PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT *CYBER CRIME PHISING* BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Edlin Reyhan[1], Potler Gultom[2]
Faculty Of Law, Dirgantara Marsekal Suryadarma University
Email : edlinreyhan43@gmail.com[1], potlergultom@unsurya.ac.id[2]

Citation: Edlin Reyhan., Potler Gultom. Perlindungan Hukum Terhadap Pengguna Sosial Media Terkait *Cyber Crime Phising* Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *LEX LAGUENS: Jurnal Kajian Hukum dan Keadilan* 3.1.2025. 111-124
Submitted: 01-10-2024 **Revised:**11-11-2024 **Accepted:**01-12-2024

Abstrak

Kejahatan phising merupakan kejahatan Cyber Crime yang terjadi di dunia digital. Perlindungan pengguna media sosial terhadap kejahatan phising diatur dalam Undang-Undang ITE dan Undang-Undang perlindungan data pribadi. Oleh karena itu, tujuan dari penelitian ini menemukan bentuk pertanggungjawaban tindak pidana phising dan perlindungan hukum atas kejahatan phising. Penelitian ini menggunakan metode pendekatan yuridis normatif. Penulis melakukan penelitian secara studi kepustakaan data sekunder berupa bahan hukum primer, sekunder, dan tersier, dan studi lapangan yang berkorelasi dengan objek penelitian ini. Penelitian ini menyimpulkan bahwa perlindungan terhadap tindak pidana phising terdapat dalam pasal 4, pasal 15 ayat (1), dan pasal 66 dan pasal 67 UU perlindungan data pribadi sedangkan pertanggungjawaban atas kejahatan phising terdapat dalam Undang-Undang ITE pasal 35 jo pasal 51.
Kata Kunci : Perlindungan terkait *Cyber Crime,* Phising, Penipuan

Abstract

Crime phishing is a crime Cyber Crime what happens in the digital world. Protection of social media users against phishing crimes is regulated in the ITE Law and the personal data protection law. Therefore, the aim of this research is to find forms of accountability for phishing crimes and legal protection for phishing crimes. This research uses a normative juridical approach. The author conducted research using secondary data literature studies in the form of primary, secondary and tertiary legal materials, and field studies that correlate with the object of this research. This research concludes that protection against phishing crimes is contained in Article 4, Article 15 paragraph (1), and Article 66 and Article 67 of the Personal Data Protection Law, while responsibility for phishing crimes is contained in Article 35 of the ITE Law in conjunction with Article 51.
Keywords: Related protection Cyber Crime, Phishing, Fraud.

A. PENDAHULUAN

Indonesia sebagai negara hukum, sebagaimana tercantum dalam Undang-Undang Dasar Negara Republik Indonesia (UUD NRI) 1945, menekankan bahwa segala kegiatan dalam kehidupan berbangsa dan bernegara harus berdasarkan hukum.[1] Hukum berfungsi sebagai pranata sosial yang penting untuk menciptakan ketentraman, keadilan, dan keamanan. Hukum mengatur segala perbuatan manusia, baik yang diperbolehkan maupun yang dilarang, dengan tegas memberikan sanksi bagi pelanggarannya.[2]

[1] Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
[2] Moeljatno. *Asas-Asas Hukum Pidana.* Jakarta: Rineka Cipta, 2009, p. 1.

Karena masyarakat memiliki berbagai kepentingan yang berbeda, hukum dibutuhkan untuk mengatur perbedaan tersebut. Hukum memandu masyarakat mengenai apa yang boleh dan tidak boleh dilakukan, sifatnya memaksa dan mengikat. Salah satu cabang hukum yang berlaku di Indonesia adalah hukum pidana, yang merupakan bagian dari keseluruhan sistem hukum yang ada di negara ini, berfungsi untuk menjaga ketertiban dan melindungi kepentingan masyarakat.

Pada era globalisasi saat ini, perkembangan teknologi dan internet yang pesat telah menyebabkan pergeseran pola pikir dan kebudayaan dalam masyarakat, yang juga memicu munculnya berbagai modus kejahatan baru, termasuk penipuan online. Kejahatan siber atau *cyber crime* kini tidak memandang usia, sehingga anak-anak, remaja, orang dewasa, hingga orang tua pun bisa menjadi korban. Kehidupan sehari-hari kita yang sangat bergantung pada dunia digital dan internet, melalui media sosial dan platform lainnya, membawa banyak manfaat. Namun, ada dampak negatif yang juga tidak bisa diabaikan, salah satunya adalah kejahatan siber.[3]

Cyber crime merujuk pada tindakan kejahatan yang berkaitan dengan penggunaan komputer dan perangkat jaringan, yang biasanya dilakukan secara daring. Kejahatan ini bisa menargetkan siapa saja dan sering kali menimbulkan kerugian yang besar, baik secara finansial maupun mental. Salah satu contoh kejahatan siber yang sangat berbahaya adalah *phishing*, yaitu pencurian data pribadi melalui media elektronik dengan tujuan untuk melakukan penipuan, pemerasan, ancaman, atau mempermalukan korban. Dengan kemajuan teknologi dan internet yang semakin pesat, ancaman kejahatan siber pun semakin beragam dan banyak bermunculan, menuntut perhatian serius dalam upaya pencegahannya.

Kejahatan siber atau cyber crime merujuk pada berbagai tindakan kriminal yang dilakukan menggunakan komputer, data, dan jaringan internet. Pelaku kejahatan siber biasanya meretas sistem untuk memperoleh data pribadi korban. Berikut adalah empat jenis kejahatan siber yang umum terjadi:

1. *Phishing*

   Phishing adalah tindakan penipuan dengan cara "memancing" korban untuk memberikan informasi pribadi, seperti kata sandi, nomor rekening, atau data sensitif lainnya. Pelaku sering menggunakan pendekatan yang sangat meyakinkan sehingga korban tidak sadar mereka sedang menjadi target penipuan.

[3] APJII, Asosiasi Penyelenggara Jasa Internet di Indonesia. "Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang." Diakses dari situs resmi APJII, 9 April 2024.

2. Peretasan *(Hacking)*

   Peretasan adalah upaya untuk menyusup ke dalam sistem komputer tanpa izin. Para peretas biasanya mencuri data pribadi, informasi keuangan, atau membobol sistem untuk kepentingan tertentu. Kejahatan ini bisa berdampak besar pada privasi dan keamanan data individu atau perusahaan.

3. *Cyber Stalking*

   Cyber stalking atau penguntitan siber adalah tindakan penggunaan internet untuk menguntit atau meneror korban secara terus-menerus. Perilaku ini dapat mengganggu kehidupan korban dan dalam beberapa kasus, membahayakan keselamatan korban. Penguntit dapat menggunakan berbagai platform online untuk melakukan ancaman dan intimidasi.

4. *Cyber Bullying*

   Cyber bullying adalah bentuk perundungan atau penindasan yang dilakukan secara online melalui media sosial atau platform digital lainnya. Biasanya, hal ini terjadi di kolom komentar atau chat, dan bisa mengarah pada dampak emosional dan psikologis yang serius bagi korban.

Penipuan online melalui phishing merupakan salah satu bentuk tindak pidana *cyber crime* yang sangat berpotensi berkembang, namun penegakan hukum terhadap kasus ini dirasa masih kurang efektif. Kejahatan ini sudah tidak lagi dilakukan secara sembunyi-sembunyi, melainkan dengan sangat terang-terangan. Media cetak dan elektronik seringkali memberitakan kasus-kasus tersebut, yang menunjukkan bahwa kejahatan ini telah merambah ke seluruh lapisan masyarakat, dari anak-anak hingga orang dewasa, bahkan orang tua yang tidak terlalu mengikuti perkembangan teknologi.[4]

Indonesia, sebagai salah satu negara dengan tingkat tinggi kasus *cyber crime,* telah menjadi target utama penipuan online. Meskipun sebelumnya *cyber crime* lebih dikenal di negara maju, kini kejahatan ini telah menyebar luas, termasuk ke negara-negara berkembang seperti Indonesia. Masyarakat Indonesia, yang dulunya kurang terbiasa dengan teknologi, kini semakin beralih ke dunia digital. Namun, banyak orang masih belum siap menghadapi perubahan yang dibawa oleh perkembangan teknologi ini. *Cyber crime* di Indonesia terjadi secara eksplisit, namun banyak dari kasus ini yang tersembunyi, seperti gunung es yang lebih besar di bawah permukaan.

[4] KOMINFO. "Polri: Indonesia Tertinggi Kedua Kejahatan Siber di Dunia." Diakses dari laman situs resmi KOMINFO, 4 April 2024. https://www.kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media.

Menurut beberapa ahli, *cyber crime* dapat didefinisikan sebagai kejahatan yang menggunakan teknologi komputer sebagai komponen utama. Forester dan Morrison mendefinisikan *cyber crime* sebagai aksi kriminal yang memanfaatkan komputer sebagai senjata utama. Girasa menyatakan bahwa *cyber crime* adalah kejahatan yang menggunakan teknologi komputer sebagai komponen utamanya. Tavani memberikan definisi yang lebih menarik, yaitu bahwa *cyber crime* adalah kejahatan yang hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia maya.[5]

Perkembangan teknologi digital telah meningkatkan ancaman *cyber crime* secara signifikan, termasuk pencurian identitas, kehilangan pekerjaan, hingga gangguan terhadap infrastruktur kritis. Pelaku *cyber crime* terus mengembangkan teknik dan strategi baru dalam melaksanakan kejahatannya. Ancaman seperti serangan malware, *denial of service (DoS), distributed denial of service (DDoS),* dan *phishing* semakin sering terjadi. Kurangnya kesadaran dan edukasi tentang keamanan siber serta minimnya penegakan hukum membuat masalah ini semakin serius. Padahal, *cyber crime* memiliki potensi besar untuk menimbulkan masalah nasional.

Upaya yang dapat dilakukan untuk mengatasi hal ini adalah dengan memperkuat penegakan hukum terhadap *cyber crime* dan meningkatkan edukasi kepada masyarakat tentang cara melindungi diri dari kejahatan di dunia maya. Sebuah pendekatan yang lebih menyeluruh dan berkelanjutan diperlukan untuk memitigasi ancaman ini.

Perkembangan *cyber crime,* terutama penipuan online, semakin pesat setelah pandemi COVID-19. Peningkatan penggunaan media sosial membuka peluang bagi pelaku kejahatan siber. Salah satu contoh adalah kasus di Sumatera Selatan, di mana seorang pemuda berinisial ES membobol rekening korban hingga merugikan 2,3 miliar rupiah. Modus yang digunakan pelaku adalah mengirimkan file APK melalui WhatsApp, yang kemudian memungkinkan pelaku meretas email dan mobile banking korban. Setelah itu, pelaku mentransfer uang ke rekening yang dibeli dari Facebook untuk mengaburkan jejaknya. Kasus ini menekankan pentingnya kewaspadaan terhadap ancaman cybercrime dan perlunya penegakan hukum serta edukasi keamanan siber.[6]

Berdasarkan uraian latar belakang diatas, maka peneliti tertarik untuk melakukan penelitian dengan mengangkat judul “Perlindungan Hukum Terhadap Pengguna Sosial Media

[5] Alan Stevenres Bentelu, Steven Sentinuwo, Steven Sentinuwo. "Animasi 3 Dimensi Pencegahan Cyber Crime." *E-Journal Teknik Informatika* Vol. 8, No. 1 (Agustus 2016): 1.
[6] KOMPAS. "Pelaku 'Phishing' Bermodus APK via WhatsApp Ditangkap, Kuras Rp 1,4 M Tabungan Korban." Diakses dari laman situs resmi KOMINFO, 19 April 2024.

Terkait *Cyber Crime Phising* Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik".

B. METODE PENELITIAN

Jenis penelitian yang dipergunakan dalam penelitian ini adalah jenis penelitian hukum yuridis normatif. Pendekatan penelitian hukum *(approach)* yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan *(statute approach)* dan pendekatan konseptual *(conceptual approach).* Jenis Data yang dipergunakan dalam penelitian ini adalah data sekunder dimana data sekunder adalah sekumpulan informasi yang telah ada sebelumnya dan digunakan sebagai pelengkap kebutuhan data penelitian. Untuk memperoleh informasi atau data yang diperlukan guna menjawab rumusan masalah penelitian, Peneliti menggunakan metode atau teknik pengumpulan data dengan Penelitian Kepustakaan *(Library Research).* Metode analisis data yang dipergunakan adalah analisis data kualitatif, yaitu proses penyusunan, mengkatagorikan data kualitatif, mencari pola atau tema dengan maksud memahami maknanya.

C. HASIL PENELITIAN DAN PEMBAHASAN

1. Perlindungan Hukum Terhadap Pengguna Sosial Media Terkait *Cyber Crime Phising* Berdasarkan Undang-Undang Republik Indonesia Nomer 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Perkembangan teknologi digital memudahkan berbagai aktivitas, seperti transaksi elektronik, namun juga membawa risiko, salah satunya adalah *cyber crime. Cyber crime* merujuk pada tindakan kriminal yang menggunakan komputer atau jaringan sebagai alat, sasaran, atau tempat kejahatan.[7] Meskipun dunia maya bersifat virtual, hukum tetap diperlukan untuk mengatur perilaku individu dan masyarakat. Hukum bertujuan melindungi nilai dan kepentingan masyarakat, baik secara pribadi maupun bersama, dengan memberikan sanksi kepada pelanggar yang ada di dunia maya.

Phishing adalah penipuan online di mana pelaku menyamar untuk mencuri informasi pribadi pengguna melalui teknik pengelabuhan. Data yang menjadi sasaran phishing meliputi

[7] Josua Sitompul. *Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana.* Jakarta: PT. Tatanusa, 2012, p. 38.

data pribadi (nama, usia, alamat), data akun (username, password), dan data finansial (informasi kartu kredit, rekening). Berikut adalah jenis phishing yang umum ditemui:

1) *Email Phishing*

   Menggunakan email untuk menjangkau korban dengan cara mengirimkan email palsu dalam jumlah besar. Data menunjukkan 3,4 miliar email palsu dikirim setiap hari.

2) *Spear Phishing*

   Merupakan variasi dari email phishing, tetapi menargetkan individu tertentu setelah mengumpulkan informasi dasar tentang korban, seperti nama dan alamat.

3) *Whaling*

   Menargetkan individu dengan kewenangan atau posisi penting, seperti eksekutif, dengan tujuan memanipulasi mereka untuk menyerahkan informasi atau melakukan tindakan tertentu yang merugikan.

Perlindungan data di Indonesia menjadi sangat penting seiring dengan pesatnya perkembangan teknologi. Pemerintah perlu melakukan upaya preventif melalui regulasi yang mengatur kewajiban tertentu untuk mencegah pelanggaran hukum. Salah satu dasar hukum terkait *cyber crime* adalah Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE bertujuan melindungi pengguna teknologi informasi di Indonesia, mengingat semakin banyaknya pengguna internet yang dapat menjadi target kejahatan dunia maya.

Meskipun internet memberikan banyak kemudahan, hal ini juga membuka peluang bagi pihak yang tidak bertanggung jawab untuk melakukan tindak pidana. Fenomena *cyber crime* yang terus berkembang memerlukan perhatian khusus, karena kejahatan ini memiliki sifat yang berbeda dan tidak terbatas oleh teritori. Oleh karena itu, pemerintah perlu mendukung pengembangan teknologi informasi dengan membangun infrastruktur hukum yang memadai, memastikan pemanfaatan teknologi dilakukan secara aman dan memperhatikan nilai-nilai sosial serta budaya masyarakat Indonesia.

Perlindungan data pribadi di Indonesia diatur dalam berbagai peraturan perundang-undangan, yang bertujuan untuk melindungi privasi individu serta memastikan keamanan data yang ada di platform digital. Beberapa pasal dalam undang-undang yang relevan adalah:

1) Pasal 4 Huruf e UU ITE menyebutkan bahwa pemerintah melindungi kepentingan umum dari gangguan yang diakibatkan oleh penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan.

2) Pasal 15 ayat (1) UU ITE mewajibkan setiap penyelenggara sistem elektronik untuk menyelenggarakan sistem yang andal dan aman, serta bertanggung jawab terhadap beroperasinya sistem elektronik tersebut. Ini berhubungan langsung dengan perlindungan data pribadi, karena sistem yang tidak aman dapat menyebabkan peretasan dan penyalahgunaan data pengguna.
3) Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi menyebutkan bahwa setiap orang dilarang menyadap informasi yang dikirim melalui jaringan telekomunikasi, yang mencakup perlindungan terhadap data pribadi yang dikirimkan melalui saluran komunikasi elektronik.
4) Pasal 42 ayat (1) UU Telekomunikasi menyatakan bahwa penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirimkan atau diterima oleh pelanggan melalui jaringan telekomunikasi yang mereka kelola, untuk melindungi kerahasiaan data pribadi.
5) Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan juga mengatur perlindungan data pribadi, terutama dalam hal data kependudukan. Pasal 1 ayat 22 UU ini menegaskan bahwa data pribadi harus dilindungi dan tidak boleh digunakan untuk tujuan yang tidak sah. Selain itu, Pasal 2 huruf C dan F mengatur kewajiban setiap orang untuk melindungi data pribadi orang lain dan tidak menyalahgunakannya.

Peraturan-peraturan ini bertujuan untuk memastikan bahwa data pribadi individu tidak disalahgunakan, dan memberikan tanggung jawab kepada pihak yang menyelenggarakan sistem elektronik dan jasa telekomunikasi untuk menjaga keamanan dan kerahasiaannya.

Kejahatan cyber crime, seperti phishing dan hacking, pada dasarnya merupakan bentuk kejahatan konvensional yang memanfaatkan teknologi internet untuk melakukan aksinya. Tujuan utama dari phishing adalah untuk mendapatkan informasi pribadi korban, seperti data diri nasabah, yang kemudian digunakan oleh pelaku hacking untuk meretas sistem elektronik dan mengambil keuntungan secara ilegal.

Infrastruktur telekomunikasi dan aktivitas digital memainkan peran penting dalam transaksi elektronik dan pertukaran informasi di era ekonomi digital. Oleh karena itu, untuk melindungi data pribadi dan privasi pengguna, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur perlindungan terhadap informasi yang dikirim melalui jaringan telekomunikasi.

1) Pasal 40 UU Telekomunikasi melarang penyadapan informasi yang dikirimkan melalui jaringan telekomunikasi, yang merupakan langkah penting dalam melindungi privasi dan data pribadi.
2) Pasal 42 ayat (1) UU Telekomunikasi menyatakan bahwa penyelenggara jasa telekomunikasi wajib menjaga kerahasiaan informasi yang dikirimkan atau diterima oleh pelanggan melalui jaringan telekomunikasi yang mereka kelola.

Selain itu, dalam konteks transaksi elektronik, setiap informasi yang terkait dengan data pribadi harus dikirim dengan izin dari orang yang bersangkutan. Hak privasi mencakup beberapa aspek, yaitu:

1) Hak untuk menjalani kehidupan pribadi tanpa gangguan.
2) Hak untuk berkomunikasi dengan orang lain tanpa pemantauan.
3) Hak untuk memantau siapa yang dapat mengakses informasi pribadi mereka.

Untuk memperkuat perlindungan data pribadi, Peraturan Pemerintah Nomor 82 Tahun 2012 mengatur bagaimana penyelenggara sistem elektronik harus melindungi data pribadi yang ada di platform digital. Semua langkah ini penting untuk mencegah penyalahgunaan data pribadi dalam kegiatan transaksi elektronik dan mendukung keamanan siber.

Dalam era ekonomi digital, instrumen hukum untuk perlindungan privasi dan data pribadi harus memenuhi dua kriteria penting:

1. Karakter Internasional: Perlindungan privasi dan data pribadi harus mengandung pengaturan lintas batas negara, seperti aturan yang mengharuskan persetujuan khusus untuk transfer data pribadi ke luar negara. Transfer hanya dapat dilakukan ke negara yang memiliki perlindungan data pribadi yang setara.
2. Elemen Perekat Individu dan Masyarakat Ekonomi: Perlindungan ini juga harus mencakup hak personal. Selain menjadi hak negatif (hak yang mengharuskan negara tidak melakukan sesuatu), perlindungan data pribadi juga harus menjadi hak positif yang pemenuhannya memerlukan peran aktif negara.

Perlindungan data pribadi merupakan bagian dari hak asasi manusia, dan tujuan utamanya adalah memastikan hak warga negara atas perlindungan data pribadi serta meningkatkan kesadaran masyarakat mengenai pentingnya perlindungan tersebut. Indonesia, dalam beberapa tahun terakhir, menjadi sasaran serangan siber yang menyebabkan kebocoran data pribadi di berbagai platform, yang semakin menunjukkan urgensi pengaturan ini.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi membedakan data pribadi menjadi dua kategori:

1) Data pribadi yang bersifat umum: Seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan sebagainya.
2) Data pribadi yang bersifat spesifik: Termasuk data kesehatan, biometrik, genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai peraturan perundang-undangan.

Undang-Undang ini juga melarang pemalsuan data pribadi yang dilakukan dengan maksud untuk menguntungkan diri sendiri atau orang lain, yang dapat merugikan orang lain. Dengan adanya UU ini, diharapkan masyarakat dapat terlindungi dari penyalahgunaan data pribadi, dan individu yang menyalahgunakan data pribadi dapat dikenakan sanksi administratif atau pidana.

Karena jumlah pengguna internet yang terus meningkat, perlindungan data pribadi sangat penting untuk menjaga identitas dan hak asasi seseorang. Jika identitas diretas, berbagai tindak pidana, seperti penipuan, pembajakan, dan manipulasi, dapat terjadi, merugikan individu dan pihak lain baik secara materiil maupun immateriil.

Perlindungan data pribadi di Indonesia semakin penting di era digital, terutama terkait dengan kejahatan siber seperti phishing yang dapat merugikan individu dan organisasi. Beberapa peraturan telah diimplementasikan untuk menangani masalah ini, di antaranya adalah Undang-Undang Nomor 19 Tahun 2016 (perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

UU PDP adalah undang-undang yang memberikan perlindungan bagi data pribadi masyarakat dan menetapkan sanksi yang tegas bagi pelaku kejahatan siber, termasuk dalam kasus phishing. UU PDP memastikan bahwa data pribadi yang dikumpulkan oleh pihak tertentu akan dilindungi dan digunakan sesuai dengan ketentuan hukum. Di dalamnya terdapat beberapa pasal penting yang mengatur hak-hak individu terkait data pribadi, termasuk hak untuk meminta perlindungan atas data pribadi mereka.

Pasal 7 UU PDP memberikan hak kepada setiap orang untuk meminta perlindungan data pribadinya. Sementara Pasal 12 mengharuskan pemerintah untuk menyediakan mekanisme perlindungan data pribadi yang efektif, sehingga data pribadi tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.[8]

[8] Indriana Firdaus. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 4, no. 2.

Kejahatan siber seperti phishing dan hacking mengancam privasi dan data pribadi individu. Phishing, sebagai bagian dari kejahatan yang dilakukan oleh cracker, bertujuan untuk memperoleh data pribadi korban dengan cara yang menipu. Praktik phishing dapat dilakukan melalui email atau pesan singkat yang terlihat resmi, tetapi sebenarnya digunakan untuk mencuri data sensitif, seperti informasi perbankan dan akun pribadi.

LOPDP adalah lembaga yang diatur dalam Pasal 58 UU PDP untuk melaksanakan perlindungan data pribadi. Lembaga ini memiliki tugas dan wewenang penting dalam mengawasi dan menegakkan peraturan perlindungan data pribadi, termasuk pemberian sanksi administratif terhadap pelanggar. LOPDP juga berperan dalam berkolaborasi dengan lembaga penegak hukum lainnya untuk menangani kasus kejahatan siber yang melibatkan pelanggaran data pribadi.

Untuk menanggulangi kejahatan siber seperti phishing, UU PDP memberikan sanksi administratif dan pidana. Pelaku phishing dapat dikenakan sanksi pidana dengan ancaman hukuman penjara maksimal 5 tahun dan/atau denda maksimal 5 miliar rupiah (Pasal 67 UU PDP). Sanksi ini diharapkan dapat memberikan efek jera bagi para pelaku dan mencegah terjadinya kejahatan siber di masa depan.

Pemerintah berperan aktif dalam mengawasi dan menegakkan UU PDP dengan memperkuat kerjasama antar lembaga, seperti Kepolisian Negara Republik Indonesia (Polri), Badan Siber dan Sandi Negara (BSSN), dan Komisi Perlindungan Anak Indonesia (KPAI). Selain itu, sektor swasta juga harus bekerjasama untuk melindungi data pribadi yang mereka kumpulkan, misalnya oleh perusahaan marketplace dan e-commerce. Peran media massa juga sangat penting dalam memberikan edukasi kepada masyarakat mengenai bahaya phishing dan cara melindungi data pribadi.

Dengan adanya UU Perlindungan Data Pribadi dan Lembaga Otoritas Perlindungan Data Pribadi, diharapkan Indonesia dapat lebih efektif dalam menangani praktik phishing dan kejahatan siber lainnya. Kerja sama antara lembaga pemerintah, sektor swasta, dan masyarakat sangat penting untuk menciptakan ekosistem yang aman dalam dunia digital dan mengurangi ancaman terhadap data pribadi masyarakat Indonesia.

Secara keseluruhan, upaya perlindungan data pribadi yang kuat melalui pengaturan hukum yang jelas, sanksi tegas, dan kerjasama antar berbagai pihak dapat meminimalkan kasus phishing dan meningkatkan keamanan siber di Indonesia.

2. Pertanggungjawaban Tindak Pidana *Cyber Crime Phising* Di Indonesia

Seiring perkembangan zaman, kejahatan tidak hanya terbatas pada bentuk fisik, tetapi juga merambah ke dunia maya, yang salah satunya adalah kejahatan siber dengan teknik

phishing. Phishing adalah bentuk kejahatan yang semakin marak, yang menyasar korban dengan cara memanipulasi dan mencuri data pribadi secara online. Meskipun teknologi membawa banyak manfaat dalam kehidupan masyarakat, kemajuan ini juga membuka peluang bagi tindakan kriminal yang merugikan individu, seperti pencurian informasi kartu kredit, nomor rekening, dan data pribadi lainnya. Oleh karena itu, korban dari kejahatan ini sangat membutuhkan perlindungan hukum agar bisa merasa aman dalam kehidupan sehari-hari.

Sebagai negara hukum, Indonesia memiliki tanggung jawab untuk memberikan perlindungan terhadap warganya, termasuk korban dari kejahatan siber. Hal ini tercermin dalam Alinea ke-IV Pembukaan UUD 1945, yang menegaskan bahwa negara berkomitmen untuk melindungi seluruh rakyat Indonesia. Namun, dalam peraturan yang ada, khususnya dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), belum ada pengaturan yang jelas mengenai perlindungan bagi korban kejahatan dalam dunia maya, seperti phishing. Meskipun demikian, data pribadi dilindungi oleh peraturan yang ada di Indonesia, dan ketika kerahasiaan data tersebut terungkap, hukum harus hadir untuk memberikan perlindungan terhadap pihak yang dirugikan.

Tindak pidana cybercrime dalam bentuk phishing dapat menimbulkan kerugian materiil bagi korban, karena informasi pribadi yang dimiliki korban, seperti nomor rekening dan data kartu kredit, bisa disalahgunakan untuk tujuan kejahatan. Kasus phishing semakin meningkat dari waktu ke waktu, dengan laporan yang diterima oleh Indonesia Anti-Phishing Data Exchange (IDADX) yang menunjukkan lonjakan serangan phishing. Pada kuartal pertama 2023, IDADX mencatat 26.675 laporan serangan phishing, jauh lebih banyak dibandingkan kuartal keempat 2022 yang hanya mencatat sekitar 6.106 laporan. Serangan phishing ini tidak hanya menargetkan individu, tetapi juga lembaga pemerintahan dan sektor industri tertentu, seperti media sosial dan lembaga keuangan.

Salah satu metode serangan phishing adalah dengan meninggalkan link URL palsu di kolom komentar media sosial, yang jika diklik korban akan mengungkapkan informasi penting, seperti username dan password. Kejahatan ini sering dilakukan dengan memalsukan situs web menggunakan protokol HTTPS yang terenkripsi, untuk menipu korban agar menganggap situs tersebut sah dan aman. Hal ini semakin menambah kerumitan dalam mengidentifikasi phishing, karena situs web palsu tersebut terlihat seperti situs resmi yang asli.

Secara hukum, tindakan phishing sebelumnya bisa dikenakan Pasal 378 KUHP yang mengatur tentang penipuan. Namun, pasal tersebut tidak sepenuhnya tepat untuk mengatur phishing, karena tidak membahas tentang informasi elektronik. Untuk itu, UU ITE yang disahkan pada tahun 2008 dan diubah pada tahun 2016, menjadi dasar hukum yang lebih sesuai

dalam mengatur tindak pidana phishing. Dalam UU ITE, khususnya Pasal 35 dan Pasal 51, tindakan manipulasi informasi elektronik, yang termasuk dalam praktik phishing, diatur dengan sanksi pidana yang cukup berat.[9]

Selain itu, Pasal 28 ayat (1) dan Pasal 45A ayat (1) UU ITE juga mengatur penyebaran berita bohong dalam transaksi elektronik yang mengakibatkan kerugian bagi konsumen. Pidana yang dijatuhkan terhadap pelaku phishing dapat dikenakan berdasarkan kombinasi pasal-pasal tersebut, yang bisa menghasilkan pidana penjara maksimal 16 tahun dan denda hingga Rp 13 miliar. Tidak hanya itu, UU Perlindungan Data Pribadi (UU PDP) juga memberikan ketentuan pidana bagi individu yang sengaja memperoleh atau mengungkapkan data pribadi tanpa izin, yang dapat mengakibatkan kerugian bagi korban.

Dengan adanya peraturan yang lebih spesifik, hukum di Indonesia kini memberikan perlindungan yang lebih jelas terhadap korban kejahatan siber, khususnya phishing. Hukum mengatur secara lebih mendetail mengenai tindakan-tindakan yang termasuk dalam kejahatan siber, serta memberikan sanksi pidana yang tegas bagi pelakunya. Hal ini diharapkan dapat mengurangi maraknya tindak pidana ini dan memberikan rasa aman bagi masyarakat dalam melakukan transaksi elektronik.

D. SIMPULAN

Perlindungan data pribadi terkait dengan tindak pidana *cyber crime* phising telah diatur dalam Undang-Undang Informasi dan Transaksi Elektonik, Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi, dan Undang-Undang 27 tahun 2022 tentang perlindungan data pribadi. UU PDP memberikan perlindungan bagi data pribadi seseorang dan memberikan sanksi tegas bagi pelaku kejahatan siber, termasuk pelaku phising. Pemerintah memiliki peran penting dalam melaksanakan UU PDP, termasuk memberikan sanksi bagi pelaku kejahatan siber, memperkuat kerja sama antara lembaga pemerintah dalam bidang keamanan siber, dan memberikan rasa aman dan nyaman bagi Masyarakat.

Pertanggungjawaban tindak pidana *cyber crime phising* diatur dalam Undang-Undang Informasi Dan Transaksi Elektronik, hal ini tertuang dalam pasal Pasal 378 KUHP tentang penipuan. Kemudian juga terdapat dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan kemudian dibentuk lagi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang

[9] Andi Hamzah. *Delik-Delik Tertentu (Speciale Delicten) di dalam KUHP*, Edisi Kedua. Jakarta: Sinar Grafika, 2015, p. 100.

Informasi Dan Transaksi Elektronik Pasal Pasal 35 jo Pasal 51 ayat (1), Pasal 30 ayat (3) jo Pasal 46 ayat (3), Pasal 32 ayat (2) jo. Pasal 48 ayat (2). Kemudian juga terdapat dalam Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi Pasal 66 dan 67.

E. SARAN

Untuk masyarakat, diharapkan untuk lebih menjaga data pribadi agar tidak terjadi kebocoran data-data pribadi yang bisa merugikan, jika para konsumen mengalami kerugian materil dalam kebocoran data pribadi dengan Pelajari informasi terbaru tentang phising agar dapat mengurangi risiko terkena phishing ,Berhati-hati sebelum mengklik tautan yang dikirimkan oleh orang,Jangan pernah mengirimkan informasi sensitif melalui email dan jangan mengklik link pada pesan yang terindikasi phishing, Berhati-hati saat menerima pesan yang meminta informasi pribadi, pastikan situs tersebut sah sebelum memberikan informasi yang diminta.Itu merupakan Upaya-upaya sederhana dalam mencegah kebocoran data pribadi.

Penerapan peraturan terkait phising agar dilakukan secara konsisten,karena seiring berkembangnya teknologi kasus penipuan secara online atau phising semakin marak dan semakin berkembang.

DAFTAR PUSTAKA

Buku :

Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara Cyber Crime*. Jakarta: PT. Refika Aditama, 2005.

Chazawi Adami. *Pelajaran Hukum Pidana Bagian Satu*. Jakarta: RajaGrafindo Persada, 2018.

Hamzah Andi. *Asas-Asas Hukum Pidana Edisi Revisi*. Jakarta: Rineka Cipta, 1994.

Ilhami Bisri. *Sistem Hukum Indonesia Cet. II*. Jakarta: PT Raja Grafindo Persada, 2005.

Muhammad Kusnardi dan Bintan Saragih Wahid, dkk. *Kejahatan Mayantara Cyber Crime*. Bandung: Refika Aditama, 2005.

Maskun. *Kejahatan Siber Cyber Crime Suatu Pengantar*. Jakarta: Kharisma Putra Utama, 2013.

Machmudin Duswara Dudu. *Pengantar Ilmu Hukum Cet. V*. Bandung: PT Refika Aditama, 2013.

Masriani, Yulies Tiena. *Pengantar Hukum Indonesia Cet. XII*. Jakarta: Sinar Grafika, 2017.

P.A.F. Lamintang. *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Sinar Baru, 1990.

Tim Redaksi BIP. *Undang-Undang Informasi dan Transaksi Elektronik Cet. 1*. Jakarta: Penerbit Bhuana Ilmu Populer, 2017.

Jurnal, Skripsi, Tesis Disertasi :

Alan Stevenres Bentelu, Steven Sentinuwo. "*Animasi 3 Dimensi Pencegahan Cyber Crime*," Teknik Informatika, Universitas Sam Ratulangi, Manado. E-Journal Teknik Informatika, Volume 8 No.1, Agustus 2016.

Andreas Agung, Hafrida, Erwin. "*Pencegahan Kejahatan Terhadap Cybercrime*," PAMPAS: Journal of Criminal, Volume 3 Nomor 2, 2022 (ISSN 2721-8325).

Destya Fidela Pratiwi. "*Pertanggungjawaban Tindak Pidana Skimming*," Jurnal Hukum, Edisi No.4, Vol. 2, Fakultas Hukum Universitas Airlangga, 2019.

Hery Firmansyah, Amad Sudiro, dkk. "*Penerapan Kebijakan Digital dalam Rangka Pencegahan Cyber Crime Ditinjau dari Undang-Undang ITE*," Seri Seminar Nasional Ke-III Universitas Tarumanagara Tahun 2021. Jakarta, 2 Desember 2021.

Indra Safitri. "*Tindak Pidana di Dunia Cyber*" dalam *Insider, Legal Journal from Indonesian Capital & Investment Market*, 1999.

Rini Retno Winarni. "*Efektivitas Penerapan Undang-Undang ITE dalam Tindak Pidana Cyber Crime*," jurnal.untagsmg.ac.id, 2016.

Peraturan Perundang-Undangan :

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Acara Pidana (KUHP)

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia No. 3881

Undang-Undang Republik Indonesia. Nomor 19 Tahun 2016. Tentang Perubahan Atas Undang-Undang. Nomor 11 Tahun 2008. Tentang Informasi Dan Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952

Undang-Undang Nomor 27 Tahun 2022 Tentang Data Pribadi Dalam Sistem Elektronik. Berita Negara Republik Indonesia Tahun 2016 Nomor 1829