JURNAL
LAWNESIA
Volume 4 (2), Desember 2025, 658-664
E-ISSN: 2829-7873

PERLINDUNGAN HUKUM TERHADAP KORBAN PERETASAN APLIKASI WHATSAPP DI INDONESIA

LEGAL PROTECTION FOR VICTIMS OF WHATSAPP HACKING IN INDONESIA

Habib Khairul 'Atho1
Mahasiswa Program Studi Hukum,
Fakultas Hukum Ilmu Sosial dan Ilmu Politik Universitas Terbuka
khairulhabib@ecampus.ut.ac.id

Nuri Hidayati²
Fakultas Hukum Ilmu Sosial dan Ilmu Politik Universitas Terbuka
Fakultas Hukum Universitas Bakti Indonesia
nurihidayati2994@gmail.com

ABSTRAK

Perkembangan pesat dalam teknologi digital telah meningkatkan ancaman kejahatan siber, yang mencakup akses ilegal atau peretasan aplikasi WhatsApp, menyebabkan kerugian bagi para pengguna dan menjadikan perlu adanya perlindungan hukum yang memadai. Fokus kajian ini diarahkan pada penelusuran mendalam mengenai ragam serta metode peretasan aplikasi WhatsApp, mengevaluasi regulasi yang ada di Indonesia berdasarkan Regulasi Tahun 2016 yang merevisi ketentuan hukum Tahun 2008 terkait sistem informasi dan aktivitas elektronik, serta merumuskan langkah-langkah untuk memperkuat perlindungan hukum bagi para korban. Pendekatan kajian ini mengandalkan metode hukum normatif berbasis analisis regulasi serta konsep melalui analisis sumber hukum primer, sekunder, dan tersier. Temuan dalam penelitian ini menunjukkan bahwa metode peretasan termasuk pembajakan akun dengan tautan palsu, kloning kartu SIM, dan penguasaan data pribadi pengguna. Regulasinya yang ada sudah memberikan aturan normatif untuk menjatuhi sanksi pada pelaku, namun pelaksanaannya terhambat oleh kurangnya bukti digital dan literasi keamanan siber yang rendah. Penelitian ini mengajak agar perlindungan hukum bagi korban perlu diperkuat dengan meningkatkan kapasitas aparat penegak hukum, memperbaiki regulasi agar sesuai dengan perkembangan teknologi, serta memberikan edukasi kepada masyarakat tentang keamanan digital. Implikasi dari penelitian ini memberikan saran kepada pemerintah dalam memperkuat kerangka hukum dan kebijakan perlindungan terhadap korban kejahatan siber di Indonesia.

Kata Kunci: Kejahatan Siber; Perlindungan Hukum; Peretasan WhatsApp.

ABSTRACT

The rapid development in digital technology has increased the threat of cybercrime, which includes illegal access or hacking of the WhatsApp application, causing losses to users and making it necessary for adequate legal protection. This study focuses on an in-depth examination of the variety and methods of hacking the WhatsApp application, evaluating existing regulations in Indonesia based on the 2016 Regulation that revised the provisions of the 2008 law related to information systems and electronic activities, as well as formulating measures to strengthen legal protection for victims. This study approach relies on normative legal methods based on regulatory analysis and concepts through primary, secondary, and tertiary legal source analysis. The findings show that hacking methods include account hijacking with fake links, SIM card cloning, and mastering user's personal data. The existing regulations have provided normative rules to impose sanctions on perpetrators, but their implementation is hindered by the lack of digital evidence and low cybersecurity literacy. This research suggests that legal protection for victims needs to be strengthened by increasing the capacity of law enforcement officers, improving regulations to be in accordance with technological developments, and providing education to the public about digital security. This study provides implications and recommendations to the government in strengthening the legal framework and protection policies for cybercrime victims in Indonesia.

Keywords: *Cyber Crime; Legal Protection; WhatsApp Hacking*

Pendahuluan

Kemajuan di sektor teknologi informasi dalam negeri telah memicu pergeseran besar pada cara orang berinteraksi satu sama lain, berbisnis, dan belajar. Prasetya et al. (2024) WhatsApp sekarang bertransformasi menjadi layanan komunikasi cepat yang mendominasi penggunaan nasional dengan lebih dari 90% pengguna internet aktif mengaksesnya setiap hari, sesuai dengan informasi dari APJII dan laporan We Are Social tahun 2025.[1] Digitalisasi menciptakan baik peluang maupun tantangan baru dalam proses komunikasi nasional.

Statistik mengenai keamanan siber pada tahun 2025 menunjukkan adanya peningkatan yang signifikan dalam insiden kejahatan digital. Laporan Cyber Blitz dari BSSN dan AwanPintar mencatat sekitar 133,4 juta serangan siber selama paruh pertama tahun 2025, menandakan bahwa ancaman siber di Indonesia sangat tinggi, meskipun jumlah ini mengalami penurunan tajam dari 2,49 miliar serangan di paruh pertama tahun sebelumnya.[2] Tipe serangan semakin beragam, mulai dari DDoS hingga pencurian kredensial melalui aplikasi pesan instan.

Di wilayah perkotaan, Jakarta diketahui sebagai kota dengan jumlah serangan tertinggi, menanggung hampir 60% dari total serangan siber nasional. Daerah metropolitan lainnya termasuk Surabaya serta Bandung juga sering menjadi target peretasan. SAFEnet menyatakan, dari 299 insiden keamanan digital yang terjadi antara Juli hingga September 2025, terdapat 32 kasus yang berkaitan dengan pencurian akun WhatsApp, di mana 59% korban berasal dari kalangan yang aktif mengkritik kebijakan pemerintah, seperti mahasiswa dan peserta aksi demonstrasi terkait revisi UU TNI.[3]

Teknik peretasan WhatsApp di Indonesia semakin rumit. Penelitian oleh Khasanah dan Sutabri (2023) menunjukkan bahwa social engineering menjadi metode utama yang digunakan pelaku untuk menipu korban, termasuk meminta kode OTP, mengelabui dengan

[1] Sofyan Mufti Prasetiyo et al., *Analisis Pertumbuhan Pengguna Internet Di Indonesia*, 2, no. 1 (2024).

[2] "Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI," CIO Healthcare Indonesia, accessed November 15, 2025, http://ciohealthcare.or.id/berita/ancaman-digital-2025-serangan-siber-ri.

[3] databoks.katadata.co.id, "Pengancaman, Jenis Serangan Digital Terbanyak di RI pada Kuartal III 2025 | Pusat Data Ekonomi dan Bisnis Indonesia | Databoks," accessed November 15, 2025, https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/691164464058b/pengancaman-jenis-serangan-digital-terbanyak-di-ri-pada-kuartal-iii-2025.

aplikasi palsu, serta melakukan sinkronisasi perangkat secara diam-diam menggunakan QR code atau tautan login palsu.[4] Serangan phishing berbasis tautan yang mencurigakan menjadi titik awal, di mana 70% pengambilalihan akun dimulai dari pesan yang terlihat datang dari kontak yang dipercaya.

Hidayah dan Amran (2023) menunjukkan bahwa penipuan melalui social engineering dan phishing pada WhatsApp sering menargetkan nasabah m-banking.[5] Para pelaku berpura-pura menjadi otoritas resmi atau teman dekat untuk menipu korban agar memberikan kode verifikasi, sehingga mereka bisa mengakses semua data, pesan, dan dokumen digital korban. Akibatnya, tidak hanya privasi yang hilang, tetapi juga kerugian finansial dan reputasi sosial korban terganggu.

Penelitian oleh Trianurahmah et al. (2025) dalam ORBIT mengidentifikasi peningkatan serangan yang berbasis tautan palsu dan penggunaan aplikasi tidak resmi yang dapat mencuri kredensial WhatsApp begitu korban mengklik tautan tersebut.[6] Teknik keylogger, permintaan login ke halaman palsu atau aplikasi WhatsApp modifikasi telah menjadi tren baru di Indonesia sejak tahun 2024. Data dari Goodstats melaporkan bahwa dari 139 kasus di awal tahun 2025, sebagian besar ditujukan kepada kelompok vokal, aktivis, dan pelaku UMKM sebagai target utama.[7]

Di tingkat lokal, kasus penyadapan WhatsApp melalui sinkronisasi perangkat semakin meningkat, terutama praktik menghubungkan WhatsApp ke perangkat lain supaya semua pesan, foto, dan dokumen korban bisa diakses oleh pelaku. Putra dan Sutabri (2023) menjelaskan bagaimana pelaku menyalin akun menggunakan QR code, membuat korban kehilangan akses terhadap data penting tanpa menyadarinya dan menjadi korban pembajakan.[8] Dampak dari peretasan WhatsApp terhadap ekonomi dan kesehatan mental sangat serius. Hasanudin dan Babussalam (2024) menekankan pengurasan saldo rekening m-banking melalui aplikasi WhatsApp.[9] Sering kali korban tidak menyadari adanya akses ilegal hingga dompet digital mereka menjadi kosong, di samping kehilangan identitas digital dan kredensial penting. Situasi ini diperparah oleh kurangnya saluran pengaduan yang efektif dan lambatnya proses pemulihan bagi korban.

---

[4] Nurul Khasanah and Tata Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP," *Blantika: Multidisciplinary Journal* 1, no. 2 (2023): 44–55, https://doi.org/10.57096/blantika.v1i2.13.

[5] Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp," *Jurnal Pustaka Cendekia Hukum Dan Ilmu Sosial* 1, no. 1 (2023): 116–27, https://doi.org/10.70292/pchukumsosial.v1i1.43.

[6] Adinda Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Link," *Orbit : Jurnal Ilmu Multidisiplin Nusantara* 1, no. 2 (2025): 74–88, https://doi.org/10.63217/orbit.v1i2.81.

[7] "Laporan Tahunan Kamsiber 2024," n.d., accessed November 15, 2025, https://csirt.komdigi.go.id/storage/uploads/document_centers/attachments/Laporan%20Tahunan%20Kamsiber%202024.pdf.

[8] Yusuf Andi Putra and Tata Sutabri, "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA," *Blantika: Multidisciplinary Journal* 1, no. 2 (2023): 132–41, https://doi.org/10.57096/blantika.v1i2.8.

[9] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking," *Jurnal Gagasan Hukum* 6, no. 01 (2024): 16–29, https://doi.org/10.31849/jgh.v6i01.18827.

Perlindungan terhadap korban peretasan WhatsApp di Indonesia secara normatif tercantum dalam Regulasi Tahun 2008 beserta pembaruannya Tahun 2016 terkait aktivitas digital dan informasi elektronik. Aturan ini menjadi landasan bagi penegakan hukum dan melarang akses yang tidak sah ke dalam sistem elektronik, tetapi penerapannya sering terhambat oleh bukti forensik digital dan keterbatasan dalam pemulihan hak-hak para korban.

Hutabarat et al. (2023) menganggap bahwa penyesuaian peraturan di zaman Society 5.0 menjadi kebutuhan utama agar sistem perlindungan hukum bisa menyesuaikan dengan perkembangan modus dan perubahan kejahatan digital.[10] Penegakan hukum, peningkatan tingkat literasi digital, dan kerja sama dalam advokasi dianggap mampu memberikan perlindungan kepada para korban. Wibowo (2024) menambahkan bahwa pendidikan serta penyesuaian kebijakan digital perlu dijadikan prioritas untuk menurunkan jumlah insiden dan memperbaiki kondisi para korban.[11]

Strategi perlindungan lebih lanjut meliputi penguatan saluran pengaduan bagi korban, kerja sama antara aparat penegak hukum, pemberdayaan lembaga bantuan hukum, serta pendidikan yang berfokus pada masyarakat. Adanya sistem pengaduan berbasis digital serta dukungan dari lembaga bantuan hukum memiliki peran penting dalam membela hak-hak korban. Namun, tingkat keterampilan digital yang masih rendah dan kurangnya infrastruktur di beberapa daerah membuat sejumlah korban mengalami kesulitan untuk mendapatkan keadilan dan pemulihan hak hukum mereka. Oleh karena itu, kerja sama antara pemerintah, sektor swasta, serta keterlibatan publik mutlak dibutuhkan untuk memastikan mekanisme perlindungan digital bekerja secara optimal dan adil.

Rumusan masalah dalam studi ini meliputi: Pertama, bagaimanakah bentuk dan modus operandi tindak akses tanpa hak (peretasan) terhadap aplikasi WhatsApp yang terjadi di Indonesia? Kedua, bagaimanakah pengaturan sistem legal yang berlaku di Indonesia dalam menjamin keamanan bagi tindak akses tanpa hak (peretasan) pada aplikasi WhatsApp berdasarkan ketentuan ketentuan hukum formal, terutama regulasi tahun 2016 yang memutakhirkan aturan 2008 mengenai aktivitas digital? Ketiga, bagaimanakah upaya dan strategi peningkatan perlindungan hukum bagi korban tindak akses tanpa hak (peretasan) terhadap aplikasi WhatsApp di Indonesia?

Melalui analisis data, tren kasus di tingkat lokal, dan tinjauan terhadap literatur hukum, diharapkan penelitian ini dapat memberikan rekomendasi bagi pemerintah dan pihak terkait. Perlindungan bagi korban WhatsApp perlu menjadi prioritaskan, dengan melakukan penguatan terhadap regulasi, membangun literasi digital, dan memastikan bahwa korban di seluruh Indonesia memperoleh akses terhadap rehabilitasi dan pemulihan.

---

[10] *CYBER-LAW (*ISBN: 978-623-8345-05-2)*, n.d., accessed November 15, 2025, https://buku.sonpedia.com/2023/07/cyber-law.html.

[11] "Hukum Siber Dan Keamanan Informasi," n.d., accessed November 15, 2025, https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_AsODON7rWAAumI-eyUfM-KqX7dg_crFXgDCn9z-EkA7XoNcA_H7XTA_1731900608.pdf.

Dalam artikel ini saya mengupas topik berjudul Perlindungan Hukum Terhadap Korban Peretasan Aplikasi WhatsApp Di Indonesia.

Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan penekanan pada analisis sumber hukum utama yuridis namatif adalah metode penelitian hukum yang mempelajari hukum sebagai suatu sistem norma yang ditentukan dalam undang-undang keputusan pengadilan sehingga penelitian ini berfokus pada analisis literatur atau dokumen hukum tanpa memasukkan data lapangan jadi tujuan utamanya adalah untuk mendefinisikan, memahami, dan menyelesaikan masalah hukum berdasarkan undang-undang yang ada serta mengembangkan teori dan kebijakan hukum yang relevan. Metode ini bersifat dogmatik yang berarti hukum dianggap sebagai kebenaran yang Harus dipatuhi dan diperkira secara menyeluruh melalui interpretasi norma dan prinsip hukum contohnya adalah literatur hukum terbaru dan regulasi tahun 2016 yang mengatur penyelenggaraan informasi dan aktivitas elektronik metode ini dipilih karena bisa mengidentifikasi norma prinsip, dan teori undang-undang yang relevan untuk melindungi korban penetasan WhatsApp di Indonesia.

Data penelitian ini dikumpulkan melalui penelitian pustaka yang mencakup peraturan perundang-undangan, artikel, jurnal, dan buku yang relevan serta analisis oleh Khasanah dan Sutabri (2023) tentang modus dan perlindungan korban penetasan whatsapp.[12] Semua informasi tersebut dianalisis secara kualitatif untuk menginterpretasikan konsep dan standar hukum yang relevan.

Proses analisis dilakukan dengan menginterpretasikan doktrin dan peraturan hukum lalu membandingkannya dengan berbagai teori regulasi dan menilai seberapa efektif perlindungan hukum cyber dalam praktik sehingga metode ini memberi penulis kesempatan untuk membuat rencana dan kebijakan untuk memperkuat perlindungan hukum secara sistematis dan terencana.

Hasil dan Pembahasan

Bentuk dan modus operandi tindak akses tanpa hak (peretasan) terhadap aplikasi WhatsApp yang terjadi di Indonesia

a. WhatsApp Menjadi Target Utama Dalam Serangan Siber di Indonesia.

Masa digital memicu transformasi mendalam pada pola komunikasi antarindividu, melakukan bisnis, serta menjalankan birokrasi di Indonesia. Namun, kemajuan dalam teknologi digital juga meningkatkan risiko kejahatan siber yang dapat mengancam keamanan data dan privasi penggunanya. Perlindungan hukum di dunia digital semakin mendesak, terutama peningkatan kasus peretasan aplikasi, seperti WhatsApp, setiap tahunnya dapat merugikan korban baik secara finansial maupun non-finansial. Pemerintah diharapkan aktif melalui peraturan seperti UU ITE untuk memastikan hak-hak digital masyarakat terlindungi di tengah berbagai macam ancaman siber.

[12] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP."

WhatsApp dianggap sebagai sasaran utama serangan siber di Indonesia karena merupakan platform komunikasi utama di berbagai sektor, mulai dari individu hingga bisnis kecil dan lembaga publik. Fitur yang memungkinkan sinkronisasi antara perangkat dan penggunaan aplikasi web pada WhatsApp memudahkan akses namun juga meningkatkan risiko pembajakan yang dilakukan melalui teknik phising, penyadapan jaringan, atau penyebaran malware. Ketidakmampuan pengguna dalam literasi digital dan lemahnya sistem deteksi awal memudahkan pelaku kejahatan siber untuk menjadikan WhatsApp sebagai titik serangan utama mereka.

Dalam hal ini penting untuk melakukan analisis mendalam terhadap cara kerja peretasan WhatsApp agar dapat melindungi hak pengguna digital dari serangan yang terus berkembang. Dengan memetakan berbagai teknik serangan, seperti rekayasa sosial, phising menggunakan kode OTP, penyebaran aplikasi berbahaya, hingga eksploitasi QR code, upaya penegakan hukum dan pencegahan gangguan siber dapat dilakukan secara lebih efektif. Penelitian oleh Hidayah dan Amran (2023) dan Trianurahmah et al. (2025) menekankan perlunya reformasi regulasi, pembaruan teknologi, dan peningkatan edukasi digital yang didasarkan pada kajian kritis terhadap metode peretasan yang ada.[13]

b. Karakteristik Teknis dan Implikasi Sistem Aplikasi WhatsApp

Mekanisme pengamanan berlapis yang ditawarkan oleh aplikasi WhatsApp secara teknis memastikan bahwa pesan yang dikirim dan diterima tetap rahasia namun fitur sinkronisasi perangkat dan penggunaan kode QR untuk mengakses WhatsApp web memungkinkan serangan tambahan jadi teknik hijacking juga dikenal sebagai QR phising yang menggunakan kelengahan pengguna bisa mengambil alih akun dengan cepat jadi menurut penelitian yang dilakukan oleh Putra dan Sutabri (2023) kelemahan dalam pembaruan perangkat lunak dan perilaku pengguna memberikan peluang yang lebih besar bagi peretas untuk melakukan tindakan mereka Melalui aplikasi ini.[14] Penelitian oleh Hasanudin dan Babussalam (2024) WhatsApp menjadi populer di sektor pemerintahan untuk mengatur dan menyimpan informasi penting yang bisa dirusak oleh penetasan data dan sistem publik secara keseluruhan[15] .

c. Bentuk Modus Operandi Peretasan Aplikasi WhatsApp di Indonesia

Modus operasi peretasan aplikasi WhatsApp di Indonesia yaitu modus operandi utama penetasan WhatsApp di Indonesia adalah rekayasa sosial terutama penipuan OTP dan manipulasi psikologis. Penipu seringkali berpura-pura sebagai pejabat resmi, teman, atau lembaga yang dipercaya oleh korban untuk memperoleh kode OTP atau akses verifikasi akun WhatsApp secara tidak sah. Peniruan identitas sangat efektif karena memanfaatkan ketakutan, keyakinan anak, atau ketidaktahuan korban tentang kemungkinan membagikan data pribadi jadi alasan verifikasi, ancaman untuk memblokir akun tanpa tawaran hadiah digital yang meningkatkan kemungkinan korban menjadi target serangan adalah kombinasi

---

[13] Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp"; Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp."

[14] Putra and Sutabri, "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA."

[15] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking."

yang umum dari taktik manipulasi psikologis.

Di Indonesia phising juga merupakan teknik yang sering digunakan oleh kejahatan cyber WhatsApp serangan ini biasanya menggunakan tautan palsu maupun situs web palsu ataupun file APK berbahaya yang terlihat seperti aplikasi resmi atau pembaruan sistem setelah korban mengklik tautan atau menginstal file penyerang bisa mencuri token akses lalu informasi autentikasi atau bahkan mengendalikan akun Whatsapp korban sepenuhnya. Penelitian oleh Trianurahmah et al. (2025) menemukan peningkatan kasus phising melalui pesan promosi karena pemak undian, lowongan kerja palsu yang disebarkan secara luas dengan sengaja kepada ribuan pengguna dalam waktu singkat.[16]

Serangan sniffing dan penyadapan jaringan juga sering terjadi, terutama di tempat umum yang menyediakan Wi-Fi gratis atau jaringan yang tidak terenkripsi. Teknik ini memungkinkan penyerang menyadap komunikasi korban tanpa berinteraksi langsung lalu melacak lalu lintas pesan atau mencuri ID. Putra dan Sutabri (2023) menekankan bahwa bisnis atau lembaga yang menggunakan WhatsApp web di kantor atau cafe yang rentan terhadap penyadapan jaringan.[17]

Di Indonesia versus batasan menggunakan QR Code dan menggunakan WhatsApp web atau yang sering disebut sebagai phising semakin meningkat penyerang mengirimkan QR Code palsu atau tautan phising kepada korban yang mana saat akun Whatsapp korban dipindai atau diklik akan terhubung ke perangkat penyerang hal ini memungkinkan penyerang untuk mengakses semua pesan dan dokumen tanpa sepengetahuan korban jadi bisnis online dan layanan pelanggan berbasis WhatsApp dilaporkan banyak menggunakan taktik ini.

Selain itu eksploitasi zero day dan penyadapan melalui aplikasi pihak ketiga juga mulai menjadi ancaman yang nyata di dunia cyber. Eksploitasi zero day memanfaatkan celah keamanan yang belum terdeteksi atau diperbaiki oleh pengembang aplikasi sehingga memungkinkan pelaku untuk mengakses data kemudian merekam pesan atau menggandakan akun tanpa meninggalkan jejak digital yang jelas penelitian oleh Hidayah dan Amran (2023) menemukan bahwa dalam industri perbankan telah terjadi kasus pencurian salinan pesan dan transaksi digital ini dimulai dengan pembajakan akun Whatsapp pelaku usaha atau nasabah.[18]

Pola kejahatan digital kolaboratif juga mencakup modus sinkronisasi perangkat ilegal dan penyebaran malware. Pelaku mengaktifkan fitur sinkronisasi pada perangkat korban tanpa izin melalui eksploitasi atau aplikasi berbahaya, kemudian menyebarkan malware untuk mencuri data dan memantau aktivitas korban secara terus-menerus. Khasanah dan Sutabri (2023) menemukan bahwa UMKM sering menggunakan metode ini mereka

[16] Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp."
[17] Putra and Sutabri, "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA."
[18] Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp."

menggunakan WhatsApp untuk menyimpan data pelanggan dan korespondensi.[19]

Menurut studi kasus yang diambil dari laporan tahunan anak rumah berita Media, dan artikel ilmiah semua metode yang disebutkan di atas bisa digunakan bersamaan dalam pelanggaran hukum. Sebuah contoh yang sering terjadi adalah sekelompok penggiat bisnis skala mikro hingga menengah yang pertama kali menjadi korban penipuan melalui tautan phishing kemudian berlanjut dengan sinkronisasi perangkat ilegal dan pencurian data konsumen dalam skala besar Oleh karena itu undang-undang dan teknologi deteksi awal harus tetap diperbaharui agar bisa mengantisipasi sepenuhnya peretasan WhatsApp di Indonesia.

d. Faktor Penyebab Peretasan Aplikasi WhatsApp di Indonesia

Kesalahan manusia terutama kurangnya pengetahuan digital mempengaruhi kerentanan individu terhadap peretasan WhatsApp di Indonesia banyak pengguna masih belum menyadari risiko berbagai data perlunya mengaktifkan fitur keamanan ganda dan risiko membuka file atau tautan dari sumber yang tidak jelas. Penelitian oleh Khasanah dan Sutabri (2023) serta Trianurahmah et al. (2025) menunjukkan bahwa faktor psikologis, seperti kepanikan, kepercayaan berlebih, atau kurangnya pengetahuan teknis sering kali dimanfaatkan oleh pelaku melalui metode rekayasa sosial, sehingga membuat korban mudah terjebak oleh kode OTP dan tautan phishing.[20] Dampak psikologis bagi korban, termasuk perasaan malu, tekanan mental, dan trauma akibat kehilangan informasi penting, semakin memperburuk dampak kerugian yang dihasilkan oleh kejahatan digital.

Secara hukum, kecenderungan korban untuk mengabaikan protokol keamanan juga dipengaruhi oleh rendahnya pemahaman hukum dan minimnya pendidikan tentang keamanan siber di sekolah, komunitas, dan tempat kerja. Hidayah dan Amran (2023) menyebutkan bahwa undang-undang mengenai siber mengharuskan pengguna untuk berhati-hati dan secara aktif melindungi privasi digital mereka.[21] Namun, banyak korban yang belum memahami kewajiban serta hak yang mereka miliki dalam menjaga data digital serta mengelola keamanan akun WhatsApp mereka. Penelitian oleh Hasanudin dan Babussalam (2024) menambahkan bahwa sebagian besar korban phishing keuangan berasal dari kalangan masyarakat dengan akses terhadap pendidikan digital yang sangat terbatas.[22] Pentingnya pendidikan dan penguatan kemampuan digital masyarakat sangat diperlukan untuk mengurangi jumlah korban yang terkena peretasan WhatsApp.

e. Praktik Penegakan Hukum dan Tantangan Yuridis

Studi tentang keputusan pengadilan di Indonesia menunjukkan bahwa kasus peretasan WhatsApp saat ini semakin sering diproses di Pengadilan Negeri dan Mahkamah Agung. Menurut analisis yang dilakukan oleh Khasanah dan Sutabri (2023), terdapat

[19] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP."

[20] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP"; Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp."

[21] Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp."

[22] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking."

berbagai keputusan dari Pengadilan Negeri dan Mahkamah Agung yang menjatuhi hukuman kepada pelaku peretasan akun WhatsApp, yang mencakup hukuman penjara hingga denda yang cukup besar.[23] Di beberapa kasus, pelaku yang terbukti mengambil alih akun melalui teknik rekayasa sosial atau penyadapan aplikasi dapat dikenakan Pasal 30 dan 32 UU ITE, seiring dengan pengakuan pengadilan terhadap bukti digital seperti log akses, rekaman pesan, atau hasil audit forensik sebagai alat bukti yang sah.

Proses untuk membuktikan kasus peretasan WhatsApp masih menghadapi berbagai tantangan dari aspek teknis dan hukum. Pengumpulan bukti digital yang valid, seperti metadata pesan, session ID akun, atau hasil forensik digital yang memerlukan kolaborasi yang kuat antara lembaga penegak hukum, penyedia aplikasi, dan laboratorium forensik digital. Penelitian oleh Trianurahmah et al. (2025) dan Hidayah dan Amran (2023) menekankan beberapa hambatan, seperti kurangnya ahli forensik digital di pengadilan, lambatnya respon penyedia terhadap permintaan data, serta sulitnya pelacakan pelaku yang bertransformasi lintas negara dengan menggunakan server asing.[24] Kendala ini secara langsung mempengaruhi keterlambatan dalam penegakan hukum dan sering kali menyebabkan hukuman yang ringan atau perkara yang gugur akibat kurangnya bukti elektronik yang kuat.

Selain tantangan dalam pembuktian, masalah lain yang mencolok adalah pelaksanaan pemulihan hak para korban dalam penegakan hukum. Meskipun undang-undang menyediakan ruang untuk ganti rugi dan restitusi, dalam kenyataannya, banyak korban mengalami kesulitan dalam merehabilitasi akun mereka, mengembalikan data, atau mendapatkan kompensasi untuk kerugian materiel. Hasanudin dan Babussalam (2024) menjelaskan bahwa dukungan dari penyelenggara aplikasi bagi korban peretasan WhatsApp masih sangat kurang, adanya keterbatasan dalam bantuan hukum, serta tidak adanya mekanisme yang efisien untuk mitigasi dan pemulihan setelah peretasan terjadi.[25] Banyak korban akhirnya memilih untuk tidak melapor atau menutup akun mereka karena proses litigasi yang terlalu panjang dan tidak menentu. Oleh karena itu, perbaikan sistem dukungan bagi korban kejahatan digital dan forensik digital perlu menjadi prioritas utama dalam memperkuat keadilan hukum di era digital.

Pengaturan hukum positif di Indonesia dalam memberikan perlindungan terhadap tindak akses tanpa hak (peretasan) pada aplikasi WhatsApp

Pengaturan hukum positif di Indonesia terkait akses ilegal terhadap sistem elektronik, termasuk aplikasi WhatsApp, diatur pada peraturan 2008 terkait informasi dan transaksi digital yang diperbarui oleh legislasi 2016, khususnya aturan mulai Pasal 32 UU ITE secara tegas melarang individu untuk secara sadar dan tanpa otorisasi memasuki, merusak, atau melakukan penyadapan pada platform digital pihak lain. Fernando dan Putra (2025) mengungkapkan bahwa pelanggaran terhadap privasi dan penyalahgunaan informasi

[23] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP."

[24] Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp"; Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp."

[25] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking."

pribadi adalah salah satu jenis viktimisasi digital yang serius, karena data para korban dapat diretas, disebarkan, atau dimanfaatkan untuk penipuan, sehingga sangat penting untuk memiliki regulasi dan praktik perlindungan data yang tanggap terhadap kebutuhan para korban.[26] Ancaman pidana untuk pelanggaran hukum ini dijelaskan dalam Pasal 46 UU ITE, yang memberikan hukuman penjara dan/atau denda bagi pelanggar yang melakukan akses tanpa hak.

Budiyanto (2025) menjelaskan bahwa upaya untuk mengatasi kejahatan siber di Indonesia tidak hanya bergantung pada UU ITE, tetapi juga mengacu pada ketentuan yang ada dalam KUHP serta peraturan perundang-undangan lainnya yang berhubungan, sehingga penegakan hukum dalam menghadapi cybercrime bersifat menyeluruh dan saling mendukung.[27] Hidayah dan Amran (2023) menambahkan dalam perkembangan teknologi komunikasi, kejahatan seperti peretasan pada aplikasi WhatsApp sering terjadi melalui penyadapan, pengambilalihan akun, atau penyalahgunaan data pengguna yang kemudian digunakan untuk aktivitas kriminal seperti penipuan digital.[28]

Unsur-unsur dari kejahatan akses tanpa hak menurut UU ITE meliputi kesengajaan (mens rea), melakukan akses terhadap sistem elektronik tanpa izin yang sah, serta objek yang merupakan sistem elektronik yang dimiliki oleh orang lain. Khasanah dan Sutabri (2023) menyatakan bahwa peretasan pada aplikasi WhatsApp adalah pelanggaran terhadap privasi serta keamanan data karena pelaku berusaha mengakses informasi atau komunikasi pribadi tanpa persetujuan dari pemilik akun.[29] Pandangan ini sejalan dengan pendapat Trianurahmah et al. (2025) yang mencatat bahwa ancaman phishing melalui aplikasi WhatsApp termasuk dalam ranah kejahatan siber yang berbasis rekayasa sosial, di mana pelaku mencoba mendapatkan akses ilegal ke akun korban dengan menggunakan manipulasi psikologis.[30]

Di samping itu, dalam konteks hukum nasional Indonesia, pengaturan mengenai akses tanpa hak juga ditemukan dalam ketentuan lain, seperti Kitab Undang-Undang Hukum Pidana (KUHP) serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Beberapa ketentuan dalam KUHP, seperti yang mengatur tentang pencurian (Pasal 362) dan penipuan (Pasal 378), dapat diterapkan secara analog terhadap tindakan peretasan yang menyebabkan penguasaan data atau informasi secara ilegal. Sementara itu, PP No. 71 Tahun 2019 mewajibkan penyelenggara sistem elektronik untuk menjaga kerahasiaan, integritas, dan ketersediaan data pengguna dan menetapkan tanggung jawab hukum jika terjadi pelanggaran atau

---

[26] "Cyber Victimology Memahami Korban Di Era Digital - Dr. Zico Junius Fernando, S.H., M.H.; Dr. Panca Sarjana Putra, S.H., M.H.," *Rajagrafindo Persada*, n.d., accessed November 25, 2025, https://www.rajagrafindo.co.id/produk/cyber-victimology-memahami-korban-di-era-digital-dr-zico-junius-fernando-s-h-m-h-dr-panca-sarjana-putra-s-h-m-h/.

[27] S. H. Dr. Budiyanto, "Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia," Text.Chapter, Sada Kurnia Pustaka, accessed November 25, 2025, https://repository.sadapenerbit.com/index.php/books/catalog/view/205/586/247.

[28] Nur Hidayah and Amran, "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp."

[29] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP."

[30] Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp."

kebocoran data.[31] Menurut Wibowo (2024), efektivitas penegakan hukum dalam kasus akses tanpa hak sangat tergantung pada kolaborasi antara regulasi hukum siber dan penerapan sistem keamanan informasi berbasis teknologi yang kokoh.[32]

Upaya dan strategi peningkatan perlindungan hukum bagi korban tindak akses tanpa hak (peretasan) terhadap aplikasi WhatsApp di Indonesia

Peningkatan perlindungan hukum untuk korban akses ilegal (peretasan) di aplikasi WhatsApp di Indonesia memerlukan pendekatan menyeluruh dengan memperhatikan literasi digital, tindakan pencegahan, respon hukum, regulasi, serta kolaborasi antar sektor. Khasanah dan Sutabri (2023) berpendapat bahwa langkah perlindungan awal dapat dimulai dengan meningkatkan literasi digital masyarakat, seperti membiasakan penggunaan fitur keamanan dua langkah, mengedukasi pengguna mengenai modus phising, serta menekankan pentingnya menjaga kerahasiaan kode verifikasi untuk mendorong upaya pencegahan secara mandiri di kalangan pengguna.[33] Hasil penelitian Trianurahmah et al. (2025) juga menekankan pentingnya edukasi dan sosialisasi mengenai bahaya peretasan serta pelatihan deteksi phising yang harus diberikan oleh pemerintah dan penyelenggara aplikasi.[34]

Selanjutnya, peran yang optimal dari pemerintah, penegak hukum, dan penyedia sistem sangat penting. Menurut Saepudin (2025) pencegahan kejahatan siber perlu dilakukan tidak hanya dengan menghukum pelakunya, tetapi juga dengan meningkatkan kemampuan aparat penegak hukum, membangun unit khusus untuk menangani kejahatan siber, dan memperkuat kerja sama antara kepolisian, kementerian terkait, dan lembaga keamanan siber nasional.[35] Wibowo (2024) serta Putra dan Sutabri (2023) menekankan perlunya pemerintah untuk memperkuat regulasi, meningkatkan kemampuan penyidik, serta menerapkan penegakan hukum yang efektif.[36] Selain itu, penyedia aplikasi seperti WhatsApp perlu memberikan mekanisme deteksi awal dan pemulihan akun yang mudah, serta memperkuat fitur keamanan data sesuai dengan kebijakan privasi baik di tingkat global maupun nasional.

Dalam menangani korban, Hasanudin dan Babussalam (2024) mengungkapkan bahwa prosedur yang sederhana bagi korban untuk melaporkan insiden, sistem pemulihan akun yang cepat, serta pemulihan kondisi bagi pengguna yang mengalami kerugian baik secara psikologis maupun finansial sangatlah penting.[37] Di samping itu, kolaborasi inovatif antara Kemenkominfo, kepolisian, lembaga pemerintah, LSM, WhatsApp/Meta sangat diperlukan untuk mendorong koordinasi dalam deteksi, penanganan kasus, sosialisasi, serta

[31] "Peraturan Pemerintah Nomor 71 Tahun 2019," accessed November 15, 2025, https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019.
[32] "Hukum Siber Dan Keamanan Informasi."
[33] Khasanah and Sutabri, "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP."
[34] Trianurahmah et al., "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp."
[35] "Hukum Cyber Crime Di Indonesia - Dr. (HC). Acep Saepudin, S.H.I., S.H.," *Rajagrafindo Persada*, n.d., accessed November 25, 2025, https://www.rajagrafindo.co.id/produk/hukum-cyber-crime-di-indonesia-dr-hc-acep-saepudin-s-h-i-s-h/.
[36] "Hukum Siber Dan Keamanan Informasi"; Putra and Sutabri, "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA."
[37] Akhmad Fery Hasanudin and A Basuki Babussalam, "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking."

pengembangan teknologi untuk keamanan digital.

Dalam hal regulasi, penyesuaian terhadap standar perlindungan data dan privasi secara adaptif sangat perlu dilakukan. Sulubara et al. (2025) menekankan penanganan kejahatan siber dan perlindungan bagi korban tidak bisa hanya bergantung pada hukum pidana, namun memerlukan pendekatan yang melibatkan berbagai disiplin ilmu, seperti meningkatkan kesadaran masyarakat, memperkuat sistem keamanan teknologi, dan membangun kolaborasi di skala nasional serta internasional untuk menghadapi sifat kejahatan siber yang melintasi batas negara.[38] Wibowo (2024) menambahkan bahwa perubahan aturan agar sesuai dengan praktik terbaik internasional dan perkembangan modus peretasan menjadi kunci untuk perlindungan jangka panjang.[39] Pentingnya harmonisasi regulasi cyberlaw Indonesia dengan prinsip perlindungan data dan keamanan informasi global.

Judijanto dan Nugroho (2025) merekomendasikan agar semua pemangku kepentingan melakukan pembaruan regulasi perlindungan data secara berkala, meningkatkan kolaborasi antar institusi, serta membentuk satuan tugas khusus untuk menangani kejahatan siber agar perlindungan terhadap korban dapat selalu beradaptasi mengikuti perubahan ancaman digital yang begitu cepat.[40]

Kesimpulan

1. Peretasan akun WhatsApp di Indonesia menggambarkan kelemahan mendasar dalam sistem keamanan siber, yang disebabkan oleh gabungan masalah teknis pada fitur sinkronisasi serta penggunaan QR code, ditambah rendahnya pemahaman mengenai keamanan digital di berbagai tingkat masyarakat. Penemuan terkait banyaknya tindakan rekayasa sosial, pencurian OTP, penyadapan jaringan, quishing, dan penyalahgunaan aplikasi pihak ketiga menunjukkan bahwa WhatsApp telah menjadi saluran utama bagi serangan yang mempengaruhi individu, pelaku bisnis, dan lembaga publik. Dalam aspek hukum, meskipun ada kerangka peraturan seperti UU ITE yang memberikan dasar untuk penegakan hukum, pelaksanaannya masih terhambat oleh kesulitan dalam membuktikan bukti elektronik, kekurangan sumber daya forensik digital, dan proses pemulihan hak korban yang belum maksimal. Oleh karena itu, penelitian ini menekankan pentingnya meningkatkan pengelolaan keamanan digital melalui penyusunan ulang kebijakan, pengembangan kemampuan aparat penegak hukum, serta perlunya pendidikan literasi digital sebagai syarat untuk melindungi hak-hak pengguna WhatsApp di Indonesia.

2. Pengaturan hukum di Indonesia menganggap akses tanpa izin ke aplikasi WhatsApp sebagai kejahatan cyber yang mengancam kerahasiaan, integritas, dan ketersediaan sistem elektronik menurut uu ite khususnya pasal 30, 32, dan 46 bisa mengakses selalu

[38] Seri Mughni Sulubara et al., *PERLINDUNGAN HUKUM TINDAK PIDANA CYBERCRIME DALAM CYBERLAW DI INDONESIA: PERKEMBANGAN TEKHNOLOGI DAN TANTANGAN HUKUM DALAM MEWUJUDKAN CYBERSECURITY*, n.d.

[39] "Hukum Siber Dan Keamanan Informasi."

[40] Loso Judijanto and Budi Nugroho, "Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia," *Sanskara Hukum Dan HAM* 3, no. 03 (2025): 118–24, https://doi.org/10.58812/shh.v3i03.544.

mengubah ataupun menyadap sistem elektronik tanpa izin termasuk penetasan dan pengambilan akun Whatsapp bisa dikenakan hukuman penjara atau denda pensil ini diperkuat oleh ketentuan dalam KUHP dan PP 71 tahun 2019 mengenai penyelenggaraan sistem dan transaksi elektronik yang menegaskan bahwa penyelenggaraan sistem elektronik bertanggung jawab untuk menjaga keamanan data dan menetapkan sanksi hukum untuk tindakan pencurian, penipuan, kebocoran data yang dilakukan oleh orang yang memiliki akses ilegal ke data. Oleh karena itu undang-undang nasional pada dasarnya telah menyediakan alat yang cukup untuk melindungi pengguna Whatsapp dari peretasan namun penegakan hukum yang kuat, kekuatan aparat, dan infrastruktur keamanan informasi yang memadai masih menjadi Kunci keberhasilan.

3. Meningkatkan perlindungan hukum bagi orang-orang di Indonesia yang menjadi korban penetasan WhatsApp memerlukan strategi komprehensif yang mencakup peningkatan literasi digital, perbaikan peraturan, dan pengakuan penegakan hukum dengan adanya penyediaan instruksi menyeluruh tentang fitur keamanan dan teknik fishing serta rekayasa sosial harus diikuti dengan penyediaan sistem pelaporan dan pemulihan akun yang mudah, cepat, dan berpusat pada kebutuhan korban. Untuk menjamin bahwa hak-hak korban yang memiliki akses tanpa izin ke aplikasi WhatsApp terlindungi peraturan cyber harus disesuaikan dengan standar perlindungan data internasional sehingga meningkatkan kemampuan aparat penegak hukum dan membentuk tim khusus untuk menangani kejahatan cyber.

Saran

1. Pemerintah dan lembaga penegak hukum harus meningkatkan pelaksanaan undang-undang ite dan PP 71 tahun 2019 termasuk meningkatkan kemampuan forensi digital untuk menyelidiki kasus peretasan WhatsApp.
2. Pengelola aplikasi WhatsApp disarankan untuk membuat fitur deteksi awal lalu sistem pemulihan akun yang cepat dan layanan bantuan khusus untuk pengguna Indonesia yang menjadi korban peretasan.
3. Program literasi dan edukasi digital harus diperluas di sekolah, komunitas standar tempat kerja untuk meningkatkan pemahaman tentang teknik social Engineering, phising OTP tanda quishing, dan malware.
4. UMKM, lembaga publik, dan pelaku bisnis perlu menerapkan standar keamanan dalam organisasi seperti memakai perangkat yang resmi kemudian melakukan pemutaran sistem secara berkala lalu menggunakan autentikasi ganda serta menerapkan prosedur standar saat memakai WhatsApp web.
5. Pembentukan tim khusus atau pusat koordinasi kejahatan cyber yang melibatkan kemenkominfo, kepolisian, lembaga pemerintah, organisasi non pemerintah, dan sektor swasta sangat dibutuhkan untuk berbagi data insiden dengan melakukan sosialisasi serta menangani masalah secara bersama-sama.
6. Akademisi dan peneliti perlu terus mendorong studi empiris mengenai pola penetasan WhatsApp dan efektivitas kebijakan yang ada sebagai dasar penyusunan rekomendasi kebijakan yang lebih sesuai dengan kondisi di lapangan.

DAFTAR PUSTAKA

JURNAL:

Akhmad Fery Hasanudin and A Basuki Babussalam. "Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking." *Jurnal Gagasan Hukum* 6, no. 01 (2024): 16–29. https://doi.org/10.31849/jgh.v6i01.18827.

Judijanto, Loso, and Budi Nugroho. "Regulasi Keamanan Siber Dan Penegakan Hukum Terhadap Cybercrime Di Indonesia." *Sanskara Hukum Dan HAM* 3, no. 03 (2025): 118–24. https://doi.org/10.58812/shh.v3i03.544

Khasanah, Nurul, and Tata Sutabri. "ANALISIS KEJAHATAN CYBERCRIME PADA PERETASAN DAN PENYADAPAN APLIKASI WHATSAPP." *Blantika: Multidisciplinary Journal* 1, no. 2 (2023): 44–55. https://doi.org/10.57096/blantika.v1i2.13.

Nur Hidayah and Amran. "Tinjauan Yuridis Tindak Pidana Penipuan Social Engineering Pada Nasabah Perbankan Melalui Aplikasi Chat Whatsapp." *Jurnal Pustaka Cendekia Hukum Dan Ilmu Sosial* 1, no. 1 (2023): 116–27. https://doi.org/10.70292/pchukumsosial.v1i1.43.

Putra, Yusuf Andi, and Tata Sutabri. "ANALISIS PENYADAPAN PADA APLIKASI WHATSAPP DENGAN MENGGUNAKAN METODE SINKRONISASI DATA." *Blantika: Multidisciplinary Journal* 1, no. 2 (2023): 132–41. https://doi.org/10.57096/blantika.v1i2.8.

Trianurahmah, Adinda, Achmad Fauzi, Eling Norma Tyas, Muhammad Afif Suryanto, Muhammad Rizky, and Pandu Wibisono. "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Link." *Orbit : Jurnal Ilmu Multidisiplin Nusantara* 1, no. 2 (2025): 74–88. https://doi.org/10.63217/orbit.v1i2.81.

Buku

"Cyber Victimology Memahami Korban Di Era Digital - Dr. Zico Junius Fernando, S.H., M.H.; Dr. Panca Sarjana Putra, S.H., M.H." *Rajagrafindo Persada*, n.d. Accessed November 25, 2025. https://www.rajagrafindo.co.id/produk/cyber-victimology-memahami-korban-di-era-digital-dr-zico-junius-fernando-s-h-m-h-dr-panca-sarjana-putra-s-h-m-h/.

*CYBER-LAW (*ISBN: 978-623-8345-05-2)*. n.d. Accessed November 15, 2025. https://buku.sonpedia.com/2023/07/cyber-law.html.

Dr. Budiyanto, S. H. "Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia." Text.Chapter. Sada Kurnia Pustaka. Accessed November 25, 2025. https://repository.sadapenerbit.com/index.php/books/catalog/view/205/586/247.

"Hukum Cyber Crime Di Indonesia - Dr. (HC). Acep Saepudin, S.H.I., S.H." *Rajagrafindo Persada*, n.d. Accessed November 25, 2025. https://www.rajagrafindo.co.id/produk/hukum-cyber-crime-di-indonesia-dr-hc-acep-saepudin-s-h-i-s-h/.

"Hukum Siber Dan Keamanan Informasi." n.d. Accessed November 15, 2025. https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_AsODON7rWAAumI-eyUfM-KqX7dg_crFXgDCn9z-EkA7XoNcA_H7XTA_1731900608.pdf.

Prasetiyo, Sofyan Mufti, Rehan Gustiawan, and Fabian Rizzel Albani. *Analisis Pertumbuhan Pengguna Internet Di Indonesia*. 2, no. 1 (2024).

Sulubara, Seri Mughni, Virdyra Tasril, S Kom, and M Kom. *PERLINDUNGAN HUKUM TINDAK PIDANA CYBERCRIME DALAM CYBERLAW DI INDONESIA: PERKEMBANGAN TEKHNOLOGI DAN TANTANGAN HUKUM DALAM MEWUJUDKAN CYBERSECURITY*. n.d.

Sumber Elektronik

CIO Healthcare Indonesia. "Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI." Accessed November 15, 2025. http://ciohealthcare.or.id/berita/ancaman-digital-2025-serangan-siber-ri.

databoks.katadata.co.id. "Pengancaman, Jenis Serangan Digital Terbanyak di RI pada Kuartal III 2025 | Pusat Data Ekonomi dan Bisnis Indonesia | Databoks." Accessed November 15, 2025. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/691164464058b/pengancaman-jenis-serangan-digital-terbanyak-di- ri-pada-kuartal-iii-2025.

"Laporan Tahunan Kamsiber 2024." n.d. Accessed November 15, 2025. https://csirt.komdigi.go.id/storage/uploads/document_centers/attachments/Laporan%20Tahunan%20Kamsiber%202024.pdf.

"Peraturan Pemerintah Nomor 71 Tahun 2019." Accessed November 15, 2025. https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+ta hun+2019.