Legal Dialogica
Volume 1 Issue 1

Perlindungan Hukum Bagi Korban Penyebaran Data Yang Diretas Secara Ilegal Melalui Link Phishing

Nadila Cindy Qarolina, Zainuddin, Azwad Rachmat Hambali
Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Ω Surel Koresponden: andirairwan0@gmail.com

Abstract:

This research aims to determine and analyze legal protection regulations for victims of illegal distribution of hacked personal data via phishing links. As well as to find out and analyze legal protection efforts for victims of illegal distribution of hacked personal data via phishing links. This research uses normative legal research methods. The findings obtained in this research are legal protection regulations for victims of illegal distribution of hacked data via phishing links. And legal protection efforts for victims of illegal distribution of hacked data via phishing links. Based on the results of the research, the author found that the existence of regulations regarding legal protection for victims of illegal distribution of hacked data via phishing links can enable victims of phishing crimes to claim their losses due to phishing crimes and also by following legal measures for victims of illegal distribution of hacked personal data. through phishing links can fight for their rights and obtain appropriate legal protection.

Keywords: *Legal Protection, Data Distribution, Hacking, Illegal, Phishing Links.*

Abstrak:

Penelitian ini bertujuan untuk mengetahui dan menganalisis peraturan perlindungan hukum bagi korban penyebaran data pribadi yang diretas secara Ilegal melalui link phishing. Serta untuk mengetahui dan menganalisis upaya Perlindungan Hukum bagi korban penyebaran data pribadi yang diretas secara Ilegal melalui link phishing. Penelitian ini memakai Metode penelitian hukum normative. Temuan yang di peroleh dalam penelitian ini adalah peraturan perlindungan hukum terhadap korban penyebaran data yang diretas Secara illegal melalui link phising. Dan Upaya perlindungan hukum bagi korban penyebaran data yang diretas Secara illegal melalui link phising. Berdasarkan hasil penelitian penulis menemukan bahwa dengan adanya peraturan terkait perlindungan hukum korban penyebaran data yang diretas Secara illegal melalui link phising dapat membuat para korban kejahatan

phising dapat menuntut kerugiannya atas kejahatan phising dan juga dengan mengikuti Upaya-upaya hukum korban penyebaran data pribadi yang diretas Secara illegal melalui link phising dapat memperjuangkan hak-hak mereka dan mendapatkan perlindungan hukum yang sesuai.
Kata Kunci: *Perlindungan Hukum, Penyebaran Data, Peretasan,Ilegal, Link Phising.*

PENDAHULUAN

Negara Indonesia menjadi salah satu negara yang masyarakatnya mengikuti perkembangan kemajuan Ilmu Pengetahuan dan Teknologi (IPTEK) yang saat ini berkembang pesat dan meningkat. Kemajuan teknologi merupakan suatu yang pasti dalam Masyarakat saat ini, karena akan selalu berjalan seiring dengan kemajuan ilmu pengetahuan. Kehadiran Internet dengan segala manfaat baik yang bisa di dapatkan penggunanya, tidak bisa di pungkiri memiliki sisi negatif. Bentuk kontribusi yang diperoleh dari penggunaan internet seperti peningkatan kesejahteraan, kemajuan dan peradaban manusia. Namun, di sisi lain internet juga merupakan wadah bagi kejahatan baru yang ada pada dunia hukum saat ini yang di kenal dengan istilah kejahatan siber atau Cyber Crime. Di zaman informasi saat ini, penggunaan teknologi informasi dan komunikasi menjadi bagian intrinsik dari kehidupan sehari-hari, baik untuk urusan pribadi maupun bisnis. Seiring dengan perkembangan dan semakin pesatnya penggunaan internet, kejahatan siber pun semakin meningkat, salah satunya adalah *phishing*. Phishing merupakan salah satu metode serangan siber yang bertujuan untuk meretas atau mencuri data pribadi pengguna dengan cara menipu mereka untuk memberikan informasi sensitif melalui link ataupun tautan palsu yang menyerupai situs resmi.

Salah satu dasar hukum terkait upaya pelaku penyebaran data yang meretas secara ilegal melalui link *Phishing* Dalam QS. Al-Mutaffifinn (83):

وَيۡلٌ لِّلۡمُطَفِّفِيۡنَ ۙ ١ الَّذِيۡنَ اِذَا اكۡتَالُوۡا عَلَى النَّاسِ يَسۡتَوۡفُوۡنَ ۖ ٢
وَاِذَا كَالُوۡهُمۡ اَوۡ وَّزَنُوۡهُمۡ يُخۡسِرُوۡنَ ؕ ٣

Artinya :

"Celakalah bagi orang-orang yang curang (dalam menakar dan menimbang), (yaitu) orang-orang yang apabila menerima takaran dari orang lain, mereka minta dipenuhi, dan apabila mereka menakar atau menimbang untuk orang lain, mereka mengurangi.".

Ayat diatas mengutuk perbuatan curang dan penipuan, yang bisa dihubungkan dengan tindakan phishing yang merupakan upaya untuk menipu korban agar memberikan informasi sensitif. Sebagaimana Allah mengingatkan pelaku kecurangan, begitu pula para pelaku kejahatan siber seperti phishing harus diingatkan tentang akibat perbuatannya. Perlindungan hukum bagi korban menjadi penting untuk memastikan bahwa mereka mendapatkan hak-haknya dan dilindungi dari kezaliman serupa di masa depan. Ayat ini juga memberikan landasan moral untuk memperjuangkan keadilan bagi korban kejahatan. Penegakan hukum

terhadap kejahatan phishing bertujuan untuk menegakkan keadilan, sama seperti larangan Allah terhadap kecurangan dalam perdagangan. Indonesia adalah negara hukum seperti yang tertuang dalam konstitusi, sebagai sebuah negara hukum tentunya negara wajib melindungi setiap warga negaranya dari setiap perbuatan yang dapat merugikan apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara. Seperti halnya kejahatan yang terjadi di dunia maya atau biasa disebut dengan cybercrime. Kejahatan yang tidak mengenal ruang dan waktu ini mengalami perkembangan yang pesat akhir-akhir ini, kecanggihan teknologi yang disalah gunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi yang menyebabkan negara-negara berkembang kesulitan untuk menindak pelaku kejahatan komputer khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber daya manusia, sarana dan prasarana yang mendukung. Dalam Kasus Cyber Crimeberperan sangat penting dimana jarang sekali terdapat saksi dalam kasus Cyber Crimedikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri yang mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan[1].

Pengaturan tindak pidana siber dalam peraturan perundang-undangan Indonesia belum cukup mendukung baik terhadap hukum pidana materil maupun hukum pidana formil. Berbagai upaya untuk mengatur pengaturan pada peraturan perundang-undangan yang dapat mencegah adanya dampak negatif akibat dari perbuatan hukum. Hukum pidana Indonesia atau yang biasa disebut dengan Kitab Undang-undang Hukum Pidana tidak menjelaskan secara tegas apa itu kejahatan siber atau Cyber Crime oleh karena itu harus ada aturan hukum yang bisa menjamin apabila kejahatan Cyber Crime ini dapat diselesaikan.

Salah satu kejahatan siber atau Cyber Crime adalah peretasan atau lebih dikenal dengan hacking, peretasan atau hacking ini ialah suatu aktivitas yang berupaya mengakses secara ilegal perangkat digital, seperti komputer, ponsel cerdas, tablet, dan bahkan seluruh jaringan. Tujuan seorang peretas seringkali untuk mendapatkan akses tidak sah ke komputer, jaringan, sistem komputer, perangkat seluler, atau sistem.[2] Kasus peretasan data pribadi melalui phishing semakin marak terjadi di Indonesia. Data yang dicuri, seperti informasi identitas, kartu kredit, atau akun media sosial, sering kali disebarluaskan dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Korban dari serangan phishing sering kali mengalami kerugian materi dan immateri, seperti kehilangan data atau kerugian reputasi. Meskipun demikian, perlindungan hukum bagi korban serangan ini masih menjadi tantangan besar.

Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Metro Jaya mengungkap kasus penipuan dengan modus “Phishing” atau mencuri akses data

[1] Adam Mulqadrn, Kamei Ahmad, & Hamza Baharuddin. (2021). Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan. Journal Of Lex Generalis (JLS). 2(3) hlm. 1113. Diakses pada tanggal 2 Oktober 2024.

[2] Try Berita Bangka,(2022), *Apa Itu Hacker Dan Peretasan* , diakses pada 23 September 2024,

pribadi menggunakan tampilan salah satu bank yang dilakukan oleh tersangka AV (25). "Tersangka AV membuat 'link' (tautan) yang diduga 'phising' dengan tampilan seolah-olah sistem dari Bank BNI," kata Dirreskrimsus Polda Metro Jaya Kombes Pol Ade Safri Simanjuntak di Jakarta, Jum'at. Ketika mengklik "link" tersebut, kata dia, akan diarahkan ke website yang menyerupai website resmi milik Bank BNI. Setelah nasabah mengklik "link" atau tautan yang dibuat oleh tersangka akan muncul tampilan form pengisian data nasabah. Kemudian tersangka membuat bot telegram untuk dihubungkan ke website yang telah dibuat. "Setelah berhasil mendapatkan data korban, kemudian tersangka berikan kepada pembeli yang memesan 'phising' tersebut," kata Ade Safri.[3]

Ade Safri menjelaskan tersangka membuat tautan sesuai pesanan (order) dari para pemesan. Sebagian besar posisi para pemesan berada di Tulung Selapan, Sumatera Selatan. "Tersangka menjual tautan 'phising' seharga Rp100 ribu-Rp500 ribu dan berhasil terjual sekitar 60 'link'. Dengan keuntungan per bulan sekitar Rp17 juta-Rp20 juta, dengan total keuntungan sekitar Rp70 juta (selama 4 bulan)," katanya. Setelah Kepolisian melakukan penyelidikan pada Senin 28 Agustus 2023 pukul 00.30 WIB, Tim Penyidik Unit II Tindak Pidana (Tipid) Siber Ditreskrimsus Polda Metro Jaya melakukan penangkapan terhadap tersangka di Kecamatan Sungai Raya, Kabupaten Kubu Raya, Kalimantan Barat. Kepolisian telah mengamankan barang bukti berupa satu buah telepon seluler (ponsel), satu buah laptop, tiga buah kartu sim, satu buah aplikasi dompet elektronik dan satu buah akun "hosting Planethost". Ade Safri menyebutkan kasus ini berawal dari Laporan Polisi Nomor: LP/B/4076/VII/2023/SPKT/POLDA METRO JAYA, pada tanggal 14 Juli 2023 atas nama pelapor Saudara 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 phising', sedang didalami dan dilakukan profiling," kata Ade Safri[4]5.

Melihat kondisi di atas diperlukan suatu perangkat aturan yang khusus mengatur tentang kejahatan komputer dan perlindungan hukum terhadap pemanfaatan teknologi informasi, media dan komunikasi agar dapat berkembang secara optimal. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah dua regulasi utama yang menjadi landasan hukum di Indonesia untuk melindungi data pribadi dari penyalahgunaan. Namun, implementasi dari regulasi ini masih sering menemui kendala, baik dari segi penegakan hukum, pengetahuan masyarakat, maupun kesadaran akan pentingnya

[3] Kombes Pol Ade Safri Simanjuntak. Dirreskrimsus Polda Metro Jaya. Jakarta, 22 Agustus 2023.

[4] Kombes Pol Ade Safri Simanjuntak. Dirresmrimsus Polda Metro Jaya. Jakarta, 22 Agustus 2023.

menjaga keamanan data pribadi. Fenomena ini menimbulkan pertanyaan mengenai efektivitas perlindungan hukum yang ada bagi korban penyebaran data pribadi yang diretas melalui phishing.

METODE

Tipe penelitian yang digunakan adalah penelitian hukum normatif, yaitu suatu proses untuk menemukan suatu aturan, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Penelitian ini bertujuan untuk menganalisis hukum dari sudut normatif, yakni berdasarkan dokumen, aturan, teori, dan prinsip-prinsip yang ada. Penelitian ini menggunakan jenis bahan hukum primer yang berupa perundang-undangan dan jenis bahan hukum sekunder yaitu studi kepustakaan dan jurnal hukum.

Penelitian ini diteliti dengan menggunakan bahan pustaka (bahan sekunder) atau penelitian hukum perpustakaan yang secara garis besar ditujukan kepada penelitian asas-asas hukum, penelitian terhadap sistematika hukum, penelitian terhadap sinkronisasi hukum, dan penelitian terhadap perbandingan hukum. Berdasarkan penjelasan di atas, penulis memutuskan menggunakan metode penelitian hukum normatif, karena penulis menggunakan bahan-bahan kepustakaan sebagai data utama dan peraturan perundang-undangan untuk menganalisis kasus.

PEMBAHASAN

A. Pengaturan Perlindungan Hukum Bagi Korban Penyebaran Data Pribadi yang Diretas Secara Ilegal Melalui Link Phishing

Pada dasarnya Korban penyebaran data pribadi adalah individu yang mengalami kebocoran atau distribusi data pribadi tanpa izin, baik Secara sengaja maupun tidak sengaja. Hal ini bisa terjadi akibat peretasan, kebocoran sistem, atau manipulasi seperti phishing, di mana data-data sensitif seperti nama, alamat, nomor identifikasi, informasi keuangan, atau informasi pribadi lainnya di sebarluaskan kepada pihak yang tidak berwenang.

Perlindungan hukum terhadap korban penyebaran data pribadi yang diretas Secara illegal di Indonesia menjadi isu yang semakin penting seiring dengan meningkatnya insiden kebocoran data. Modus kejahatan ini adalah pelaku sengaja mengirimkan surel yang berisi pernyataan-pernyataan yang bersifat mengelabui korban, guna mendaptkan data diri, nomor telepon, kode OTP (On Time Password) pada akun-akun keuangan seperti: Mobile bangking, internet banngkiing, dompet digital dan lain sebagainya.[6] Secara umum perlindungan hukum bagi korban penyebaran data pribadi yang diretas Secara illegal melalui link phishing di atur melalui beberapa perundang-perundangan yang mengatur terkait pengaturan perlindungan hukum bagi korban antara lain:

[6] Polce Aryanto Bessie.(2024). Mental Bahasa Forensik. Indonesia : Penerbit Andi. Hlm. 63.

a. Undang-Undang No. 1 Tahun 1946 tentang Kitab Undang-Undang Hukum Pidana

Dalam kitab Undang-undang Hukum Pidana pasal yang dapat menjadi acuan untuk menegakkaan 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 ain 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.[7] Nico Keijzer berpendapat bahwa pasal 378 adalah delik yang paling relevan bagi seseorang yang memanipulasi computer untuk tujuan keuntungan, karena melibatkan aspek hak.[8] Namun, Pasal 378 tidak mencakup unsur mengenai informasi elektronik dan/atau dokumen elektronik yang salah, sehingga sebenarnya Pasal 378 bukanlah pasal yang cocok untuk menangani cybercrime dalam bentuk phising. Pemahaman dari pasal tersebut masih umum yaitu diperuntukan untuk hal di alam nyata ini. Berbeda dengan penipuan di internet yang diatur dalam UU ITE. Penipuan ini memiliki ruang yang lebih sempit daripada pengaturan dalam KUHP.[9]

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

Praktik kejahatan phising di Indonesia di atur dalam UU ITE. Pasal-pasal yang relevan antara lain pasal 30 UU ITE yang berbunyi : "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau sistem elektronik milik orang lain dengan cara apapun" Maksud dari pasal 30 UU ITE yakni untuk mencegah penggunaan informasi atau dokumen elektronik palsu yang dapat menyesatkan dan merugikan pihak lain, memberikan landasan hukum untuk menindak pelaku yang sengaja melakukan Tindakan tersebut. Sehingga melarang akses illegal terhadap sistem kommputer serta perbuatan yang mengakibatkan kehilangan, perusakan, atau perubahan data elektronik.[10] Pasal 30 Undang-undang Informasi dan Transaksi Elektronik menjelaskan ketentuan yang Secara khusus mengatur tentang pengertian tindak pidana peretasan komputer, dan perbuatan ini

[7] Yazid Haikal Lokapala, et.al, (2024). "Aspek Yuridis Kejahatan Phising dalam Ketentuan Hukum di Indonesia". Indonesia Journal Of Criminal Law and Criminology (IJCLC), Fakultas Hukum Universitas Muhammadiyah Yogyakarta, 5(1). Hlm. 21

[8] Aura Nasha Ramadhanti, et.al, (2024). "Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia". Journal Pendidikan Tambusai. Programm Studi Ilmu Hukum Universitas Pakuan Bogor, 8(1). Hlm.1303.

[9] Chindy Oeliga Yensi Afita (2022). Hukum Pidana Bagi Pelaku Penipuan Transaksi Elektronik Jual Beli Online (E-Commerce) Di Indonesia. Datin Law Jurnal. Fakultas Hukum Universitas Muara Bungo. 3(2).Hlm. 148.

[10] Akhmad Fery Hasanudin & A Basuki Babussalam, (2024). "Upaya Hukum Bagi Korban Phising Yang Menguras Saldo M-Banking. Journal Gagasan Hukum. Fakultas Hukum Universitas Muhammadiyah Surabaya. 6(1). Hlm. 20.

diartikan sebagai setiap orang yang mencoba mengakses sistem elektronik atau computer orang lain dengan segaja melawan hukum untuk memperoleh informasi elektronik.[11] Ancaman pidana yang dapat diterapkan kepada pelaku peretasan dijelaskan Secara rinci dalam pasal 46 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang berbunyi : "Menyatakan siapa pun yang memenuhi kriteria pasal 30 ayat 1 dapatt dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda palling banyak Rp.600.0000.000,00."

Kemudian pada ayat (2) pasal 46 di sebutkan: "Siapapun yang memenuhi kriteria ayat 2 pasal 30 dapat dipidana penjara palling lama 6 tahun/atau denda paling banyak Rp. 700.000.000,00." Selain itu, dalam ayat 3 pasal 46 disebutkan bahwa: "Siapapun yang memenuhi kriteria ayat 3 pasal 30 dapat dipidana dengan pidana penjara paing lama 8 tahun dan/atau denda paling banyak Rp. 800.000.000,00". Pasal di atas mengatur terkait hukuman yang dapat di kenakan pada para pelaku kejahatan phising yang melanggar ketentuan pada pasal 30 UU ITE. Selain itu pasal 35 Undang-Undang Informasi dan Teknologi Elektronik (UU ITE) juga mengatur terkait kejahatan phising tersebut, pasal 35 Undang-undang tersebut berbunyi: "Setiap orang dengan sengaja dan tanpa hak tau melawan hukum melakukan manipulasi, penciptaan, perubahan,penghilangan,pengrusakan informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik". Pasal di atas mengatur mengenai Tindakan pelaku yang menggunakan link palsu untuk mengakses data pribadi korban tanoa izin jelas melanggar ketentuan tersebut.

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

Dalam Undang-undang No.27 tahun 2022 tentang Perlindungan Data Pribadi membahas terkait hak perlindungan data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam pasal 12 ayat (1) yang berbunyi: "Subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemmrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan." Disebutkan dalam CNN Indonesia bahwa pada Pasal di atas menyatakan bahwa Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.[12] Selain itu ada beberapa hak hak subjek data pribadi yang di kecualikan sebagaimana di atur dalam Pasal 15 ayat (1):

"Hak-hak Subjek Data Prribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk:

a. Kepentingan Pertahanan dan Keamanan nasional;

[11] Tri Andika Hidayatullah,et.al. (2023). "Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data". Journal UNES LAW REVIEW. Fakultas Hukum Universitas Andalas Padang. 6(1). Hlm.1361

[12] CNN Indonesia (2022, 20 September). Pasal-pasal Krusial di UU PDP yang Baru Disahkan apa saja?. CNN Indonesia. Diakses pada tanggal 4 November 2024.

b. Kepentingan proses penegakan hukum;
c. Kepentingan umum dalam rangka penyelenggara negara;
d. Kepentingan…"

Meskipun ada pengecualian, pasal ini tetap menekankan pentingnya perlindungan data pribadi sebagai bagian dari hak asasi manusia. Penerapan pasal ini memberikan kerangka hukum yang jelas bagi korban untuk memahami situasi Dimana hak mereka mungkin tidak sepenuhnya dilindungi. Pasal ini mencerminkan Upaya untuk mencapai keseimbangan antara melindungi hak individu dan memenuhi kepentingan umum atau negara.[13] Pasal 58 di atas membahas terkait Pembentukan Lembaga Perlindungan Data Pribadi. Lembaga otoritas tersebut ditugaskan untuk melindungi data pribadi warga negara Indonesia dan menjalankan amanat yang tertuang pada Undang-Undang Data Pribadi.[14] Dimana dengan adanya Lembaga yang khusus di bentuk untuk menangani masalah perlindungan data pribadi, korban penyebaran data yang diretas melalui phising memiliki saluran resmi untuk melaporkan pelanggaran dan mencari keadilan. Lembaga Perlindungan Data Pribadi ini dapat berfungsi sebagai mediator antara korban dan pihak-piihak yang bertanggung jawab atas pelanggaran tersebut.[15] Sementara dalam pasal 60 membahas terkait wewenang LPDP untuk memberikan sanksi administratif kepada pihak yang melanggar ketentuan perlindungan data pribadi, serta melalukan Tindakan lain yang diperlukan untuk melindungi data pribadi. Pasal ini memberikan kerangka hukum yang jelas untuk pengawasan terhadap pelanggaran perlindungan data pribadi. Korban penyebaran data melalui phising dapat melaporkan pelanggaran kepada LPDP, yang kemudian dapat mengambil Tindakan sesuai dengan wewenangnya.[16] LPDP memberikan alternatif bagi korban untuk menyelesaikan masalah mereka tanpa harus melalui proses litigasi yang Panjang dan mahal. Proses ini dapat membantu korban mendapatkan keadilan lebh cepat. Keberadaan LPDP sebagai Lembaga yang bertanggung jawab dalam perlindungan data pribadi dapat meningkatkan kepercayaan Masyarakat terhadap sistem hukum dan perlindungan data di Indonesia. Masyarakat akan merasa lebih aman jika ada Lembaga yang berfungsi untuk melindungi hak-hak mereka terkait data pribadi.

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

Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan sistem dan Transaksi Elektronik diterbitkan karena ketentuan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memerlukan pengaturan lebih

[13] Elfian Fauzi & Nabila Alif Radika Shandy (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Journal Lex Renaissance, Universitas Islam Indonesia Yogyakarta Indonesia. 3(7)

[14] Yati Nurhayati,(2020). Pengantar Ilmu Hukum, Bandung, Nusa Media, hal. 2.

[15] Berita (2023,Mei 17). Sanksi Hukum Dalam Undang-Undang Perlindungan Data Pribadi. SipLawFirm.Id. Diakses pada tanggal 7 November 2024.

[16] Mochamad Januar Rizki. (2022, Oktober 5). Tugas-tugas Lembaga Penyeleggara Perlindungan Data Pribadi dalam UU PDP. Hukum Online.com. Diakses pada tanggal 7 Novemmber 2024.

lanjut dalam Peraturan Pemerintah.[17] Dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), terdapat beberapa pasal yang relevan dengan perlinndungan hukum korban penyebaran data yang diretas Secara illegal melalui link phising. Dalam Pasal 11 ayat (1) berbunyi: "Penyelenggara Sistem Elektronik wajib memastikan Sistem Elektroniknya tidak memuat Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang." Dalam pasal di atas membahas terkait Penyelenggara sistem elektronik harus menjamin tersedianya perjanjian Tingkat layanan; dan tesedianya perjanjian keamanan informasi terhadap layanan layanan teknologi informasi yang digunakan; serta keamanan informasi dan sarana komunikasi internal yang diselenggarakan.[18] Dalam hal ini penyelenggara sistem elektronik bertanggung jawab Secara hukum atas penyelenggaraaan sistemnya. Ini berarti jika terjadi kebocoran data akibat serangan phising, mereka dapat dimintai pertanggung jawaban.

B. 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 illegal melalui link phising di Indonsia melibatkan berbagai mekanisme dan regulasi yang telah di tetapkan. Dengan adanya peraturan peraturan yang terkait perlindungan data pribadi seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Peraturan Pemerintah no. 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik merupakan Upaya negara untuk melindungi privasi dan hak-hak dasar manusia. Undang-undang memberikan suatu jaminan terhadap upaya untuk perorangan atau badan hukum yang pada suatu hal tertentu untuk melawan suatu putusan yang telah diputuskan oleh hakim yang dianggap tidak memenuhi asas keadilan atau merugikan salah satu pihak disebut dengan upaya hukum[19]. Korban yang dirugikan karena kejahatan phising yang menyebabkan tersebarnya data pribadi korban dapat melakukan beberapa tuntutan atas keruugian-kerugian yang telah diderita, Langkah hukum yang dapat di tempuh yaitu:

1. **Langkah Hukum Non-Litigasi.**
   Korban penyebaran data pribadi yang diretas Secara illegal melalui link phising dapat melaporkan tndakan melanggar hukum tersebut kepada atau dapat melakukan Upaya hukum non litigasi, yakni:

[17] Nathania Salasabila Marikar Sahib., et.al. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. Pancasakti Law Journal (PLJ). Fakultas Hukum Universitas Pancasakti Tegal. 1(1). Diakses pada tanggal 7 November 2024.

[18] Dr. Edy Santoso (2023) HUKUM SIBER Permasalahan Hukum Bisnis di Bidang Teknologi Informasi dan Komunikasi. Jakarta : KENCANA. Hlm. 250.

[19] Syahrul Sitorus, "Upaya Hukum Dalam Perkara Perdata (Verzet, Banding, Kasasi, Peninjauan Kembali dan Derden Verzet)" Jurnal Hikmah 15, No. 1 (2018): 63. Dalam Weka Adreana Septia Putri & I Made Sarjana.(2023). Perlindungan Hukum Terhadap Konsumen Korban Kebocoran Dan Penyalahgunaan Data Pribadi Pada Perdaganagan Elektronik. Jurnal Kertha Negara. 11(4). Hlm. 418.

a. Kementrian Komunikasi dan Informatika Republik Inndonesia. Korban dapat mengajukan laporan untuk melaporkan insiden penyebaran data pribadi (Kebocoran Data) yang di retas kepada Kemenkominfo, yang memiliki kewenangan untk 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. Arbitase menjadi salah satu Upaya penyelesaian sengketa lewat jalur di luar peradilan umum berdasarkan suatu perjanjian yang dinamakan dengan perjanjian arbitrase, perjanjiann tersebut dibuat oleh semua pihak yang berselisih dalam bentuk tertulis.[20] Arbiter sendiri adalah orang atau kelompok yang ditunjuk Secara langsung oleh Pengadilan Negeri/ suatu Lembaga yang bertugas mengambil Keputusan terhadap permasalahan yang penyelesainnya dialkukan melalui arbitrase. Hasil putusan dari Upaya hukum arbitrase ini memiliki sifat "win-lose" judgement, mutlak dan berkekuatan hukum untuk mnegikat setiap pihakk 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 mnejatuhkan sanksi andiministratif, 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

Tindakan hukum dalam sengketa melalui Lembaga peradilan formal merupakan Tindakan hukum yang terakhir apabila Langkah non- litigasi tidak menemukan jalan keluar. Upaya atau Tindakan penyelesaian suatu sengketa melalui jalur litigasi ini bisa dilakukan Secara pidana atau perdata. Ada 2 langkah yang dapat di tempuh korban yaitu:

a. Langkah Hukum Pidana
   Jika korban menempuh langkah hukum pidana, pihak yang dilaporkan kepada kepolisian adalah pihak yang membobol dan menyalahgunakan data pribadi korban. Penyelesaian perkara secara pidana dimulai dengan melaporkan kasus kebocoran data pribadi kepada pihak kepolisian setempat atas dugaan pencurian data sebagaimana Pasal 362 KUHP atau dugaan pengaksesan komputer dan/atau

[20] 8 Grace Henni Tampongangoy, "Arbitrase Merupakan Upaya Hukum Dalam Penyelesaian Sengketa Dagang Internasional'' Jurnal Lex et Societatis 3, No. 1 (2015): 161, Dalam Weka Adreana Septia Putri & I Made Sarjana.(2023).Perlindungan Hukum Terhadap Konsumen Korban Kebocoran Dan Penyalahgunaan Data Pribadi Pada Perdaganagan Elektronik. Jurnal Kertha Negara. 11(4). Hlm. 418.

sistem komputer secara ilegal berdasarkan Pasal 30 ayat (2) UU ITE.[21] Suatu upaya melalui lingkup hukum pidana dapat menghasilkan sanksi yang berupa pidana kurungan/pidana alternatif. Dalam hukum perdata, hal ini menimbulkan sanksi denda/ganti rugi. Tahapan yang bisa ditempuh oleh para konsumen selaku korban kebocoran dan penyalahgunaan data pribadi adalah sebagai berikut:

a) Melakukan pelaporan ke kepolisian setempat sesuai dengan cakupan wilayahnya.
b) Mengajukan tuntutan ke Pengadilan Negeri untuk upaya tingkat pertama.
c) Jika putusan pada upaya tingkat pertama di Pengadilan Negeri dirasa tidak sesuai dan memberatkan maka konsumen dapat mengajukan upaya banding ke Pengadilan Tinggi.
d) Jika kemudian putusan dari upaya banding masih dirasa tidak adil atau tidak sebanding dengan kerugian-kerugian yang telah diderita atau dialami. Maka konsumen selaku korban di sini bisa melakukan upaya kasasi dan peninjauan kembali di Mahkamah Agung.[22]

b. Langkah Hukum Perdata

Korban yang dirugikan dan hak haknya dilanggar karena kebocoran dan penyalahgunaan data pribadi dapat melakukan penyelesaian secara hukum perdata. Gugatan perdata dilakukan dengan tujuan memulihkan kerugian yang harus diderita oleh konsumen atau korban dengan sanksi atau hukuman berupa ganti kerugian/denda dan sanksi tersebut nantinya akan dijatuhkan pada pengendal data pribadi apabila terbukti bersalah. jika korban ingin menuntut ganti kerugian secara keperdataan atas terjadinya kegagalan perlindungan data pribadi, maka pihak yang diperkarakan casu quo adalah penyelenggara sistem elektronik dengan cara mengajukan gugatan perdata ke pengadilan negeri sebagaimana gugatan ganti rugi dalam Pasal 1365 KUHPerdata.[23] Gugatan yang diajukan dalam hal ini berupa perbuatan melawan hukum. Pihak yang di rugikan dapat mengambil tindakan selaku korban kebocoran dan penyalahgunaan data pribadi adalah sebagai berikut:

a) Memperkarakan permasalahan atas dasar perbuatan melawan hukum ke Pengadilan Negeri.
b) Dalam hal upaya banding, konsumen atau korban dapat mengajukan upaya banding tersebut ke Pengadilan Tinggi.
c) Untuk upaya kasasi dan peninjauan kembali, konsumen dapat mengajukan upaya tersebut ke Mahkamah Agung.

C. Analisis Penulis

[21] A.A. Ngurah Oka Yudistira Darmadi & Nyoman Satyayudha Dananjaya. (2023). PERLINDUNGAN HUKUM TERHADAP KORBAN KEBOCORAN DATA PRIBADI (STUDI KASUS DI KOTA DENPASAR). Jurnal Kertha Semaya. 11(5). Hlm. 1128.

[22] Weka Adreana Septia Putri & I Made Sarjana.(2023).Perlindungan Hukum Terhadap Konsumen Korban Kebocoran Dan Penyalahgunaan Data Pribadi Pada Perdaganagan Elektronik. Jurnal Kertha Negara. 11(4). Hlm. 419.

[23] A.A. Ngurah Oka Yudistira Darmadi & Nyoman Satyayudha Dananjaya. (2023). Loc. Cit.

Berdasarkan hasil pemaparan mulai dari bagaimana Pengaturan Perlindungan Hukum Terhadap Terhadap Korban Penyebaran Data Yang Diretas Secara Ilegal Melalui Link Phising sampai dengan Upaya Perlindungan Hukum Bagi Korban Penyebaran Data Pribadi yang Diretas Secara Ilegal Melalui Link Phishing. Dengan adanya peraturan terkait perlindungan hukum korban ini dapat membuat para korban kejahatan phising dapat menuntut kerugiannya atas kejahatan phising dan juga dengan mengikuti Langkah-langkah di atas, korban penyebaran data pribadi yang diretas Secara illegal melalui link phising dapat memperjuangkan hak-hak mereka dan mendapatkan perlindungan hukum yang sesuai. Pentingnya edukasi dan pemahaman hukum kepada Masyarakat mengenai resiko phising dan cara meliindungi dara pribadi mereka juga menjadi bagian dari Upaya perlindungan hukum. Kesadaran akan hak-hak mereka sebagai individu dapat membantu korban mengambil Tindakan yang tepat Ketika menghadapi insiden kebocoran data. Melalui Upaya-upaya tersebut, perlindungan hukum bagi korban penyebaran data pribadi yyang diretas Secara illegal melalui link phising diharapkan dapat diperkuat, memberikan jaminan keaman bagi individu dalam era digital yang semakin kompleks.

KESIMPULAN

Berdasarkan pembahasan hasil penelitian yang telah di bahas pada bab sebelumnya, dapat disimpulkan bahwa untuk memberikan perlindungan hukum, Indonesia memiliki beberapa regulasi yang relevan. Pasal 378 KUHP mengatur "penipuan" namun belum spesifik mengakomodasi kejahatan siber, sehingga peranannya terbatas dalam penanganan kasus phishing. UU ITE, khususnya Pasal 30 dan 46, menawarkan perlindungan yang lebih spesifik terhadap kejahatan peretasan dan phishing, termasuk hukuman pidana untuk pelaku. Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) memberikan hak kepada subjek data pribadi untuk menggugat atas pelanggaran data. Lembaga Perlindungan Data Pribadi (LPDP) dibentuk untuk mengawasi pelaksanaan undang-undang ini dan memberikan sanksi administratif kepada pelanggar. Selain itu, PP No. 71 Tahun 2019 mengatur bahwa Penyelenggara Sistem Elektronik (PSE) wajib menjaga keamanan data pribadi pengguna dan melaporkan kebocoran data secara transparan. PSE juga diwajibkan untuk memberikan kompensasi bagi pengguna yang dirugikan. Kesimpulannya, berbagai regulasi yang ada telah memberikan kerangka dasar untuk perlindungan data pribadi, namun tantangan masih ada dalam penerapan yang komprehensif dan efektif untuk melindungi korban kejahatan phishing dan peretasan data di Indonesia. Sosialisasi mengenai pentingnya menjaga keamanan data pribadi dan mengenali ancaman phising perlu dilakukan Secara berkala. Edukasi ini dapat meningkatkan kewaspadaan Masyarakat dalam melindungi data mereka, terutama di lingkungan digital yang rentan terhadap kejahatan siber. Penegak hukum perlu mendapatkan pelatihan khusus dalam menangani kejahatan siber, terutama kasus phising yang melibatkan data pribadi. Koordinasi antar-lembaga seperti kepolisian, Kementrian Komunikasi dan Informatika, serta Lembaga Perlindungan Data Pribadi perlu diperkuat agar mampu memberikan perlindungan dan penanganan yang efektif terhadap korban.

REFERENSI

1) Tri Andika Hidayatullah, Ismansyah, Nani Mulyati.(2023).Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data. UNES LAW REVIEW,6(1), hlm. 1357
2) Adam Mulqadrn, Kamei Ahmad, & Hamza Baharuddin. (2021). Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan. Journal Of Lex Generalis (JLS). 2(3) hlm. 1113. Diakses pada tanggal 2 Oktober 2024.
3) Try Berita Bangka,(2022), Apa Itu Hacker Dan Peretasan , diakses pada 23 September 2024,
4) Kombes Pol Ade Safri Simanjuntak. Dirreskrimsus Polda Metro Jaya. Jakarta, 22 Agustus 2023.
5) Polce Aryanto Bessie.(2024). Mental Bahasa Forensik. Indonesia : Penerbit Andi. Hlm. 63.
6) Yazid Haikal Lokapala, et.al, (2024). "Aspek Yuridis Kejahatan Phising dalam Ketentuan Hukum di Indonesia". Indonesia Journal Of Criminal Law and Criminology (IJCLC), Fakultas Hukum Universitas Muhammadiyah Yogyakarta, 5(1). Hlm. 21
7) Aura Nasha Ramadhanti, et.al, (2024). "Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia". Journal Pendidikan Tambusai. Programm Studi Ilmu Hukum Universitas Pakuan Bogor, 8(1). Hlm.1303.
8) Chindy Oeliga Yensi Afita (2022). Hukum Pidana Bagi Pelaku Penipuan Transaksi Elektronik Jual Beli Online (E-Commerce) Di Indonesia. Datin Law Jurnal. Fakultas Hukum Universitas Muara Bungo. 3(2).Hlm. 148.
9) Akhmad Fery Hasanudin & A Basuki Babussalam, (2024). "Upaya Hukum Bagi Korban Phising Yang Menguras Saldo M-Banking. Journal Gagasan Hukum. Fakultas Hukum Universitas Muhammadiyah Surabaya. 6(1). Hlm. 20.
10) Tri Andika Hidayatullah,et.al. (2023). "Perlindungan Hukum terhadap Korban Tindak Pidana Peretasan (Hacking) Berkaitan dengan Pencurian Data". Journal UNES LAW REVIEW. Fakultas Hukum Universitas Andalas Padang. 6(1). Hlm.1361
11) CNN Indonesia (2022, 20 September). Pasal-pasal Krusial di UU PDP yang Baru Disahkan apa saja?. CNN Indonesia. Diakses pada tanggal 4 November 2024.
12) Elfian Fauzi & Nabila Alif Radika Shandy (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Journal Lex Renaissance, Universitas Islam Indonesia Yogyakarta Indonesia. 3(7)
13) Mochamad Januar Rizki (2022,4 Oktober). Ancaman Sanksi Administratif Hingga Pidana dalam UU Pelindungan Data Pribadi. Hukum Online.Com. Diakses pada tanggal 5
14) Ady Thea DA. (2022, 25 September). Menkominfo Beberkan 4 Poin Penting yang Diatur UU PDP. Hukum Online.Com. Diakses pada tanggal 6 November 2024.
15) Yati Nurhayati,(2020). Pengantar Ilmu Hukum, Bandung, Nusa Media, hal. 2.
16) Berita (2023,Mei 17). Sanksi Hukum Dalam Undang-Undang Perlindungan Data Pribadi. SipLawFirm.Id. Diakses pada tanggal 7 November 2024.
17) Mochamad Januar Rizki. (2022, Oktober 5). Tugas-tugas Lembaga Penyeleggara Perlindungan Data Pribadi dalam UU PDP. Hukum Online.com. Diakses pada tanggal 7

Novemmber 2024.
18) Nathania Salasabila Marikar Sahib., et.al. (2023). Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia. Pancasakti Law Journal (PLJ). Fakultas Hukum Universitas Pancasakti Tegal. 1(1). Diakses pada tanggal 7 November 2024.
19) Dr. Edy Santoso (2023) HUKUM SIBER Permasalahan Hukum Bisnis di Bidang Teknologi Informasi dan Komunikasi. Jakarta : KENCANA. Hlm. 250.
20) Leski Rizkinaswara. (2020, Juni 10). Penyelenggaraan Sistem Elektronik BertanggungJawab terhadap Pelanggaran Data. KOMINFO. Diakses pada tanggal 7 November 2024.
21) Edman Makarim (2020, Januari 1). Pelindungan Privacy dan Personal Data. Berkas.dpr.go.id. Diakses pada tanggal 8 November 2024.
22) Syahrul Sitorus, "Upaya Hukum Dalam Perkara Perdata (Verzet, Banding, Kasasi, Peninjauan Kembali dan Derden Verzet)" Jurnal Hikmah 15, No. 1 (2018): 63. Dalam Weka Adreana Septia Putri & I Made Sarjana.(2023). Perlindungan Hukum Terhadap Konsumen Korban Kebocoran Dan Penyalahgunaan Data Pribadi Pada Perdaganagan Elektronik. Jurnal Kertha Negara. 11(4). Hlm. 418.
23) 8 Grace Henni Tampongangoy, "Arbitrase Merupakan Upaya Hukum Dalam Penyelesaian Sengketa Dagang Internasional'' Jurnal Lex et Societatis 3, No. 1 (2015): 161, Dalam Weka Adreana Septia Putri & I Made Sarjana.(2023).Perlindungan Hukum Terhadap Konsumen Korban Kebocoran Dan Penyalahgunaan Data Pribadi Pada Perdaganagan Elektronik. Jurnal Kertha Negara. 11(4). Hlm. 418.
24) A.A. Ngurah Oka Yudistira Darmadi & Nyoman Satyayudha Dananjaya. (2023). PERLINDUNGAN HUKUM TERHADAP KORBAN KEBOCORAN DATA PRIBADI (STUDI KASUS DI KOTA DENPASAR). Jurnal Kertha Semaya. 11(5). Hlm. 1128.