AKADEMIK E-ISSN 2774-8863
Jurnal Mahasiswa Humanis
Vol. 6, No. 1, Januari 2026

# Analisis Perlindungan Hukum Korban Kehilangan Data dan Akun Pribadi melalui Broadcast Whatsapp (Studi Pasal 32 Undang-Undang Nomor 11 Tahun 2016 tentang Informasi dan Transaksi Elektronik)

**Imelta Santalova Wanmea Susanto**
Universitas Lampung, Indonesia
imeltasantalovaws@gmail.com

**Submitted**: 01st Oct 2025 | **Edited**: 04th Nov 2025 | **Issued**: 01st January 2026

**Cited on**: Susanto, I. S. W. (2026). Analisis Perlindungan Hukum Korban Kehilangan Data dan Akun Pribadi melalui Broadcast Whatsapp (Studi Pasal 32 Undang-Undang Nomor 11 Tahun 2016 tentang Informasi dan Transaksi Elektronik). *AKADEMIK: Jurnal Mahasiswa Humanis, 6*(1), 1-11.

**ABSTRACT**

The rapid development of information and communication technology has led to an increase in cybercrimes, particularly phishing attacks targeting personal data and online accounts. One of the most common modes occurs through broadcast messages on WhatsApp, where victims lose access to their accounts and sensitive information after opening malicious files or links. This study aims to analyze the legal protection for victims of data and account loss through WhatsApp broadcasts based on Article 32 of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Using a normative and empirical juridical approach, data were collected through literature studies and interviews with investigators from the Special Criminal Investigation Directorate of the Lampung Regional Police. The results indicate that although Articles 30, 32, and 35 of the ITE Law provide a partial legal framework, they do not comprehensively regulate phishing activities, leading to legal uncertainty for victims. The study recommends that the government harmonize the ITE Law with the 2022 Personal Data Protection Law and strengthen preventive measures through public education and digital security awareness programs.

**Keywords:** Legal Protection, Phishing, Personal Data, WhatsApp, ITE Law

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah mengubah cara manusia berinteraksi dan bertransaksi di berbagai aspek kehidupan. Dunia digital yang bersifat tanpa batas (borderless) memungkinkan pertukaran informasi secara cepat dan efisien, namun sekaligus memunculkan tantangan baru berupa meningkatnya tindak kejahatan siber. Salah satu bentuk kejahatan siber yang sering terjadi adalah phishing, yaitu tindakan penipuan untuk memperoleh informasi pribadi atau sensitif seseorang dengan menyamar sebagai pihak yang sah melalui media elektronik (Adisa & Andriyanto, 2024).

Di Indonesia, penggunaan media sosial seperti WhatsApp, Facebook, dan Instagram telah menjadi bagian penting dari kehidupan masyarakat. WhatsApp, sebagai aplikasi pesan instan paling populer, digunakan tidak hanya untuk komunikasi pribadi tetapi juga bisnis dan layanan publik (Isadora et al., 2024). Namun, kemudahan akses ini turut dimanfaatkan oleh pelaku kejahatan siber untuk melancarkan aksi phishing dengan mengirimkan tautan atau file berbahaya melalui pesan siaran (broadcast message). Ketika korban membuka tautan atau file tersebut, akun pribadi dan data sensitif dapat diambil alih tanpa izin (Universitas Telkom Surabaya, 2023).

Fenomena kehilangan data dan akun pribadi akibat phishing melalui WhatsApp terus meningkat setiap tahun. Kasus ini tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak pada reputasi, privasi, dan keamanan digital masyarakat (Adiputra, 2021). Kondisi ini menuntut adanya perlindungan hukum yang jelas dan efektif terhadap korban kejahatan siber. Dalam konteks hukum Indonesia, pengaturan mengenai perlindungan data pribadi masih bersandar pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Namun, beberapa pasal dalam UU ITE, khususnya Pasal 30, 32, dan 35, belum secara eksplisit mengatur unsur tindak pidana phishing, sehingga menimbulkan ketidakpastian hukum (Utama, 2020).

Kelemahan pengaturan ini semakin terasa mengingat kejahatan siber berkembang sangat cepat seiring transformasi digital. Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) baru mulai diberlakukan dan masih memerlukan sinkronisasi dengan UU ITE agar penerapannya dapat memberikan kepastian hukum bagi korban (Lestari, 2023). Menurut Putra (2021), harmonisasi regulasi menjadi langkah penting untuk menjamin hak privasi warga negara dan memperkuat kerangka perlindungan data di era digital.

Dari perspektif cyber law, lemahnya perlindungan terhadap korban phishing menunjukkan adanya kesenjangan antara perkembangan teknologi dan adaptasi regulasi hukum (Siregar, 2022). Negara lain seperti Amerika Serikat dan Singapura telah menerapkan kebijakan cybersecurity governance yang menekankan aspek pencegahan, edukasi, dan sistem perlindungan hukum yang komprehensif (Nugraha, 2020). Indonesia masih perlu memperkuat sinergi antar lembaga penegak hukum, meningkatkan literasi digital masyarakat, serta mengembangkan norma hukum yang lebih responsif terhadap

ancaman dunia maya (Wulandari, 2024).

Berdasarkan latar belakang tersebut, penelitian ini memfokuskan kajian pada bagaimana bentuk perlindungan hukum terhadap korban kehilangan data dan akun pribadi melalui broadcast WhatsApp berdasarkan Pasal 32 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta bagaimana upaya hukum dan pencegahan terhadap kejahatan siber tersebut dapat diterapkan secara efektif. Penelitian ini diharapkan dapat memberikan kontribusi dalam memperkuat sistem perlindungan hukum terhadap kejahatan siber, khususnya phishing, di Indonesia.

## LANDASAN TEORI

### Konsep Perlindungan Hukum

Perlindungan hukum merupakan salah satu prinsip fundamental dalam sistem hukum modern yang bertujuan menjamin hak dan kepentingan warga negara agar tidak dirugikan oleh tindakan sewenang-wenang, baik oleh individu maupun oleh negara. Menurut Rahardjo (2021), perlindungan hukum dapat dipahami sebagai bentuk pengakuan dan jaminan terhadap hak-hak manusia yang bersumber dari norma hukum yang berlaku. Dalam konteks kejahatan siber, perlindungan hukum berfungsi sebagai mekanisme pertanggungjawaban dan pemulihan bagi korban atas kerugian yang ditimbulkan (Fitriani, 2022).

Perlindungan hukum dibedakan menjadi dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif (Tahir, 2020). Perlindungan preventif bertujuan mencegah terjadinya pelanggaran hukum melalui pengaturan norma dan kebijakan yang jelas, sementara perlindungan represif diberikan setelah pelanggaran terjadi untuk mengembalikan hak korban. Dalam kasus kehilangan data pribadi akibat phishing, kedua bentuk perlindungan ini harus berjalan beriringan agar korban memperoleh keadilan dan kepastian hukum.

### Kejahatan Siber dan Tindak Pidana Phishing

Kejahatan siber (cybercrime) merupakan segala bentuk pelanggaran hukum yang dilakukan melalui jaringan komputer atau internet. Salah satu bentuk paling umum adalah phishing, yaitu kejahatan dengan cara menipu pengguna agar menyerahkan data pribadi melalui situs palsu, pesan elektronik, atau aplikasi digital (Nugroho, 2023). Phishing pada aplikasi WhatsApp biasanya dilakukan melalui file atau tautan yang tampak sah, namun

sebenarnya berisi malware yang dapat mencuri data pengguna (Aini & Fadli, 2021).

Phishing termasuk dalam kategori tindak pidana karena melanggar hak privasi dan integritas data seseorang. Sesuai dengan Budhihardjo (2022), kejahatan ini menimbulkan kerugian material maupun immaterial dan menuntut adanya regulasi yang secara eksplisit mengatur bentuk dan sanksinya. Indonesia sendiri telah memiliki Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang kemudian diperbarui dengan Undang-Undang Nomor 19 Tahun 2016, namun belum mengatur secara tegas unsur tindak pidana phishing (Wijayanti, 2020).

**Dasar Hukum Perlindungan Data Pribadi di Indonesia**

Konsep perlindungan data pribadi di Indonesia terus berkembang seiring dengan meningkatnya ancaman kebocoran data digital. Lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam memberikan jaminan hukum terhadap pengelolaan, penyimpanan, dan penyebaran data pribadi (Halim, 2023). UU ini menegaskan bahwa setiap individu memiliki hak atas privasi dan kendali terhadap data pribadinya, sehingga setiap penyalahgunaan data tanpa izin dapat dikenai sanksi hukum.

Namun, sinkronisasi antara UU PDP dan UU ITE masih menjadi tantangan. Menurut Pratama (2024), masih terdapat tumpang tindih dalam penegakan hukum terhadap kasus pencurian data melalui media digital, karena belum adanya aturan teknis yang mengatur kolaborasi antar lembaga penegak hukum. Hal ini menyebabkan korban phishing melalui WhatsApp sering kesulitan mendapatkan pemulihan hukum yang efektif.

**Asas Hukum dalam Penegakan Cybercrime**

Dalam penerapan hukum terhadap tindak pidana siber, asas lex specialis derogat legi generali menjadi landasan penting. Artinya, peraturan khusus (UU ITE) mengesampingkan peraturan umum (KUHP) dalam kasus yang bersifat khusus (Subekti, 2019). Namun demikian, efektivitas penerapan asas tersebut bergantung pada sejauh mana undang-undang khusus mampu mencakup semua unsur tindak pidana yang terjadi.

Selain asas lex specialis, asas kepastian hukum juga berperan penting dalam menjamin perlindungan bagi korban. Asas ini menuntut adanya kejelasan norma dan penerapan hukum yang konsisten (Hasanah, 2021). Dalam konteks phishing, ketidakjelasan unsur pasal dalam UU ITE menimbulkan kekaburan norma (vague norms)

yang menghambat penegakan hukum secara optimal.

**Kerangka Teori Perlindungan Hukum terhadap Korban Phishing**

Berdasarkan teori hukum perlindungan korban (victim protection theory), negara memiliki kewajiban untuk melindungi setiap warga negara dari ancaman kejahatan digital dan memberikan akses terhadap keadilan (Latifah, 2022). Perlindungan ini mencakup upaya pemulihan, restitusi, serta jaminan agar korban tidak mengalami kerugian berulang. Dalam konteks kejahatan siber, teori ini menekankan bahwa perlindungan hukum tidak hanya berfokus pada penghukuman pelaku, tetapi juga pada pemulihan korban.

Dengan demikian, perlindungan hukum terhadap korban kehilangan data dan akun pribadi melalui broadcast WhatsApp harus dilihat sebagai bagian dari upaya negara dalam mewujudkan keamanan digital nasional dan hak atas privasi. Kerangka hukum yang kuat dan responsif terhadap dinamika kejahatan siber akan menciptakan keseimbangan antara perlindungan hak individu dan kepastian hukum bagi semua pihak.

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif dan yuridis empiris secara bersamaan untuk memperoleh gambaran komprehensif mengenai perlindungan hukum terhadap korban kehilangan data dan akun pribadi akibat kejahatan phishing melalui broadcast WhatsApp. Pendekatan yuridis normatif digunakan untuk menelaah norma-norma hukum positif yang berlaku, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pendekatan ini memungkinkan peneliti mengidentifikasi kesesuaian antara ketentuan peraturan perundang-undangan dengan praktik penegakan hukum terhadap kejahatan siber (Rukmini, 2021).

Sementara itu, pendekatan yuridis empiris digunakan untuk memahami penerapan hukum dalam praktik, khususnya dalam penanganan kasus kehilangan data pribadi melalui media digital. Data empiris diperoleh melalui wawancara dengan penyidik pada Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Kepolisian Daerah Lampung yang memiliki pengalaman langsung dalam menangani kasus phishing. Pendekatan ini dipilih karena dapat menjembatani kesenjangan antara norma hukum dan realitas sosial dalam penerapan hukum siber (Harahap & Sulaiman, 2022).

Jenis data dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh dari hasil wawancara dan observasi lapangan, sedangkan data sekunder bersumber dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan seperti UU ITE, UU PDP, dan KUHP. Bahan hukum sekunder mencakup buku, jurnal ilmiah, laporan penelitian, dan artikel akademik yang berhubungan dengan perlindungan data pribadi dan tindak pidana siber (Kusuma, 2020). Adapun bahan hukum tersier digunakan untuk memperkuat interpretasi istilah hukum melalui kamus hukum dan kamus besar bahasa Indonesia (Mustari, 2021).

Teknik pengumpulan data dilakukan melalui dua tahap, yaitu studi kepustakaan dan studi lapangan. Studi kepustakaan dilakukan dengan menelaah berbagai literatur hukum, jurnal ilmiah, dan dokumen kebijakan yang relevan dengan topik penelitian. Studi lapangan dilakukan melalui wawancara semi-terstruktur dengan narasumber utama dari aparat penegak hukum dan akademisi di bidang hukum siber. Tahapan ini dimaksudkan agar diperoleh pandangan empiris yang mendukung temuan normatif.

Data yang diperoleh dianalisis menggunakan metode analisis deskriptif kualitatif. Analisis ini dilakukan dengan cara menelaah, mengklasifikasikan, dan menafsirkan data untuk menggambarkan kondisi aktual penerapan hukum dalam kasus kehilangan data pribadi akibat phishing. Menurut Fatimah (2023), analisis kualitatif dalam penelitian hukum tidak hanya memaparkan fakta, tetapi juga mencari hubungan antara norma hukum dan praktik sosial agar diperoleh pemahaman yang lebih kontekstual. Selanjutnya, hasil analisis diinterpretasikan untuk menilai sejauh mana efektivitas peraturan yang ada dalam memberikan perlindungan hukum kepada korban.

## HASIL PENELITIAN

### Perlindungan Hukum terhadap Korban Kehilangan Data dan Akun Pribadi Melalui Broadcast WhatsApp

Hasil penelitian lapangan menunjukkan bahwa kasus kehilangan data dan akun pribadi (phishing) melalui aplikasi WhatsApp semakin meningkat di wilayah Lampung. Berdasarkan keterangan dari penyidik Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Lampung, mayoritas korban kehilangan akses ke akun WhatsApp setelah membuka tautan atau file berformat APK yang dikirim melalui pesan broadcast. Modus ini digunakan untuk memperoleh akses jarak jauh ke perangkat korban sehingga

pelaku dapat mencuri data pribadi dan keuangan yang terhubung dengan aplikasi digital seperti DANA, Gopay, dan M-Banking.

Secara normatif, pengaturan terhadap tindak pidana phishing mengacu pada Pasal 30, 32, dan 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Namun, hasil analisis menunjukkan bahwa pasal-pasal tersebut belum sepenuhnya mampu menjangkau unsur-unsur perbuatan phishing, karena norma yang terdapat di dalamnya masih bersifat umum dan tidak secara eksplisit menyinggung kejahatan pencurian data pribadi digital. Kondisi ini menimbulkan kekaburan norma (vague norm) yang berdampak pada lemahnya perlindungan hukum terhadap korban.

Hasil ini sejalan dengan temuan Lestari (2023) yang menyatakan bahwa UU ITE masih menimbulkan multitafsir dalam kasus kebocoran data pribadi, sehingga diperlukan harmonisasi dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Selain itu, penelitian oleh Halim (2023) juga menegaskan bahwa pengaturan tentang perlindungan data pribadi dalam UU PDP masih membutuhkan aturan pelaksana agar dapat berfungsi efektif di lapangan. Dengan demikian, hasil empiris dari penelitian ini memperkuat pendapat bahwa UU ITE memiliki kelemahan dalam aspek kepastian hukum bagi korban kejahatan siber.

Dari sisi teori hukum, hasil penelitian ini mendukung pandangan Rahardjo (2021) yang menegaskan bahwa perlindungan hukum tidak hanya bersifat represif (setelah pelanggaran terjadi), tetapi juga harus preventif untuk mengurangi potensi kerugian masyarakat. Dalam konteks ini, perlindungan hukum yang efektif bagi korban phishing menuntut penguatan regulasi dan penerapan kebijakan yang lebih responsif terhadap perkembangan teknologi.

Temuan lapangan juga menunjukkan bahwa penegakan hukum dalam kasus phishing menghadapi kendala teknis, antara lain sulitnya pelacakan pelaku karena penggunaan server luar negeri dan kurangnya sumber daya penyidik siber. Menurut penyidik Ditreskrimsus, sebagian besar korban tidak memahami pentingnya perlindungan data digital, sehingga terlambat melapor atau bahkan tidak mengetahui bahwa mereka telah menjadi korban. Faktor ini memperkuat hasil penelitian Adisa dan Andriyanto (2024), yang menunjukkan bahwa lemahnya kesadaran masyarakat terhadap keamanan digital menjadi salah satu penyebab meningkatnya kasus phishing di Indonesia.

**Upaya Hukum dan Pencegahan terhadap Kejahatan Peretasan Data dan Akun Pribadi**

Upaya penanggulangan kejahatan peretasan data pribadi dapat ditempuh melalui dua pendekatan, yakni upaya penal (represif) dan upaya non-penal (preventif).

1. Upaya Penal (Represif)

   Hasil penelitian menunjukkan bahwa penegakan hukum terhadap kasus phishing dilakukan berdasarkan Pasal 30, 32, dan 35 UU ITE, serta Kitab Undang-Undang Hukum Pidana (KUHP). Namun, dalam praktiknya, aparat penegak hukum menghadapi kendala pembuktian karena pelaku sering menggunakan fake account dan server internasional. Hal ini memperlihatkan perlunya peningkatan kapasitas digital forensik di tubuh Kepolisian (Hidayat, 2021).

   Selain itu, aparat penegak hukum menilai bahwa peraturan yang ada masih bersifat fragmentaris. Oleh karena itu, sinergi antara UU ITE, UU PDP, dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menjadi hal yang mendesak. Penelitian oleh Pratama (2024) mengonfirmasi pentingnya pembentukan lembaga koordinatif lintas sektor untuk menangani kejahatan siber agar tidak terjadi tumpang tindih kewenangan antarinstansi.

2. Upaya Non-Penal (Preventif)

   Dari sisi preventif, hasil penelitian menunjukkan bahwa tingkat kesadaran masyarakat terhadap keamanan data digital masih rendah. Banyak korban yang dengan mudah membuka tautan mencurigakan tanpa melakukan verifikasi. Oleh karena itu, upaya pencegahan dilakukan melalui sosialisasi dan edukasi publik. Pemerintah perlu menggandeng lembaga pendidikan, penyedia layanan digital, serta media untuk meningkatkan literasi keamanan siber (Wulandari, 2024).

Studi sebelumnya oleh Aini dan Fadli (2021) juga menegaskan bahwa peningkatan kesadaran pengguna melalui pendidikan digital menjadi langkah paling efektif untuk menekan angka cybercrime. Di sisi lain, penerapan sistem keamanan dua faktor (two-factor authentication) dan kebijakan privasi yang lebih ketat dari penyedia layanan aplikasi perlu diperkuat agar masyarakat lebih terlindungi.

**Pembahasan**

Temuan penelitian ini sesuai dengan beberapa studi terdahulu yang menyoroti lemahnya sistem perlindungan data pribadi di Indonesia. Nugroho (2023) menunjukkan bahwa hukum siber Indonesia masih bersifat reaktif, belum mampu mengantisipasi munculnya modus baru kejahatan digital. Sementara itu, Fitriani (2022) menekankan bahwa perlindungan hukum terhadap korban kejahatan digital masih cenderung simbolik, belum menyentuh aspek pemulihan hak korban secara konkret.

Dari perspektif hukum perbandingan, negara seperti Amerika Serikat dan Singapura telah menerapkan sistem perlindungan data berbasis cybersecurity governance, di mana regulasi dan edukasi digital dilaksanakan secara paralel (Budhihardjo, 2022). Hal ini dapat menjadi model bagi Indonesia dalam memperkuat sistem penegakan hukum terhadap kejahatan siber, khususnya phishing melalui media sosial. Dengan memperhatikan hasil empiris dan temuan penelitian terdahulu, dapat ditegaskan bahwa efektivitas perlindungan hukum terhadap korban kehilangan data dan akun pribadi melalui WhatsApp sangat bergantung pada sinergi antara aspek regulasi, penegakan hukum, dan literasi digital masyarakat.

## KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa perlindungan hukum terhadap korban kehilangan data dan akun pribadi melalui broadcast WhatsApp di Indonesia masih belum optimal. Ketentuan dalam Pasal 30, 32, dan 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 belum secara tegas mengatur unsur tindak pidana phishing. Akibatnya, terdapat kekaburan norma hukum yang menimbulkan ketidakpastian dalam penegakan hukum terhadap kejahatan siber yang berkaitan dengan pencurian data pribadi.

Secara empiris, penelitian menunjukkan bahwa aparat penegak hukum menghadapi kendala teknis dalam pelacakan pelaku phishing karena keterbatasan sumber daya forensik digital serta rendahnya kesadaran masyarakat terhadap keamanan data pribadi. Hal ini menunjukkan bahwa perlindungan hukum terhadap korban masih bersifat represif dan belum diimbangi dengan upaya preventif yang memadai.

Temuan ini konsisten dengan penelitian terdahulu (Lestari, 2023; Adisa & Andriyanto, 2024; Halim, 2023) yang menyebutkan bahwa regulasi terkait perlindungan

data pribadi di Indonesia belum sepenuhnya harmonis. Diperlukan sinergi antara UU ITE, UU Perlindungan Data Pribadi (UU No. 27 Tahun 2022), serta peraturan pelaksananya agar dapat menciptakan sistem hukum yang adaptif terhadap dinamika kejahatan digital.

Dengan demikian, dapat disimpulkan bahwa efektivitas perlindungan hukum terhadap korban phishing melalui aplikasi WhatsApp sangat bergantung pada kejelasan norma hukum, peningkatan kapasitas lembaga penegak hukum, dan kesadaran digital masyarakat. Reformulasi pasal-pasal dalam UU ITE menjadi urgensi yang tidak dapat dihindarkan untuk menjamin kepastian dan keadilan hukum di era transformasi digital.

## DAFTAR PUSTAKA

Adiputra, R. (2021). Dampak serangan *phishing* terhadap individu dan organisasi di Indonesia. *Jurnal Teknologi dan Informasi*, 5(2), 115–126.

Adisa, A. Z., & Andriyanto, A. (2024). Perlindungan hukum terhadap korban *phishing* terkait pengiriman file APK. *Jurnal Hukum dan Teknologi Informasi*, 10(1), 45–56.

Aini, S., & Fadli, R. (2021). Fenomena *phishing* dan perlindungan hukum terhadap pengguna media sosial. *Jurnal Hukum dan Teknologi Informasi*, 4(1), 22–35.

Budhihardjo, T. (2022). Analisis yuridis tindak pidana *cybercrime* dalam perspektif hukum pidana Indonesia. *Jurnal Ilmu Hukum Modern*, 6(2), 101–113.

Fatimah, N. (2023). Pendekatan kualitatif dalam penelitian hukum normatif dan aplikasinya di Indonesia. *Jurnal Penelitian Hukum dan Masyarakat*, 11(1), 56–68.

Fitriani, D. (2022). Implementasi perlindungan hukum bagi korban kejahatan digital di Indonesia. *Jurnal Penelitian Hukum dan Keadilan*, 8(1), 56–70.

Halim, F. (2023). Harmonisasi UU ITE dan UU Perlindungan Data Pribadi dalam era digitalisasi. *Jurnal Legislasi dan Kebijakan Publik*, 9(3), 88–99.

Harahap, R., & Sulaiman, D. (2022). Integrasi pendekatan normatif dan empiris dalam penelitian hukum kontemporer. *Jurnal Ilmu Hukum Indonesia*, 8(2), 77–89.

Hasanah, L. (2021). Asas kepastian hukum dalam penerapan Undang-Undang ITE terhadap kejahatan siber. *Jurnal Hukum dan Pembangunan Sosial*, 12(2), 110–124.

Hidayat, M. (2021). Kapasitas forensik digital dalam penegakan hukum kejahatan siber. *Jurnal Hukum dan Kriminologi Digital*, 5(1), 40–54.

Isadora, K., Rahman, N., & Yuliani, S. (2024). Analisis modus *phishing* terhadap aplikasi WhatsApp. *Jurnal Akuntansi dan Teknologi Informasi*, 3(2), 77–89.

Kusuma, A. P. (2020). Metodologi penelitian hukum dalam menghadapi tantangan era digital. *Jurnal Kajian Hukum dan Teknologi*, 6(3), 101–115.

Latifah, M. (2022). Teori perlindungan korban dalam sistem hukum pidana Indonesia. *Jurnal Hukum Humaniora dan Sosial*, 3(4), 65–78.

Lestari, M. (2023). Kepastian hukum dalam kasus kebocoran data pribadi di era digital. *Jurnal Hukum dan Hak Asasi Manusia*, 8(1), 33–47.

Mustari, E. (2021). Peran bahan hukum tersier dalam analisis yuridis penelitian hukum. *Jurnal Metodologi Hukum dan Sosial*, 7(1), 22–34.

Nugraha, R. (2020). *Cybersecurity governance* dan perlindungan data pribadi di era globalisasi digital. *Jurnal Keamanan Siber dan Teknologi Informasi*, 2(3), 55–68.

Nugroho, P. (2023). Karakteristik tindak pidana *phishing* dalam sistem hukum nasional. *Jurnal Siber dan Kriminologi*, 5(1), 40–54.

Pratama, R. (2024). Tantangan penegakan hukum terhadap kejahatan siber di era perlindungan data pribadi. *Jurnal Reformasi Hukum dan Teknologi Digital*, 11(1), 27–39.

Putra, I. N. G. (2021). Perlindungan data pribadi dalam perspektif hukum siber di Indonesia. *Jurnal Ilmu Hukum dan Sosial*, 7(1), 23–36.

Rahardjo, S. (2021). Prinsip perlindungan hukum terhadap warga negara dalam perspektif hukum modern. *Jurnal Hukum dan Keadilan Sosial*, 7(2), 15–29.

Rahmawati, L. (2019). Model penelitian hukum normatif-empiris dalam kajian perlindungan data pribadi. *Jurnal Penegakan Hukum dan Kebijakan Publik*, 4(2), 91–103.

Rukmini, S. (2021). Telaah kritis pendekatan yuridis normatif dalam penelitian hukum di Indonesia. *Jurnal Filsafat dan Ilmu Hukum*, 9(1), 45–58.

Siregar, A. (2022). Tantangan hukum pidana dalam menghadapi kejahatan siber di Indonesia. *Jurnal Penegakan Hukum dan Teknologi*, 9(2), 102–118.

Subekti, R. (2019). Penerapan asas *lex specialis derogat legi generali* dalam penegakan hukum pidana siber. *Jurnal Ilmu Hukum dan Etika Digital*, 4(3), 77–90.

Susilawati, D. (2023). Penggunaan metode deskriptif kualitatif dalam penelitian hukum siber. *Jurnal Transformasi Hukum Digital*, 4(2), 88–99.

Tahir, M. (2020). Perlindungan hukum preventif dan represif terhadap kejahatan siber di Indonesia. *Jurnal Hukum dan Kebijakan Nasional*, 5(2), 91–104.

Universitas Telkom Surabaya. (2023). *Phishing: Pengertian, jenis, dan cara menghindari*. https://surabaya.telkomuniversity.ac.id/phishing-pengertian-jenis-dan-cara-menghindari-phising/

Utama, A. S. (2020). Bentuk-bentuk tindak pidana di media sosial dan sanksi hukumnya. *Jurnal Hukum dan Masyarakat Digital*, 1(2), 89–99.

Wijayanti, D. (2020). Kajian normatif tentang kejahatan *phishing* dalam hukum pidana Indonesia. *Jurnal Ilmiah Hukum dan Teknologi*, 3(1), 12–25.

Wulandari, D. (2024). Penguatan regulasi dan literasi hukum dalam menghadapi kejahatan siber di Indonesia. *Jurnal Transformasi Hukum Digital*, 5(1), 14–27.