Co-Value: Jurnal Ekonomi, Koperasi & Kewirausahaan
Volume 14, Nomor 12 Mei 2024
p-ISSN: 2086-3306 e-ISSN: 2809-8862

Pencurian Data Pribadi di Dunia Maya *(Phising Cybercrime)* yang ditinjau dalam Perspektif Kriminologi

Muhammad Fadli[1], Dijan Widijowati[2], Dwi Andayani[3]
[1,2,3] Universitas Bhayangkara, Jakarta Raya, Indonesia.
Email: Mfadliabdulsalam@gmail.com

Abstrak

Phishing cybercrime merupakan kriminal yang muncul dari efek buruk teknologi yang kini tumbuh begitu pesat. Kejahatan *phishing cybercrime* bersifat virtual dikarenakan pelaku tidak tampil atau menyerang secara fisik. Penelitian ini bertujuan untuk mengkaji fenomena pencurian data pribadi di dunia maya, khususnya dalam konteks kejahatan siber phishing, dari perspektif kriminologi. Dalam era teknologi informasi yang maju pesat, kejahatan siber menjadi ancaman serius bagi individu dan masyarakat. Penelitian ini menyoroti dua faktor penting yang mempengaruhi terjadinya kejahatan siber phishing, yaitu faktor teknis dan faktor ekonomi. Faktor teknis mencakup dampak buruk perkembangan teknologi informasi yang memudahkan para pelaku dalam melancarkan kegiatan kriminal. Sementara faktor ekonomi berkaitan dengan motif ekonomi yang mendorong para pelaku untuk mencuri data pribadi dan menggunakannya untuk tujuan yang merugikan. Penelitian ini menggunakan metode analisis deskriptif dengan mengumpulkan data dari berbagai sumber terkait kejahatan siber phishing dan perspektif kriminologi. Dari segi perspektif kriminologi *phishing cybercrime*, ada 2 (dua) faktor penting yang mempengaruhi terjadinya tindak kejahatan komputer (cybercrime) yakni Faktor Teknis dan Faktor Ekonomi. Perlindungan hukum mengenai kejahatan *phishing cybercrime* sudah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP). Kejahatan *Phishing cybercrime* tidak dapat dihilangkan secara total. Dengan adanya Undang-Undang tersebut setidaknya dapat mengurangi jumlah cybercrime yang terjadi di Indonesia. Hasil penelitian menunjukkan bahwa kejahatan siber phishing memiliki dampak yang signifikan terhadap individu dan masyarakat, baik secara finansial maupun emosional. Oleh karena itu, peningkatan kesadaran, pendidikan, dan pengawasan terhadap keamanan data pribadi menjadi sangat penting dalam menghadapi tantangan kejahatan siber.

Kata Kunci: *Phising, Cybercrime,* Kriminologi.

Abstract

Cybercrime phishing is a crime that arises from the adverse effects of technology that is now growing so rapidly. Cybercrime phishing crimes are virtual because the perpetrator does not appear or physically attack. This study aims to examine the phenomenon of personal data theft in cyberspace, especially in the context of phishing cybercrime, from a criminological perspective. In the era of rapidly advancing information technology, cybercrime poses a serious threat to individuals and society. This research highlights two important factors that influence the occurrence of phishing cybercrimes, namely technical factors and economic factors. Technical factors include the adverse effects of the development of information technology that makes it easier for perpetrators to carry out criminal activities. While economic factors are related to economic motives that encourage perpetrators to steal personal data and use it for harmful purposes. This study uses a descriptive analysis method by collecting data from various sources related to phishing cybercrime and criminological perspectives. In terms of cybercrime phishing criminology perspective, there are 2 (two) important factors that influence the occurrence of computer crime (cybercrime), namely Technical Factors and Economic Factors. Legal protection regarding phishing cybercrime is regulated in the Electronic Information and Transaction Law (ITE Law) and the Personal Data

Protection Law (PDP Law). Phishing cybercrime cannot be completely eliminated. With the existence of this law, at least it can reduce the number of cybercrimes that occur in Indonesia. The results show that phishing cybercrime has a significant impact on individuals and society, both financially and emotionally. Therefore, increased awareness, education, and surveillance of personal data security are critical in facing the challenges of cybercrime.

***Keywords**: Phishing, Cybercrime, Criminology.*

PENDAHULUAN

Kemajuan teknologi informasi telah dianggap sebagai kekuatan yang memiliki kemampuan untuk mengendalikan nasib manusia. Hampir semua aktivitas sehari-hari dilakukan melalui internet, yang menghubungkan pengguna dengan data pribadi. Namun, masalah keamanan dan privasi data menjadi hal utama dari sistem informasi tersebut (Rustam, 2018). Kemajuan dalam teknologi informasi telah dianggap sebagai kekuatan yang mampu mempengaruhi nasib seseorang (Tampubolon, 2019). Meskipun teknologi informasi mempercepat kemajuan dalam kehidupan manusia, namun tidak dapat diabaikan bahwa hal tersebut juga membawa risiko. Pemanfaatan teknologi secara tidak etis dapat menyebabkan timbulnya kejahatan daring yang dikenal sebagai *"cyber crime"*. Sehingga, perlindungan data dan keamanan siber menjadi semakin penting dalam menghadapi tantangan ini (Rumlus & Hartadi, 2020).

Fenomena cybercrime, atau kejahatan daring, telah menjadi sumber kekhawatiran yang signifikan karena melibatkan berbagai aktivitas seperti carding, hacking, penipuan, terorisme, dan penyebaran informasi yang merugikan. Keberadaan kegiatan kriminal online tersebut menjadi perhatian serius karena dampaknya yang meluas dan merugikan. Tindak kejahatan yang terjadi di dunia maya seringkali memiliki motif tertentu yang mendasarinya. Penting untuk diakui bahwa kejahatan *cyber* dapat menyebabkan kerugian bagi pihak lainnya. *Cybercrime* merujuk pada serangkaian aktivitas kriminal yang dilakukan melalui internet. Contoh-contoh kejahatan ini mencakup pencurian identitas, penipuan online, serangan malware seperti virus dan ransomware, penyebaran konten ilegal seperti pornografi anak, serta hacking yang bertujuan untuk mengakses informasi pribadi atau data sensitif. Selain itu, aktivitas seperti cyberbullying, penipuan finansial, dan serangan terhadap infrastruktur kritis juga termasuk dalam kategori cybercrime. Kejahatan ini menimbulkan dampak serius terhadap individu, perusahaan, dan masyarakat secara keseluruhan (Suharto & Kurniawan, 2020).

Ada dua faktor yang dapat memicu munculnya *cybercrime*, yaitu faktor teknis dan faktor sosio-ekonomi. Secara teknis, perkembangan teknologi informasi dapat memiliki dampak negatif pada kemajuan masyarakat. Keberhasilan teknologi tersebut dapat menghilangkan batas-batas wilayah negara dan mempersempit dunia. Keterhubungan antar jaringan juga dapat memudahkan pelaku kejahatan untuk melakukan aktivitas kriminal. Selain itu, ketidakmerataan distribusi teknologi juga dapat menyebabkan ketimpangan kekuatan antara individu atau kelompok.

Pencurian data di dunia online dikenal dengan istilah phishing, yang merupakan kejahatan untuk memperoleh informasi pribadi atau rahasia seseorang secara ilegal.

Tindakan ini bertujuan untuk memperoleh nomor kartu kredit, PIN, User ID, nomor telepon, nomor rekening, dan informasi pribadi lainnya (Latumahina, 2014). Salah satu metode yang digunakan oleh pelaku phishing adalah dengan menyebarkan tautan palsu di akun media sosial melalui iklan yang menarik dan menggiurkan. Dengan cara ini, pelaku dapat mencuri informasi pribadi dari orang tersebut untuk mendapatkan keuntungan, misalnya dengan mencuri uang dari rekening pengguna atau menggunakan rekening tersebut sebagai media pembayaran online.

Kejadian pelanggaran privasi yang melibatkan bocornya informasi pribadi sering terjadi di Indonesia (Disemadi & Prasetyo, 2021). Dalam sektor perbankan, informasi pribadi dapat terungkap dalam berbagai kegiatan seperti pertukaran data pribadi antara lembaga keuangan, penyaluran informasi kepada pihak ketiga terkait transaksi keuangan, atau melalui penyedia jasa pihak ketiga yang mengelola data transaksi. Di bidang medis, data pasien sering kali tersedia untuk tujuan asuransi atau program dukungan pemerintah tanpa persetujuan langsung dari pasien dan kadang-kadang dapat disalahgunakan untuk kepentingan yang tidak sah. Pada platform jual beli online, informasi pribadi seperti preferensi belanja dan riwayat transaksi sering kali diambil secara tidak sah menggunakan cookies yang dapat membahayakan privasi konsumen dan digunakan untuk kepentingan yang tidak diinginkan. Dalam platform transportasi online, penggunaan nomor telepon konsumen dapat disalahgunakan untuk tujuan yang tidak terkait dengan layanan, seperti mengirim pesan tidak relevan atau mengancam konsumen atas ulasan negatif (Yuniarti, 2019).

Pada tanggal 12 Mei 2021, Indonesia mengalami kasus serius terkait kebocoran informasi atau data pribadi yang melibatkan sekitar 279 juta data warga. Informasi yang tersedia mencakup detail seperti nama lengkap sesuai Kartu Tanda Penduduk (KTP), nomor telepon, alamat email, Nomor Identitas (NIK), lokasi tinggal, serta perkiraan pendapatan. Lebih dari 20 juta data juga dilengkapi dengan foto pribadi penduduk. Akun Kotz menawarkan sampel data gratis kepada pengguna dengan menyediakan 1 juta sampel dan memperkenalkan 3 tautan yang membutuhkan kata sandi untuk mengaksesnya. Kasus ini menimbulkan keprihatinan serius terhadap privasi data dan keamanan informasi pribadi masyarakat (Luthiya et al., 2021).

Meningkatnya jumlah insiden pencurian data pribadi di Indonesia membuat pemerintah harus mengambil langkah-langkah tegas untuk mencegah atau setidaknya meminimalkan risiko kejadian serupa di masa depan. Hal ini dapat dilakukan dengan mengimplementasikan perlindungan hukum yang lebih kuat untuk merespons segera kejadian pencurian data. Kasus semacam ini memiliki potensi untuk menimbulkan kerugian bagi korban, baik dalam bentuk materiil maupun non-materiil. Pencurian informasi pribadi tidak hanya berdampak pada pengunjung situs web atau sistem elektronik, tetapi juga dapat merugikan perusahaan yang menggunakan sistem elektronik dan lembaga keuangan seperti bank sebagai mitra pembayaran. Oleh karena itu, korban pencurian data tidak hanya melibatkan individu, tetapi juga lembaga terkait dan secara luas, masyarakat Indonesia. Dalam hal ini, tindakan preventif dan responsif yang tepat dari pemerintah menjadi sangat penting untuk menjaga keamanan dan privasi data pribadi masyarakat (Luthiya et al., 2021). Akibatnya, tindakan pencurian data di ranah cybercrime seperti phishing dapat dikenai sanksi hukum sesuai dengan ketentuan yang tercantum

dalam Undang-Undang Nomor 11 Tahun 2008 yang telah mengalami revisi melalui Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), dan juga Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Tujuan dari penelitian ini untuk menyelidiki perlindungan hukum yang ada bagi korban pencurian data pribadi di dunia maya (phishing) dalam perspektif kriminologi. Ini melibatkan pemahaman mendalam tentang mekanisme hukum yang ada, identifikasi celah atau kekurangan dalam perlindungan hukum yang ada, serta evaluasi efektivitasnya dalam menangani kasus-kasus pencurian data pribadi di ranah cybercrime dan menganalisis pengaturan perlindungan hukum terkait pencurian data pribadi di Indonesia. Hal ini mencakup pemahaman terhadap regulasi yang berkaitan dengan perlindungan data pribadi, serta identifikasi kebijakan atau langkah-langkah yang telah diambil oleh pemerintah atau lembaga terkait untuk mengatasi masalah ini.

Manfaat dari penelitian ini untuk memberikan pemahaman yang lebih baik tentang perlindungan hukum bagi korban pencurian data pribadi di dunia maya (phishing), yang dapat membantu dalam penyusunan kebijakan yang lebih efektif dalam mengatasi cybercrime. Dengan demikian, penelitian ini dapat berkontribusi dalam meningkatkan keamanan cyber bagi individu dan organisasi serta memberikan wawasan yang lebih mendalam tentang keadaan pengaturan perlindungan hukum terkait pencurian data pribadi di Indonesia. Hal ini dapat menjadi dasar untuk merekomendasikan perbaikan atau peningkatan dalam undang-undang dan regulasi yang ada, sehingga dapat meningkatkan perlindungan terhadap data pribadi masyarakat di Indonesia. Dengan demikian, penelitian ini dapat berpotensi untuk membawa dampak positif dalam mencegah dan menangani kasus-kasus pencurian data pribadi di tingkat nasional.

METODE PENELITIAN

Penelitian ini merupakan jenis penelitian yuridis normatif yang menggunakan studi pustaka sebagai metode untuk mengumpulkan data sekunder. Pendekatan ini bertujuan untuk menganalisis peraturan-peraturan hukum dan doktrin-doktrin hukum terkait dengan suatu isu spesifik. Metode analisis meliputi kajian terhadap teori-teori hukum, prinsip-prinsip hukum, serta konsep-konsep hukum yang relevan yang terdapat dalam bahan hukum primer dan sekunder. Tujuan dari penelitian yuridis normatif adalah memberikan pemahaman yang komprehensif tentang kerangka hukum yang mengatur suatu masalah atau fenomena hukum, serta menyusun rekomendasi untuk pengembangan atau peningkatan regulasi hukum yang ada.

HASIL DAN PEMBAHASAN

Perlindungan Hukum bagi korban *Phising Cybercrime* dalam Perspektif Kriminologi

Bertambahnya jumlah pengguna internet, kebutuhan untuk melindungi informasi atau data pribadi juga semakin meningkat (Disemadi, 2021). Kasus-kasus yang kerap terjadi terkait dengan penyalahgunaan informasi pribadi dan kejahatan, seperti

e-ISSN: 2809-8862
p-ISSN: 2086-3306

perdagangan data pribadi, pencurian identitas online, penyebaran informasi pribadi seseorang tanpa izin, penipuan, dan kejahatan pornografi.

Phising adalah salah satu bentuk kejahatan cyber yang terjadi di platform jaringan komputer. Dalam keamanan komputer, *phishing* merupakan tindak kriminal elektronik yang melibatkan penipuan. (Saputra Gulo et al., 2020). Seiring dengan kemajuan zaman, tindak kriminal juga mengalami perkembangan dan penyebaran yang luas. Ancaman kejahatan saat ini dapat juga datang melalui jaringan komputer. Kemajuan teknologi memberikan banyak manfaat dalam bentuk peluang untuk mendapatkan informasi, pekerjaan, partisipasi politik, demokrasi, dan berbagai keuntungan lainnya. Namun, kriminalitas di dunia maya semakin berbahaya karena cakupannya yang sangat luas (Alhakim & Sofia, 2021).

Orang yang melakukan *phishing* biasanya disebut sebagai *hacker*. *Hacker* memiliki pengetahuan dan keterampilan dalam menguasai serta menerapkan bahasa pemrograman. Cara kerja *hacker* untuk memahami sistem dan infrastruktur yang digunakan di target tertentu adalah dengan menyusup atau mengakses jaringan komputer yang menjadi sasaran. Penetrasi atau akses ke jaringan komputer target dilakukan dengan mengeksploitasi kelemahan yang ada dalam sistem tersebut. Dengan kata lain, *hacke*r masuk ke dalam situs secara ilegal tanpa izin. Dengan keahliannya, *hacker* dapat memasuki dan mengakses situs korban bahkan jika situs tersebut telah dilengkapi dengan sistem keamanan. Misi utama *hacker* adalah untuk merusak sistem yang digunakan oleh pemilik situs tersebut. *Hacker* yang berhasil masuk ke dalam sistem orang lain dianggap sebagai kejahatan *cybercrime* karena situs tersebut merupakan properti pribadi milik pemiliknya. Dengan mengubah tampilan situs web secara tidak sah dan menghapus beberapa file yang ada di dalamnya, ini tidak hanya merupakan tindakan keingintahuan biasa, tetapi juga merupakan tindakan kriminal karena menyebabkan kerugian bagi pemilik akun.

Melihat kenyataan hukum saat ini, pentingnya untuk mengantisipasi dampak negatif dari perkembangan teknologi yang telah disalahgunakan sebagai alat kriminal. Hal ini memerlukan kebijakan hukum yang dapat mengatasi kejahatan cybercrime melalui hukum pidana, termasuk dalam hal pembuktian kasus tersebut. Pentingnya hal ini karena dalam penegakan hukum pidana, seseorang hanya dapat dihukum atau dianggap bersalah atas tindakannya jika telah terbukti secara sah dan meyakinkan, sesuai dengan prinsip asas legalitas yang diatur dalam Pasal 1 ayat (1) KUHP. Prinsip ini menyatakan bahwa tidak ada tindak pidana dan hukuman tanpa adanya aturan hukum pidana yang telah ada sebelumnya (Aldriano & Priyambodo, 2022).

Tindak kejahatan di bidang teknologi informasi sering dikategorikan sebagai white crime karena pelakunya memiliki pemahaman dan keahlian dalam menggunakan aplikasi internet atau bidang terkait. Karena kejahatan ini sering melintasi batas negara dan dilakukan secara transnasional, kejahatan dunia maya ini dapat digolongkan sebagai dua jenis kejahatan, yaitu white crime dan transnational crime. Di Indonesia, beberapa kasus cybercrime yang sering terjadi meliputi penipuan, perjudian online, penyebaran berita palsu, pencurian identitas, dan pencurian data pribadi melalui internet (Aryyaguna, 2017).

Dalam sudut pandang kriminologi, ada beberapa faktor dan alasan yang menyebabkan kasus cybercrime phishing terjadi. Dari segi alasan, kejahatan ini biasanya dapat dibagi menjadi dua kategori, yaitu:

1. Motif intelektual kriminal terjadi saat seseorang melakukan kejahatan semata-mata untuk kepuasan pribadi dan untuk menunjukkan kemampuannya dalam merancang dan menerapkan teknologi informasi. Motif ini umumnya dilakukan oleh individu.
2. Motif ekonomi, politik, dan kriminalitas merujuk pada alasan di balik suatu tindak kriminal yang dilakukan dengan tujuan memperoleh keuntungan pribadi atau kelompok yang dapat merugikan pihak lain baik secara ekonomi maupun politis. Kriminalitas dengan motif ini, bertujuan untuk menciptakan dampak besar dan sering kali dilakukan oleh perusahaan atau korporasi..

Kriminologi berasal dari kata "crimen" dan "logos", yang mengacu pada ilmu pengetahuan tentang kejahatan. Istilah ini awalnya diperkenalkan oleh seorang antropolog Prancis bernama P. Topinard pada tahun 1879. Kriminologi dapat dijelaskan sebagai ilmu yang mempelajari tentang kejahatan. Kejahatan yang dimaksud adalah tindakan yang dilarang oleh undang-undang. Pemahaman ini memberikan pandangan yang tepat tentang kriminologi sebagai bagian dari ilmu yang mempelajari perilaku kriminal (Yuliartini, 2019). Kriminologi dibagi menjadi tiga bidang ilmu utama, yaitu:

1. Sosiologi hukum adalah kajian tentang bagaimana tindakan tertentu dianggap sebagai kejahatan berdasarkan norma-norma hukum yang melarangnya dan mengancam dengan sanksi. Oleh karena itu, penentuan apakah suatu tindakan dianggap sebagai tindak kriminal bergantung pada prinsip-prinsip hukum.
2. Etiologi Kriminal adalah bagian dari kriminologi yang bertujuan untuk melakukan analisis ilmiah tentang asal-usul kejahatan.
3. Penologi adalah ilmu yang mempelajari hukuman, mencakup penerapan hak-hak yang berkaitan dengan usaha pengendalian kejahatan, baik melalui tindakan represif maupun preventif.

Beberapa faktor utama yang dapat menyebabkan timbulnya kejahatan *cyber phishing* (Hariyono & Simangunsong, 2023) adalah: 1) Ketidakseimbangan antara kemajuan suatu negara dan kesejahteraan masyarakatnya yang meningkatkan potensi ketimpangan sosial; 2) Gaya hidup; 3) Kurangnya sosialisasi atau edukasi baik dari lembaga pendidikan seperti sekolah maupun dari orang tua mengenai penggunaan internet yang dapat menyebabkan penyalahgunaan beragam; 4) Peningkatan penggunaan media sosial, media elektronik, dan penyimpanan data virtual (cloud), yang membuat individu semakin terpaku pada akses internet dalam kehidupan sehari-harinya; 5) Kelalaian; 6) Ingin diakui tentang keahliannya oleh orang lain; 7) Kemajuan teknologi dan kemudahan akses internet.

Secara umum, asal-usul terjadinya kejahatan phishing dapat dipilah menjadi dua faktor, diantaranya: 1) Faktor Teknis, koneksi yang saling terhubung antar jaringan mempermudah pelaku kejahatan dalam melaksanakan tindakannya, sedangkan peningkatan penggunaan teknologi yang tidak merata menyebabkan ketimpangan kekuatan antara pihak-pihak yang terlibat; 2) Faktor Ekonomi, Kejahatan *phishing cybercrime* bisa dianggap sebagai bagian dari aktivitas ekonomi. Permasalahan yang perlu diperhatikan dalam kejahatan ini adalah keamanan jaringan. Sebagai komoditas ekonomi, cybercrime menjadi bagian dari skenario besar dalam aktivitas ekonomi global.

Berdasarkan analisis penulis terhadap peningkatan kasus *phishing cybercrime*, terdapat beberapa faktor yang mempengaruhinya, antara lain: 1) Kurangnya pemahaman

hukum di kalangan masyarakat, dimana pemahaman ini merujuk pada pengetahuan tentang tindakan yang sesuai dengan hukum yang berlaku. Saat ini, pemahaman hukum masyarakat terkait dengan kegiatan *phishing cybercrime* masih dianggap kurang karena kurangnya kesadaran tentang tindakan dan konsekuensi yang timbul dari aktivitas tersebut. Semakin rendah tingkat pemahaman tentang teknologi, semakin besar peluang bagi pelaku kejahatan untuk memanfaatkannya (Setiawan, 2018). Melalui pemahaman tentang *phishing cybercrime*, peran masyarakat menjadi sangat berarti dalam upaya penanggulangan fenomena ini. Tanpa pemahaman yang memadai, aktivitas *phishing cybercrime* dapat meluas karena masyarakat tidak menyadari tindakan yang sebenarnya dilakukan sehingga bisa mengakibatkan penipuan dan kerugian finansial lainnya. Keamanan juga menjadi faktor penting karena pelaku menggunakan akses internet yang fleksibel, baik di lingkungan terbuka maupun tertutup. Namun, tingkat keamanan internet yang masih rentan membuat siapa pun dapat melakukan aktivitas di dunia maya tanpa menyadari batasan-batasan ini sehinga dapat mendorong pertumbuhan kejahatan *phishing cybercrime*..

Penerapan hukuman terhadap pelaku tindak pidana telah memberikan ancaman bagi pengguna internet. Sejak diberlakukannyaUU ITE dan UU PDP, para pelaku kejahatan *phishing cybercrime* yang merupakan pengguna internet aktif yang sengaja mengambil informasi data dari korban dapat dijerat dengan Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE dan Pasal 67 ayat 1 UU PDP. Hukum yang diatur dalam UU ITE tersebut dapat digunakan untuk menindak segala bentuk kegiatan cybercrime terkait pencurian data pribadi, tanpa terkecuali.

Pengaturan Perlindungan Hukum Pencurian Data Pribadi di Indonesia

Di Indonesia, terdapat kerangka hukum yang relevan untuk melindungi data pribadi. Pertama, UU PDP yang menjadi implementasi dari Pasal 28G ayat (1) UUD 1945, menjamin hak setiap individu terhadap perlindungan privasi, kehormatan, serta harta benda yang dimilikinya, dan juga hak atas rasa aman dan perlindungan dari ancaman ketakutan. Kedua, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) mengatur bahwa kebebasan dan kerahasiaan dalam korespondensi, termasuk komunikasi melalui sarana elektronik, tidak boleh diintervensi, kecuali atas perintah dari pengadilan. Dengan demikian, kerahasiaan informasi dalam surat maupun komunikasi elektronik harus dijaga dan tidak boleh dilanggar, kecuali berdasarkan keputusan hukum (Djafar, 2019). Ketiga, secara spesifik UU ITE juga mengatur tentang penggunaan data pribadi dalam Pasal 26 ayat (1), (2), dan (3). Pasal-pasal tersebut menetapkan bahwa penggunaan data pribadi harus memperoleh persetujuan dari pemilik data, data tersebut harus dihapus jika diminta oleh pemiliknya melalui keputusan pengadilan, dan jika data yang disimpan oleh penyedia layanan elektronik tidak lagi relevan, data tersebut juga harus dihapus (Sujamawardi, 2018).

Pemerintah Indonesia telah mengesahkan UU PDP sebagai upaya untuk melindungi informasi pribadi penduduknya. Akibatnya, setiap pelanggaran atas kebijakan penggunaan data pribadi akan dikenakan sanksi sesuai dengan ketentuan yang berlaku. Menurut Pasal 1 Ayat 1 UU PDP, data pribadi didefinisikan sebagai informasi mengenai individu yang dapat diidentifikasi secara langsung maupun tidak langsung, baik melalui sistem elektronik maupun non-elektronik.

Ada beberapa klasifikasi data pribadi yang penting untuk diketahui oleh masyarakat. Menurut Pasal 4 Ayat 1 dari UU PDP, terdapat dua jenis data pribadi, yaitu: data pribadi yang bersifat spesifik merujuk pada informasi pribadi yang jika diproses dapat memiliki dampak signifikan pada individu yang bersangkutan. Sementara itu, data pribadi yang bersifat umum mengacu pada informasi pribadi yang dapat diketahui oleh orang lain.

Data pribadi yang memiliki karakteristik spesifik mencakup beberapa jenis informasi, termasuk namun tidak terbatas pada:

1. Informasi terkait kesehatan
2. Data biometrik
3. Informasi genetik
4. Catatan kejahatan
5. Data anak
6. Data keuangan pribadi
7. Informasi pribadi lainnya yang diatur oleh undang-undang.

Di sisi lain, data pribadi yang bersifat umum terdiri dari:

1. Nama lengkap
2. Jenis kelamin
3. Kewarganegaraan
4. Agama
5. Status pernikahan
6. Informasi pribadi yang digabungkan untuk mengidentifikasi individu..

Penegakan hukum terhadap pelanggaran informasi pribadi oleh penyelenggara data harus disesuaikan dengan sifat pelanggaran yang dilakukan oleh penyelenggara tersebut. Ketentuan-ketentuan ini biasanya terkait dengan kewajiban-kewajiban yang harus dipatuhi dalam pengelolaan data pribadi, terutama dalam bentuk elektronik. Sebagai contoh, Pasal 26 ayat (3) UU ITE mengharuskan penyelenggara sistem elektronik untuk menghapus informasi yang sudah tidak relevan berdasarkan permintaan dari pemiliknya yang didukung oleh keputusan pengadilan (Budhijanto, 2017). Ayat 4 menetapkan bahwa penyelenggara wajib menyediakan mekanisme untuk menghapus dokumen elektronik tersebut. Pasal 15 ayat (1) menegaskan bahwa penyelenggara harus mengelola sistem mereka dengan andal dan aman serta bertanggung jawab atas operasional sistem secara cermat. Hal ini menunjukkan bahwa jika terjadi pelanggaran data pribadi, tanggung jawab utama jatuh pada penyelenggara sistem elektronik tersebut. Artinya, mereka dapat dituntut langsung oleh pihak yang menjadi korban pelanggaran data pribadi karena kewajiban mereka dalam menjaga keamanan dan keandalan sistem.

Apabila terjadi pelanggaran, maka pemilik data berhak untuk menghapus informasi yang tidak relevan. Permintaan penghapusan ini merupakan bagian dari hak yang disebut sebagai hak untuk dilupakan (right to erasure) dan hak untuk tidak dicantumkan (right to delisting). Hak ini merupakan perkembangan dari hak untuk dilupakan yang memungkinkan individu untuk menghapus informasi pribadi mereka dari basis data online dan menghentikan penyebaran informasi tersebut. Dengan demikian, hak ini memberikan kontrol kepada individu atas informasi pribadi mereka dan memberikan perlindungan terhadap penyalahgunaan data (Al Fahri, n.d.). Hal ini menekankan bahwa individu memiliki hak untuk menjaga kerahasiaan dan kontrol atas data pribadi mereka. Karena

e-ISSN: 2809-8862
p-ISSN: 2086-3306

risiko potensial terhadap kebocoran atau penyalahgunaan data pribadi, baik pengendali maupun pemroses data pribadi memiliki tanggung jawab untuk mengelola sistem mereka dengan baik guna memastikan keamanan dalam pemrosesan data pribadi. Dengan kata lain, keberadaan hak untuk menghapus data pribadi menggarisbawahi pentingnya perlindungan privasi dan keamanan dalam pengelolaan informasi pribadi dalam lingkungan digital (Giurgiu & Lommel, 2014).

UU PDP mengatur perlindungan data pribadi dengan lebih tegas. Undang-undang tersebut menegaskan bahwa jika ada kegagalan dalam menjaga keamanan data pribadi, penyelenggara data diwajibkan memberitahukan hal tersebut kepada pemilik data. Kegagalan dalam melindungi data pribadi merujuk pada situasi di mana kerahasiaan, integritas, dan ketersediaan data pribadi terganggu. Hal ini termasuk pelanggaran keamanan yang disengaja maupun tidak disengaja yang dapat mengakibatkan kerusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap data pribadi tersebut. Contohnya adalah ketika sebuah perusahaan besar menjadi korban serangan cyber yang mengakibatkan jutaan data pribadi pengguna mereka terungkap, baik karena kelemahan dalam sistem keamanan, kurangnya pengawasan terhadap akses data, atau kurangnya kesadaran akan ancaman keamanan cyber.. Selain itu, berdasarkan Pasal 47 UU PDP, penyelenggara diwajibkan untuk mematuhi prinsip-prinsip perlindungan data pribadi sebagai bentuk tanggung jawab mereka dalam pengolahan data.

Tuntutan terhadap pelanggaran data pribadi juga bisa didasarkan pada Pasal 1365 KUHPerdata. Pasal tersebut menegaskan bahwa pihak yang melakukan pelanggaran hukum dan menyebabkan kerugian pada pihak lain harus mengganti kerugian yang ditimbulkan. Gugatan ini tidak hanya berlaku untuk tindakan yang disengaja, tetapi juga dapat berdasarkan kelalaian, sebagaimana diatur dalam Pasal 1366 KUHPerdata. Dengan demikian, Pasal 1365 dan 1366 KUHPerdata memberikan landasan hukum bagi individu yang ingin menuntut ganti rugi atas pelanggaran data pribadi, baik yang disengaja maupun yang terjadi karena kelalaian.

Gugatan terhadap pelanggaran data pribadi bertujuan untuk mendapatkan ganti rugi bagi korban. Namun, untuk berhasil dalam gugatan tersebut, korban harus dapat membuktikan beberapa aspek. Pertama, bahwa penyelenggara data pribadi bertanggung jawab untuk melindungi data pribadi. Kedua, terjadi pelanggaran oleh penyelenggara. Ketiga, bahwa korban mengalami kerugian nyata. Dan keempat, bahwa kerugian tersebut diakibatkan oleh kelalaian penyelenggara data pribadi. Dengan membuktikan keempat aspek ini, korban dapat berhasil dalam memperoleh ganti rugi atas pelanggaran data pribadi yang dialaminya (Romanosky & Acquisti, 2009). Sebagai contoh, jika penyelenggara sistem elektronik memiliki kewajiban untuk memberikan pemberitahuan kepada pengguna tentang akses yang tidak sah ke sistem informasi, maka wajib bagi penyelenggara sistem elektronik untuk memberikan pemberitahuan tersebut. Namun, jika kewajiban tersebut tidak dipenuhi, pemilik data pribadi dapat menuntut ganti rugi atas kerugian yang ditimbulkan.

Dalam gugatan terkait pelanggaran data pribadi dalam kerangka UU PDP, penyelenggara data pribadi yang mencakup pengendali dan/atau prosesor, bertanggung jawab untuk membuktikan apakah ada atau tidak ada pelanggaran data pribadi yang terjadi. Pasal 24 menjelaskan bahwa pengendali data pribadi harus dapat menunjukkan bukti

persetujuan dari subjek data. Hal ini berarti bahwa jika terjadi pelanggaran, salah satu hal yang harus dibuktikan oleh pengendali data pribadi adalah bahwa pemilik data telah memberikan persetujuan terhadap pemrosesan data pribadi tersebut. Dengan demikian, bukti persetujuan menjadi penting sebagai salah satu syarat yang harus dipenuhi oleh pengendali data pribadi untuk memastikan bahwa pemrosesan data dilakukan secara sah dan sesuai dengan peraturan yang berlaku. Pasal 47 memperjelas bahwa pengendali data pribadi memiliki kewajiban untuk bertanggung jawab atas setiap tindakan pemrosesan data yang dilakukan dengan membuktikan kepatuhan mereka terhadap prinsip-prinsip pelindungan data pribadi. Oleh karena itu, jika penyelenggara data pribadi dihadapkan pada tuntutan hukum karena kesalahan yang mengakibatkan kerugian bagi pemilik data, mereka harus menunjukkan bahwa pemrosesan data tersebut telah dilakukan sesuai dengan prinsip-prinsip pelindungan data pribadi. Sebagai pihak yang memiliki pengetahuan yang pasti dan rinci tentang pemrosesan data, beban pembuktian mengenai pemenuhan prinsip pelindungan data pribadi seharusnya ditempatkan pada penyelenggara data pribadi.

Ada empat hal yang ditegaskan sebagai larangan terkait pengelolaan data pribadi menurut UU PDP, yaitu mengenai larangan untuk memperoleh dan mengumpulkan, mengungkapkan, meggunakan, dan memalsukan data pribadi dengan maksud untuk keuntungan pribadi atau keuntungan orang lain yang dapat merugikan orang lain. (Pasal 66 UU PDP).

Orang yang melanggar atau menyalahgunakan data pribadi seseorang akan dikenai sanksi atau hukuman sesuai dengan ketentuan dalam UU PDP. Pasal 65 dan Pasal 66 UU PDP mengatur larangan-larangan terkait penggunaan data pribadi beserta ancaman pidananya. Pelanggaran terhadap pasal 65 UU PDP dapat dikenai pidana penjara maksimal empat sampai dengan lima tahun dan/atau denda maksimal Rp. 4 miliar - Rp. 5 miliar. Sedangkan, pelanggaran terhadap pasal 66 UU PDP dapat dijatuhi pidana penjara maksimal enam tahun dan/atau denda maksimal Rp6 miliar.

KESIMPULAN

Pencurian data dalam ranah digital sering disebut sebagai phising, suatu tindakan kriminal yang melibatkan perolehan informasi pribadi atau rahasia seseorang secara ilegal. Phising cybercrime merupakan hasil dari perkembangan teknologi yang cepat, di mana pelaku kejahatan dapat melakukan aksinya tanpa perlu secara fisik hadir di tempat kejadian. Dalam kriminologi, terdapat dua faktor utama yang memengaruhi kemunculan tindak kejahatan komputer, yaitu Faktor Teknis dan Faktor Ekonomi. Dalam penegakan hukum terkait pencurian data di dunia maya, hukum yang relevan termasuk Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah mengalami perubahan melalui Undang-Undang No. 19 Tahun 2016, serta Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

DAFTAR PUSTAKA

Al Fahri, S. M. (n.d.). *Implementasi Kebijakan Privasi Terhadap Data Pribadi Pengguna E-Commerce Ditinjau dari UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Lazada)*. Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta.

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1), 2169–2175.

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377–385.

Aryyaguna, A. D. (2017). Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online. *Tidak Dipublikasikan). Universitas Hasanuddin*.

Budhijanto, D. (2017). *Revolusi cyberlaw Indonesia: pembaruan dan revisi Undang-Undang Informasi dan Transaksi Elektronik 2016*. PT Refika Aditama.

Disemadi, H. S. (2021). Legal Aspects Of 'Gali Lubang Tutup Lubang'in Fintech P2p Lending Business During Covid-19. *Tadulako Law Review*, *6*(2), 237–256.

Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Wajah Hukum*, *5*(1), 13–20.

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. *Seminar Hukum Dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*, *26*.

Giurgiu, A., & Lommel, G. (2014). A New Approach to EU Data Protection:-More Control over Personal Data and Increased Responsibility. *KritV, CritQ, RCrit. Kritische Vierteljahresschrift Für Gesetzgebung Und Rechtswissenschaft/Critical Quarterly for Legislation and Law/Revue Critique Trimestrielle de Jurisprudence et de Législation*, 10–27.

Hariyono, A. G., & Simangunsong, F. (2023). Perlindungan Hukum Korban Pencurian Data Pribadi (*Phishing cybercrime*) Dalam Perspektif Kriminologi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(1), 428–439.

Latumahina, R. E. (2014). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*.

Luthiya, A. N., Irawan, B., & Yulia, R. (2021). Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi. *Jurnal Hukum Pidana Dan Kriminologi*, *2*(2), 14–29.

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, *24*, 1061.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, *11*(2), 285–299.

Rustam, S. (2018). Analisa Clustering Phising Dengan K-Means Dalam Meningkatkan Keamanan Komputer. *ILKOM Jurnal Ilmiah*, *10*(2), 175–181.

Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal*, *1*(2), 68–81.

Setiawan, D. A. (2018). Perkembangan Modus Operandi Kejahatan Skimming Dalam

Pembobolan Mesin Atm Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime). *Era Hukum-Jurnal Ilmiah Ilmu Hukum*, *16*(2).

Suharto, B., & Kurniawan, A. B. (2020). Tindak Pidana Cybercrime bagi Pelaku Pemalsuan Data pada Situs E-Commerce (Phising). *JHP*, *17*, 57–61.

Sujamawardi, L. H. (2018). Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Dialogia Iuridica*, *9*(2).

Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurist-Diction*, *2*(2), 539–554.

Yuliartini, N. P. R. (2019). Kenakalan Anakdalam Fenomena Balapan Liardi Kota Singaraja Dalam Kajian Kriminologi. *Jurnal Advokasi*, *9*(1).

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147–154.