



Analisis Hukum Terhadap Penipuan Penyalahgunaan Data Pribadi Melalui Media Sosial Whatsapp

Sitti Nur Halija¹, Wahyu Rasyid², Muthmainnah MS³, Hartono Hamzah⁴

¹⁻⁴Program Studi Ilmu Hukum, Universitas Muhammadiyah Parepare

¹sittinurhalija1304@gmail.com, ²wahyurasyid03@gmail.com, ³msmutmainnah@gmail.com, ⁴hartonohamzah30@gmail.com

Abstrak

Keanekaragaman Perkembangan teknologi informasi dan komunikasi meningkatkan penggunaan media sosial, melainkan menimbulkan risiko penyalahgunaan data pribadi, termasuk melalui WhatsApp. Penelitian ini tujuannya menganalisis penipuan melalui penyalahgunaan data pribadi pada WhatsApp dalam sistem hukum Indonesia serta pertanggungjawaban pidana pelakunya menurut peraturan perundang-undangan. Penelitian ini memakai metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum primer, sekunder, dan tersier dianalisis secara kualitatif. Hasil penelitian menjelaskan bahwa penyalahgunaan data pribadi melalui WhatsApp umumnya dilakukan melalui *phishing*, pencurian identitas, pengambilalihan akun, dan pemanfaatan informasi pribadi secara melanggar hukum. Perlindungan hukum sudah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, serta Kitab Undang-Undang Hukum Pidana. Berdasarkan teori pertanggungjawaban pidana Roeslan Saleh, pelaku bisa dimintai pertanggungjawaban apabila memenuhi unsur tindak pidana, mempunyai kebiasaan bertanggung jawab, terdapat kesalahan, serta tidak terdapat alasan pembenar ataupun pemaaf. Namun, penerapannya masih menghadapi kendala berupa rendahnya literasi digital, perkembangan modus kejahatan siber, dan belum optimalnya penegakan hukum. Oleh sebab itu, diperlukan peningkatan literasi digital dan efektivitas penegakan hukum guna memperkuat perlindungan data pribadi.

Kata kunci: Penipuan, Data Pribadi, WhatsApp, Pertanggungjawaban Pidana

Abstract

Advancements in information and communication technology have increased social media usage but also created risks regarding the misuse of personal data, including via WhatsApp. This study aims to analyze fraud involving the misuse of personal data on WhatsApp within the Indonesian legal system and the criminal liability of perpetrators under prevailing legislation. The research employs a normative legal method utilizing statutory and conceptual approaches, with qualitative analysis of primary, secondary, and tertiary legal materials. The findings indicate that the misuse of personal data via WhatsApp typically occurs through phishing, identity theft, account takeovers, and the unlawful use of personal information. Legal protections are established under Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning Electronic Information and Transactions, and the Criminal Code. Based on Roeslan Saleh's theory of criminal liability, a perpetrator can be held liable if the elements of the criminal offense are met, the individual possesses the capacity for liability, fault is established, and there are no grounds for justification or excuse. However, implementation faces challenges such as low digital literacy, evolving cybercrime methods, and suboptimal law enforcement. Therefore, enhancing digital literacy and the effectiveness of law enforcement is essential to strengthen personal data protection.

Keyword : Fraud, Personal Data, WhatsApp, Criminal Liability.



PENDAHULUAN

Indonesia termasuk salah satu negara yang mempunyai jumlah pengguna media sosial terbesar di dunia. Tingginya tingkat penggunaan media sosial menunjukkan semakin besarnya ketergantungan masyarakat terhadap platform digital dalam berbagai kegiatan, mulai dari komunikasi, pertukaran informasi, hingga pelaksanaan transaksi secara daring. Salah satu platform yang banyak digunakan oleh masyarakat yaitu WhatsApp, yang dalam proses pendaftaran dan verifikasi akun mengharuskan pengguna memberikan data pribadi, salah satunya berupa nomor telepon. Kondisi di atas menyebabkan data pribadi mempunyai nilai penting sehingga diperlukan perlindungan untuk mencegah terjadinya berbagai bentuk penyalahgunaan. Oleh sebab itu, pemahaman mengenai kebijakan privasi serta keamanan data yang diterapkan oleh setiap platform media sosial menjadi hal yang penting guna mengurangi risiko kebocoran dan penyalahgunaan data pribadi (Hanafi, 2023).

Kemajuan yang sangat pesat pada bidang teknologi dan informasi sudah membawa dampak signifikan terhadap akselerasi secara umum, di mana hal di atas bisa dibuktikan dengan terdeteksi dan dikelolanya seluruh tindakan kita melalui teknologi. Kemajuan teknologi di atas memberikan pengaruh yang signifikan terhadap kehidupan masyarakat seiring dengan meningkatnya penggunaan teknologi digital dalam berbagai aktivitas sehari-hari (Alfiana & Aisyah, 2025). Kemajuan teknologi yang terjadi dalam beberapa waktu terakhir dan dirasakan oleh sebagian besar masyarakat Indonesia semakin meningkatkan kesadaran akan pentingnya menjaga kerahasiaan data pribadi dari berbagai potensi pelanggaran ataupun penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab (Manurung & Thalib, 2022).

Media sosial merupakan media digital yang dipergunakan untuk saling berkomunikasi serta berinteraksi satu sama lain bagi penggunaannya dan menjadi media untuk membagikan konten – konten berupa video, foto, serta tulisan yang menjadikan media sosial sekarang platform digital yang memfasilitasi penggunaannya untuk melakukan aktivitas sosial di dunia digital. Media sosial juga menjadi sarana untuk bisa bersosialisasi satu sama lain yang dilakukan secara daring atau online yang memungkinkan bagi penggunaannya untuk saling berinteraksi tanpa dibatasi ruang dan waktu. Masyarakat modern seperti saat ini sudah menjadikan media sosial sebagai kebutuhan mendasar dalam bersosialisasi satu sama lain, bisa dilihat mayoritas masyarakat saat ini pada umumnya mempunyai akun media sosial mereka masing – masing dan jarang dijumpai masyarakat saat ini yang tidak mempunyai akun media sosial (Mussa & M.Si, 2024).

Kebocoran data pribadi menimbulkan dampak yang sangat serius terhadap aspek psikologis individu sebagai subjek data. Hilangnya kendali atas data pribadi menyebabkan individu kehilangan rasa aman dalam menjalani kehidupan sosial dan aktivitas digitalnya. Kondisi di atas berpotensi menimbulkan berbagai gangguan psikologis, seperti meningkatnya kecemasan, rasa takut akan penyalahgunaan data, serta perasaan tidak nyaman yang berlangsung dalam jangka waktu tertentu. Dampak psikologis di atas pada akhirnya berimplikasi pada menurunnya kualitas hidup individu, baik dalam aspek sosial ataupun emosional. Selain itu, kebocoran data juga bisa berdampak terhadap kerugian finansial dan menurunkan kepercayaan publik terhadap pihak yang terkait (Yuwana et al., 2025).

Dalam konteks data pribadi, di negara-negara maju, terminologi “privasi” sering digunakan sebagai hak yang wajib ditegakkan, yaitu hak individu guna menjaga hidupnya sendiri tanpa gangguan (Angnesia & Wiraguna, 2025). Di era saat ini, tingkat akses internet dan penggunaan perangkat bergerak semakin tinggi. Aplikasi berbasis internet atau disebut juga *over the top* sudah menjadi elemen integral dari kehidupan harian masyarakat, termasuk di Indonesia (Sadillah Ahmad et al., 2025).

Penyalahgunaan data pribadi melalui media WhatsApp bisa terjadi dalam berbagai bentuk, seperti pengambilalihan akun (*hacking*), penipuan dengan modus mengatasnamakan korban, penyebaran tautan palsu (*phishing*), hingga pencurian identitas pribadi untuk melakukan tindak kejahatan tertentu. Modus kejahatan ini umumnya memanfaatkan kelalaian pengguna dan lemahnya perlindungan data pribadi, sehingga pelaku bisa dengan mudah mengakses informasi penting milik korban seperti nomor telepon, foto, data kontak, hingga percakapan pribadi. Akibatnya, banyak masyarakat yang kehilangan harta benda, serta mengalami kerugian non-materi berupa gangguan privasi dan reputasi. Fenomena ini menjelaskan bahwa kejahatan siber melalui aplikasi WhatsApp bukan lagi hal yang sederhana, melainkan sudah menjadi berbahaya (Fritiana & Wiraguna, 2025) (Fritiana & Wiraguna, 2025).

Kewajiban pemerintah negara Indonesia dalam memberikan perlindungan data pribadi didasarkan pada ketentuan pada pasal 28G Ayat (1) Undang- Undang Negara Republik Indonesia Tahun 1945 menyebutkan bahwa: “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”. Meskipun ketentuan di atas tidak secara eksplisit mengatur mengenai privasi dan perlindungan data pribadi, secara implisit ketentuan di atas mencerminkan adanya perlindungan terhadap hak individu dalam masyarakat yang berkaitan dengan proses pengumpulan, pengolahan, pengelolaan, serta penyebaran data pribadi (Paminto et al., 2024).

Dengan maraknya para pengguna media sosial Indonesia tidak bisa dipungkiri bahwa banyaknya kasus penyalahgunaan data pribadi diakibatkan kebocoran data pribadi para pengguna. Menurut data Otoritas Jasa Keuangan (OJK) melalui Indonesia Anti – Scam Center (IASC) melaporkan bahwa dari 299.237 laporan penipuan digital sejak akhir 2024 hingga 2025, sekitar 14.229 kasus merupakan penipuan yang terjadi melalui media sosial diakibatkan terjadinya kebocoran data pribadi. Kondisi di atas menjelaskan bahwa kejahatan berbasis teknologi informasi masih



marak terjadi, padahal pemerintah Indonesia sudah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai regulasi utama yang diharapkan bisa memberikan perlindungan hukum yang kuat terhadap hak-hak privasi warga negara (Rinjani & Firmansyah, 2025).

Menurut uraian di atas, penelitian ini tujuannya untuk menganalisis hukum terhadap penipuan data pribadi melalui media sosial WhatsApp dalam konteks sistem hukum Indonesia serta menganalisis pertanggungjawaban hukum dan sanksi yang bisa dikenakan terhadap pelaku menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penelitian ini diharapkan bisa memberikan kontribusi dalam pengembangan kajian hukum mengenai perlindungan data pribadi serta menjadi bahan pertimbangan dalam memperkuat penegakan hukum terhadap penyalahgunaan data pribadi melalui media sosial, khususnya WhatsApp.

METODOLOGI PENELITIAN

Penelitian ini memakai metode yuridis normatif, yaitu penelitian hukum yang berfokus pada pengkajian norma dan ketentuan hukum melalui peraturan perundang-undangan serta bahan hukum yang relevan.¹ Metode ini digunakan untuk menganalisis hukum terhadap penipuan melalui penyalahgunaan data pribadi melalui media sosial WhatsApp, khususnya mengenai pengaturan, pertanggungjawaban hukum, dan sanksi terhadap pelaku (Sukmawan & Damayanti, 2025).

Pendekatan yang digunakan yaitu pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan dilakukan dengan menelaah ketentuan hukum yang berkaitan dengan perlindungan data pribadi dan penipuan, sedangkan pendekatan konseptual digunakan untuk memahami konsep perlindungan data pribadi dan pertanggungjawaban hukum. Bahan hukum yang digunakan terdiri atas bahan hukum primer berupa peraturan perundang-undangan dan bahan hukum sekunder berupa buku, jurnal, serta pendapat ahli. Seluruh bahan hukum diperoleh melalui studi kepustakaan dan dianalisis secara kualitatif untuk menjawab permasalahan penelitian (Wiraguna, 2024).

HASIL DAN PEMBAHASAN

Pertanggungjawaban Pidana Pelaku Penyalahgunaan Data Pribadi Melalui WhatsApp

Perkembangan teknologi informasi dan komunikasi sudah memberikan kemudahan bagi masyarakat dalam melakukan komunikasi dan pertukaran informasi. Salah satu media komunikasi yang banyak digunakan yaitu WhatsApp. Kemudahan di atas, di sisi lain, juga menimbulkan risiko terhadap keamanan dan perlindungan data pribadi. Salah satu bentuk penyalahgunaan yang berkembang yaitu *phishing*, yaitu tindakan memperoleh data pribadi dengan memakai teknik pengelabuan melalui tautan, file, ataupun rekayasa sosial (*social engineering*). Data yang diperoleh bisa digunakan untuk melakukan penipuan, pencurian identitas, pengambilalihan akun, hingga kejahatan finansial (Prasetyaningtyas & Zainsyah, 2025; Sutarli & Kurniawan, 2023).

Penyalahgunaan data pribadi melalui WhatsApp pada umumnya dilakukan dengan menyamarkan identitas pelaku sebagai pihak yang bisa dipercaya. Pelaku mengirimkan pesan yang berisi tautan atau file tertentu, seperti undangan digital, informasi hadiah, pemberitahuan tilang elektronik, ataupun informasi lain yang bisa menarik perhatian korban. Ketika korban membuka tautan atau file di atas, korban bisa diarahkan untuk memberikan informasi berupa NIK, nomor telepon, identitas, informasi rekening, ataupun data lainnya (Trianurahmah et al., 2025). Modus di atas menjelaskan bahwa *phishing* tidak semata-mata mengandalkan kebiasaan teknologi, melainkan memanfaatkan kelemahan dan kepercayaan korban melalui rekayasa sosial (Hasanudin & Babussalam, 2024).

Data pribadi yang berhasil diperoleh selanjutnya bisa digunakan untuk berbagai kepentingan melawan hukum. Pelaku bisa memakai data di atas untuk mengambil alih akun WhatsApp, memperoleh kode OTP, mengakses layanan keuangan, melakukan penipuan dengan mengatasnamakan korban, ataupun melakukan pencurian identitas. Dengan demikian, *phishing* bisa dipahami sebagai salah satu cara yang digunakan pelaku untuk memperoleh data pribadi, sedangkan penyalahgunaan data merupakan bentuk penggunaan data di atas untuk kepentingan yang tidak sah (Suciara et al., 2026). Perbuatan di atas pada akhirnya bukan cuman merugikan korban secara materiil, melainkan bisa mengganggu privasi, keamanan, dan rasa aman korban dalam memakai teknologi digital.

Secara normatif, perlindungan data pribadi di Indonesia memperoleh landasan utama melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pengaturan di atas diperkuat dengan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik serta ketentuan pidana lainnya yang relevan dengan bentuk perbuatan yang dilakukan pelaku (Maharani et al., 2024; Utomo, 2025). Perlindungan data pribadi juga merupakan bagian dari perlindungan terhadap hak atas privasi. Hak di atas berkaitan dengan kewenangan seseorang untuk mengendalikan informasi mengenai dirinya dan menentukan penggunaan informasi di atas oleh pihak lain (Argiansyah & Prawira, 2024; Fauzi & Shandy, 2022).

Dalam menentukan bisa atau tidaknya pelaku penyalahgunaan data pribadi dimintai pertanggungjawaban pidana, penelitian ini memakai teori pertanggungjawaban pidana Roeslan Saleh. Menurut Roeslan Saleh, pertanggungjawaban pidana merupakan diteruskannya celan yang secara objektif terdapat pada suatu perbuatan pidana kepada pelakunya sebab pelaku memenuhi syarat untuk dipidana (Idfira, 2026). Artinya, seseorang tidak bisa dipidana hanya sebab terdapat perbuatan yang dilarang, tetapi harus bisa dibuktikan bahwa perbuatan di atas dilakukan oleh orang

yang mempunyai kesalahan dan kebiasaan untuk mempertanggungjawabkan perbuatannya.

Menurut teori di atas, pertanggungjawaban pidana pada dasarnya berkaitan dengan beberapa unsur, yaitu adanya perbuatan pidana, adanya kesalahan, adanya kebiasaan bertanggung jawab, serta tidak terdapat alasan pemaaf ataupun alasan pembenar. Keempat unsur di atas bisa digunakan untuk menganalisis pertanggungjawaban pidana pelaku penyalahgunaan data pribadi melalui WhatsApp (Gaib, 2018). Dalam konteks phishing, unsur perbuatan pidana bisa dilihat dari tindakan pelaku memperoleh atau mengumpulkan data pribadi milik korban tanpa hak, kemudian memakai data di atas untuk memperoleh keuntungan atau melakukan perbuatan lain yang merugikan korban (Setyawan & Mahardhika, 2025).

Unsur kesalahan dalam penyalahgunaan data pribadi melalui WhatsApp pada umumnya berbentuk kesengajaan (dolus). Hal di atas bisa dilihat dari adanya persiapan dan rangkaian tindakan yang dilakukan pelaku sebelum menjalankan aksinya. Pelaku biasanya membuat identitas atau akun palsu, menyusun pesan yang menyerupai komunikasi resmi, menyediakan tautan tertentu, ataupun membuat file berbahaya yang disamarkan sebagai dokumen biasa. Rangkaian di atas menjelaskan bahwa pelaku mengetahui sifat perbuatannya dan menghendaki supaya korban menyerahkan atau membuka akses terhadap data pribadinya. Dengan demikian, tindakan di atas menunjukkan adanya kehendak dan kesadaran untuk melakukan perbuatan yang melawan hukum (Husna et al., 2025).

Selain kesalahan, kebiasaan bertanggung jawab juga merupakan unsur penting dalam pertanggungjawaban pidana. Pelaku yang melakukan phishing pada umumnya merupakan orang yang bisa memahami sifat perbuatannya serta bisa menentukan kehendaknya. Tidak terdapat keadaan yang menjelaskan bahwa pelaku kehilangan kebiasaan untuk memahami atau mengendalikan perbuatannya. Oleh sebab itu, selama tidak terdapat kondisi khusus yang menyebabkan pelaku tidak bisa bertanggung jawab, pelaku bisa dimintai pertanggungjawaban atas perbuatan yang dilakukan. Demikian pula, tindakan memperoleh data pribadi melalui phishing pada umumnya tidak bisa dibenarkan menurut alasan pemaaf ataupun alasan pembenar sebab dilakukan tanpa hak dan bertentangan dengan kepentingan hukum korban.

Pertanggungjawaban Pidana berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Pertanggungjawaban pidana terhadap pelaku penyalahgunaan data pribadi melalui WhatsApp bisa dianalisis menurut ketentuan pidana dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Ketentuan di atas mengatur berbagai perbuatan yang dilarang terkait data pribadi beserta sanksi pidana yang bisa dikenakan kepada pelaku. Dalam konteks phishing, ketentuan di atas relevan untuk menilai perbuatan pelaku yang memperoleh, mengumpulkan, mengungkapkan, atau memakai data pribadi secara melawan hukum.

Undang-Undang Nomor 27 Tahun 2022 memberikan pengaturan khusus mengenai larangan penggunaan data pribadi dan ketentuan pidanya. Pasal 65 melarang setiap orang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang bisa mengakibatkan kerugian terhadap subjek data pribadi. Pasal di atas juga melarang pengungkapan dan penggunaan data pribadi yang bukan miliknya secara melawan hukum.

Ketentuan di atas mempunyai hubungan langsung dengan penyalahgunaan data pribadi melalui WhatsApp. Pelaku phishing memperoleh data pribadi korban melalui cara yang tidak sah, kemudian data di atas bisa digunakan untuk kepentingan pelaku. Oleh sebab itu, perbuatan di atas bisa memenuhi karakteristik perbuatan yang dilarang dalam Pasal 65 UU PDP. Apabila dilakukan dengan sengaja dan memenuhi unsur yang ditentukan undang-undang, pelaku bisa dikenai ketentuan pidana sebagaimana diatur dalam Pasal 67 UU PDP.

Pasal 67 ayat (1) UU PDP mengatur bahwa orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang bisa mengakibatkan kerugian terhadap subjek data pribadi bisa dikenai pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar. Selanjutnya, Pasal 67 ayat (2) mengatur perbuatan mengungkapkan data pribadi secara melawan hukum dengan ancaman pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp4 miliar. Pasal 67 ayat (3) mengatur penggunaan data pribadi yang bukan miliknya secara melawan hukum dengan ancaman pidana penjara paling lama 5 tahun dan/atau denda paling banyak Rp5 miliar.

Ketentuan di atas memperlihatkan bahwa UU PDP membedakan bentuk perbuatan dalam penyalahgunaan data pribadi. Perolehan atau pengumpulan data, pengungkapan data, dan penggunaan data merupakan perbuatan yang masing-masing bisa menimbulkan pertanggungjawaban pidana. Dalam kasus phishing melalui WhatsApp, pelaku bisa melakukan lebih dari satu bentuk perbuatan. Misalnya, pelaku terlebih dahulu memperoleh data pribadi korban melalui tautan palsu, kemudian memakai data di atas untuk mengambil alih akun atau melakukan transaksi tertentu. Rangkaian perbuatan di atas bisa dianalisis menurut ketentuan pidana UU PDP sesuai dengan fakta dan pembuktian dalam perkara.

Selain itu, Pasal 68 UU PDP mengatur perbuatan membuat data pribadi palsu atau memalsukan data pribadi dengan maksud menguntungkan diri sendiri atau orang lain yang bisa mengakibatkan kerugian bagi orang lain. Perbuatan di atas bisa dikenai pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp6 miliar. Pasal 69 juga memungkinkan dijatuhkannya pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari tindak pidana serta pembayaran ganti kerugian.

Dengan adanya ketentuan di atas, UU PDP memberikan dasar hukum yang cukup jelas dalam meminta pertanggungjawaban pelaku penyalahgunaan data pribadi. Namun, penerapan ketentuan pidana tetap harus memperhatikan pembuktian setiap unsur tindak pidana. Artinya, tidak setiap kejadian kebocoran atau penyalahgunaan data secara otomatis menyebabkan seseorang bisa dipidana. Aparat penegak hukum harus membuktikan siapa pelakunya, bagaimana data diperoleh, apakah terdapat unsur kesengajaan, tujuan penggunaan data, serta kerugian yang ditimbulkan.

Pertanggungjawaban menurut Undang-Undang Informasi dan Transaksi Elektronik

Selain UU PDP, penyalahgunaan data pribadi melalui WhatsApp juga mempunyai keterkaitan dengan Undang-Undang Informasi dan Transaksi Elektronik. UU ITE memberikan dasar hukum terhadap perbuatan yang dilakukan melalui sistem elektronik, terutama apabila penyalahgunaan data disertai dengan akses tanpa hak atau tindakan terhadap informasi elektronik milik orang lain. Dengan demikian, penggunaan UU PDP dan UU ITE bisa saling melengkapi sesuai dengan karakteristik perbuatan pelaku.

Pasal 26 ayat (1) UU ITE pada prinsipnya memberikan perlindungan terhadap data pribadi dengan mensyaratkan persetujuan orang yang bersangkutan dalam penggunaan informasi melalui media elektronik yang menyangkut data pribadi. Ketentuan di atas memperlihatkan bahwa data pribadi tidak bisa digunakan secara bebas oleh pihak lain tanpa memperhatikan hak pemilik data. Dalam kasus phishing, pelaku memperoleh dan memakai data tanpa persetujuan korban sehingga tindakan di atas bertentangan dengan prinsip perlindungan terhadap data pribadi.

Selain itu, apabila pelaku memperoleh akses terhadap akun atau sistem elektronik korban secara tanpa hak, ketentuan mengenai akses tanpa hak dalam UU ITE juga bisa diterapkan. Hal ini menjadi relevan ketika data yang diperoleh melalui phishing digunakan untuk mengambil alih akun WhatsApp, email, rekening, dompet digital, atau sistem elektronik lainnya. Dengan demikian, pertanggungjawaban pelaku bukan cuman berkaitan dengan data pribadi yang diperoleh, melainkan dengan tindakan terhadap sistem elektronik korban.

Pasal 30 UU ITE mengatur larangan mengakses komputer dan/atau sistem elektronik milik orang lain secara sengaja dan tanpa hak atau melawan hukum. Apabila unsur di atas terpenuhi, ketentuan pidana dalam Pasal 46 bisa diterapkan. Demikian pula, apabila pelaku melakukan perubahan, pemindahan, penghilangan, atau tindakan lain terhadap informasi elektronik milik orang lain tanpa hak, ketentuan Pasal 32 dan Pasal 48 UU ITE bisa menjadi dasar pertanggungjawaban pidana sesuai dengan perbuatannya.

Dengan demikian, UU PDP dan UU ITE mempunyai ruang perlindungan yang saling berkaitan. UU PDP secara khusus memberikan perlindungan terhadap data pribadi, sedangkan UU ITE memberikan perlindungan terhadap informasi dan sistem elektronik. Penggunaan kedua instrumen hukum di atas memungkinkan aparat penegak hukum menyesuaikan dasar pertanggungjawaban pidana dengan rangkaian perbuatan yang dilakukan pelaku.

Upaya Penanggulangan Penyalahgunaan Data Pribadi

Penanggulangan penyalahgunaan data pribadi melalui WhatsApp bisa dilakukan melalui upaya preventif dan represif. Upaya preventif diarahkan untuk mencegah terjadinya tindak pidana, sedangkan upaya represif dilakukan sesudah tindak pidana terjadi melalui proses penegakan hukum dan pemberian sanksi. Kedua bentuk upaya di atas diperlukan sebab penyalahgunaan data pribadi bukan cuman berkaitan dengan perilaku pelaku, melainkan dengan keamanan sistem dan tingkat kesadaran masyarakat.

Upaya preventif menurut UU PDP bisa dilakukan melalui penerapan prinsip perlindungan data pribadi, pemberian persetujuan dalam pemrosesan data, serta pemenuhan hak subjek data. Subjek data mempunyai hak untuk memperoleh informasi, mengakses, memperbaiki, dan menghapus data dalam kondisi yang ditentukan undang-undang. Pengendali data juga mempunyai kewajiban untuk memastikan keamanan data dari akses, penggunaan, pengungkapan, perubahan, ataupun penyalahgunaan yang tidak sah (Agustina & Wiraguna, 2025).

Upaya preventif juga perlu diarahkan kepada masyarakat. Rendahnya literasi digital bisa menjadi salah satu faktor yang menyebabkan masyarakat mudah menjadi korban phishing. Masyarakat perlu diberikan pemahaman mengenai pentingnya memeriksa identitas pengirim, tidak membuka tautan yang mencurigakan, tidak memberikan kode OTP, serta tidak menyerahkan data pribadi kepada pihak yang belum terverifikasi. Edukasi dan sosialisasi secara berkelanjutan diperlukan untuk membentuk perilaku masyarakat yang lebih berhati-hati dalam memakai media digital (Athallah et al., 2026).

Sementara itu, upaya represif dilakukan melalui penerapan sanksi administratif dan pidana. UU PDP mengatur sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif. Sanksi pidana diberikan terhadap pihak yang melakukan perolehan, pengungkapan, penggunaan, atau pemalsuan data pribadi secara melawan hukum (Satria & Handoyo, 2022).

Penerapan sanksi pidana mempunyai fungsi untuk memberikan pembalasan atas perbuatan yang dilakukan sekaligus memberikan efek jera kepada pelaku. Namun, efektivitas sanksi sangat bergantung pada kebiasaan aparat penegak hukum dalam menemukan pelaku, mengamankan bukti elektronik, menelusuri jejak digital, dan membuktikan hubungan antara pelaku dengan perbuatan yang dilakukan. Karakter kejahatan siber yang bisa dilakukan dengan identitas



palsu dan memakai sarana teknologi tertentu menyebabkan proses pembuktian sering kali lebih kompleks dibandingkan tindak pidana konvensional.

Analisis Efektivitas Penegakan Hukum menurut Teori Soerjono Soekanto

Efektivitas penegakan hukum terhadap penyalahgunaan data pribadi melalui WhatsApp bisa dianalisis memakai teori Soerjono Soekanto yang mengemukakan lima faktor yang memengaruhi penegakan hukum, yaitu faktor hukum, penegak hukum, sarana atau fasilitas, masyarakat, dan kebudayaan (Fadhilatunnisa et al., 2026).

Pertama, faktor hukum. Indonesia sudah mempunyai UU PDP sebagai regulasi khusus mengenai perlindungan data pribadi serta UU ITE sebagai instrumen hukum yang berkaitan dengan penggunaan sistem elektronik. Dari sisi normatif, keberadaan kedua regulasi di atas memberikan dasar yang cukup untuk menindak penyalahgunaan data pribadi. Namun, efektivitas hukum bukan cuman ditentukan oleh keberadaan aturan, melainkan oleh penerapannya. Masih diperlukan kejelasan dan konsistensi dalam penerapan ketentuan hukum, mekanisme pengaduan, pembuktian, serta pemulihan hak korban.

Kedua, faktor penegak hukum. Penanganan penyalahgunaan data pribadi bisa melibatkan kepolisian, kejaksaan, pengadilan, kementerian terkait, serta penyelenggara sistem elektronik. Banyaknya pihak yang berkaitan dengan penanganan perkara menuntut koordinasi yang baik. Keterbatasan koordinasi ataupun belum optimalnya fungsi pengawasan bisa memengaruhi efektivitas perlindungan data pribadi.

Ketiga, faktor sarana atau fasilitas. Kejahatan digital membutuhkan sarana penegakan hukum yang sesuai dengan karakteristik tindak pidana. Aparat membutuhkan kebiasaan digital forensik, perangkat untuk menelusuri bukti elektronik, serta sumber daya manusia yang mempunyai kompetensi di bidang teknologi informasi. Tanpa dukungan sarana yang memadai, proses pelacakan pelaku dan pembuktian tindak pidana bisa mengalami hambatan.

Keempat, faktor masyarakat. Masyarakat mempunyai posisi penting dalam mencegah dan mengungkap penyalahgunaan data pribadi. Rendahnya kesadaran untuk memeriksa kebenaran informasi dan tingginya kepercayaan terhadap pesan yang diterima melalui WhatsApp bisa meningkatkan risiko menjadi korban phishing. Oleh sebab itu, masyarakat bukan cuman menjadi pihak yang harus dilindungi, melainkan mempunyai peran dalam mencegah tindak pidana melalui peningkatan kewaspadaan dan pelaporan ketika terjadi penyalahgunaan data.

Kelima, faktor kebudayaan. Faktor kebudayaan berkaitan dengan kebiasaan dan pola perilaku masyarakat dalam memakai teknologi. Kebiasaan membagikan informasi pribadi secara berlebihan, kurang melakukan verifikasi terhadap pesan, serta menganggap data pribadi sebagai informasi yang biasa dibagikan bisa meningkatkan kerentanan masyarakat terhadap penyalahgunaan data. Oleh sebab itu, diperlukan pembentukan budaya hukum yang menempatkan data pribadi sebagai sesuatu yang harus dijaga dan dilindungi.

Menurut kelima faktor di atas, bisa diketahui bahwa efektivitas penegakan hukum terhadap penyalahgunaan data pribadi melalui WhatsApp bukan cuman bergantung pada beratnya ancaman pidana. Keberadaan UU PDP dan UU ITE harus didukung oleh aparat penegak hukum yang kompeten, sarana digital forensik yang memadai, koordinasi antarlembaga, serta masyarakat yang mempunyai literasi digital yang baik. Dengan demikian, penegakan hukum harus dilaksanakan secara terpadu antara pendekatan hukum, teknologi, dan sosial.

Menurut hasil analisis, penyalahgunaan data pribadi melalui WhatsApp pada dasarnya merupakan perbuatan yang bisa menimbulkan pertanggungjawaban pidana apabila seluruh unsur tindak pidana dan pertanggungjawaban pidana bisa dibuktikan. Dalam perspektif teori Roeslan Saleh, pelaku yang secara sengaja memperoleh, mengumpulkan, mengungkapkan, atau memakai data pribadi milik orang lain secara melawan hukum bisa dimintai pertanggungjawaban apabila mempunyai kebiasaan bertanggung jawab dan tidak terdapat alasan pembenar ataupun alasan pemaaf.

Secara normatif, UU PDP sudah memberikan dasar yang lebih khusus dalam menangani penyalahgunaan data pribadi. Pasal 65 melarang perolehan, pengungkapan, dan penggunaan data pribadi secara melawan hukum, sedangkan Pasal 67 memberikan ancaman pidana terhadap perbuatan di atas. Ketentuan di atas menunjukkan adanya upaya negara untuk memberikan perlindungan terhadap individu sebagai pemilik data.

Namun, dalam praktiknya, keberadaan regulasi belum secara otomatis menjamin perlindungan yang efektif. Penyalahgunaan data melalui phishing berkembang mengikuti perkembangan teknologi dan memanfaatkan kelemahan manusia. Pelaku bisa menyembunyikan identitas, memakai akun palsu, dan melakukan tindakan dari lokasi yang berbeda dengan korban. Keadaan di atas menyebabkan proses identifikasi, pelacakan, dan pembuktian membutuhkan kebiasaan teknis dan koordinasi yang kuat.

Oleh sebab itu, perlindungan hukum terhadap penyalahgunaan data pribadi harus dilakukan melalui dua pendekatan. Pendekatan pertama yaitu preventif, berupa peningkatan literasi digital, edukasi keamanan data, penguatan sistem keamanan, dan peningkatan kesadaran masyarakat. Pendekatan kedua yaitu represif, berupa penyelidikan, penyidikan, pembuktian memakai alat bukti elektronik, serta penerapan sanksi pidana terhadap pelaku menurut ketentuan yang berlaku. Dengan demikian, bisa disimpulkan bahwa pertanggungjawaban pidana pelaku penyalahgunaan data pribadi melalui WhatsApp sudah mempunyai dasar hukum yang kuat melalui UU Nomor 27 Tahun 2022 dan UU ITE. Pelaku bisa dimintai pertanggungjawaban apabila terbukti melakukan perbuatan pidana secara sengaja, mempunyai kebiasaan bertanggung jawab, dan tidak terdapat alasan pembenar ataupun alasan pemaaf. Akan tetapi, efektivitas penegakan hukum masih dipengaruhi oleh lima faktor sebagaimana dikemukakan Soerjono Soekanto, yaitu faktor hukum,



penegak hukum, sarana atau fasilitas, masyarakat, dan kebudayaan. Oleh sebab itu, perlindungan data pribadi membutuhkan penguatan regulasi dan penegakan hukum yang disertai peningkatan kapasitas aparat, pengembangan sarana digital forensik, koordinasi antarlembaga, serta peningkatan literasi dan budaya hukum masyarakat.

KESIMPULAN

Menurut hasil penelitian, penipuan penyalahgunaan data pribadi melalui WhatsApp merupakan perbuatan melawan hukum yang bisa dilakukan melalui *phishing*, akun palsu, tautan, file, dan rekayasa sosial untuk memperoleh serta memakai data pribadi korban. Secara normatif, perbuatan di atas sudah mempunyai dasar hukum melalui UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan UU ITE. UU PDP secara khusus mengatur larangan memperoleh, mengungkapkan, dan memakai data pribadi secara melawan hukum serta memberikan ancaman pidana terhadap pelakunya. Namun, penerapan perlindungan hukum belum sepenuhnya optimal sebab masih menghadapi hambatan dalam pelacakan pelaku, pembuktian elektronik, koordinasi penegak hukum, serta rendahnya literasi digital masyarakat.

Pertanggungjawaban pidana pelaku bisa diterapkan apabila terbukti adanya perbuatan pidana, kesalahan, kebiasaan bertanggung jawab, serta tidak terdapat alasan pembenar ataupun pemaaf. Menurut UU PDP, pelaku bisa dikenai pidana sesuai dengan bentuk perbuatannya, sedangkan UU ITE bisa diterapkan apabila perbuatan di atas berkaitan dengan akses tanpa hak terhadap sistem elektronik. Efektivitas penegakan hukum dipengaruhi oleh faktor hukum, penegak hukum, sarana atau fasilitas, masyarakat, dan kebudayaan. Oleh sebab itu, penanggulangan penyalahgunaan data pribadi melalui WhatsApp perlu dilakukan melalui penguatan penegakan hukum dan digital forensik, koordinasi antarlembaga, serta peningkatan literasi dan kesadaran masyarakat dalam melindungi data pribadi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Muhammadiyah Parepare atas dukungan yang diberikan selama proses penulisan artikel ini. Penulis juga menyampaikan apresiasi kepada seluruh pihak yang sudah memberikan masukan konstruktif dalam penyusunan artikel ini.

DAFTAR PUSTAKA

- Agustina, W., & Wiraguna, S. A. (2025). *Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan*. 2(6), 117–127.
- Alfiana, R., & Aisyah, N. N. (2025). *Perlindungan Hukum Terhadap Data Pribadi Pasca Undang-Undang Data Pribadi Nomor 27 Tahun 2022 (Studi Kasus BPJS Kesehatan)*. 27. <https://doi.org/10.57250/ajsh.v5i2.1542>
- Angnesia, K. M., & Wiraguna, S. A. (2025). *Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital*. 2(April). <https://doi.org/10.62383/perspektif.v2i2.249>
- Argiansyah, H. Y., & Prawira, M. R. Y. (2024). *Analisis Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Menurut Perspektif Hak Asasi Manusia*. 1(1), 61–75.
- Athallah, M. A., Djanggi, H., & Mustamin, M. (2026). *Melawan Tindak Pidana Pencurian Identitas Di Era Digital*. 1(2).
- Fadhilatunnisa, R., Rama, A., Resalda, A. A., Thaiib, M. S. R., Saputri, R. Y., & Sari, D. P. (2026). *Relevansi faktor penegakan hukum menurut soerjono soekanto dalam menghadapi fenomena cyber crime*. 03(April), 42–49. <https://doi.org/10.70134/pakehum.v3i1.1432>
- Fauzi, E., & Shandy, N. A. R. (2022). *Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. 445–461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>
- Fritiana, A., & Wiraguna, S. A. (2025). *Tanggung Jawab Hukum terhadap Pemrosesan Data Pribadi oleh Aplikasi Pinjol Legal yang Melampaui Batas : Studi Kasus terhadap Adakami 2023*. 9, 17287–17296.
- Gaib, R. (2018). *Elemen-Elemen Perbuatan Pidana dan Kebiasaan Pertanggungjawaban Pidana menurut Kitab Undang-Undang Hukum Pidana*. VII(5), 41–48.
- Hanafi. (2023). *Urgensi Pengaturan Hukum tentang Perlindungan Data Pribadi pada Sistem Digital dalam Pemenuhan Hak Privasi di Indonesia*. 3.
- Hasanudin, A. F., & Babussalam, A. B. (2024). *Upaya Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking*. 6(01). <https://doi.org/10.31849/jgh.v6i01.18827>
- Husna, S. U., Darmawijaya, E., & Fithria, N. (2025). *ANALISIS PENETAPAN HUKUMAN PIDANA MENURUT TEORI PERTANGGUNGJAWABAN PIDANA (STUDI TERHADAP PUTUSAN NOMOR 234/PID.SUS/2023/PT BNA)*. 1, 67–79.
- Idfira, R. (2026). *Pertanggungjawaban Pidana Penyeloenggara Jalan menurut Pasal 273 Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan*. 14(1), 60–71. <https://doi.org/10.48171/cr477961>
- Maharani, P., Hafrida, & Rapik, M. (2024). *Pertanggungjawaban Pidana Hacktivist dalam Perspektif Hukum Pidana di Indonesia*. 5, 242–252. <https://doi.org/10.22437/pampas.v5i2.33291>
- Manurung, E. A. P., & Thalib, E. F. (2022). *TINJAUAN YURIDIS PERLINDUNGAN DATA PRIBADI MENURUT UU*



NOMOR 27 TAHUN 22. 139–148. <https://doi.org/10.36733/jhshs.v4i2>

- Mussa, R. A., & M.Si, D. L. S. (2024). *Media Sosial (Instagram, Facebook, Twitter, Whatsapp) dan Pergeseran Pola Interaksi Sosial Mahasiswa / Wi Program Studi Pembangunan Sosial Angkatan 2017 Univeristas Mulawarman*. 12(2), 271–284.
- Paminto, S. R., Hidayat, A., Nabila, B., Husaeni, M. R., Putri, R. A., Jenar, S., & Maharani. (2024). *Perlindungan Hukum Bagi Korban Pencurian Data Dan Informasi Pribadi Di Era Kejahatan Siber*. 2, 54–61. <https://doi.org/10.59435/jurdikum.v2i2.453>
- Prasetyaningtyas, I. D., & Zainsyah, L. A. (2025). *Implementasi GDPR Untuk Mengatasi Kekosongan Hukum Tindak Pidana Phishing Melalui Whatsapp di Indonesia*. 8(3), 5–11. <https://doi.org/10.26623/julr.v8i3.13114>
- Rinjani, M. A., & Firmansyah, R. (2025). *Hambatan Implementasi UU 27 / 2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia*. 8(1), 70–83. <https://doi.org/10.38043/jah.v8i1.6793>
- Sadillah Ahmad, R., Puspaningtyas, D. A., & Ismariy, M. N. K. Al. (2025). *Perlindungan Hukum Terhadap Privasi Data Pribadi Di Era Digital*. *The Juris*, 9(1), 15–23. <https://doi.org/10.56301/juris.v9i1.1307>
- Satria, M., & Handoyo, S. (2022). *Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online dalam Aplikasi Kreditpedia*. 8(2), 108–121.
- Setyawan, A., & Mahardhika, V. (2025). *Kualifikasi yuridis Phishing sebagai Kejahatan Manipulasi Informasi Elektronik dan Perolehan Data Pribadi Secara Melawan Hukum*. 1–17.
- Suciara, A., Michelin, D., Loway, G. A., Huberta, G. A., Fewsan, K., Fathoni, M. A., Tombeg, M. L. L., Maukar, M. R. M., & Guntoro, M. B. (2026). *Pencurian Identitas Digital sebagai Bentuk Kejahatan Pendahuluan dalam Cybercrime*. 5373–5387. <https://doi.org/10.61104/alz.v4i2.5005>
- Sukmawan, Y. A., & Damayanti, D. (2025). *Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum*. 4(1), 114–128. <https://doi.org/10.32801/nolaj.v4i3.116>
- Sutarli, A. F., & Kurniawan, S. (2023). *Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia*. 3, 4208–4221.
- Trianurahmah, A., Fauzi, A., Tyas, E. N., Muhammad Afif Suryanto, Rizky, M., & Wibisono, P. (2025). *Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspada Maraknya Kejahatan Phising Dengan Modus Berbasis Link*. *Orbit : Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 74–88. <https://doi.org/10.63217/orbit.v1i2.81>
- Utomo, S. (2025). *Perlindungan Data Pribadi Melalui Undang-Undang Nomor 27 Tahun 2022: Jawaban Tantangan Cybercrime Era Globalisasi Serba Digitalisasi*. 4, 237–244. <https://doi.org/10.46839/lexstricta.v4i2.1630>
- Wiraguna, S. A. (2024). *Metode Normatif dan Empiris dalam Penelitian Hukum : Studi Eksploratif di Indonesia*. 3(3). <https://doi.org/10.59818/jps.v3i3.1390>
- Yuwana, M. A. S. A., Surya, A. P. A., Baihaqy, A. H. Al, & Fauzi, M. A. N. (2025). *Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM*. 4(156), 31–37. <https://doi.org/10.57123/wicarana.v3i1.167>