PENEGAKAN HUKUM PIDANA DALAM MEMBERANTAS KEJAHATAN PENCURIAN DATA ELEKTRONIK *(PHISING)*[1]

Oleh :
Bonaventura Deogratia Manorek [2]
Adi Tirto Koesomo[3]
Meylan Maramis[4]

ABSTRAK

Penelitian ini bertujuan untuk mengkaji peran hukum pidana dalam melakukan pemberantasan tindak pidana *phising* dan untuk menganalisa hukum pidana serta peraturan terkait penegakan hukum serta peran hukum pidana dalam memberantas tindak pidana *phising*. Metode yang digunakan adalah penelitian normatif, dengan kesimpulan yaitu: 1. Penegakan hukum pidana dalam memberantas kejahatan pencurian data elektronik *(phishing)* menjadi hal yang sangat penting untuk melindungi hak masyarakat dalam era digital. Penegakan hukum melibatkan berbagai pihak, yang bekerja sama untuk mengidentifikasi, menangkap, dan memberikan sanksi kepada pelaku phishing. Namun, keberhasilan pemberantasan kejahatan *phishing* juga memerlukan edukasi kepada masyarakat tentang pentingnya menjaga kerahasiaan data pribadi dan mengenali modus-modus phishing. 2. Peraturan hukum pidana yang mengatur kejahatan phising di Indonesia terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP). Namun, meskipun regulasi ini telah mengkriminalisasi tindakan phising, masih terdapat tantangan dalam implementasinya, terutama terkait dengan identifikasi pelaku yang sering beroperasi lintas negara.

Kata Kunci : *kejahatan pencurian data elektronik*

PENDAHULUAN

A. Latar Belakang

Internet telah menjadi permasalahan khusus sejak dimanfaatkan dalam kegiatan perdagangan atau bisnis yang dikenal dengan transaksi *e-commerce*.[5] Transaksi melalui internet bisa terjadi hanya dengan membuat kesepakatan atau kontrak yang dilakukan melalui media *online*.[6] Kegiatan teknologi informasi dapat dimanfaatkan untuk penyebaran dan pencarian data yang bermanfaat untuk berbagai kegiatan keseharian. Kegiatan ini tidak dapat berlangsung jika tidak didukung oleh suatu sistem telekomunikasi.[7] Perkembangan teknologi informasi komunikasi berbasis komputer telah berkembang sangat pesat di masyarakat. Masyarakat kemudian dimudahkan dengan perkembangan teknologi tersebut.[8] Kemajuan teknologi inilah yang mengakibatkan banyak orang untuk terus berinovasi dalam mempermudah komonikasi, salah satunya dengan adanya media sosial. Media sosial merupakan sebuah media online, dimana para penggunanya bisa dengan mudah berbagi dan berkomunikasi dalam dunia virtual.

Phising merupakan bentuk cyber crime jenis baru. Sebelum diundangkannya Undang Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, praktis tidak ada satu aturan baku yang dapat menjerat pelaku tindak pidana komputer, utamanya pelaku phising. Namun ternyata setelah diundangkannya Undang Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pun, masih dirasa belum mencukupi untuk menjerat pelaku phising. Hal ini disebabkan karena belum dicantumkannya definisi phising dalam undang-undang tersebut. Undang-undang nomor 11 tahun 2008 hanya mencantumkan unsur-unsur serta kualifikasi cyber crime secara umum melalui pasal 28 ayat (1) dan pasal 35. Kedua pasal tersebut tidak membedakan apakah cyber crime itu termasuk dalam kategori carding, hacking, cracking, defacing, spamming, malware atau phising, padahal kualifikasi perbuatannya jelas berbeda. Permasalahan mengenai cyber crime atau ITE ini juga di atur dalam Undang- undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik adalah undang-undang yang dibentuk guna mengatur informasi dan transaksi elektronik, atau teknologi informasi secara umum. Undang-undang ini mengatur segala jenis yang berhubungan dengan media online.

Phising memiliki arti yaitu kejahatan dunia maya (cybercrime) dimana seseorang menyamar sebagai lembaga yang sah menghubungi target atau korban melalui email, telepon, atau pesan

---

1 Artikel Skripsi
2 Mahasiswa Fakultas Hukum Unsrat, NIM 20071101424
3 Fakultas Hukum Unsrat, Magister Ilmu Hukum
4 Fakultas Hukum Unsrat, Doktor Ilmu Hukum
5 Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, UII Press, Yogyakarta, 2003, hlm. 113.
6 Abdul Halim Barkatullah, *Perlindungan Hukum Bagi Konsumen Dalam Trnasaksi E- cvommerce Lintas Negara di Indonesia*, FH UII Press, Yogyakarta, 2009, hlm. 11.
7 Judhariksawan, *Pengantar Hukum Telekomunikasi*, Raja Grafindo Perkasa, Jakarta, 2005, hlm. 12.
8 Aswandi R, Putri R, Muhammad S, *Perlindungan Data Dan Informasi Pribadi MelaluiIndonesia Data Protection System (IDPS)*, Legislatif, Vol. 3 No. 2, hlm. 167-180.

teks, agar ia memberikan data sensitive seperti informasi identitas pribadi, detail perbankan atau kartu kredit serta kata sandi. Setelah korban atau target memberikan informasi tersebut kemudian nantinya akan digunakan untuk mengakses akun penting yang dapat mengakibatkan pencurian identitas dan kerugian finansial.[9]

Berdasarkan Anti Phising Working Group (APWG) Tercatat secara global laporan jumlah penipuan dengan modus phising yang berhasil terdeteksi selama tahun 2020 terus meningkat, di kuartal ke 4 pada bulan Desember terdapat 200.000 aktifitas phising yang terdeteksi. Selanjutnya pada tahun 2021. kuartal awal jumlah serangan phising yang diamati oleh APWG meningkat dua kali lipat selama tahun 2020, serangan phising kemudian mencapai puncaknya akan diretas, ataupun memasukan data pribadi pada sebuat website tertentu sebagai pemancingan.

Di Indonesia salah satu contoh kasus phising yang baru saja terjadi pada tanggal 2 Juni 2022 kemarin adalah terjadi kepada nasabah bank BRI menjadi korban phising yang berada di Padang, videonya menjadi viral di facebook setelah menjadi korban kejahatan phising, kedua nasabah mengaku telah kehilangan uang sebesar Rp. 1,114 Miliar dari rekeningnya. tindak kejahatan ini bermula ketika seorang nasabah pria mendapatkan pesan whatsapp mengenai perubahan biaya transaksi menjadi Rp 150 ribu dan ia pun ditawari untuk melakukan perubahan agar tidak dibebankan biaya Rp 150 ribu. 10 Nasabah ini terjebak oleh metode phising yang mana nasabah meng-klik sebuah link palsu dan kemudian diarahkan untuk mengikuti sejumlah petunjuk pengelabuan agar nasabah secara tak sadar penyerahkan data pribadi.[11]

Penegakan hukum memiliki peran penting untuk mencapai suatu kepastian, keadilan serta kemanfaatan hukum dalam tindak pidana cybercrime phising ini. Oleh karenanya hal ini dilakukan agar terciptanya suatu ketertiban di masyarakat.[12] Pelanggaran hukum akan mengakibatkan tatanan masyarakat yang rusak untuk itu reaksi atas perlanggaran hukum diperlukan sebagai bukti adanya penegakan hukum. Penegakan hukum ditinjau dari prespektif hukum pidana akan berkaitan dengan kebijakan penegakan hukum pidana terutama dari sistem peradilan pidana itu sendiri dan memiliki dua komponen yaitu proses peradilan pidana dan lembaga peradilan pidana, yang mana prosesnya ini tidak terlepas dari penyelidikan penyidikan, penuntutan dan pemeriksaan di sidang pengadilan dan pemidanaan. Sedangkan lembaga peradilannya meliputi kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan.[13]

Penegakan hukum tidak luput dari peran aparat penegak hukumnya yaitu aparat kepolisian, aparat kejaksaan, para hakim serta advokat. Para penegak hukum tersebut haruslah melaksanakan dan menjalankan aturan hukum sebagaimana mestinya dengan baik dan benar demi tercapainya supremasi hukum. Aparat penegak hukum sudah seharusnya mengedepankan hak asasi manusia dan menjamin semua warganya memiliki kedudukan hukum yang sama dengan tidak ada pengecualian.[14]

Proses Penegakan hukum dengan fungsi sistem peradilan pidana sangat diperlukan untuk menanggulangi kejahatan. Tahap pertama dalam sistem peradilan pidana adalah pada tingkat penyelidikan dan penyidikan yang dilakukan oleh aparat kepolisian. Dalam tahap penyelidikan kepolisian mencari kebenaran dari sebuah peristiwa pidana yang berasal dari laporan masyarakat atau karena tertangkap tangan. Sebagaimana tercantum dalam Pasal 13 dan Pasal 14 ayat (1) huruf g Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia yang berbunyi: kebenaran dari sebuah peristiwa pidana yang berasal dari laporan masyarakat atau karena tertangkap tangan.

B. Rumusan Masalah

1. Bagaimana penegakan hukum tindak pidana pencurian data elektronik (*Phising*)?
2. Bagaimana pengaturan hukum tindak pidana *phising* terhadap perlindungan korban tindak pidana pencurian data elektronik di Masyarakat?

C. Metode Penulisan

Penelitian ini adalah penelitian hukum normatif.

---

[9] Erizka Permatasari, Jeat Hukum Pelaku Phishing dan Modusnya, diakses dari https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnyn-c15050,

[10] Ade suhendra, Diduga Kena Phising Nasabah BRI di Padang Kehilangan Uang Rp1,114 Miliar, diakses dari https://www.harianhaluan.com/news/pr-103582510/diduga-kena-phising- nasabah-bri-di-padang-kehilangan-uang-rp1114-miliar

[11] Ibid

[12] Musa Darwin Pane, Sahat Maruli Tua Situmeang, "Penegakan Hukum Cyber Crime dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi" Jurnal Loyalitas Sosial, Vol. 3, No.2, 2021, hlm. 95

[13] Titik Suharti, "Proses Penegakan Hukum di Indonesia dalam Perspektif Hukum Pidana", Norma, Vol no. 1, 2004, hlm. 43.

[14] Vivi Ariyanti, "Kebijakan Penegakan Hukum dalam Sistem Peradilan Pidana Indonesia", Jurnal Yuridis, Vol. 6 No.2, 2019, hlm. 35.

PEMBAHASAN

A. Penegakan Hukum Tindak Pidana Pencurian Data Elektronik *(Phising)*

Undang-Undang Nomor 1 Tahun 2024 adalah perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Perubahan ini bertujuan untuk memperkuat regulasi terkait kejahatan siber, termasuk pencurian data Elektronik melalui phishing.

Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang No.11 Tahun 2008 Tentang Infomasi dan Transaksi Elektronik Pasal 28 ayat 1 "Setiap Orang dengan sengaja dan/atau mentransmisikan Informasi Elektronik dan/ atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik".

Pasal 45 ayat 1 "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (ll dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)".

Dalam Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan perlindungan lebih spesifik terhadap data pribadi dan menetapkan sanksi bagi pelaku kejahatan siber, termasuk phishing. Dalam Pasal 67 ayat (1) dan (3).

Phising berasal dari kata fishing yang berarti memancing, yang merupakan salah satu upaya untuk mendapatkan informasi data seseorang dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/legitimate organization dan biasanya berkomunikasi secara elektronik. Data yang menjadi sasaran biasanya berupa data diri seperti nama, usia, alamat, kemudian data akun seperti username dan password, dan data finansial yang berkaitan dengan informasi kartu kredit atau nomor rekening.[15] Kegiatan phishing bertujuan untuk menipu korban agar tanpa sadar memberikan informasi pribadi mereka, yang kemudian akan digunakan untuk tujuan kejahatan. Biasanya, modus operandi kejahatan ini dimulai dengan berpura-pura menjadi instansi resmi melalui penggunaan website atau email yang palsu untuk menipu korban.

Indonesia sendiri pernah mengalami kasus tentang phishing yang paling terkenal adalah kasus dari Internet banking milik bank BCA terjadi pada tahun 2001, saat itu terdapat seseorang berinisial Steven Haryanto yang membeli beberapa domain yang mirip dengan domain milik bca yaitu klikbca.com, Steven Haryanto sendiri melakukan aksinya dengan membuat domain serupa dengan mengubah ejaan dari website asli seperti clickbca.com, klickbca.com, klikbac.com. Steven Haryanto juga mendesain website tersebut sedemikian rupa sehingga mirip dengan website asli milik bca sehingga banyak orang yang tertipu[33]. Namun Steven Haryanto melakukan hal tersebut bukan untuk mencuri data dari nasabah, melainkan Steven Haryanto bertujuan untuk menguji tingkat keamanan dari situs milik bank BCA tersebut, akan tetapi perbuatan Steven Haryanto yang mengganggu sebuah sistem milik orang lain yang dilindungi privasinya dan pemalsuan situs internet banking milik BCA sehingga perkara ini dikategorikan sebagai perkara perdata.[16]

Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang bertujuan untuk mengatur perlindungan data pribadi secara menyeluruh. UU ini mencakup informasi yang dapat mengidentifikasi individu baik secara langsung maupun tidak langsung, baik melalui sistem elektronik maupun non- elektronik. Tujuan utama dari UU PDP adalah menyediakan kerangka hukum yang memadai untuk melindungi masyarakat dan pemerintah dari kejahatan digital, termasuk pencurian data pribadi Kementerian Komunikasi dan Informatika menyatakan bahwa UU PDP akan menandai langkah penting dalam pengelolaan data pribadi di Indonesia. Undang-undang ini terdiri dari 18 bab dan 78 pasal, yang mengatur berbagai aspek seperti transfer data pribadi, sanksi administratif, kelembagaan, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan dalam penggunaan data pribadi, serta ketentuan pidana dan peralihan.[17] Undang-Undang PDP memberikan kerangka hukum yang lebih komprehensif untuk perlindungan data pribadi,

---

[15] Efvy Zam, PHISING Trik Mudah Penyadapan Password Dan Pencegahannya (Jakarta: Mediakita, 2014)

[16] Setiyardi, 'Kreasi Pelesetan Pemicu Delik' (Tempo, 2017) , https://majalah.tempo.co/read/ilmu-danteknologi/80886/kreasi-pelesetan-pemicu-delik/ diakses pada 15 Maret 2024

[17] Anggi Tondi Martano, "Pengesahan UU PDP Era Baru Tata Kelola Data Pribadi", https://mediaindonesia.com/politik-dan-hukum/523832/pengesahan-uu-pdp-era-baru-tata-kelola-data-pribadi

masih terdapat gap dalam penegakan hukum terhadap kejahatan siber, khususnya dalam hal penyesuaian dengan praktikpraktik kejahatan baru seperti phishing yang terus berkembang. Ada kebutuhan mendesak untuk terus memperbarui dan menyempurnakan regulasi dan implementasi hukum guna menghadapi tantangan baru di ranah kejahatan siber.

Cyber Crime merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari dunia international. Volodymyr Golubev menyebutnya sebagai the new form of anti-social behavior.[18] Beberapa sebutan lain yang cukup terkenal diberikan kepada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain sebagai kejahatan dunia maya (cyber space/ virtual space offence), dimensi baru dari high tech crime, dimensi baru dari transnational crime, dan dimensi baru dari white collar crime (WCC). Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai The Prevention of Crime and the Treatment of Offenders di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian cyber crime, yaitu cyber crime dan computer related crime. Dalam back ground paper untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah cyber crime dibagi dalam dua kategori. Pertama, cyber crime dalam arti sempit (in a narrow sense) disebut computer crime. Kedua, cyber crime dalam arti luas (in a broader sense) disebut computer related crime.

Dalam UU No. 19 Tahun 2016 dinyatakan, Pasal 31 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. (3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang. (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Undang- Undang. Adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan. (3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang. (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Undang- Undang. Walaupun Undang-undang Nomor 11 Tahun 2008 yang kemudian dirubah dengan UU No. 19 tentang Perubahan atas UU No. 11 Tahun 2008, namun belum cukup mencakup semua aspek dari kejahatan dunia maya. Selain itu, kita tidak bisa terus mengacu pada Undang-Undang Informasi dan Transaksi Elektronik saja, mealainkan kita harus menyusun konsep Kitab Undang-undang Hukum Pidana yang baru. Karena KUHP lama sudah tidak dapat lagi menjangkau tindak-tindak pidana baru yang tercipta oleh perkembangan jaman, untuk itu dibutuhkan konsep- konsep baru tentang KUHP kita. Pengaturan untuk menangani kejahatan komputer sebaiknya diintegrasikan ke dalam KUHP dan bukan ke dalam undang-undang tersendiri. Terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku cyber crime terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

a. KUHP.
b. Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang -Undang No.11 Tahun 2008 Tentang Infomasi dan Transaksi Elektronik
c. Undang-Undang Nomor 11 tahun 2008 tentang ITE.
d. Undang-Undang Nomor 44 tahun 2008 tentang Pornografi.
e. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.
f. Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat.
g. Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen.
h. Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta.

[18] Volodymyr Golubev dalam Barda NA. 2007. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia, Raja Grafindo Persada. Jakarta, hal. 1.

i. Undang-Undang Nomor 8 Tahun 1997 tentang Dokumen Perusahaan.
j. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas UndangUndang. Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang.
k. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Terorisme.

Meski Indonesia menduduki peringkat pertama dalam cyber crime pada tahun 2004, akan tetapi jumlah kasus yang diputuskan oleh pengadilan tidaklah banyak. Dalam hal ini angka dark number cukup besar dan data yang dihimpun oleh Polri juga bukan data yang berasal dari investigasi Polri, sebagian besar data tersebut berupa laporan dari para korban.[19]

B. Pengaturan Hukum Tindak Pidana *Phising* Terhadap Perlindungan Korban Tindak Pidana *Phising* di Masyarakat Indonesia

Phishing adalah jenis serangan rekayasa sosial yang sering digunakan untuk mencuri data pengguna, termasuk kredensial login (akun), dan nomor kartu kredit. Serangan siber itu terjadi ketika penyerang (intruder) menyamar sebagai entitas tepercaya (baik berupa website atau email palsu), menipu korban untuk membuka email, pesan instan, atau pesan teks. Praktiknya kadang pula phisher (pelaku phishing) mengirim email palsu yang menyerupai email dari sumber terpercaya. Menurut IGN Mantra dosen peneliti cyber war dan security inspection menjelaskan bahwa phishing adalah percobaan penipuan menggunakan surel (surat elektronik) dengan tujuan untuk mendapatkan username, password, token, dan informasi-informasi sensitif lainnya yang dikirim melalui surel. Surel phishing datang seolah-olah dari perusahaan/organisasi di mana user adalah anggota/member.[20]

Modus operandi yang paling banyak ditemui saat ini adalah usaha phishing melalui SMS pada telepon genggam, di mana sudah banyak korban yang harus kehilangan uangnya karena diminta untuk melakukan transaksi ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga menjebak sang korban.[21] Phishing menjadi pilihan yang populer di kalangan para peretas karena dinilai murah dan kemudahan, serta efektifitasnya cukup tinggi. Meskipun banyak organisasi yang telah menerapkan sistem keamanan untuk memblokir serangan phishing, namun penyerang juga semakin memiliki peralatan phishing yang lebih canggih.

Pemalsuan website dan gambar-gambar sangat mudah dilakukan melalui internet dan pengguna awam biasanya tidak menyadari hal tersebut. Hanya dengan melakukan copy dan paste, sebuah website yang mirip dengan asli akan langsung tercipta. Pelaku phishing juga bisa membuat website yang tampak sangat bagus dengan berbagai komentar pengguna yang semuanya fiktif untuk meyakinkan calon korbannya.

Undang-Undang No. 27 Tahun 2022 adalah UU yang mengatur tentang perlindungan data pribadi[22] yang berhubungan dengan teknologi (cyber crime). Maka dari itu diperlukan landasan hukum dalam menjaga hak privasi dan keamanan informasi setiap individu karena tindak pidana cyber phishing merupakan bagian dari cyber crime. Pada 17 Oktober 2022 presiden Jokowi mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dengan mengakui adanya hak terhadap perlindungan diri pribadi warga negaranya yang tercantum dalam pasal 28 huruf G yaitu "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".[23] Pasal ini dengan jelas mengatur bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan dilindungi dari ancaman ketakutan akan kejahatan[24] dengan jelas menegaskan bahwa setiap warga negara tanpa terkecuali mempunyai hak untuk melindungi dirinya sendiri, keluarganya, kehormatannya, martabatnya dan harta benda yang dikuasainya. Hak atas data pribadi merupakan hak milik yang melekat pada setiap individu sebagai subjek data pribadi.

[19] Jakarta, Tribun-Timur.Com. Diakses terakhir tanggal 26 Februari 2024
[20] IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", Info Komputer, (9 Maret 2024), 71.
[21] Richardus Eko Indrajit, Konsep dan Strategi Keamanan Informasi di Dunia Cyber, (Yogyakarta: Graha Ilmu, 2014), 116
[22] JDIH Kemenko Bidang Kemaritiman dan Investasi, "UU No.27/2022: Perlindungan Data Pribadi," JDIH Kemenko Bidang Kemaritiman dan Investasi, 2022, https://jdih.maritim.go.id/uu-no-272022-pelindungandata-pribadi.
[23] Nurmalasari, "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum",Jurnal Syntax Idea, Vol. 3 (Agustus,2021), hal. 1959
[24] Anggraeni, SF, 2018, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", Jurnal Hukum & Pembangunan, Vol. 48 No. 4, 814 - 825

Perlindungan data pribadi berlaku bagi semua individu, baik warga negara Indonesia maupun orang asing di Indonesia, sehubung dengan seluruh pemrosesan data pribadi termasuk pengumpulan, penggunaan, penyimpanan, transmisi, dan penghapusan. Undang-Undang ini muncul karena keprihatinan akan pelanggaran terhadap data pribadi yang dapat dialami oleh orang atau badan hukum yang dapat menimbulkan kerugian materil dan nonmateril. Menurut Undang-Undang Pelindungan Data Pribadi, definisi data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya, baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.[25] Perlindungan data pribadi sebagai hak konstitusional yang harus dipenuhi oleh pemerintah secara hierarki peraturang perundang-undangan yang diturunkan dalam peraturan perundang-undangan.[26]

Perlindungan data pribadi sejatinya telah diakui sebagai salah satu jenis Hak Asasi Manusia dan telah diakomodir dalam instrumen hukum internasional. Dalam hal ini, perlindungan data pribadi merupakan suatu irisan dari hak atas informasi dan hak atas privasi melalui proses evolusi yang panjang sejak diakuinya Hak Asasi Manusia melalui *The Universal Declaration of Human Rights* (UDHR) di tahun 1948. Secara substantif, dapat dilihat bahwa UDHR memberikan perlindungan yang sangat luas mengenai hak privasi. Pertama, *phisical privacy*, yang bertujuan untuk memberikan perlindungan privasi yang berhubungan dengan tempat tinggal seseorang. Contohnya yaitu ketika seseorang tidak diperkenankan memasuki rumah orang lain tanpa izin pemilik, negara tidak diperbolehkan menggeledah rumah seseorang tanpa adanya surat tugas dan penahanan, dan negara tidak diperbolehkan untuk melakukan penyadapan di dalam tempat tinggal warga negaranya.[27] Kedua, *decisional privacy*, bertujuan untuk memberikan perlindungan privasi terhadap seseorang untuk dapat menentukan kehidupannya sendiri termasuk kehidupan keluarganya. Contohnya yaitu ketika seseorang memiliki hak untuk menentukan dan mengurusi rumah tangganya sendiri tanpa campur tangan orang lain. Ketiga, *dignity*, yang bertujuan untuk memberikan perlindungan privasi berkaitan dengan harga diri seseorang termasuk nama baik dan reputasi seseorang. Keempat, *informational privacy*, yang bertujuan untuk memberikan perlindungan privasi terhadap seseorang untuk dapat melakukan dan menyimpan data pribadi miliknya.

Undang-Undang Perlindungan Data Pribadi mengatur 4 jenis perbuatan yang dilarang (tindak pidana) berupa perbuatan secara melawan hukum untuk memperoleh atau mengumpulkan; mengungkapkan; atau menggunakan data pribadi yang bukan miliknya dan perbuatan membuat data pribadi palsu/memalsukan data pribadi itu sendiri. Pelanggaran atas ketentuan ini dikenakan sanksi pidana berupa denda maupun penjara sesuai yang tertuang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai berikut:

1. Sanksi Pidana
   a. Pasal 65 ayat (1), "setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain, yang dapat mengakibatkan kerugian bagi subjek data pribadi". Pelanggaran terhadap ketentuan ini diatur dalam Pasal 67 ayat (1), yang menyatakan bahwa "setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud tersebut dapat dipidana dengan pidana penjara paling lama lima tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)".
   b. Pasal 65 ayat (2) melarang "setiap orang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya". Pelanggaran ini, sebagaimana diatur dalam Pasal 67 ayat (2), dapat dikenakan sanksi pidana berupa penjara paling lama empat tahun dan/atau denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah) bagi mereka yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya.
   c. Pasal 65 ayat (3) "Setiap orang dilarang secara melawan hukum menggunakan Data Pribadi yang bukan miliknya". Sesuai dengan Pasal 67 ayat (3), pelaku yang sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya dapat dikenakan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

[25] UU tentang Perlindungan Data Pribadi Nomor 27 Tahun 2022 Pasal 1 ayat 1

[26] Erlina Maria Christin Sinaga, "Formulasi Legislasi Perlindungan Data Pribadi," Jurnal RechtVinding, 9.2 (2020), 237–56.

[27] Asbojrn Eide, The Universal Declaration of Human Rights: A Commentary, hlm. 190

d. Terakhir, Pasal 66 “Setiap orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain”. Sesuai dengan Pasal 68, setiap orang yang dengan sengaja membuat atau memalsukan data pribadi dengan maksud tersebut dapat dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah).

2. Sanksi Perdata Pada Pasal 69 selain dijatuhi pidana sebagaimana yang dimaksud dalam Pasal 67 dan Pasal 68 juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.[28]
3. Sanksi Administratif
   Pasal 70
   a. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh Korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi.
   b. Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda.
   c. Pidana denda yang dijatuhkan kepada Korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan.
   d. Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:
      1) Perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
      2) Pembekuan seluruh atau sebagian usaha Korporasi;
      3) Pelarangan permanen melakukan perbuatan tertentu;
      4) Penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi; Melaksanakan kewajiban yang telah dilalaikan;
      5) Pembayaran ganti rugi;
      6) Pencabutan izin; dan/atau
      7) Pembubaran Korporasi.

Adapun sanksi administasi ini bertujuan untuk menegakkan tanggung jawab korporasi dan memastikan telah mematuhi ketentuan perlindungan data pribadi. Misalnya, jika sebuah perusahaan (korporasi) terlibat dalam tindakan phishing, mereka dapat dikenakan denda besar, pembekuan atau penutupan usaha, dan bahkan pembubaran jika tindak pidana tersebut serius. Penjatuhan pidana ganti rugi, walaupun begitu tidak serta merta menghapuskan adanya pidana penjara kepada pelaku kejahatan terhadap harta benda. Jika pidana penjara sama sekali dihilangkan, akan berdampak pada berkurangnya efek jera bagi pelaku kejahatan terhadap harta benda. Mereka kemungkinan berpikir bahwa kejahatan ini dapat mudah dilakukan karena dengan mudah dapat ditebus. Harus ada pengecualian penerapan pidana ganti rugi sebagai pidana pokok. Terhadap kasus-kasus pengulangan (recidive), atau kejahatan terhadap harta benda yang jumlahnya besar, berencana, bersama-sama, atau korbannya orang yang tidak mampu, maka penjatuhan pidana penjara tetap diperlukan.[29]

Sanksi untuk menjerat pelaku tindak pidana phishing disebutkan juga dalam Undang-Undang Informasi dan Transaksi Elektronik:

1. Pasal 28 ayat (1), menyebutkan bahwa: “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.”
2. Pasal 35, yaitu: “Setiap Orang dengan sengaja dan tanpa hak atau 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 dikenakan ancaman pidana Pasal 51 ayat (1): Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00. (dua belas miliar rupiah)”.[30]
3. Pasal 45 ayat (2), menyebutkan bahwa: “Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda

[28] Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, hal. 31

[29] Erdianto Effendi, “Penjatuhan Pidana Ganti Rugi Sebagai Pidana Pokok Dalam Kejahatan Terhadap Harta Benda” Jurnal USM Law Review 5, no. 2 (2022): 617–32, https://doi.org/10.26623/julr.v5i2.5355.

[30] UU ITE Pasal 35

paling banyak Rp1.000.000.000,00 (satu miliar rupiah)".[31]

4. Pasal 48 ayat (2) menyebutkan "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah)".
5. Pasal 51 ayat (1) menyebutkan "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak rp. 12.000.000.000,00 (dua belas miliar rupiah)".[32]

Bentuk perlindungan masyarakat merupakan wujud dari pertanggungjawaban negara kepada seluruh masyarakat Indonesia sebagai negara hukum. Esensi perlindungan dari negara pun telah terkandung dalam Alinea ke-IV Pembukaan Undang-Undang Dasar 1945, dimana negara mempunyai cita-cita untuk melindungi bangsa Indonesia, sehingga kepada setiap masyarakat yang membutuhkan perlindungan hukumdapat dipenuhi setiap hak yang seharusnya ia miliki sebagai warga negara Indonesia, terlebih khusus bagi korban-korban kejahatan.Untuk perlindungan dari kerugian yang dialami korban, telah disebutkan secara yuridis dimana tercantum dalam:

1. Pasal 28 D ayat(1) Undang-Undang 1945 menyebutkan "Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum."
2. Selanjutnya, dicantumkan lagi dalam Pasal 3 ayat (2) Undang- Undang No. 39 Tahun 1999 Tentang Hak Asasi Manusia yang menyebutkan, "Setiap orang berhak atas pengakuan, jaminan, perlindungan dan perlakuan hukum yang adil serta mendapat kepastian hukum dan perlakuan yang sama di depan hukum."
3. Pasal 40 ayat (2) UU ITE bahwa "Pemerintah melindungikepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan."
4. Pasal 1 Angka 8 Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang menyebutkan, "Perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada Saksi dan/atau Korban yang wajib dilaksanakan oleh LPSK atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini. Perlindungan terhadap korban disebutkan oleh Barda Nawawi Arief, bahwa pengertiannya terbagi atas 2 (dua) makna, yaitu:[33]
    a. Dapat diartikan, sebagai perlindungan hukum supayatidak menjadi seorang korban tindak pidana.
    b. Dapat diartikan, sebagai perlindungan agar supaya korban dapat memperoleh jaminan atau santunan hukum dari kerugian yang dialami korban, seperti rehabilitasi, pemulihan keseimbangan batin (seperti; pemaafan), pemberian ganti rugi (seperti; restitusi, kompensasi atau jaminan kesejahteraan sosial.

Cyber crime atau dengan istilah lain yaitu kejahatan dunia maya dalam peraturan untuk transaksi elektronik yakni UU ITE, tidak mengatur secara jelas bentuk perlindungan bagi para korban atas kejahatan dalam sebuah transaksi elektronik tersebut. Untuk cyber crime berbentuk phising adalah jenis kejahatan yang dapat mengakibatkan kerugian terhadap korban-korbannya secara materiil, seperti data pribadi. Pada dasarnya, data pribadi dilindungi berdasarkan peraturan perundang- undangan di Indonesia. Oleh karena itu, ketika kerahasiaan terhadap suatu (barang) hak milik tidak lagi sempurna maka membutuhkan perlindungan hukum dalam bentuk perlindungan kepada pihak-pihak yang dirugikan. Karena ketika data pribadi telah diketahui oleh pihak lain dapat mengakibatkan pembobolan terhadap data tersebut, seperti yang marak terjadi yaitu ketertarikan pelaku terhadap data kartu kredit dan/atau nomor rekening sehingga dapat membuat kerugian ekonomi bagi korban. Akan tetapi, menurut UU ITE bentuk dari pemenuhan hak atas perlindungan bagi para korban dalam sebuah transaksi elektronik atau cyber crime ini hanya ditandai dengan adanya bentuk penyelesaian

[31] Hardianto Djanggih, 2013, "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime". Jurnal Media Hukum Vol 1 dan 2, hlm.24

[32] Erizka Permatasari. "Jerat Hukum Pelaku Phishing Dan Modusnya" (2021) https://new.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphising-i-dan- modusnya) diakses 15 Mei 2024

[33] Mahesa J. Kusuma, "Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan, Cet 2", (Bandung: Nusa Media, 2019), hlm.36

perkara berupa ketentuan pemidanaan atas perbuatan-perbuatan yang dilarang dalam undang-undang ini kepada pelaku tindak pidana dimana hal tersebut tercantum dari Pasal 45 sampai Pasal 52 UU ITE berupa pidana penjara dan/atau pidana denda. Pemidanaan pada pelaku untuk menegakan hukum bagi para korban merupakan langkah yang tepat sehingga kebanyakan bentuk ketentuan pidana yang tercantum dalam UU ITE maupun KUHP, dirangkaikan dengan pemberian sanksi berupa pidana penjara dan pidana denda. Sehingga pada akhirnya, pidana penjara dan pidana denda bagi pelaku tindak pidana dirasa kurang cukup untuk melindungi dan memenuhi hak para korban terlebih khusus bagi korban cyber crimeberbentuk phising untuk mengganti kerugian secara materiil yang tidak sepantasnya ia alami, apalagi bagi korban yang memiliki perekonomian lemah.

Berkaitan peraturan yang mengatur secara khusus mengenai perlindungan kepada korban, di Indonesia terdapat peraturan perundang-undangan yang mengaturnya yaitu dalam UU No. 31 Tahun 2014 Tentang Perubahan Atas UU No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban dengan didampingi oleh LPSK atau Lembaga Perlindungan Saksi dan Korban yang adalah lembaga aktif untuk membantu saksi dan korban tindak pidana untuk mendapatkan perlindungan dan pemenuhan haknya.

Korban phising yang pada dasarnya memiliki kebutuhan terhadap pemenuhan kerugian material yang dialaminya, dalam UU Perlindungan Saksi dan Korban atau disebut dengan UUPSK menyebutkan terdapat adanya perlindungan korban dan/atau saksi tindak pidana yaitu dalam bentuk Kompensasi, Restitusi dan Bantuan.

Terhadap kerugian materiil bagi korban tindak pidana cyber crimeberbentuk phising ini, Restitusi adalah metode yang tepat. Seperti dalam Pasal 1 Angka 11 yang menyebutkan bahwa "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga." Untuk memperoleh perlindungan bagi korban tindak pidana melalui LPSK, harus melalui tahap pengajuan permohonan yang diajukan ke bagian UP2 LPSK, dengan memperhatikan syarat-syarat yang tercantum dalam Pasal 21 Peraturan Pemerintah No. 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi dan Bantuan Kepada Saksi dan Korban.

Pada hakikatnya pengajuan permohonan Restitusi kepada LPSK dapat diajukan sebelum perkara didakwakan, dan setelah perkara memperoleh putusan pengadilan. Dengan ditangani oleh LPSK, untuk mengajukan permohonan Restitusi dari pemohon ke pihak terkait. Untuk perkara yang belum didakwakan, permohonan diajukan kepada penuntut umum agar dapat memuat permohonan kedalam tuntutannya sekaligus, dan untuk perkara yang telah memperoleh putusan pengadilan diajukan kepada pengadilan agar dapat diberikan penetapan.[34] Dalam Pasal 7A ayat (1) UUPSK menyebutkan bahwa Korban tindak pidana berhak memperoleh Restitusi, berupa:

1. ganti kerugian atas kehilangan kekayaan atau penghasilan;
2. ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana; dan/atau
3. penggantian biaya perawatan medis dan/atau psikologis.

Akan tetapi, dilanjutkan dalam Pasal 7A ayat (2) yang menyebutkan bahwa "Tindak pidana sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan LPSK". Keputusan LPSK yang dimaksud yaitu keputusan berdasarkan Rapat Paripurna LPSK untuk menyatakan penolakan atau diterimanya permohonan perlindungan bagi korban tindak pidana yang diajukan oleh pemohon.

Dalam Peraturan Ketua LPSK No. 6 Tahun 2010 tentang Tata Cara Pemberian Perlindungan Saksi dan Korban, Pasal 16 ayat (1) menyebutkan bahwa, "Keputusan Rapat Paripurna anggota LPSK sebagaimana dimaksud dalam pasal 15 ayat (4) memuat:

1. Klasifikasi kasus atau perkara: berat, sedang, atau ringan yang dihadapi oleh pemohon;
2. Bentuk perlindungan yang diberikan kepada pemohon; atau
3. Pemberian bantuan pemenuhan hak procedural."

Sehingga, kelanjutan pada tahap yang berikutnya hanya bergantung dari hasil Rapat Paripurna Anggota LPSK ini, kemudian selanjutnya jika dinyatakan diterima dapat dilimpahkan ke bidang perlindungan untuk masuk ke tahap pemberian perlindungan sebagaimana yang dimaksud dalam permohonan tersebut. Apabila, permohonan ditolak LPSK tetap menyampaikan pemberitahuan tersebut kepada pihak pemohon secara tertulis. Akan tetapi, perlindungan hukum yang dimaksud menurut UUPSK ini ialah siapa saja yang mengajukan permohonan perlindungan yang dapat dilindungi ditinjau dari kerugian yang benar-benar dialami oleh korban. Kontrak elektronik adalah perjanjian

[34] Penetapan pengadilan yaitu ketatapan yang diberikan oleh hakim terhadap suatu permasalahan hukum yang diajukan kepadanya agar dapat diberi ketetapan, yang hanya dihadiri oleh pihak pemohon yang selanjutnya disebut pemohon I dan pemohon II.

antar pihak yang dilakukan dengan menggunakan sistem elektronik,jelas Pasal 1 angka 17 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE melarang adanya perjanjian di luar pihak yang tidak mengetahui perjanjian awal mula tersebut.

PENUTUP

A. Kesimpulan

1. Penegakan hukum pidana dalam memberantas kejahatan pencurian data elektronik *(phishing)* menjadi hal yang sangat penting untuk melindungi hak masyarakat dalam era digital. *Phishing*, sebagai salah satu bentuk kejahatan siber, dilakukan dengan cara mengelabui korban untuk memberikan data pribadi, yang kemudian digunakan oleh pelaku untuk tujuan ilegal, seperti penipuan finansial atau penyalahgunaan identitas. Penegakan hukum melibatkan berbagai pihak, termasuk kepolisian, Kementerian Kominfo, dan otoritas terkait lainnya, yang bekerja sama untuk mengidentifikasi, menangkap, dan memberikan sanksi kepada pelaku phishing. Namun, keberhasilan pemberantasan kejahatan *phishing* juga memerlukan edukasi kepada masyarakat tentang pentingnya menjaga kerahasiaan data pribadi dan mengenali modus-modus phishing. Penegakan hukum terhadap pelaku phising masih menghadapi kendala dalam hal pelacakan pelaku, koordinasi antar lembaga penegak hukum, serta kurangnya kesadaran masyarakat mengenai metode dan bahaya phising. Selain itu, perbedaan regulasi hukum siber antar negara juga menyulitkan ekstradisi dan penindakan terhadap pelaku yang beroperasi di luar yurisdiksi nasional.
2. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan dasar hukum yang kuat dalam memberantas kejahatan ini. Melalui pasal-pasal yang mengatur tentang akses ilegal, pengambilan data tanpa izin, dan penyebaran informasi yang menyesatkan, UU ITE memberikan ancaman pidana yang berat bagi pelaku. Peraturan hukum pidana yang mengatur kejahatan phising di Indonesia terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP). Namun, meskipun regulasi ini telah mengkriminalisasi tindakan phising, masih terdapat tantangan dalam implementasinya, terutama terkait dengan identifikasi pelaku yang sering beroperasi lintas negara.

B. Saran

1. Penguatan Regulasi dan Penegakan Hukum yang Transparan dan Tegas Pemerintah perlu terus memperbarui dan menyempurnakan regulasi terkait kejahatan siber, termasuk *phishing*, agar dapat mengakomodasi perkembangan teknologi dan modus operandi yang semakin canggih. Kolaborasi antara Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dengan Undang-Undang Perlindungan Data Pribadi harus terus diperkuat untuk memberikan perlindungan yang lebih komprehensif serta proses penegakan hukum terhadap pelaku phishing harus dilakukan secara transparan dan tegas untuk memberikan efek jera. Publikasi kasus *phishing* yang telah ditangani juga dapat meningkatkan kepercayaan masyarakat terhadap upaya pemerintah dalam memberantas kejahatan ini.
2. Edukasi Masyarakat dan Layanan Pengaduan dan Dukungan Korban. Edukasi dan literasi digital bagi masyarakat harus terus dilakukan secara masif untuk meningkatkan kesadaran tentang pentingnya menjaga data pribadi dan mengenali modus phishing. Kampanye edukasi dapat dilakukan melalui media sosial, seminar, atau program di sekolah dan universitas serta Pemerintah atau instansi terkait perlu menyediakan layanan pengaduan dan dukungan yang cepat bagi korban phishing. Hal ini meliputi pemulihan kerugian korban, pemblokiran akses pelaku terhadap data curian, serta panduan pemulihan data.
3. Peningkatan Teknologi Keamanan, Perusahaan teknologi dan penyedia layanan elektronik diharapkan mengembangkan sistem keamanan yang lebih canggih untuk melindungi data pengguna. Penggunaan teknologi seperti autentikasi dua faktor (two-factor authentication) harus menjadi standar dalam setiap platform digital.

DAFTAR PUSTAKA

BUKU

Abdul Halim Barkatullah, *Perlindungan Hukum Bagi Konsumen Dalam Trnasaksi E-cvommerce Lintas Negara di Indonesia*, FH UII Press, Yogyakarta, 2009.

Adami Chazawi, *Pelajaran Hukum Pidana Bagian I*, Jakarta: Rajawali Pers, 2011.

Agus Rahardjo, 2002, *Cyber crime-Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung.

Ahmad Ramli, 2004, *Cyber Law dan HAKI-Dalam System Hukum Indonesia*, Rafika Aditama, Bandung

Aswandi R, Putri R, Muhammad S, *Perlindungan Data Dan Informasi Pribadi MelaluiIndonesia Data Protection System (IDPS)*, Legislatif, Vol. 3 No. 2.

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Predana Media Group, Jakarta, 2007.

Barda Nawawi Arief, *Sari Kuliah Hukum Pidana II*, Fakultas Hukum Undip, Bandung, 1984.

Barda Nawawi, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, PT. RajaGrafindo Persada, Jakarta, 2005.

Budi Agus Riswandi, *Hukum dan Internet di Indonesia*, UII Press, Yogyakarta, 2003.

Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," *Jurnal Saintkom*, Vol. 13, No. 3, 2014.

Dr. Leden Marpaung, S.H. 2009. *Asas-Teori-Praktik: Hukum Pidana, (Jakarta; Sinar Grafika)*, Cet Ke VI.

Eril, 'Langkah Terbaik Untuk Mengatasi Phising Dan Pencegahannya' (Gudang. SSL, 2020) , diakses pada 15 Maret 2024.

Judhariksawan, *Pengantar Hukum Telekomunikasi*, Raja Grafindo Perkasa, Jakarta, 2005.

Lamintang, *Dasar-dasar Hukum Pidana Indonesia*. Sinar Baru, Bandung, 1984.

Mahesa J. Kusuma, "Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan, Cet 2", (Bandung: Nusa Media, 2019).

Mahrus Ali, *Dasar-Dasar Hukum Pidana*, Cetakan ke-1, Jakarta: Sinar Grafika, 2011.

Moeljatno, *Asas-asas Hukum Pidana*, Cetakan ke-8, Jakarta, Rineka Cipta, 2008.

Rahmanuddin Tomalili, *Hukum Pidana*, Yogyakarta: CV. Budi Utama, 2012.

Rasyid Ariman dan Fahmi Raghib, *Hukum Pidana*, Setara Press, Malang, 2015.

Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta: Graha Ilmu, 2014.

Siswanto Sunarso, *Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari*, PT. Rineka Cipta, Jakarta, 2009.

Tri Andrisman. 2009. *Hukum Pidana, Azas-Azas Dan Aturan Umum Hukum Pidana Indonesia*, (Bandar Lampung: Universitas Lampung). Hal. 70

Volodymyr Golubev dalam Barda NA. 2007. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime Di Indonesia*, Raja Grafindo Persada. Jakarta.

JURNAL

Anggraeni, SF, 2018, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia", Jurnal Hukum & Pembangunan, Vol. 48 No. 4, 814 – 825

Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", PAMPAS: Journal of Criminal

Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi, hlm. 72.

Asbojrn Eide, *The Universal Declaration of Human Rights: A Commentary*

Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber", Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211.

Dikdik, Elisatris, Cyber Law Aspek Hukum Teknologi Informasi, Bandung, Refika Aditama, 2009, hlm.8

Efvy Zam, PHISING Trik Mudah Penyadapan Password Dan Pencegahannya (Jakarta: Mediakita, 2014)

Erdianto Effendi, "Penjatuhan Pidana Ganti Rugi Sebagai Pidana Pokok Dalam Kejahatan Terhadap Harta Benda" Jurnal USM Law Review 5, no. 2 (2022

Erlina Maria Christin Sinaga, "Formulasi Legislasi Perlindungan Data Pribadi," Jurnal RechtVinding, 9.2 (2020), 237–56.

Hardianto Djanggih, 2013, "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime". Jurnal Media Hukum Vol 1 dan 2

IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", Info Komputer, (9 Maret 2024), 71.

Machyudin Agung Harahap dan Susri Adeni, *Tren Pengguna Media Sosial Selama Pandemi Di Indonesia*, Jurnal Professional FIS UNIVED Program Studi Ilmu Komonikasi Fakultas Ilmu Politik dan Sosial Unoversitas Bengkulu. Vol. 7 No. 2 Desember 2020, Hlm 18

Musa Darwin Pane, Sahat Maruli Tua Situmeang, "Penegakan Hukum Cyber Crime dalam Upaya Penanggulangan Tindak Pidana

Teknologi Informasi" Jurnal Loyalitas Sosial, Vol. 3, No.2, 2021, hlm. 95
Nurmalasari, "Urgensi Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi Demi Mewujudkan Kepastian Hukum",Jurnal Syntax Idea, Vol. 3 (Agustus,2021), hal. 1959
Penjelasan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Paragraf 2.
Sahuri Lasmadi, "Pengaturan Alat Bukti Dalam Tindak Pidana Dunia Maya," Jurnal Ilmu Hukum, 2014, hlm. 3.
Titik Suharti, "Proses Penegakan Hukum di Indonesia dalam Perspektif Hukum Pidana", Norma, Vol no. 1, 2004, hlm. 43.
Vivi Ariyanti, "Kebijakan Penegakan Hukum dalam Sistem Peradilan Pidana Indonesia", Jurnal Yuridis, Vol. 6 No.2, 2019, hlm. 35.

PERATURAN PERUNDANG-UNDANGAN

Undang undang nomor 11 tahun 2008
UU No. 11 Tahun 2008 jo UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
UU No. 1 Tahun 2024 tentang Informasi dan transaksi elektronik UU No. 39 Tahun 1999 tentang Hak Asasi Manusia,
UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik
UU No. 23 Tahun 2006 tentang mengenai hak dan kewajiban penduduk KUHPidana
UU tentang Perlindungan Data Pribadi Nomor 27 Tahun 2022 Pasal 1 ayat 1 KUHPidana No. 8 UU ITE Pasal 35
"Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

INTERNET

Ade suhendra, Diduga Kena Phising Nasabah BRI di Padang Kehilangan Uang Rp1,114 Miliar, diakses dari https://www.harianhaluan.com/news/pr-103582510/diduga-kena-phising-nasabah-bri-di-padang-kehilangan- uang-rp1114-miliar
Anti Phising Working Group, Phising activity trends report, https://apwg.org/trendsreports/,
Anti Phising Working Group, Phising activity trends report, https://apwg.org/trendsreports/
Erizka Permatasari, Jeat Hukum Pelaku Phishing dan Modusnya, diakses dari https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnyn-c15050,
Fino Yurio Kristo, 2009, Facebook Jadi Lahan Subur Pencurian Identitas (online), http://www.detikinet.com/read/2009/10/12/161616/1220092/398/facebo ok-jadi-lahan-suburpencurian-identitas,
Ivia Kristiani, 5.579 laporan "phising" di kuartal kedua, kata PANDI, diakses dari https://jabar.antaranews.com/berita/397305/5579-laporan-phising-di- kuartal-kedua-kata- pandi?page=all,
Pengertian Internet dan Fungsinya, https://bsi.today/pengertian-internet/,
Ronal, Tinjauan Yuridis Terhadap Cyber Crime. diakses dari https://media.neliti.com/media/publications/149003-11-none.pdf,
https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024
Setiyardi, 'Kreasi Pelesetan Pemicu Delik' (Tempo, 2017) , https://majalah.tempo.co/read/ilmu-danteknologi/80886/kreasi- pelesetan-pemicu-delik/ diakses pada 15 Maret 2024
Anggi Tondi Martano, "Pengesahan UU PDP Era Baru Tata Kelola Data Pribadi", https://mediaindonesia.com/politik-dan-hukum/523832/pengesahan-uu- pdp-era-baru-tata-kelola-data-pribadi
JDIH Kemenko Bidang Kemaritiman dan Investasi, "UU No.27/2022: Perlindungan Data Pribadi," JDIH Kemenko Bidang Kemaritiman dan Investasi, 2022, https://jdih.maritim.go.id/uu-no-272022-pelindungandata-pribadi.
Erizka Permatasari. "Jerat Hukum Pelaku Phishing Dan Modusnya" (2021) (https://new.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum- pelaku-iphising-i-dan-modusnya) diakses 15 Mei 2024
https://internetworldstats.com/asia.htm
Prudential, "Apa itu Phising? Pengertian, Ciri-Ciri, dan Cara Menghindarinya" https://www.prudential.co.id/id/pulse/article/apa-itu-phising/#:~:text=Phising%20merupakan%20metode%20penipuan%20yang%20digunakan%20oleh%20penjahat,sandi%2C%20nomor%20kartu%20kredit%2C%20atau%20detail%20akun%20bank, diakses pada tanggal 18 Januari