukum terhadap pelaku pencurian data pribadi melalui *WhatsApp* di Samarinda menghadapi hambatan kompleks yang meliputi aspek teknis, hukum, kelembagaan, sumber daya manusia, serta faktor sosial budaya. Berdasarkan penelitian di Kepolisian Resor Kota Samarinda, hambatan-hambatan tersebut menyebabkan 114 kasus pencurian data pribadi melalui *WhatsApp* periode 2021–2025 tidak ada yang mencapai tahap persidangan.

1. Aspek Teknis Kejahatan siber memiliki karakteristik yang menyulitkan proses penegakan hukum, di antaranya penggunaan identitas anonim oleh pelaku yang menghambat upaya pelacakan, serta kerentanan barang bukti digital terhadap manipulasi dan penghapusan. Keterlambatan pelaporan oleh korban turut memperlemah proses pembuktian. Di samping itu, modus operandi kejahatan siber yang terus berkembang secara dinamis seringkali melampaui kapasitas adaptasi teknologi aparat penegak hukum.
2. Aspek Hukum Pembuktian kejahatan siber jauh lebih kompleks dibandingkan kejahatan konvensional, mengingat sifat barang bukti elektronik yang rentan terhadap manipulasi dan penghapusan. Proses autentikasi alat bukti digital memerlukan kompetensi khusus dalam bidang forensik digital, meliputi ekstraksi data, verifikasi integritas, serta penyusunan berita acara sesuai standar yang berlaku. Selain itu, yurisdiksi lintas negara menambah kompleksitas penegakan hukum karena membutuhkan mekanisme kerja sama internasional yang rumit dan memerlukan waktu yang tidak singkat.
3. Aspek Kelembagaan Struktur kelembagaan kepolisian pada tingkat Polres belum sepenuhnya mendukung penanganan kejahatan siber secara optimal, yang tercermin dari belum adanya unit khusus *cybercrime* yang terpisah dari satuan reserse kriminal umum. Keterbatasan jumlah penyidik yang memiliki kompetensi forensik digital, ditambah dengan belum meratanya fasilitas laboratorium forensik di tingkat Polres, menyebabkan proses analisis barang bukti bergantung pada institusi di tingkat yang lebih tinggi sehingga berimplikasi pada lamanya waktu penyelidikan. Koordinasi dengan pihak ketiga seperti penyedia platform digital, perusahaan telekomunikasi, dan lembaga perbankan juga kerap terhambat oleh regulasi perlindungan data dan prosedur birokrasi yang berlaku.

Ketiga hambatan tersebut saling berkaitan dan membentuk siklus yang mempersulit penegakan hukum kejahatan pencurian data melalui *WhatsApp*, mulai dari lemahnya

identifikasi pelaku akibat keterbatasan sumber daya manusia dan peralatan, hingga koordinasi yang tidak efektif dan rendahnya literasi digital masyarakat yang terus memperbesar jumlah korban. Tanpa upaya serius dan komprehensif yang meliputi peningkatan kompetensi penyidik, pengadaan peralatan forensik digital yang memadai, perbaikan mekanisme koordinasi antarlembaga, serta edukasi digital kepada masyarakat, dikhawatirkan tingkat penyelesaian kasus akan tetap stagnan di angka nol persen dan pada akhirnya semakin mengikis kepercayaan publik terhadap efektivitas sistem penegakan hukum di Indonesia dalam era digital.

KESIMPULAN

Kejahatan pencurian data pribadi melalui WhatsApp di Samarinda periode 2021–Oktober 2025 mencapai 114 kasus dengan modus pengiriman file APK bermalware melalui iklan dan penawaran kerja palsu. Meskipun perbuatan tersebut telah diatur secara jelas dalam UU ITE dan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, seluruh kasus masih terhenti pada tahap penyelidikan bukan karena ketiadaan dasar hukum, melainkan akibat keterbatasan kapasitas teknis aparat penegak hukum di tingkat kota. Dengan demikian, permasalahan utama bukan terletak pada substansi hukum yang sudah memadai, melainkan pada aspek struktural yaitu lemahnya kapasitas penyidik dalam menghadapi kejahatan siber.

Penegakan hukum terhadap kejahatan pencurian data pribadi melalui WhatsApp di Samarinda mengalami kegagalan sistemik, dimana 114 kasus periode 2021–2025 tidak satupun mencapai tahap persidangan meskipun regulasi UU ITE dan UU Perlindungan Data Pribadi telah memadai. Kegagalan ini disebabkan oleh hambatan multidimensional meliputi keterbatasan kapasitas penyidik, kompleksitas pembuktian digital, serta lemahnya koordinasi antarlembaga, sehingga diperlukan reformasi menyeluruh mencakup peningkatan kompetensi sumber daya manusia, pengadaan teknologi forensik digital, dan penguatan edukasi masyarakat.

Saran

Untuk meningkatkan penegakan hukum diarapkan Kepolisian Resor Kota Samarinda diharapkan meningkatkan profesionalisme penanganan laporan dengan menyediakan peralatan forensik digital yang memadai, menetapkan batas waktu yang jelas dalam setiap tahapan penyelidikan, serta menjalin koordinasi aktif dengan platform digital, institusi perbankan, dan Kementerian Komunikasi dan Informatika, disertai pelatihan berkelanjutan di bidang investigasi cybercrime agar kapasitas aparat senantiasa mengikuti perkembangan teknologi. Di sisi lain, masyarakat diharapkan meningkatkan literasi digital dengan tidak sembarangan mengakses tautan atau file mencurigakan, tidak membagikan informasi sensitif seperti kode OTP dan data perbankan, serta mengaktifkan fitur verifikasi dua langkah pada WhatsApp, dan apabila menjadi korban agar segera melapor kepada pihak kepolisian dengan mengamankan bukti digital terlebih dahulu sebagai langkah pencegahan bersama.

DAFTAR PUSTAKA

Adami Chazawi dab Ardi Ferdian, 2015, Tindak Pidana Informasi & Transaksi Elektronik, Cetakan Pertama, Malang: Media Nusa Creative.

Fiqqih Anugerah, Tantimin, Pencurian Data Pribadi di Internet Dalam Perspektif Krimonologi, Jurnal Komunikasi Hukum, Vol 8, No 1, Febuari 2022.

Hakim A.A, Setiawan D.A, Perlindungan Korban Kejahatan Penipuan Online Bermodus APK (Android Package Kit) melalui Whatsapp, Jurnal Riset Ilmu Hukum, Vol. 4, No. 1, Juli 2024.

Judijanto, L., Nugroho, B, Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. Sanskara Hukum dan HAM, Vol 3, No.03, 2025.

Kornelius Benuf, Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi, Majalah Hukum Nnasional, Vol. 51, No. 2, 2021.
Makarim, Edmon. (2010). Tanggung Jawab Hukum Penyelenggara Sistem Elektronik. Jakarta: PT RajaGrafindo Persada.
Mulyadi, Aulia, Axara dkk, Analsiis Penipuan Online Melalui Media Sosial Dalam Perspekstif Krimonologi, Media Hukum Indonesia, Vol. 2, No. 2, April-Juni 2024.
Risti Dwi Ramasari, Angga Alfiyan, Yuli Sintiya Pratiwi, Perlindungan Hukum Terhadap Data Pengguna Whatsapp Berdasarkan Undang-Undang No 19 Tahun 2016, Jurnal Of Law, Vol. 7, No. 1, April 2024.
Rona Suroya Zain, Tinjauan Yuridis Penegakan Hukum Kejahatan Pencurian Data Melalui File Yang Memuat Hasil Retasan, Vol 01, No. 01, 2023.
Sinta Dewi Rosadi, 2022, Cyber Law, Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Cetakan kedua, Bandung: PT. Refika Aditama
Widodo, 2013, Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law): Telaah Teoritik dan Bedah Kasus, Cetakan pertama, Yogyakarta: Aswaja Pressinndo.