TERTIPU LINK, TERKURAS PRIVASI, DI MANA KEADILAN HUKUM?

Muhammad Fauzi Ramadhan^{1*}, Miftahul Jannah², Airlangga Putera³.

^{1,2,3} Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

*Correspondence: fauzi.ramadhan@umi.ac.id

ARTICLE HISTORY

Terkirim: 07.05.2025

Diterima: 05.06.2025

Publikasi: 29.06.2025

ARTICLE LICENSE

Copyright © 2025 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution ShareAlike 4.0 International (CC BY-SA 4.0)

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis ketentuan hukum yang mengatur perlindungan bagi korban penyebaran data pribadi yang diperoleh secara ilegal melalui metode *phishing*. Selain itu, penelitian ini juga bertujuan untuk menelaah bentuk-bentuk perlindungan hukum yang dapat ditempuh oleh para korban. Metode yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif. Hasil yang diperoleh menunjukkan bahwa telah terdapat ketentuan hukum yang mengatur perlindungan bagi korban peretasan data pribadi melalui link *phishing* secara ilegal, serta berbagai upaya hukum yang tersedia bagi para korban untuk memperoleh keadilan. Berdasarkan hasil kajian, penulis menyimpulkan bahwa keberadaan regulasi hukum tersebut memberikan dasar bagi para korban kejahatan *phishing* untuk menuntut ganti rugi, sekaligus membuka ruang bagi mereka untuk memperjuangkan hak-haknya melalui jalur hukum guna mendapatkan perlindungan yang layak dan proporsional.

Kata kunci: Perlindungan Hukum, Penyebaran Data, Peretasan, Illegal, Phising

ABSTRACT

This study aims to identify and analyze legal provisions governing protection for victims of the distribution of personal data obtained illegally through phishing methods. Furthermore, this study also aims to examine the forms of legal protection that victims can pursue. The method used in this study is a normative legal research method. The results obtained indicate that there are legal provisions governing protection for victims of personal data hacking through illegal phishing links, as well as various legal remedies available for victims to obtain justice. Based on the results of the study, the author concludes that the existence of these legal regulations provides a basis for victims of phishing crimes to claim compensation, while also opening up space for them to fight for their rights through legal channels to obtain appropriate and proportional protection.

Keywords : Legal Protection, Data Dissemination, Hacking, Illegal, Phishing

A. Pendahuluan

Indonesia merupakan salah satu negara yang penduduknya aktif mengikuti perkembangan pesat dalam bidang Ilmu Pengetahuan dan Teknologi (IPTEK). Perkembangan teknologi dewasa ini menjadi suatu keniscayaan dalam kehidupan masyarakat modern, karena kemajuan teknologi selalu berjalan seiring dengan kemajuan ilmu pengetahuan. Meskipun kehadiran internet membawa berbagai manfaat positif bagi penggunaannya seperti peningkatan kesejahteraan, kemajuan, serta perkembangan peradaban manusia tidak dapat dipungkiri bahwa internet juga menyimpan sisi gelap. Di balik kontribusinya, internet telah menjadi medium munculnya bentuk-bentuk kejahatan baru dalam ranah hukum yang dikenal

sebagai kejahatan siber atau *cyber crime*. (Tri Andika Hidayatullah, Ismansyah, 2023) Di era informasi saat ini, teknologi informasi dan komunikasi telah menjadi bagian yang tak terpisahkan dari aktivitas sehari-hari, baik dalam konteks pribadi maupun kegiatan bisnis. Seiring dengan pesatnya pertumbuhan penggunaan internet, tingkat kejahatan siber pun mengalami peningkatan, salah satunya dalam bentuk serangan *phishing*. *Phishing* adalah salah satu bentuk serangan dalam kejahatan siber yang dirancang untuk mencuri atau mengakses data pribadi seseorang dengan cara menipu korban agar secara tidak sadar mengungkapkan informasi sensitif melalui tautan palsu yang dibuat menyerupai situs resmi.

Penegakan hukum terhadap tindak pidana *phishing* bertujuan untuk menjamin keadilan, sejalan dengan prinsip moral dan agama, sebagaimana larangan Allah terhadap praktik kecurangan dalam perdagangan. Sebagai negara hukum yang diatur dalam konstitusi, Indonesia memiliki kewajiban untuk melindungi seluruh warga negaranya dari berbagai perbuatan yang merugikan, terlebih lagi jika tindakan tersebut berpotensi merusak tatanan kehidupan bermasyarakat, berbangsa, dan bernegara. Salah satu ancaman serius tersebut adalah kejahatan di ruang digital yang dikenal sebagai *cybercrime*. Kejahatan siber, yang bersifat lintas ruang dan waktu, mengalami perkembangan pesat seiring kemajuan teknologi. Sayangnya, kemajuan ini sering kali disalahgunakan oleh pihak-pihak tidak bertanggung jawab demi kepentingan pribadi, yang pada gilirannya menyulitkan negara-negara berkembang dalam menindak pelaku kejahatan siber, khususnya bagi aparat penegak hukum seperti kepolisian. Untuk mengatasi hal ini, tidak hanya dibutuhkan perangkat regulasi yang komprehensif terkait penyalahgunaan teknologi informasi, tetapi juga diperlukan dukungan sumber daya manusia yang andal serta sarana dan prasarana yang memadai. Penanganan kasus *cybercrime* memiliki tantangan tersendiri, terutama karena ketiadaan saksi langsung, yang umumnya berada di lokasi geografis berbeda, bahkan di luar negeri. Kondisi ini menyulitkan penyidik dalam melakukan pemeriksaan saksi dan menyusun berkas perkara hasil penyelidikan secara optimal. (Ridwan et al., 2016)

Pengaturan mengenai tindak pidana siber dalam sistem perundang-undangan di Indonesia hingga saat ini masih belum sepenuhnya mendukung baik dari sisi hukum pidana materiel maupun hukum pidana formil. Berbagai upaya telah dilakukan untuk merumuskan ketentuan yang mampu mencegah dan meminimalisasi dampak negatif dari tindakan melawan hukum di ranah digital. Namun demikian, hukum pidana Indonesia – dalam hal ini Kitab Undang-Undang Hukum Pidana (KUHP) belum secara eksplisit mendefinisikan dan mengatur mengenai kejahatan siber (*cyber crime*). Oleh karena itu, diperlukan suatu regulasi yang komprehensif dan memadai agar penanganan terhadap kejahatan siber dapat dijalankan secara efektif dan memberikan kepastian hukum bagi semua pihak yang terlibat. Salah satu bentuk kejahatan siber atau *cyber crime* adalah peretasan, yang lebih dikenal dengan istilah *hacking*. Peretasan merupakan tindakan yang dilakukan untuk mengakses perangkat digital secara ilegal, seperti komputer, smartphone, tablet, maupun jaringan secara keseluruhan. Umumnya, tujuan dari aktivitas ini adalah untuk memperoleh akses tanpa izin terhadap sistem komputer, jaringan, perangkat seluler, atau infrastruktur digital lainnya. (Tri Andika Hidayatullah, Ismansyah, 2023) Kasus pencurian data pribadi melalui metode *phishing* kian meningkat di Indonesia. Informasi yang berhasil dicuri seperti data identitas, rincian kartu kredit, maupun akun media sosial sering kali disebar dan dimanfaatkan oleh pihak-pihak

yang tidak bertanggung jawab. Para korban serangan *phishing* umumnya mengalami kerugian, baik secara materiil maupun immateriil, termasuk kehilangan data penting hingga rusaknya reputasi. Namun demikian, upaya perlindungan hukum terhadap korban serangan semacam ini masih menghadapi berbagai kendala dan menjadi persoalan yang kompleks dalam penegakan hukum di Indonesia.

Sebagai contoh, kasus yang diungkap oleh Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Metro Jaya terhadap tersangka AV (25) menunjukkan modus penipuan siber dengan menggunakan teknik *phishing*. Modus ini bekerja melalui pembuatan tautan palsu yang menyerupai tampilan resmi sebuah bank, dalam hal ini Bank BNI, sehingga menimbulkan kesan keaslian di mata korban. Ketika korban mengakses tautan tersebut, sistem akan mengarahkan ke laman tiruan yang meminta pengisian data pribadi. Data tersebut kemudian diteruskan secara otomatis melalui bot Telegram yang telah disiapkan oleh pelaku, sehingga seluruh informasi sensitif dapat langsung dikendalikan oleh tersangka. Dari perspektif hukum, praktik ini termasuk dalam kategori tindak pidana siber yang melibatkan pencurian dan penyalahgunaan data pribadi. Indonesia sebenarnya telah memiliki instrumen hukum yang dapat digunakan, misalnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya, yang mengatur larangan akses ilegal, manipulasi data elektronik, serta perbuatan yang merugikan pihak lain. Selain itu, kasus ini juga memiliki keterkaitan dengan isu perlindungan data pribadi, terutama setelah lahirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menegaskan hak-hak subjek data serta kewajiban pihak yang menguasai maupun memproses data. Fenomena ini mengindikasikan adanya celah pada sisi literasi digital masyarakat dan lemahnya pengawasan terhadap distribusi tautan berbahaya di ruang siber. Di satu sisi, hal tersebut menjadi tantangan bagi aparat penegak hukum dalam menindak pelaku kejahatan digital lintas platform. Di sisi lain, kasus ini menegaskan pentingnya penguatan regulasi dan penegakan hukum dalam perlindungan data pribadi. Dengan demikian, peristiwa yang menimpa nasabah bank melalui modus *phishing* bukan sekadar tindak kriminal individu, tetapi juga refleksi dari kebutuhan akan sistem hukum yang adaptif, efektif, dan responsif terhadap perkembangan teknologi informasi. (Maharlina Darni Purwandari, 2024)

Ade Safri menjelaskan bahwa tersangka membuat tautan *phishing* berdasarkan permintaan dari sejumlah pemesan. Mayoritas pemesan diketahui berdomisili di wilayah Tulung Selapan, Sumatera Selatan. "Tersangka menjual tautan *phishing* dengan harga berkisar antara Rp100.000 hingga Rp500.000, dan telah berhasil menjual sekitar 60 tautan," ungkapnya. Dari aktivitas tersebut, tersangka memperoleh keuntungan bulanan antara Rp17 juta hingga Rp20 juta, dengan total estimasi keuntungan mencapai sekitar Rp70 juta dalam kurun waktu empat bulan. Setelah dilakukan penyelidikan pada hari Senin, 28 Agustus 2023 pukul 00.30 WIB, tim penyidik Unit II Tindak Pidana Siber Direktorat Reserse Kriminal Khusus Polda Metro Jaya melakukan penangkapan terhadap tersangka di wilayah Kecamatan Sungai Raya, Kabupaten Kubu Raya, Kalimantan Barat. Dalam penangkapan tersebut, polisi berhasil mengamankan sejumlah barang bukti, antara lain satu unit telepon seluler, satu unit laptop, tiga kartu SIM, satu aplikasi dompet digital, serta satu akun hosting Planethost. Ade Safri juga mengungkapkan bahwa pengungkapan kasus ini bermula dari laporan polisi dengan Nomor:

LP/B/4076/VII/2023/SPKT/POLDA METRO JAYA, tertanggal 14 Juli 2023, yang dilaporkan oleh seorang warga bernama GF.

Tersangka dikenakan Pasal 35 jo Pasal 51 ayat (1) dan atau Pasal 30 jo Pasal 46 dan atau Pasal 32 jo Pasal 48 dan atau Pasal 36 jo Pasal 51 ayat (2) dan atau Pasal 28 ayat (1) jo Pasal 45A ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan atau Pasal 263 KUHP dengan ancaman pidana penjara maksimal enam tahun dan denda maksimal Rp1 miliar. "Kemudian untuk para pemesan 'link phishing', sedang didalami dan dilakukan profiling," kata Ade Safri. (Maharlina Darni Purwandari, 2024) Mengingat kompleksitas tindak kejahatan siber yang terus berkembang, maka diperlukan regulasi yang lebih spesifik dan komprehensif guna mengatur tindak pidana terkait teknologi informasi, serta memberikan perlindungan hukum terhadap pemanfaatan teknologi komunikasi dan media digital. Dalam konteks ini, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi dua instrumen hukum utama di Indonesia yang dirancang untuk melindungi data pribadi dari potensi penyalahgunaan. Meskipun demikian, penerapan kedua regulasi tersebut masih menghadapi berbagai tantangan, antara lain dalam aspek penegakan hukum, tingkat literasi masyarakat terhadap isu perlindungan data, serta rendahnya kesadaran publik mengenai pentingnya menjaga keamanan informasi pribadi.

Meskipun Indonesia telah memiliki instrumen hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), penanganan kasus *phishing* masih menyisakan sejumlah kesenjangan. Pertama, efektivitas sanksi pidana yang diterapkan kepada pelaku kejahatan siber sering dipertanyakan karena meskipun ancaman pidana cukup berat, tingkat kejadian serupa tetap tinggi. Hal ini mengindikasikan bahwa instrumen pidana belum sepenuhnya mampu memberikan efek jera maupun mencegah terjadinya pengulangan tindak pidana. Kedua, dari perspektif perlindungan korban, mekanisme kompensasi perdata masih lemah. UU PDP memang mengakui hak korban atas ganti rugi, namun implementasi dalam praktik belum memberikan kepastian hukum yang memadai, sehingga kerugian materiil maupun immateriil akibat *phishing* jarang dipulihkan secara tuntas. Ketiga, dari sisi kelembagaan, peran lembaga pengawas seperti OJK, Bank Indonesia, Kominfo, maupun otoritas perlindungan data pribadi masih berjalan parsial dan belum terintegrasi dalam satu sistem yang efektif. Akibatnya, upaya pencegahan, pengawasan, dan penegakan hukum sering kali bersifat reaktif serta kurang memiliki daya antisipatif terhadap perkembangan modus kejahatan digital.

Dengan demikian, terdapat kesenjangan penelitian yang penting untuk diisi, yakni perlunya kajian yang tidak hanya menekankan efektivitas pidana atau kompensasi perdata secara terpisah, tetapi juga mengintegrasikan keduanya dengan penguatan peran lembaga pengawas. Sebuah penelitian yang menyoroti pendekatan terpadu dalam penegakan hukum terhadap tindak pidana *phishing* akan memberikan kontribusi akademik sekaligus praktis dalam membangun sistem perlindungan hukum yang adaptif, komprehensif, dan responsif terhadap dinamika kejahatan siber di Indonesia.

B. Metode Penelitian

Jenis penelitian yang digunakan dalam studi ini adalah penelitian hukum normatif, yaitu suatu metode yang bertujuan untuk menemukan norma, asas hukum, dan doktrin-doktrin hukum sebagai jawaban atas permasalahan hukum yang dikaji. (Nurul Qamar, 2020) Pendekatan ini menitikberatkan pada analisis hukum secara normatif, yang didasarkan pada dokumen-dokumen hukum, peraturan perundang-undangan, teori hukum, serta prinsip-prinsip hukum yang relevan. Dalam pelaksanaannya, penelitian ini menggunakan bahan hukum primer berupa peraturan perundang-undangan yang berlaku, serta bahan hukum sekunder seperti literatur hukum dan jurnal ilmiah yang relevan. Penelitian dilakukan dengan metode studi kepustakaan, yang secara umum diarahkan pada kajian terhadap asas-asas hukum, sistematika hukum, harmonisasi atau sinkronisasi peraturan perundang-undangan, serta studi perbandingan hukum. Berdasarkan uraian tersebut, penulis memilih metode penelitian hukum normatif, mengingat fokus utama penelitian ini adalah pada analisis terhadap bahan pustaka dan regulasi yang berlaku, sebagai dasar dalam mengkaji dan memahami permasalahan hukum yang diteliti.

C. Pembahasan

3.1. Kerangka Hukum Perlindungan Bagi Korban Peretasan Data Pribadi Melalui Link Phising Secara Illegal

Secara umum, korban penyebaran data pribadi merupakan individu yang datanya mengalami kebocoran atau didistribusikan tanpa persetujuan, baik secara disengaja maupun karena kelalaian. Peristiwa ini dapat terjadi akibat berbagai bentuk pelanggaran keamanan, seperti peretasan, kerentanan sistem, atau melalui metode manipulatif seperti *phishing*, yang menyebabkan informasi sensitif – seperti nama, alamat, nomor identitas, data keuangan, dan informasi pribadi lainnya – jatuh ke tangan pihak yang tidak berwenang. Isu perlindungan hukum terhadap korban peretasan data pribadi secara ilegal di Indonesia menjadi semakin relevan seiring meningkatnya insiden kebocoran data di era digital. Salah satu modus yang kerap digunakan oleh pelaku adalah dengan mengirimkan pesan elektronik (email) yang mengandung informasi menyesatkan untuk mengecoh korban, dengan tujuan memperoleh data pribadi, nomor telepon, serta kode OTP (One Time Password) yang terhubung dengan akun-akun keuangan seperti mobile banking, internet banking, dompet digital, dan layanan keuangan elektronik lainnya. (Terintegrasi & Berkesinambungan, 2019) Pada dasarnya, perlindungan hukum terhadap korban penyebaran data pribadi yang diretas secara ilegal melalui tautan *phishing* diatur dalam sejumlah peraturan perundang-undangan yang secara khusus memuat ketentuan mengenai jaminan perlindungan hukum bagi korban. Regulasi-regulasi tersebut mencakup antara lain:

1. Undang-Undang Nomor 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana

Dalam kitab Undang-undang Hukum Pidana pasal yang dapat menjadi acuan untuk menegakkan hukum terakait Tindakan phising adalah pasal 378 KUHP yang berbunyi: “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain Secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun”. Pasal 378 KUHP diatas

menjelaskan tentang "penipuan" yang melibatkan manipulasi atau tipu muslihat untuk menggerakkan orang lain menyerahkan sesuatu atau memberikan hutang dengan jalan yang melawan hukum. (Lokapala et al., 2024) Nico Keijzer berpendapat bahwa pasal 378 adalah delik yang paling relevan bagi seseorang yang memanipulasi computer untuk tujuan keuntungan, karena melibatkan aspek hak. (Karunia et al., 2024) Namun demikian, Dalam Kitab Undang-Undang Hukum Pidana (KUHP), ketentuan mengenai tindak pidana penipuan diatur dalam Pasal 378 KUHP. Rumusan norma tersebut menegaskan bahwa seseorang dapat dipidana karena penipuan apabila ia dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan nama palsu, martabat palsu, tipu muslihat, maupun rangkaian kebohongan untuk menggerakkan orang lain agar menyerahkan sesuatu, memberikan utang, atau menghapuskan piutang. Dari rumusan pasal ini, terdapat beberapa elemen pokok tindak pidana penipuan, yakni:

- a) Adanya maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Unsur ini menekankan pada tujuan pelaku untuk memperoleh keuntungan yang tidak sah, baik dalam bentuk materi maupun manfaat lainnya.
- b) Penggunaan cara-cara yang bersifat menyesatkan, seperti: Nama palsu atau martabat palsu, Tipu muslihat, atau Rangkaian kebohongan.
- c) Adanya perbuatan menggerakkan korban agar: Menyerahkan suatu benda, Memberikan suatu pinjaman (utang), atau Menghapuskan suatu piutang.

Dengan demikian, penipuan konvensional dalam KUHP berorientasi pada hubungan interpersonal antara pelaku dan korban, di mana korban "digiring" untuk mengambil suatu tindakan hukum atau tindakan nyata karena terpedaya oleh kebohongan pelaku. Namun, ketika ketentuan ini diterapkan terhadap modifikasi kejahatan siber seperti *phishing*, muncul sejumlah permasalahan mendasar. Pertama, modus *phishing* bekerja melalui media elektronik dan algoritma sistem digital, bukan semata-mata interaksi langsung antarindividu. Pelaku tidak selalu menggunakan identitas palsu secara personal (nama palsu atau martabat palsu), melainkan memanfaatkan rekayasa digital berupa situs palsu atau tautan yang dibuat menyerupai sistem resmi. Dalam konteks ini, kebohongan tidak berbentuk verbal atau rangkaian kata secara fisik, melainkan manipulasi dokumen elektronik yang secara visual menipu korban agar percaya bahwa ia sedang berinteraksi dengan pihak resmi. Kedua, objek yang dituju dalam *phishing* berbeda dengan penipuan konvensional. Dalam KUHP, penipuan lazimnya mengakibatkan korban menyerahkan barang berwujud, uang, atau hak tertentu. Sedangkan dalam *phishing*, objek yang disasar adalah data pribadi korban (username, password, PIN, OTP, atau nomor kartu kredit), yang pada saat KUHP disusun belum dikenal sebagai komoditas hukum. Hal ini menimbulkan kesenjangan normatif, karena penyerahan data pribadi tidak secara eksplisit masuk dalam kategori "menyerahkan suatu benda" sebagaimana dimaksud Pasal 378 KUHP.

Ketiga, mekanisme "menggerakkan korban" dalam KUHP memiliki bentuk yang lebih sederhana (misalnya korban tertipu oleh janji atau kebohongan pelaku secara langsung). Sementara itu, dalam *phishing*, korban digerakkan melalui mekanisme teknis yang kompleks, yakni klik tautan, mengisi formulir digital, lalu sistem secara otomatis mengirimkan data ke server atau bot pelaku. Dengan kata lain, proses perbuatan tercipta karena rekayasa sistem elektronik, bukan sekadar persuasi verbal.

Keempat, cakupan locus dan tempus delicti dalam penipuan konvensional relatif jelas, sedangkan *phishing* melibatkan lintas yurisdiksi. Korban dapat berada di Indonesia, sementara server, domain, atau pelaku berada di luar negeri. Hal ini menimbulkan kesulitan dalam mengaitkan perbuatan dengan ketentuan Pasal 378 KUHP yang masih berlandaskan paradigma kejahatan tradisional.

Oleh karena itu, dapat disimpulkan bahwa elemen penipuan dalam KUHP tidak sepenuhnya sesuai dengan karakteristik kejahatan *phishing*. KUHP didesain untuk mengatur bentuk penipuan konvensional yang berbasis interaksi langsung antara pelaku dan korban, sedangkan *phishing* merupakan bentuk kejahatan digital yang memanfaatkan manipulasi dokumen elektronik, rekayasa visual, dan teknologi informasi. Inilah sebabnya kejahatan *phishing* lebih relevan untuk dijerat menggunakan instrumen hukum khusus seperti UU ITE dan UU PDP, yang secara eksplisit mengatur perbuatan manipulasi data elektronik dan perlindungan data pribadi.

Dalam perspektif hukum pidana, tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP memiliki keterbatasan ketika dihadapkan pada modus operandi kejahatan siber, khususnya *phishing*. Pasal 378 KUHP menitikberatkan pada adanya maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, yang dilakukan dengan tipu muslihat atau rangkaian kebohongan untuk menggerakkan korban menyerahkan suatu benda, memberikan utang, atau menghapuskan piutang. Konsepsi tersebut lahir dalam konteks penipuan konvensional, yakni hubungan interpersonal yang berlangsung secara langsung antara pelaku dan korban. Namun, *phishing* bekerja melalui mekanisme yang berbeda. Pelaku tidak serta-merta melakukan tipu muslihat verbal atau tatap muka, melainkan melakukan rekayasa dokumen elektronik berupa situs atau tautan palsu yang menyerupai sistem resmi. Dalam praktiknya, korban tidak menyerahkan benda berwujud sebagaimana dikehendaki Pasal 378 KUHP, tetapi memberikan data pribadi yang dikategorikan sebagai informasi elektronik. Data ini kemudian dapat dieksploitasi untuk memperoleh keuntungan ekonomi, misalnya mengakses rekening bank, menggunakan kartu kredit, atau menjual data tersebut kepada pihak ketiga. Oleh karena itu, rumusan delik penipuan dalam KUHP menjadi kurang memadai karena belum mengenali data pribadi dan dokumen elektronik sebagai objek perlindungan hukum. Sebaliknya, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) justru memberikan instrumen yang lebih tepat dalam menjerat pelaku *phishing*. Pasal 30 jo Pasal 46 UU ITE melarang akses ilegal ke sistem elektronik orang lain, Pasal 32 jo Pasal 48 mengatur mengenai perbuatan mentransmisikan atau memindahkan informasi elektronik tanpa hak, sementara Pasal 35 jo Pasal 51 ayat (1) secara khusus melarang perikayasaan informasi elektronik seolah-olah otentik. Ketentuan ini secara normatif mencakup modus *phishing*, sebab pelaku memanipulasi tampilan digital untuk menyesatkan korban, lalu memperoleh data yang tidak seharusnya diakses.

Dengan demikian, terdapat perbedaan mendasar antara KUHP dan UU ITE. KUHP lebih menekankan aspek klasik penipuan dengan objek berupa barang berwujud, sedangkan UU ITE sudah mengantisipasi perkembangan teknologi informasi dengan memasukkan informasi elektronik dan data pribadi sebagai objek perlindungan. Hal ini menjelaskan mengapa dalam praktik peradilan, aparat penegak hukum lebih banyak menggunakan UU

ITE untuk menjerat pelaku *phishing* dibanding hanya mengandalkan Pasal 378 KUHP. Secara akademik, kondisi ini menegaskan bahwa hukum pidana nasional memerlukan pembaruan paradigma, dari semata-mata menekankan tipu daya konvensional menuju pengakuan terhadap modus penipuan berbasis digital yang memanfaatkan manipulasi dokumen elektronik. (Oeliga et al., 2022)

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Tindak pidana *phishing* di Indonesia diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Salah satu pasal yang relevan adalah Pasal 30 UU ITE, yang menyatakan: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun." Ketentuan ini bertujuan untuk mencegah penyalahgunaan informasi atau dokumen elektronik palsu yang dapat menyesatkan serta merugikan pihak lain, sekaligus memberikan dasar hukum bagi penegakan terhadap pelaku yang dengan sengaja melakukan tindakan tersebut. Pasal ini secara tegas melarang akses ilegal terhadap sistem komputer, serta mencakup tindakan-tindakan yang mengakibatkan hilangnya, rusaknya, atau berubahnya data elektronik milik pihak lain. (Azzahrah, 2018) Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) memuat ketentuan yang secara khusus mengatur mengenai definisi tindak pidana peretasan sistem komputer. Dalam pasal ini, peretasan dimaknai sebagai perbuatan yang dilakukan oleh seseorang dengan sengaja dan secara melawan hukum untuk mengakses sistem elektronik atau komputer milik pihak lain, dengan tujuan memperoleh informasi elektronik yang bukan menjadi haknya. (Tri Andika Hidayatullah, Ismansyah, 2023) Ancaman pidana terhadap pelaku peretasan diatur secara rinci dalam Pasal 46 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pada ayat (1) disebutkan bahwa setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dapat dijatuhi pidana penjara paling lama enam tahun dan/atau denda maksimal sebesar Rp600.000.000,00. Selanjutnya, ayat (2) Pasal 46 menyatakan bahwa siapa pun yang memenuhi ketentuan dalam Pasal 30 ayat (2) dapat dikenakan sanksi pidana berupa penjara maksimal enam tahun dan/atau denda hingga Rp700.000.000,00. Sementara itu, ayat (3) Pasal 46 menegaskan bahwa pelanggaran terhadap Pasal 30 ayat (3) dapat diancam pidana penjara paling lama delapan tahun dan/atau denda maksimal sebesar Rp800.000.000,00.

Ketentuan-ketentuan tersebut mengatur secara spesifik jenis sanksi pidana yang dapat dikenakan terhadap pelaku kejahatan *phishing* yang melakukan peretasan atau akses ilegal sebagaimana dimaksud dalam Pasal 30 UU ITE. Selain itu, Pasal 35 UU ITE juga mengatur mengenai tindak kejahatan *phishing*. Pasal tersebut menyatakan bahwa: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar informasi atau dokumen tersebut dianggap seolah-olah data yang otentik." Ketentuan ini secara jelas mencakup tindakan pelaku *phishing* yang menggunakan tautan palsu untuk memperoleh akses terhadap data pribadi korban tanpa izin, yang merupakan pelanggaran terhadap keaslian dan otentisitas informasi elektronik sebagaimana diatur dalam pasal tersebut.

3. Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur mengenai hak-hak individu atas perlindungan data pribadinya dalam seluruh proses pemrosesan data, guna menjamin terpenuhinya hak-hak konstitusional subjek data pribadi. Salah satu ketentuan penting dalam undang-undang tersebut tercantum dalam Pasal 12 ayat (1), yang menyatakan bahwa: "Subjek data pribadi berhak untuk mengajukan gugatan dan memperoleh ganti rugi atas pelanggaran terhadap pemrosesan data pribadi yang berkaitan dengan dirinya, sesuai dengan ketentuan peraturan perundang-undangan yang berlaku." Sebagaimana dikutip dari CNN Indonesia, pasal ini menegaskan bahwa individu sebagai pemilik data pribadi memiliki hak hukum untuk menuntut ganti rugi apabila terjadi pelanggaran terhadap pengelolaan data pribadinya, sesuai dengan mekanisme dan aturan yang diatur dalam perundang-undangan. (Naufal, 2020) Selain itu, terdapat sejumlah hak subjek data pribadi yang dikecualikan, sebagaimana diatur dalam Pasal 15 ayat (1) Undang-Undang Nomor 27 Tahun 2022. Pasal tersebut menyatakan bahwa hak-hak subjek data pribadi sebagaimana tercantum dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, serta Pasal 13 ayat (1) dan (2), dapat dikecualikan dalam keadaan tertentu, antara lain untuk: a. Kepentingan pertahanan dan keamanan nasional; b. Kepentingan dalam proses penegakan hukum; c. Kepentingan umum dalam konteks penyelenggaraan negara; d. (dan seterusnya).

Meskipun terdapat ketentuan pengecualian, peraturan ini tetap menegaskan bahwa perlindungan data pribadi merupakan bagian yang tidak terpisahkan dari hak asasi manusia yang wajib dihormati dan dilindungi. Penerapan Pasal 15 memberikan landasan hukum yang tegas bagi subjek data untuk memahami kondisi tertentu di mana hak-haknya dapat dibatasi secara sah. Ketentuan ini menunjukkan adanya upaya untuk menciptakan keseimbangan antara perlindungan terhadap hak individu dan pemenuhan kepentingan yang lebih luas, baik dalam konteks kepentingan umum maupun kebutuhan negara. (Fauzi & Radika Shandy, 2022) Pasal 58 mengatur mengenai pembentukan Lembaga Perlindungan Data Pribadi, yang berfungsi sebagai otoritas independen dalam bidang pengawasan dan perlindungan data pribadi. Lembaga ini diberi mandat untuk menjalankan tugas perlindungan terhadap data pribadi milik warga negara Indonesia, serta melaksanakan amanah yang telah ditetapkan dalam Undang-Undang Perlindungan Data Pribadi. (Yati Nurhayati, 2015) Dengan dibentuknya lembaga khusus yang menangani perlindungan data pribadi, korban penyebaran data akibat peretasan melalui *phishing* kini memiliki mekanisme resmi untuk melaporkan pelanggaran yang dialaminya serta menempuh upaya hukum guna memperoleh keadilan. Lembaga Perlindungan Data Pribadi tersebut juga dapat berperan sebagai mediator antara korban dan pihak-pihak yang bertanggung jawab atas terjadinya pelanggaran, sehingga memfasilitasi penyelesaian sengketa secara lebih terarah dan adil. (Runtunuwu, 2025) Pasal 60 mengatur mengenai kewenangan Lembaga Perlindungan Data Pribadi (LPDP) dalam menjatuhkan sanksi administratif terhadap pihak-pihak yang melanggar ketentuan perlindungan data pribadi, serta melakukan tindakan lain yang dianggap perlu guna menjamin keamanan data tersebut. Ketentuan ini memberikan landasan hukum yang tegas bagi LPDP dalam melakukan fungsi pengawasan dan penegakan atas pelanggaran yang terjadi. Dalam konteks penyebaran data pribadi melalui *phishing*, korban dapat mengajukan laporan kepada LPDP, yang selanjutnya memiliki kewenangan untuk menindaklanjuti

pelanggaran tersebut sesuai dengan ketentuan yang berlaku. (Erlyns Yolanda, 2023) Lembaga Perlindungan Data Pribadi (LPDP) menyediakan alternatif penyelesaian sengketa bagi korban pelanggaran data pribadi tanpa harus menempuh proses litigasi yang panjang, rumit, dan memerlukan biaya besar. Mekanisme ini memungkinkan korban memperoleh keadilan secara lebih cepat dan efisien. Keberadaan LPDP sebagai otoritas yang bertanggung jawab atas perlindungan data pribadi turut berkontribusi dalam meningkatkan kepercayaan publik terhadap sistem hukum dan perlindungan data di Indonesia. Dengan adanya lembaga ini, masyarakat akan merasa lebih terlindungi karena hak-hak mereka atas data pribadi memiliki wadah resmi untuk mendapatkan perlindungan dan penyelesaian jika terjadi pelanggaran.

4. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik diterbitkan sebagai bentuk pengaturan lebih lanjut dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang memerlukan ketentuan teknis dan operasional tambahan untuk mendukung implementasinya secara efektif. (Salsabila et al., 2023) Dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), terdapat sejumlah ketentuan yang berkaitan dengan perlindungan hukum bagi korban penyebaran data pribadi yang diretas secara ilegal melalui tautan *phishing*. Salah satu pasal yang relevan adalah Pasal 11 ayat (1), yang menyatakan bahwa: "Penyelenggara Sistem Elektronik wajib memastikan bahwa sistem elektronik yang mereka kelola tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang." Ketentuan ini menegaskan bahwa penyelenggara sistem elektronik memiliki tanggung jawab untuk menjamin tersedianya perjanjian tingkat layanan (*service level agreement*) dan perjanjian keamanan informasi atas layanan teknologi informasi yang mereka sediakan. Selain itu, mereka juga diwajibkan menjaga keamanan informasi serta memastikan ketersediaan sarana komunikasi internal yang aman sebagai bagian dari penyelenggaraan sistem yang andal dan bertanggung jawab. (Ramli et al., 2019) Dalam konteks ini, penyelenggara sistem elektronik memiliki tanggung jawab hukum atas operasional sistem yang mereka kelola. Artinya, apabila terjadi kebocoran data sebagai akibat dari serangan *phishing*, maka pihak penyelenggara dapat dikenai pertanggungjawaban hukum atas kelalaian atau kegagalan dalam memastikan keamanan sistemnya.

3.2. Upaya Perlindungan Hukum bagi korban penyebaran data pribadi yang diretas secara Ilegal melalui link *phishing*.

Upaya perlindungan hukum bagi korban penyebaran data pribadi yang diretas secara ilegal melalui tautan *phishing* di Indonesia mencakup berbagai mekanisme dan instrumen hukum yang telah ditetapkan dalam peraturan perundang-undangan. Kehadiran regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, merupakan wujud komitmen negara dalam melindungi hak atas privasi dan hak-

hak dasar setiap individu. Undang-undang ini juga memberikan jaminan hukum bagi individu maupun badan hukum untuk menempuh upaya hukum, yakni mekanisme yang memungkinkan suatu pihak mengajukan perlawanan terhadap putusan pengadilan yang dianggap tidak adil atau merugikan, guna memperoleh keadilan sesuai prinsip negara hukum. (Sitorus, 2018) Korban yang mengalami kerugian akibat tindak pidana *phishing* yang mengakibatkan tersebarnya data pribadi memiliki hak untuk mengajukan tuntutan atas kerugian yang ditimbulkan. Terdapat beberapa langkah hukum yang dapat ditempuh oleh korban dalam rangka menuntut pertanggungjawaban atas pelanggaran tersebut, antara lain:

1. Langkah Hukum Non-Litigasi.

Korban atas penyebaran data pribadi yang diperoleh secara ilegal melalui serangan *phishing* dapat melaporkan tindakan melawan hukum tersebut kepada pihak berwenang, atau menempuh upaya hukum melalui jalur non-litigasi, antara lain: a. Kementerian Komunikasi dan Informatika Republik Indonesia. Korban dapat mengajukan laporan untuk melaporkan insiden penyebaran data pribadi (Kebocoran Data) yang di retas kepada Kemenkominfo, yang memiliki kewenangan untuk menyelidiki dan memberikan sanksi kepada penyelenggara sistem yang gagal melindungi data. b. Arbitrase dan Penyelesaian Sengketa. Korban juga dapat memilih arbitrase sebagai alternatif penyelesaian sengketa, yang dapat lebih cepat dan efisien. Arbitrase menjadi salah satu Upaya penyelesaian sengketa lewat jalur di luar peradilan umum berdasarkan suatu perjanjian yang dinamakan dengan perjanjian arbitrase, perjanjian tersebut dibuat oleh semua pihak yang berselisih dalam bentuk tertulis. (Tampongangoy, 2015) Arbiter sendiri adalah orang atau kelompok yang ditunjuk secara langsung oleh Pengadilan Negeri/ suatu Lembaga yang bertugas mengambil Keputusan terhadap permasalahan yang penyelesaiannya dilakukan melalui arbitrase. Hasil putusan dari Upaya hukum arbitrase ini memiliki sifat "win-lose" judgement, mutlak dan berkekuatan hukum untuk mengikat setiap pihak yang terlibat di dalamnya. c. Undang-undang Nomor 300 tahun 1999 tentang Arbitrase dan alternatif Penyelesaian Sengketa mengatakan, "terdapat badan penyelesaian sengketa lain selain arbitrase yaitu melalui negosiasi, dengar pendapat, mediasi, konsiliasi atau pendapat ahli." Di dalam UU PDP pada pasal 58 ayat 1,3, dan 4 terdapat bagian yang menjelaskan penetapan presiden terkait pembentukan suatu Lembaga yang harus mempertanggungjawabkan tugasnya langsung ke presiden. Lembaga ini memiliki wewenang di antaranya adalah menegakkan sanksi administratif, menerima laporan, atau pengaduan, memeriksa serta menelusuri dugaan terjadinya pelanggaran, menghadirkan semua pihak yang terlibat dalam dugaan pelanggaran perlindungan data pribadi, menghadirkan ahli-ahli yang mungkin diperlukan selama proses pemeriksaan.

2. Langkah Hukum Litigasi

Dalam kerangka *ius constitutum*, sistem hukum Indonesia saat ini masih mengandalkan kombinasi antara Kitab Undang-Undang Hukum Pidana (KUHP), Kitab Undang-Undang Hukum Perdata (KUHPerdata), serta Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya (UU ITE), untuk menjerat pelaku kebocoran maupun penyalahgunaan data pribadi. Dari sisi pidana, Pasal 362 KUHP tentang pencurian serta Pasal 30 ayat (2) UU ITE mengenai akses ilegal terhadap sistem elektronik

dapat dijadikan dasar pemidanaan. Namun, penerapan ketentuan ini kerap menghadapi kendala karena modus operandi berbasis teknologi, seperti phishing atau manipulasi sistem elektronik, tidak selalu dapat dipetakan ke dalam unsur-unsur tindak pidana konvensional yang mengedepankan “barang” sebagai objek pencurian. (Ramdhan et al., 2024) Hal ini menimbulkan problematika penafsiran dalam praktik, karena data pribadi memiliki sifat yang tidak berwujud (*intangible*), tetapi nilai ekonominya nyata dan dapat merugikan pemiliknya. Pada sisi perdata, *ius constitutum* mengandalkan Pasal 1365 KUHPerdata yang mengatur perbuatan melawan hukum sebagai dasar gugatan. Korban dapat menuntut ganti kerugian kepada penyelenggara sistem elektronik yang lalai melindungi data pribadi. Walaupun mekanisme ini memberikan ruang pemulihan kerugian, kelemahan mendasarnya terletak pada orientasi yang semata-mata bersifat kompensatoris tanpa memberi efek jera kepada pelaku. Dalam konteks praktik, gugatan perdata atas dasar perbuatan melawan hukum juga masih bergantung pada kapasitas korban dalam membuktikan adanya kerugian nyata serta hubungan kausal antara kebocoran data dan kelalaian penyelenggara sistem elektronik. (Sangojoyo et al., 2022)

Beranjak pada *ius constituendum*, perlindungan hukum terhadap data pribadi di Indonesia perlu diperkuat melalui instrumen hukum yang lebih spesifik dan responsif terhadap kejahatan siber. Kehadiran Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sesungguhnya merupakan langkah awal menuju rezim hukum yang lebih modern. UU PDP memberikan dasar hukum yang jelas terkait kewajiban pengendali data, hak-hak subjek data, serta sanksi administratif, perdata, dan pidana. Namun, secara normatif, implementasi UU PDP masih memerlukan aturan turunan dan infrastruktur kelembagaan yang memadai agar mampu menjawab kompleksitas serangan siber yang semakin berkembang. Dalam perspektif *ius constituendum*, sistem hukum Indonesia sebaiknya menekankan pendekatan hibrida yang mengintegrasikan instrumen pidana, perdata, dan administratif dalam satu kerangka perlindungan data pribadi. Jalur pidana berfungsi memberikan efek jera dan perlindungan publik, jalur perdata berorientasi pada pemulihan kerugian individu, sedangkan sanksi administratif berperan sebagai mekanisme preventif sekaligus korektif. Dengan demikian, perlindungan data pribadi tidak hanya dipandang sebagai isu privat semata, melainkan juga sebagai isu publik yang berkaitan dengan hak asasi manusia serta kedaulatan digital negara.

Dalam praktik, persoalan kebocoran data pribadi di Indonesia telah beberapa kali muncul ke ruang publik dan menimbulkan diskursus hukum. Salah satu kasus menonjol adalah kebocoran data pada platform Tokopedia tahun 2020, di mana sekitar 91 juta data pengguna beserta 7 juta data merchant diduga diperjualbelikan di forum gelap (*dark web*). Kasus ini menunjukkan kelemahan *ius constitutum*, karena meskipun kebocoran data tersebut nyata, instrumen hukum saat itu belum memberikan mekanisme pemulihan yang memadai bagi para korban. Gugatan perdata berbasis Pasal 1365 KUHPerdata memang diajukan ke pengadilan, namun perdebatan utama terletak pada beban pembuktian mengenai kelalaian penyelenggara sistem elektronik. Kasus lain terjadi pada tahun 2021 ketika data peserta BPJS Kesehatan dengan estimasi 279 juta catatan bocor dan juga diperjualbelikan di forum *daring*. Dalam perkara ini, meskipun pemerintah melalui Kementerian Kominfo menyatakan bahwa investigasi dilakukan, tidak terdapat kepastian hukum yang jelas terkait pertanggungjawaban

pidana maupun ganti rugi bagi korban. Situasi ini menunjukkan keterbatasan rezim hukum sebelum hadirnya UU PDP, karena baik KUHP maupun UU ITE tidak sepenuhnya mampu menjerat perbuatan yang berupa kelalaian penyelenggara data publik dalam menjaga sistem elektronik. Demikian pula pada kasus *MyIndiHome* di tahun 2021, kebocoran data pelanggan berupa riwayat penelusuran internet menjadi isu publik yang serius. Namun, penyelesaiannya hanya berujung pada klarifikasi dan komitmen penyelenggara untuk meningkatkan keamanan, tanpa adanya tindak lanjut pidana ataupun perdata. Kondisi ini semakin menegaskan bahwa dalam *ius constitutum*, penegakan hukum atas pelanggaran perlindungan data pribadi masih bersifat parsial dan belum memberikan perlindungan maksimal kepada korban.

Dari berbagai kasus tersebut terlihat bahwa *ius constituendum* melalui hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan arah yang lebih progresif. UU PDP tidak hanya menegaskan kewajiban pengendali data, tetapi juga mengatur sanksi pidana bagi pihak yang dengan sengaja atau melawan hukum memperoleh maupun mengungkapkan data pribadi orang lain. Selain itu, UU PDP menempatkan hak subjek data sebagai bagian dari hak asasi manusia yang wajib dijamin oleh negara. Apabila instrumen ini diimplementasikan secara konsisten, maka ke depan korban kebocoran data akan memiliki jalur hukum yang lebih jelas, baik melalui mekanisme administratif, pidana, maupun perdata. Dengan demikian, analisis normatif atas kasus-kasus Tokopedia, BPJS Kesehatan, dan *MyIndiHome* memperlihatkan transisi penting dari *ius constitutum* yang cenderung lemah dalam menjawab tantangan kejahatan siber, menuju *ius constituendum* yang berpotensi menghadirkan perlindungan hukum komprehensif terhadap data pribadi sebagai bagian dari kedaulatan digital dan hak asasi manusia.

Dalam perspektif hukum, penyelesaian sengketa akibat kebocoran maupun penyalahgunaan data pribadi melalui jalur litigasi dapat ditempuh melalui dua mekanisme utama, yakni hukum pidana dan hukum perdata. Kedua mekanisme ini memiliki karakteristik berbeda namun saling melengkapi, sehingga dapat berjalan secara paralel sesuai dengan kepentingan hukum korban. Pertama, jalur hukum pidana ditempuh apabila perbuatan yang dilakukan oleh pelaku dikualifikasikan sebagai tindak pidana, misalnya pencurian data, akses ilegal, maupun penyalahgunaan informasi elektronik. Dasar hukum yang digunakan antara lain Pasal 362 KUHP yang mengatur mengenai pencurian, Pasal 30 jo. Pasal 46 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terkait akses tanpa izin terhadap sistem elektronik, serta ketentuan dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) khususnya Pasal 65 sampai dengan Pasal 67 yang menegaskan larangan penggunaan data pribadi secara melawan hukum. Langkah konkret dalam jalur pidana dimulai dengan pelaporan ke kepolisian, dilanjutkan dengan proses penyidikan, penuntutan di kejaksaan, hingga pemeriksaan dan putusan perkara oleh pengadilan negeri. Jika putusan pada tingkat pertama dianggap belum memberikan rasa keadilan, para pihak dapat menempuh upaya hukum lanjutan berupa banding ke Pengadilan Tinggi, kasasi ke Mahkamah Agung, bahkan Peninjauan Kembali (PK). Hasil akhir dari jalur pidana biasanya berupa sanksi kurungan, denda, atau pidana tambahan lain yang bersifat represif.

Kedua, jalur hukum perdata difokuskan pada pemulihan hak-hak korban melalui mekanisme ganti kerugian. Dalam hal ini, korban sebagai pihak yang dirugikan berhak

mengajukan gugatan ke pengadilan negeri dengan dasar hukum Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) tentang perbuatan melawan hukum serta Pasal 58 sampai Pasal 60 UU PDP yang memberikan legitimasi bagi pemilik data untuk menuntut kompensasi. Substansi gugatan yang diajukan dapat meliputi kerugian materiil maupun immateriil akibat kebocoran atau penyalahgunaan data pribadi. Sama halnya dengan jalur pidana, perkara perdata juga membuka ruang upaya hukum lanjutan berupa banding, kasasi, hingga Peninjauan Kembali jika putusan pengadilan dianggap tidak memenuhi asas keadilan.

Dengan demikian, dapat dipahami bahwa mekanisme litigasi dalam penyelesaian sengketa data pribadi menempatkan jalur pidana sebagai sarana untuk menghukum pelaku, sedangkan jalur perdata berfungsi sebagai instrumen pemulihan kerugian korban. Kedua jalur tersebut dapat dipilih secara alternatif maupun simultan, bergantung pada strategi hukum yang diambil korban dalam rangka memperoleh perlindungan hukum yang maksimal.

Berdasarkan uraian sebelumnya yang mencakup pengaturan perlindungan hukum terhadap korban penyebaran data pribadi yang diretas secara ilegal melalui tautan *phishing* hingga langkah-langkah perlindungan hukum yang dapat ditempuh oleh para korban dapat disimpulkan bahwa keberadaan regulasi yang relevan memberikan landasan hukum yang penting bagi korban kejahatan *phishing* untuk menuntut ganti rugi atas kerugian yang mereka alami. Dengan mengikuti mekanisme yang tersedia, para korban memiliki kesempatan untuk memperjuangkan hak-haknya dan memperoleh perlindungan hukum yang layak dan proporsional. Selain instrumen hukum, edukasi dan peningkatan kesadaran masyarakat terkait risiko *phishing* serta pentingnya menjaga data pribadi juga merupakan bagian integral dari strategi perlindungan hukum. Pemahaman yang memadai mengenai hak-hak individu akan mendorong masyarakat untuk lebih tanggap dan tepat dalam mengambil tindakan saat menghadapi insiden kebocoran data. Melalui kombinasi antara regulasi yang kuat, penegakan hukum yang efektif, dan literasi publik yang memadai, perlindungan hukum bagi korban peretasan data pribadi melalui *phishing* diharapkan semakin kokoh dan mampu memberikan rasa aman di tengah dinamika era digital yang semakin kompleks.

D. Penutup

Berdasarkan hasil analisis yang telah diuraikan pada bab sebelumnya, dapat disimpulkan bahwa Indonesia telah memiliki sejumlah regulasi yang relevan dalam memberikan perlindungan hukum terhadap korban kejahatan siber, khususnya dalam kasus *phishing* dan peretasan data pribadi. Pasal 378 KUHP, meskipun mengatur tentang tindak pidana penipuan, belum secara khusus mengakomodasi bentuk-bentuk kejahatan siber, sehingga efektivitasnya dalam menangani kasus *phishing* masih terbatas. Sebaliknya, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 30 dan Pasal 46, memberikan dasar hukum yang lebih spesifik dalam menangani kejahatan siber, termasuk ancaman pidana terhadap pelaku peretasan dan *phishing*. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga memperkuat posisi hukum korban dengan memberikan hak kepada subjek data pribadi untuk mengajukan gugatan apabila terjadi pelanggaran terhadap data miliknya. Dalam mendukung implementasi undang-undang tersebut, dibentuk Lembaga Perlindungan Data Pribadi (LPDP) yang memiliki fungsi

pengawasan serta kewenangan untuk menjatuhkan sanksi administratif terhadap pelanggaran perlindungan data. Selain itu, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) mewajibkan Penyelenggara Sistem Elektronik (PSE) untuk menjaga keamanan data pribadi pengguna, melaporkan insiden kebocoran data secara transparan, serta memberikan kompensasi kepada pihak yang indo. Secara keseluruhan, kerangka regulasi yang tersedia telah membentuk fondasi hukum perlindungan data pribadi di Indonesia. Namun demikian, tantangan masih muncul pada aspek implementasi yang menyeluruh dan efektif, khususnya dalam menjamin perlindungan optimal bagi korban *phishing* dan kejahatan digital lainnya. Oleh karena itu, edukasi dan sosialisasi yang berkelanjutan mengenai pentingnya perlindungan data pribadi dan kewaspadaan terhadap *phishing* perlu ditingkatkan agar masyarakat lebih siap menghadapi ancaman siber. Di sisi lain, penegak hukum perlu memperoleh pelatihan khusus dalam menangani tindak pidana siber, terutama yang berkaitan dengan pelanggaran data pribadi melalui *phishing*. Selain itu, sinergi antar-lembaga, seperti antara kepolisian, Kementerian Komunikasi dan Informatika, serta LPDP, harus diperkuat guna menciptakan sistem penanganan yang terpadu dan efektif, sehingga mampu memberikan perlindungan hukum yang maksimal kepada korban di era digital yang semakin kompleks.

DAFTAR PUSTAKA

- Azzahrah, W. (2018). PERLINDUNGAN HUKUM TERHADAP KORBAN TINDAK PIDANA DALAM KASUS PENCURIAN DATA NASABAH BANK MANDIRI. FAKULTAS HUKUM UNIVERSITAS ISLAM INDONESIA YOGYAKARTA, 5(1), 86-96.
- Erlyns Yolanda, R. R. H. (2023). URGENSI LEMBAGA PELINDUNGAN DATA PRIBADI DI INDONESIA BERDASARKAN ASAS HUKUM RESPONSIF. *Syntax Literate: Jurnal Ilmiah Indonesia*, 87(1,2), 149-200.
- Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, 7(3), 445-461. <https://doi.org/10.20885/jlr.vol7.iss3.art1>
- Karunia, Fauzan Al Fikri, M., & Prihatini, L. (2024). Analisis Tindak Pidana Kejahatan Siber "Studi Kasus Penipuan Tiket Konser NCT Dream the Dream Show 2." *Doktrina : Journal of Law*, 7(2), 111-121.
- Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan *Phishing* dalam Ketentuan Hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 5(1), 19-24. <https://doi.org/10.18196/ijclc.v5i1.19853>
- Maharlina Darni Purwandari. (2024). Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus *Phishing*. Skripsi.
- Naufal, R. A. (2020). Tanggung Jawab PT Tokopedia Dalam Kasus Kebocoran Data Pribadi Pengguna. 163.
- Nurul Qamar, F. S. R. (2020). Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal. In *Sustainability (Switzerland)* (Vol. 11, Issue 1).
- Oeliga, C., Rasmini, & Johaness. (2022). Hukum Pidana Bagi Pelaku Penipuan Transaksi Elektronik Jual Beli Online (E-Commerce) di Indonesia. *Datin Law Journal*, 3(2), 145-152.

- Ramdhan, T. W., Florina, I. D., & Permadi, D. (2024). Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo.co. *Journal of Education Research*, 5(3), 3368–3379. <https://doi.org/10.37985/jer.v5i3.1491>
- Ramli, T. S., Ramli, A. M., Budhijanto, D., Permata, R. R., Adolf, H., Damian, E., & Palar, M. R. A. (2019). Prinsip Prinsip Cyber Law Pada Media Over the Top E-Commerce Berdasarkan Transformasi Digital Di Indonesia. *Jurnal Legislasi Indonesia*, 16(3), 392–398.
- Ridwan, Thalib, H., & Baharuddin, H. (2016). *Journal of Lex Generalis (JLS)*. *Journal of Lex Theory*, 1(2), 116–128.
- Runtuuwu, G. T. J. (2025). PERTANGGUNGJAWABAN PIHAK BANK TERHADAP KASUS CARD TRAPPING YANG DIALAMI OLEH NASABAH. *Lex Crimen Jurnal Fakultas Hukum, Unsrat*, 13(1).
- Salsabila, N., Sahib, M., Idayanti, S., & Rahayu, K. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. *Pancasakti Law Journal*, 1, 61–74.
- Sangojoyo, B. F., Kevin, A., & Sunlaydi, D. B. (2022). Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce di Indonesia. *Kosmik Hukum*, 22(1), 27. <https://doi.org/10.30595/kosmikhukum.v22i1.12154>
- Sitorus, S. (2018). Upaya Hukum Dalam Perkara Perdata (Verzet , Banding, Kasasi, Peninjauan Kembali dan Derden Verzet). *Jurnal Hikmah*, 15(64), 63–71.
- Tampongangoy, G. H. (2015). Arbitrase Merupakan Upaya Hukum Dalam Penyelesaian Sengketa Dagang Internasioanal. *Lex et Societatis*, III(1), 140–150.
- Terintegrasi, S., & Berkesinambungan, K. D. A. N. (2019). *Adil indonesia jurnal volume 1 nomor 1, januari 2019*. 1(3), 51–60.
- Tri Andika Hidayatullah, Ismansyah, N. M. . (2023). Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data. *Unes Law Review*, 4(2), 11–56.
- Yati Nurhayati. (2015). Pengantar Ilmu Hukum. In *Proceedings of the National Academy of Sciences (Vol. 3, Issue 1)*.