Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105




# Implementasi GDPR Untuk Mengatasi Kekosongan Hukum Tindak Pidana *Phishing* Melalui Whatsapp di Indonesia

## *Implementation of GDPR in Addressing the Legal Vacuum On Phishing Crimes via WhatsApp in Indonesia*

**Ivanna Damai Prasetyaningtyas, Luthfillah Arrizqi Zainsyah**
Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia
ivanna.23631@mhs.unesa.ac.id

***Abstract***

*This article examines the legal regulation of phishing crimes conducted via WhatsApp in Indonesia and evaluates the relevance of the General Data Protection Regulation (GDPR) as a normative model for strengthening personal data protection. Although Indonesia has established a legal framework through the Criminal Code, the Electronic Information and Transactions Law, and Law Number 27 of 2022 on Personal Data Protection, these instruments do not specifically regulate preventive mechanisms, data controller obligations, or victim remedies for phishing based on social engineering. This study employs a normative juridical method using statutory, conceptual, and case approaches, including an analysis of the Pekanbaru District Court Decision Number 958/Pid.Sus/2020/PN.Pbr. The findings indicate that Indonesia's regulatory framework remains fragmented and predominantly punitive, limiting its effectiveness in addressing evolving digital phishing practices. In contrast, the GDPR provides a more preventive and accountable model through mandatory risk assessments, the appointment of Data Protection Officers, data breach notification requirements, and independent supervisory authorities. The novelty of this study lies in identifying regulatory gaps within Indonesian law and proposing a GDPR-based normative framework to enhance personal data protection against WhatsApp-based phishing crimes.*
***Keywords:*** *Criminal; Law; Phishing; Protection; WhatsApp*

**Abstrak**

Artikel ini menganalisis pengaturan hukum tindak pidana *phishing* melalui aplikasi WhatsApp di Indonesia serta menilai relevansi prinsip General Data Protection Regulation (GDPR) sebagai model normatif untuk memperkuat perlindungan data pribadi. Meskipun Indonesia telah memiliki dasar hukum melalui KUHP, Undang-Undang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, regulasi tersebut belum secara spesifik mengatur mekanisme pencegahan, pengendalian data, dan pemulihan hak korban *phishing* berbasis social engineering. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, termasuk analisis Putusan Pengadilan Negeri Pekanbaru Nomor 958/Pid.Sus/2020/PN.Pbr. Hasil penelitian menunjukkan bahwa kerangka hukum nasional masih bersifat fragmentaris dan represif, sehingga belum mampu merespons karakter kejahatan *phishing* yang berkembang secara digital. Sebaliknya, GDPR menawarkan model perlindungan yang lebih preventif melalui kewajiban *Data Protection Impact Assessment*, penunjukan *Data Protection Officer*, mekanisme notifikasi pelanggaran data, serta pengawasan oleh otoritas independen. Kebaruan artikel ini terletak pada pemetaan kekosongan norma dalam hukum nasional dan perumusan model penguatan perlindungan data pribadi berbasis prinsip GDPR yang adaptif terhadap kejahatan *phishing* melalui WhatsApp.
**Kata kunci:** Hukum; *Phishing*; Perlindungan; Pidana; WhatsApp

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



## 1. PENDAHULUAN

Peningkatan penggunaan WhatsApp sebagai media komunikasi turut diiringi oleh meningkatnya serangan *phishing* yang menggunakan media rekayasa social untuk memperoleh data pribadi secara illegal, sehingga menimbulkan kerentanan baru terkait masalah siber masyrakat Indonesia.[1] Serangan *phishing* ini tidak hanya muncul melalui tautan palsu yang disebarkan via pesan atau undangan digital, tetapi juga melalui panggilan yang ditujukan kepada korban dengan berbagai macam modus lainnya didalamnya.[2] Dengan ini pencurian data pribadi korban dapat dengan mudah terjadi dan potensi kerugian material ataupun dampak psikologis yang timbul didalamnya.Sebelum lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), regulasi terkait data pribadi masih tersebar dalam berbagai peraturan, seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya. Meskipun Indonesia telah memiliki KUHP,UU ITE,dan UU PDP ketiga regulasi tersebut belum mengatur secara spesifik mekanisme pencegahan,pertanggungjawaban atas pengendalian data,serta perlindugan korban *phishing*, sehingga menimbulkan kekosongan norma dalam kejahatan berbasis rekayasa social melalui WhatsApp, dan kekosongan hukum ini menjadi masalah utama yang hendak diselesaikan pada artikel ini.

Penelitian sebelumnya masih membahas *phishing* dan perlindungan data pribadi secara parsial. Muhammad menyoroti pasal-pasal dalam KUHP dan UU ITE yang secara tidak tegas menjerat pelaku penipuan berbasis *phishing* dan lemahnya perlindungan bagi korban, namun dalam penilitiannya tidak menelaah konteks *phishing* melalui WhatsApp ataupun relevasinya dengan UU PDP.[3] Trianurahmah mengkaji pola kejahatan *phishing* pada aplikasi WhatsApp, namun dalam penilitiannya tidak menghubungkannya dengan kerangka hukum nasional maupun potensi adopsi GDPR.[4] Sementara itu khansa menekankan urgensi dari pembentukan otoritas pengawas independent dalam konteks UU PDP, tetapi belum mengaikan kelembagaan tersebut dengan karakteristik kejahatan siber seperti *phishing*.[5] Dengan demikian peneliti terdahulu hanya menelaah *phishing* dalam konteks criminal umum dan tidak secara komperhensif mengkaji keterkaitan anatara *phishing*, whatsapp, kelemahan hukum nasional terkait (KUHP,UU ITE,UU PDP), dan kemungkinan penerapan prinsip GDPR sebagai model normatif.

---

[1] Nur Jamal Sahid, "Apa Itu Phising? Definisi, Cara Kerja, Ciri-Ciri, Dan Cara Mencegahnya," kompas.com, 2022, https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya.

[2] "Ancaman Nyata Cyber Crime Dalam Bentuk Phising," RHP lawfirm, 2024.

[3] Faiz Emery Muhammad and Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *Jurnal USM Law Review* 6, no. 1 (2023): 226–41, https://doi.org/10.26623/julr.v6i1.6649.

[4] 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.

[5] Farah Naurah Khansa, "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Dalam Pelindungan Data Pribadi Di Indonesia," *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 649–62, https://doi.org/10.56370/jhlg.v2i8.114.

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



Berbeda dari peneliti terdahulu, artikel ini menawarkan kontribusi baru dengan analisis yang menghubungkan pengaturan nasional dengan prinsip-prinsip GDPR. Secara khusus juga menyoroti relevansi risiko tinggi (article 36 GDPR) dan kewajiban penunjuk *data Protection Officer* (article 37 GDPR) yang digunakan sebagai mekanisme preventif meninjau kekosongan hukum dalam perlindungan data pribadi korban *phishing* melalui WhatsApp. Kontribusi ini menekankan integrasi anatara hukum nasional dengan model regulasi internasional dalam merespons kejahatan siber berbasis rekayasa sosial. Dengan ini artikel dibuat dengan dasar tujuan untuk mengalisis pengaturan tindak pidana *phishing* melalui WhatsApp dalam KUHP,UU ITE, dan UU PDP; mengidentifikasi kekosongan hukum terkait pencegahan dan perlindungan korban; serta evaluasi relevansi dari prinsip GDPR sebagai memperkuat perlindungan data pribadi dengan model normatif.

## 2. METODE

Artikel ini merupakan artikel hukum normatif (*doctrinal research*) yang mengkaji norma,konsep hukum, dan kerangka regulasi tindak pidana *phishing* dan perlindungan data pribadi. Selain itu, artikel ini menggunakan pendekatan perundang-undangan (*statute approach*), untuk menelaah sinkronisasi dan kesesuaian antara KUHP, UU ITE, dan UU PDP dalam konteks penanggulangan tindak pidana *phishing*; pendekatan konseptual (*conceptual approach*), untuk memahami konsep-konsep hukum seperti "data pribadi", "akses tanpa hak", dan "*phishing*"; serta pendekatan kasus (*case approach*), melalui analisis Putusan Pengadilan Negeri Pekanbaru Nomor 958/Pid.Sus/2020PN.Pbr, yang merupakan salah satu putusan pengadilan yang mengadili tindak pidana *phishing* dangan tujuan memperoleh data pribadi korban melalui pembuatan situs palsu. Putusan itu dipilih sebagai contoh konkret peraktik penegakan hukum dan bagaimana pengadilan dalam menerapkan dengan UU ITE tehadap modus pencurian data pribadi. Bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer (peraturan perundang-undangan dan putusan pengadilan), bahan hukum sekunder (literatur akademik dan artikel jurnal), serta bahan hukum tersier, serta konstruksi argumentatif terhadap prinsip-prinsip GDPR—khususnya Article 36 tentang konsultasi risiko tinggi dan Article 37 tentang *Data Protection Officer*—sebagai model normatif untuk memperkuat perlindungan data pribadi dalam tindak pidana *phishing* melalui WhatsApp

## 3. HASIL DAN PEMBAHASAN

### 3.1 Pengaturan Tindak Pidana *Phishing* Yang Berkaitan Dengan Pencurian Dan Penyalahgunaan Data Pribadi Di Indonesia

Perkembangan penggunaan WhatsApp di Indonesia, yang kini hampir menjamah seluruh lapisan masyarakat, konsekuensi munculnya modus kejahatan siber dengan pola baru, yakni *phishing*. Modus ini biasanya dilakukan dengan menyebarkan tautan atau file yang seolah-olah resmi, misalnya undangan pernikahan digital,situs *platform online*, surat tilang elektronik ternyata palsu. Korban yang kurang berhati-hati akan mengunduh atau mengklik tautan tersebut, sehingga tanpa disadari memberikan akses terhadap data

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



pribadinya. Delik formil kejahatan *phishing* seperti ini tertuju pada pelaku yang mengakses perangkat milik orang lain tanpa izin atau secara illegal,[6] data pribadi inilah yang kemudian dicuri dan disalahgunakan, baik untuk penipuan, pengurasan rekening maupun untuk kejahatan lain seperti pemalsuan identitas.Sebagai negara hukum jamin negara dalam mengupayakan masyarakat mendapatkan kehidupan aman dan tentram. Dalam kehidupan masyarakat banyak ditemukan tindak pidana sehingga harus diterapkannya bentuk penegakan hukum yang efektif, agar keberadaan rasa aman dan tentram masyrakat dapat diperhatikan dengan baik.[7]

Bentuk pemidanaan terhadap pelaku kejahatan ini bertujuan untuk memberikan efek jera dan salah satu upaya bagi negara dalam menegakan keadilian di negara. Suatu perbuatan dapat dikategorikan sebagai tindak pidana apabila perbuatan tersebut dilarang dan diancam pidana oleh peraturan perundang-undangan yang berlaku.[8] Penjatuhan sanksi pidana hanya bisa dilakukan jika terdapat unsur kesalahan pada diri pelaku, sehingga ia dapat dimintai pertanggungjawaban hukum.

Pembentukan dan pembaruan regulasi hukum perlu diarahkan untuk menciptakan keseimbangan sosial (*social equilibrium*), yaitu tatanan kehidupan masyarakat yang tertib, adil, dan mampu menjamin kesejahteraan secara berkelanjutan.[9] Hukum positif Indonesia, *phishing* belum didefinisikan secara eksplisit sebagai tindak pidana. Namun, perbuatan ini dapat dijerat dengan beberapa perangkat hukum yang sudah ada, yaitu KUHP, UU ITE,dan UU PDP. Sebelum adanya pengaturan khusus yang secara eksplisit mengatur terkait perlindungan data pribadi seperti Undang-Undang No. 27 Tahun 2022 tentang perlindungan data pribadi dan peraturan tentang ITE dengan peraturan terbarunya dalam Undang-Undang No.1 Tahun 2024. Tindak pidana *Phishing* masuk kedalam kategori tindak pidana penipuan atau kejahatan terhadap kerugian ekonomi sebagaimana diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) lama, meskipun dalam KUHP lama tidak secara jelas diterangkan tentang *phishing*, karena masih terdapat keterbatasan normatif dalam menangkap karakter kejahatan *phishing* yang berbasis *social engineering*. namun beberapa pasal didalamnya dapat dijadikan dasar hukum yang berlaku untuk tindakan pelaku *phishing* karena mengandung unsur yang serupa dengan kejahatan *phishing* didalamnya.[10] Dalam KUHP lama dapat dikaitkan dengan Pasal 378 yang membahas tentang penipuan, yang modusnya pada *phishing* sering ditemukan aksi tipu muslihat dari pelaku kepada korbannya dengan berbagai modus kejahatan, dan Pasal 362 yang membahas tentang

[6] Subaidah Ratna Juita, Dhian Indah Astanti, and Dian Septiandani, "Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan Skimming," *Jurnal USM Law Review* 6, no. 1 (2023): 407–19, https://doi.org/10.26623/julr.v6i1.6353.

[7] "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," Pub. L. No. Pasal 1 Ayat (3 (n.d.).

[8] Andi Hamzah, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 2019).

[9] Arif Hidayat and Zaenal Arifin, "Politik Hukum Legislasi Sebagai Socio-Equilibrium Di Indonesia," *Jurnal Ius Constituendum* 4, no. 2 (2019): 147–59, https://doi.org/10.26623/jic.v4i2.1654.

[10] Afifah Sahfitri and Rosmalinda Rosmalinda, "Penipuan Digital Melalui Tautan Phishing," *Jurnal Dialektika Hukum* 6, no. 2 (2024): 211–28, https://doi.org/10.36859/jdh.v6i2.2881.

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



pencurian, walaupun KUHP lama tidak secara eksplisit mengakui data pribadi sebagai "barang", namun menurut Barda Nawawi Arief seiring perkembangan teknologi informasi yang menimbulkan perluasan objek perlindungan hukum pidana, termasuk data dan informasi elektronik sebagai bentuk kekayaan atau kepemilikan baru yang perlu dilindungi.[11] Sehingga data pribadi seperti nama, nomor telepon, atau informasi keuangan korban dianalogikan *sebagai theft of digital assets* yang dapat dicuri, meskipun secara tak berwujud.[12] Pengaturan mengenai tindak pidana pencurian data elektronik dalam KUHP Baru, fokus utama daripada KUHP baru untuk memberikan sanksi terhadap perbuatan yang mengakses, atau memanipulasi data elektronik milik orang lain yang mengakibatkan kerugian individu. tercantum dalam Undang-Undang Nomor 1 Tahun 2023, Pasal 332 sampai dengan Pasal 334, secara tegas undang-undang ini menyatakan bahwa siapa saja yang dengan sengaja dan tanpa hak menghancurkan, mengubah, mengambil, menguasai, atau menggunakan data elektronik milik orang lain bisa dikenai pidana. Dalam KUHP masih memiliki kelemahan mendasar dengan tidak memberikan definisi khusus mengenai *phishing*, sehingga modus kejahatan dengan manipulasi psikologis dan pemalsuan identitas digital pelaku tidak selalu memenuhi unsur penipuan dan pencurian materiil[13], disisi lain data pribadi belum diakui sebagai objek kejahatan sehingga bentuk pencurian data secara digital ini dianggap belum menimbulkan kerugian finansial dan berujung pemerosesan hukum yang rumit. Pada KUHP baru memperluas perlindungan terhadap data elektronik, dengan mencakup perihal akses tanpa hak, penggunaan tanpa izin, dan akses dengan tujuan memperoleh keuntungan finansial. Tetapi dalam KUHP baru fokus utamanya masih dalam lingkup akses dan penggunaan bukan pada tahap awal rekayasa social yang menjadi inti pada modus *phishing*.[14]

Undang-Undang No. 1 tahun 2024 Tentang Informasi dan Transaksi Elektronik (UU ITE) juga dapat mengatur tindak pidana *phishing*, karena undang-undang ini memang dibuat untuk menangani perkembangan teknologi informasi.keterkaitan *pidana (cyber crime)* termasuk *phishing* ada pada UU ITE. meskipun terdapat juga pada KUHP lama dan KUHP baru pasal-pasal yang dapat menjerat pelaku *phishing*. Dengan demikian keberlakukan asas "*lex specialis derogate legi generalis*" memiliki makna bahwa hukum khusus dapat mengalahkan hukum umum yang berlaku. Tetapi keberadaan UU ITE tidak memiliki pasal-pasal yang secara khusus mengatur terkait *phishing*, pasal yang mendekati unsur daripada *phishing* yang juga menjelaskan menipu dan menyesatkan korbannya tersebut. Terdapat pada Pasal 28 ayat (1) UU ITE mengatur tantang larangan penyebaran informasi elektronik yang merugikan orang lain (akses ilegal). Dalam konteks *cyber*

[11] Barda Nawawi Arief, *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya* (Jakarta: Kencana, 2018).
[12] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Westport, CT: Prager, 2010).
[13] Hamzah, *Asas-Asas Hukum Pidana*.
[14] Budiyanto, *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia* (Bandung: sada Karunia Pustaka, 2025).

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



*phishing*, pasal ini menjadi landasan hukum untuk menindak pelaku yang melakukan penipuan melalui media elektronik ketentuan ini bertujuan untuk memberi perlindungan hukum kepada korban dan menciptakan efek jera bagi pelaku.[15] Namun dalam UU ITE belum mengatur *phishing* sebagi delik khusus, sehingga modus manipulasi korban seringkali tidak memenuhi unsur dari pasal terkait. Penanggulangan tindak pidana penipuan seperti *phishing* yang akan datang memerlukan respon yang proaktif dari pemerintah dan lembaga terkait. Pembaharuan UU ITE menjadi penting untuk menyesuaikan dengan perkembangan teknologi dan modus operandi baru dari pelaku kejahatan siber.[16] Hal ini juga tercemin pada putusan PN Pekanbaru nomor 958/Pid.Sus/2020 dimana hakim menjatuhkan sanksi menggunakan pasal 35 UU ITE, padahal inti kejahatan ini merupakan kejahatan berbasis rekayasa sosial.[17] UU ITE juga tidak menyediakan terkait mekanisme pencegahan atau pemulihan bagi korban ataupun standar keamana aspek yang terlibat.

Selain melalui UU ITE 2024, pengaturan mengenai tindak pidana *phishing* yang melibatkan pencurian dan penyalahgunaan data pribadi juga berkaitan erat dengan Undang-Undang No. 27 Tahun 2022 Tentang perlindungan Data Pribadi (UU PDP). Undang-undang ini bisa dikatakan payung hukum utama yang memberikan perlindungan terhadap hak privasi individu dan memberikan kerangka hukum yang mewajibkan pengendali dan pemroses data untuk menerapkan langkah-langkah keamanan yang memadai guna melindungi data pribadi dari akses, pengungkapan, perubahan, dan penghapusan yang tidak sah.[18] Definisi Pasal 1 dan Pasal 4 UU PDP menegaskan bagimana bentuk data pribadi yang dimaksud dalam undang-undang ini, dapat dianalogikan informasi pribadi yang terdapat dalam aplikasi platform online termasuk WhatsApp, dengan demikian, tindakan pengumpulan, penggunaan, atau penyebaran data tanpa izin pemiliknya merupakan pelanggaran hukum.[19] Dampak dari *phishing* sangatlah merugikan dan dapat terjadi dalam berbagai bentuk. Salah satunya adalah kehilangan uang dalam jumlah yang signifikan. Penipu memiliki kemampuan untuk mengakses akun keuangan korban dan melakukan transaksi yang ilegal. Dengan berbagai modus manipulasi, begitu korban memberikan izin akses aplikasi atau perangkat, pelaku dapat mengambil data pada perangkat korban dan mengirimkannya ke *server* yang dikendalikan oleh penipu. Atau terdapat juga yang namanya teknik *man-in-the-middle* (MITM). Teknik ini memungkinkan peretas untuk melewati koneksi komunikasi antara keduanya tanpa harus melakukan autentikasi. Setelah

[15] H. Boma, "Pasal 28 Undang–Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Terhadap Perlindungan Korban Cyber Phising Perspektif Siyasah Tanfidziah (Studi Kasus Polres Mukomuko), Disertasi Doktoral" (UIN Fatmawati Sukarno Bengkulu, 2025).

[16] Naavi'u Emal Maaliki, "Kebijakan Hukum Pidana Sebagai Upaya Penanggulangan Tindak Pidana Penipuan Online," *Jurnal USM Law Review* 7, no. 3 (2024): 1409–18, https://doi.org/10.26623/julr.v7i3.10023.

[17] Pengadilan Negeri Pekanbaru, Pengadilan Negeri Pekanbaru Putusan Nomor 958/Pid.Sus/2020/PN Pbr (2020).

[18] Yuyut Prayuti, "Implications of Personal Data Protection Law in Consumer Health Data Management to Improve Secure and Confidential Handling in Indonesia," *Jurnal Ius Constituendum* 9, no. 3 (2024): 461–78, https://doi.org/10.26623/jic.v9i3.9289.

[19] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 168 (2022).

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



pelaku berhasil mengakses perangkat korban, mereka dapat membaca data yang anda kirimkan, memodifikasinya, atau menggunakannya untuk tujuan yang ilegal.[20] Pasal 65 hingga Pasal 67 UU PDP mengatur sanksi pidana atas penyalahgunaan data, pada praktik *phishing* melalui WhatsApp yang mencakup pengiriman file berformat *Android Package Kit* (APK) dengan tujuan mencuri data pribadi korban, seringkali tidak dapat ditangani secara optimal karena kekosongan norma pada tahap awal modus dengan aksi manipulasi.[21]

Melihat kekosongan pada KUHP,UU ITE, UU PDP sangat mempengaruhi dalam aspek perlindungan bagi korban, restitusi khusus bagi kerugian privasi korban sulit diperoleh karena data pribadi belum diakui sebagai objek kejahatan yang lengkap, tidak ada kewajiban notifikasi insiden, dan standar minimum untuk *platform digital*.[22] Pembuktiannya juga menjadi tantangan karena tidak ditemukan delik yang mengatur terkait *social engineering*, di mana pemulihan hak korban masih ditinjau berdasarkan kerugian materiil.[23] Dengan adanya kasus putusam PN Pekanbaru Nomor 958/Pid.Sus/2020PN.Pbr menjadi ilustrasi nyata terkait celah regulasi mempersulit apparat penegak hukum menjerat pelaku *phishing*, dengan ini juga menggambarkan kerangka hukum yang dimiliki Indonesia masih tertinggal, dan perlu terjadi reformulasi normatif adopsi prinsip perlindungan data pribadi internasional,seperti model GDPR dalam memperkuat perlindungan hukum terhadap korban *phishing*.[24]

### 3.2 Penegakan Hukum Tindak *Phishing* Melalui Whatsapp Persektif Hukum Pidana Perbandingan Dengan Hukum Uni Eropa

Penegakan hukum terhadap *phishing* melalui WhatsApp di Indonesia menghadapi tantangan serius karena belum ada hukum nasional pengaturan yang secara spesifik menangani tindakan ini, dengan indenfikasi kelemahan pada tidak adanya mekanisme pelaporan data dan pembentukan lembaga pengawas independent sebagaimana dalam praktik perlindungan data di Uni Eropa. Lingkup Internasional terkait perlindungan data pribadi terdapat di dalam *Universal Declaration of Human Rights* (UDHR), menegaskan pada Pasal 12 UDHR  Menjelaskan bahwasanya data pribadi adalah data dan informasi yang berkenaan dengan kehidupan individu serta berkaitan dengan konsep kerahasianaan atau hak privasi seseorang yang harus dijaga oleh perundang-undangan untuk mencapai kepastian dan keadilan.

[20] F. Bastian, "Bagaimana Cara Kerja Link APK Penipuan Yang Lagi Marak Sekarang Hingga Bisa Mengambil Data Kita," Quora Indonesia, diakses, 2025.

[21] Devi Anjheli, "Privasi Digital Dan Kejahatan Phishing Di Indonesia: Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP," *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2025): 165–89, https://doi.org/10.14421/990epf27.

[22] Zico Junius Fernando, Anis Widyawati, and Kasmanto Rinaldi, "Cyber Victimology and Legal Gaps in Southeast Asia," *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1–39, https://doi.org/10.15294/ildisea.v4i1.20147.

[23] Chandra Sekhar Bhusal, "Systematic Review on Social Engineering: Hacking by Manipulating Humans," *Journal of Information Security* 12, no. 01 (2021): 104–14, https://doi.org/10.4236/jis.2021.121005.

[24] Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security (Google EBook)* (USA: John Wiley & Sons, 2001).

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105




Dan menurut Menurut Thomass J.Smedinghoff ada tiga aspek dari privasi yaitu privasi mengenai pribadi seseorang (*Privacy of a Person's Persona*), privasi dari data tentang seseorang (*Privacy of Data About a Person*) dan privasi atas komunikasi seseorang (*Privacy of a Person's Communication*).[25] Dalam konteks internasional, best practice yang paling banyak diadopsi adalah *European Union General Data Protection Rules* (GDPR). GDPR berlaku untuk tiap aktivitas 'pemrosesan' atas 'data pribadi', sebagian atau sepenuhnya, oleh pengendali data (*controller*) maupun prosesor, dengan cara otomatis yang merupakan bagian dari sistem pengarsipan (*filing system*) atau dimaksudkan untuk menjadi bagian dari sistem pengarsipan.[26] Di sisi lain penerapan UU PDP terkait semua pihak swasta maupun publik, yang memproses data pribadi di wilayah hukum Indonesia atau yang menyangkut warga negara Indonesia. Konsep ini sejalan dengan prinsip *extraterritoriality* yang terdapat dalam GDPR, di mana entitas yang berada di luar Uni Eropa juga diwajibkan untuk mematuhi aturan tersebut jika mereka mengelola data warga negara Uni Eropa. Yang dimana masing-masing UU PDP dan GDPR juga sama-sama memiliki pengategorian data pribadi.[27] *Articlel 4 lid 1 AVG – Begripsbepalingen (Definities)* "Data pribadi' meruju pada identitas digital seseorang seperti IP address, aspek ini berkaitan karena dalam konteks *phishing* pada WhatsApp sering ditemukan kegiatan pengumpulan data pribadi korban oleh pelaku, dalam sistem hukum Indonesia melalui UU PDP cakupannya masih sempit dan belum mengatur identitas digital secara eksplisit, hal ini yang berpotensi menyulitkan pembuktian unsur kerugian pada kasus *phishing*.[28] Bentuk perlindungan preventif pada *Article* 36 yang mengatur bahwa pengendali data wajib melakukan konsultasi dengan otoritas pengawas apabila hasil *Data Protection Impact Assessment* (DPIA) menunjukkan kegiatan pemrosesan data terdapat risiko tinggi terhadap hak dan kebebasan individu,[29] dalam konteks *phishing* wajib aturannya untuk mengidentifikasi potensi ancaman keamanan data, seperti penggunaan *multi-factor authentication*, *anti-phishing filter*, dan diteksi aktivitas mencurigakan.[30] Indonesia tidak memiliki instrument preventif yang setara karena dalam UU PDP tidak mewajibkan DPIA,tidak mengatur konsultasi risiko tinggi, dan standar keamanan yang minimum. Hal seperti ini yang membuat insiden *phishing* semakin

[25] T. J. S. Smedinghoff, ed., *Online Laws: The SPA's Legal Guide to Doing Business on the Internet* (Canada: Addison-Wesley Developers Press, n.d.).

[26] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Pub. L. No. Regulation (EU) 2016/679 (2016).

[27] Siti Yuniarti, "Petugas/Pejabat Pelindungan Data Pribadi Dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa Dan Singapura," *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 4, no. 2 (2022): 111–20, https://doi.org/10.21512/becossjournal.v4i2.8377.

[28]European Union, *The General Data Protection Regulation* (Regulation [EU] 2016/679), *Official Journal of the European Union* (2016), Article 4.

[29] European Union, *The General Data Protection Regulation* (Regulation [EU] 2016/679), *Official Journal of the European Union* (2016), Article 36.

[30] European Data Protection Board, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' (WP248 Rev. 01)" (Brussels, 2017).

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



berkembang dan berkurangnya akuntabilitas terhadap data pengguna. *Article* 37 mewajibkan penunjukan *protection officer* yang melakukan pemantauan dan pemrosesan data sensitif. Perana DPO yaitu pengawasan dan tanggung jawab berkelanjutan dalam merespon ancaman *phishing* yang mengancam data pribadi.[31] Peranan DPO dalam konteks *phishing* dengan melaksanakan keamanan siber internal dan melaporkan insiden kebocoran data akibat *phishing* kepada otoritas dalam waktu 72 jam, sesuai dengan *Article* 33 GDPR.[32] Di Indonesia belum mengatur kewajiban DPO dan tidak memiliki standar pelaporan insiden data. Tidak adanya batas waktu pelaporan dan kewajiban langsung kepada korban, hal ini yang membuat korban *phishing* kehilangan akses atas pemulihan hak karena prosedur yang tidak jelas. Penegakan hukum terhadap kasus *phishing* dinilai lebih efektif bila sistem hukumnya memberikan kewenangan yang luas dan independen kepada *Autoriteit Persoonsgegevens* (AP) sebagai otoritas perlindungan data untuk melakukan penyelidikan, penindakan, hingga pemberian sanksi administratif,dengan mengeluarkan perintah pengamanan data, dan memberikan ganti rugi terhadap korban.[33]

Di Indonesia belum terbentuk lembaga pengawas independen dalam amanat UU PDP, dan sistem pengawasan saat ini masih pada kementrian komunikasi dan informatika, yang strukturalnya tidak independent. Kekosongan dalam aspek pengawasan independent ini membuat penegakan hukum *phishing* tidak efektif, karena tidak ada lembaga independent yang melakukan pengawasan dan investigasu secara langsung. Pada *Article* 17 *Recht op gegevenswissing (“recht op vergetelheid”),* menjelaskan hak untuk penghapusan (hak untuk dilupakan),dimana pemberian hak penghapusan data kepada individu yang data pribadinya sedang dirposes dengan tujuan melindungi privasi. Karena biasanya *phishing* bentuk pengumpulan data pribadi secara illegal.[34] Dan bilamana pemilik akun gagal menghapus data mereka bisa dikenakan sanksi hingga 20 juta EUR (dua puluh juta euro) sebagaimana yang dimaksud dalam *Article* 83 *Algemene voorwaarden voor het opleggen van administratieve geldboeten*, syarat keberlakuan denda administratif. Terdapat tanggungjawab yang ditegaskan disini.[35] Mengkriminalisasi akses illegal dan penipuan berbasi data dengan ancaman maksimum 4 tahun penjara. Indonesia memiliki skema dan denda melalui hukum nasional terkait, namun tidak adanya sanksi admintratif yang proposional serta tidak adanya ketentuan khusus mengenai *unlawful processing* yang menyebabkan pelaku *phishing* sulit dijera, dan didukung dengan pembuktian kerugian korban yang tidak eksplisit.

[31] European Union, *The General Data Protection Regulation* (Regulation [EU] 2016/679), *Official Journal of the European Union* (2016), Article 37.
[32] European Commission, “Data Protection Officer (DPO) Explained,” 2023.
[33] Autoriteit Persoongegevens, “Tax Administration Fined for Discriminatory and Unlawful Data Processing,” Autoriteit Persoonsgegevens, 2021.
[34] European Union, *The General Data Protection Regulation* (Regulation [EU] 2016/679), *Official Journal of the European Union* (2016), Article 17.
[35] European Union, *The General Data Protection Regulation* (Regulation [EU] 2016/679), *Official Journal of the European Union* (2016), Article 83.

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



Di Indonesia melihat rangkaian terkait pengaturan data pribadi, belum sepenuhnya mimiliki klasifikasi terhadap data pribadi yang dapat dilakukan penghapusan, dan konsep teknis terkait data pribadi belum mimiliki peraduran perundang-undangan yang mengikat. Tidak ada mekanisme terkait penghapusan data pribadi melainkan melalui putusan pengadilan, hal ini merujuk pada keterlibatan dari tidak adanya lembaga khusus dan independen yang tugasnya dalam aspek bidang pengawasan penggunaan data, serta tidak adanya standarisai *privacy policy* yang seragam jika dibandingkan dengan sanksi utama maupun sanksi tambahan sebagai pinalti yang diberikan atas kelalaian menjaga sitem elektronik pada GDPR Uni Eropa sangat jauh dari segi denda atau *fines* yang diberikan. Ditambah dalam aspek hak pemusnahan data pribadi sesuai dengan prinsip the *right to be forgotten* pada UU ITE masih sangan rumit dan terbelit-belit.[36] GDPR memberikan model pencegahan melalui Pasal 36 tentang konsultasi risiko tinggi dan Pasal 37 tentang *Data Protection Officer*. Indonesia harus mengintegrasikan ini ke dalam derivasi UU PDP dan pengawasan independen untuk melindungi lebih baik terhadap penyalahgunaan data, GDPR secara tegas mensyaratkan bahwa persetujuan tersebut harus "diberikan dengan bebas, spesifik, terinformasi, dan tidak ambigu," yang juga secara implisit diadopsi dalam Undang-Undang Perlindungan Data Pribadi.[37]

## 4. PENUTUP

Artikel ini menyimpulkan bahwa pengaturan hukum nasional terkait tindak pidana phishing melalui aplikasi WhatsApp masih belum memadai dalam memberikan perlindungan yang efektif bagi korban, karena belum adanya perumusan delik phishing secara spesifik, kewajiban preventif bagi pengendali data, serta mekanisme operasional pelaporan dan penanganan insiden kebocoran data. Meskipun KUHP, Undang-Undang ITE, dan Undang-Undang Perlindungan Data Pribadi telah menyediakan dasar normatif, ketiganya masih bersifat fragmentaris dan represif sehingga belum mampu merespons karakter kejahatan phishing yang berbasis social engineering. Melalui analisis komparatif dengan penerapan *General Data Protection Regulation* (GDPR) di Uni Eropa, artikel ini menunjukkan bahwa model perlindungan data yang preventif—melalui kewajiban konsultasi risiko tinggi, penunjukan *Data Protection Officer*, notifikasi kebocoran data dalam batas waktu tertentu, serta pengawasan oleh otoritas independen—lebih efektif dalam menjamin perlindungan hak subjek data. Kebaruan artikel ini terletak pada perumusan relevansi prinsip-prinsip GDPR sebagai acuan normatif untuk menutup kekosongan hukum dalam perlindungan korban phishing di Indonesia. Oleh karena itu, penelitian ini merekomendasikan penguatan regulasi turunan UU PDP yang secara eksplisit mengatur pencegahan, pelaporan insiden, pembentukan otoritas pengawas independen, serta

[36] Syafira Agata Ramadhani, "Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa," *Jurnal Hukum Lex Generalis* 3, no. 1 (2022): 73–84, https://doi.org/10.56370/jhlg.v3i1.173.

[37] Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 237, https://doi.org/10.33331/rechtsvinding.v9i2.428.

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



mekanisme pemulihan dan kompensasi bagi korban, guna mewujudkan sistem hukum nasional yang adaptif, akuntabel, dan berorientasi pada perlindungan hak asasi di era digital.

## DAFTAR PUSTAKA

"Ancaman Nyata Cyber Crime Dalam Bentuk Phising." RHP lawfirm, 2024.

Arief, Barda Nawawi. *Masalah Penegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Dunia Maya*. Jakarta: Kencana, 2018.

Autoriteit Persoongegevens. "Tax Administration Fined for Discriminatory and Unlawful Data Processing." Autoriteit Persoonsgegevens, 2021.

Bastian, F. "Bagaimana Cara Kerja Link APK Penipuan Yang Lagi Marak Sekarang Hingga Bisa Mengambil Data Kita." Quora Indonesia, diakses, 2025.

Board, European Data Protection. "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' (WP248 Rev. 01)." Brussels, 2017.

Boma, H. "Pasal 28 Undang–Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Terhadap Perlindungan Korban Cyber Phising Perspektif Siyasah Tanfidziah (Studi Kasus Polres Mukomuko), Disertasi Doktoral." UIN Fatmawati Sukarno Bengkulu, 2025.

Brenner, Susan W. , *Cybercrime: Criminal Threats from Cyberspace*. Westport, CT: Prager, 2010.

Budiyanto. *Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*. Bandung: sada Karunia Pustaka, 2025.

Commission, European. "Data Protection Officer (DPO) Explained," 2023.

Devi Anjheli. "Privasi Digital Dan Kejahatan Phishing Di Indonesia: Evaluasi Kritis Terhadap Efektivitas UU ITE Dan UU PDP." *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam* 4, no. 1 (2025): 165–89. https://doi.org/10.14421/990epf27.

Fernando, Zico Junius, Anis Widyawati, and Kasmanto Rinaldi. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1–39. https://doi.org/10.15294/ildisea.v4i1.20147.

Hamzah, Andi. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2019.

Hidayat, Arif, and Zaenal Arifin. "Politik Hukum Legislasi Sebagai Socio-Equilibrium Di Indonesia." *Jurnal Ius Constituendum* 4, no. 2 (2019): 147–59. https://doi.org/10.26623/jic.v4i2.1654.

Juita, Subaidah Ratna, Dhian Indah Astanti, and Dian Septiandani. "Perlindungan Hukum Terhadap Nasabah Bank Korban Kejahatan Skimming." *Jurnal Usm Law Review* 6, no. 1 (2023): 407–19. https://doi.org/10.26623/julr.v6i1.6353.

Khansa, Farah Naurah. "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Dalam Pelindungan Data Pribadi Di Indonesia." *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 649–62. https://doi.org/10.56370/jhlg.v2i8.114.

Maaliki, Naavi'u Emal. "Kebijakan Hukum Pidana Sebagai Upaya Penanggulangan Tindak Pidana Penipuan Online." *Jurnal USM Law Review* 7, no. 3 (2024): 1409–18. https://doi.org/10.26623/julr.v7i3.10023.

Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security (Google EBook)*. USA: John Wiley & Sons, 2001.

Received: 5-11-2025
Revised: 8-11-2025
Accepted: 13-12-2025
e-ISSN: 2621-4105



Muhammad, Faiz Emery, and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal USM Law Review* 6, no. 1 (2023): 226–41. https://doi.org/10.26623/julr.v6i1.6649.

Pekanbaru, Pengadilan Negeri. Pengadilan Negeri Pekanbaru Putusan Nomor 958/Pid.Sus/2020/PN Pbr (2020).

Prayuti, Yuyut. "Implications of Personal Data Protection Law in Consumer Health Data Management to Improve Secure and Confidential Handling in Indonesia." *Jurnal Ius Constituendum* 9, no. 3 (2024): 461–78. https://doi.org/10.26623/jic.v9i3.9289.

Ramadhani, Syafira Agata. "Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa." *Jurnal Hukum Lex Generalis* 3, no. 1 (2022): 73–84. https://doi.org/10.56370/jhlg.v3i1.173.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Pub. L. No. Regulation (EU) 2016/679 (2016).

Sahfitri, Afifah, and Rosmalinda Rosmalinda. "Penipuan Digital Melalui Tautan Phishing." *Jurnal Dialektika Hukum* 6, no. 2 (2024): 211–28. https://doi.org/10.36859/jdh.v6i2.2881.

Sahid, nur jamal. "Apa Itu Phising? Definisi, Cara Kerja, Ciri-Ciri, Dan Cara Mencegahnya." kompas.com, 2022.

Sekhar Bhusal, Chandra. "Systematic Review on Social Engineering: Hacking by Manipulating Humans." *Journal of Information Security* 12, no. 01 (2021): 104–14. https://doi.org/10.4236/jis.2021.121005.

Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 237. https://doi.org/10.33331/rechtsvinding.v9i2.428.

Smedinghoff, T. J. S., ed. *Online Laws: The SPA's Legal Guide to Doing Business on the Internet*. Canada: Addison-Wesley Developers Press, n.d.

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.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pub. L. No. Pasal 1 Ayat (3 (n.d.).

Yuniarti, Siti. "Petugas/Pejabat Pelindungan Data Pribadi Dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa Dan Singapura." *Business Economic, Communication, and Social Sciences (BECOSS) Journal* 4, no. 2 (2022): 111–20. https://doi.org/10.21512/becossjournal.v4i2.8377.