Riau Law Journal
Fakultas Hukum Universitas Riau, Jalan Pattimura Nomor 9 Gobah, Kel. Cinta Raja, Kec. Sail, Pekanbaru, Riau, Kode Pos 28127. Telp: (+62761)-22539, Fax : (+62761)-21695
E-mail: riaulawjournal@gmail.com / riaulawjournal@unri.ac.id
Website: https://rlj.ejournal.unri.ac.id

Urgensi Penegakan Hukum Terhadap Perbuatan Phising Sebagai Upaya Pencegahan Kejahatan Siber

Nanang Tomi Sitorus[a], Wahida Ariyanti Nasution[b], Gita Sari Efelin[c]

[a] Fakultas Hukum, Universitas Medan Area, Indonesia, Email: nanang@staff.uma.ac.id
[b] Fakultas Hukum, Universitas Medan Area, Indonesia, Email: wahidaariyantinasution2@gmail.com
[c] Fakultas Hukum, Universitas Medan Area, Indonesia, Email: celinesarisari730@gmail.com

Article Info

Article History:
Received : 28-03-2024
Revised : 20-05-2024
Accepted : 27-05-2024
Published : 31-05-2024

Keywords:
Urgency of Law Enforcement,
Phishing Acts,
Cyber Crime,

Abstract

Phishing crimes have recently been rampant and targeting smartphone users young and old, thus reminding the entire community to be careful. Phishing crimes that occur include invitations in the form of Application Package Files (APK) which cause many victims to lose money in accounts. The increase in these crimes requires countermeasures and actions so that phishing crimes can be reduced and the government must make policies so that smartphone users have knowledge and understanding related to this matter. The Anti Phishing Working Group noted that there are already 165,772 phishing websites that are ready to attract victims. In addition, the rule of law needs to be strengthened in order to anticipate and protect people's personal data from phishing crimes.

Informasi Artikel

Histori Artikel:
Diterima : 28-03-2024
Direvisi : 20-05-2024
Disetujui : 27-05-2024
Diterbitkan : 31-05-2024

Kata Kunci:
Urgensi Penegakan Hukum
Perbuatan Phising
Kejahatan Siber

Abstrak

Kejahatan phishing akhir-akhir ini marak terjadi dan mengincar para pengguna smartphone baik tua maupun muda, sehingga mengingatkan seluruh masyarakat untuk berhati-hati. Kejahatan phising yang terjadi antara lain berupa ajakan dalam bentuk Application Package File (APK) yang menyebabkan banyak korban kehilangan uang di rekening. Meningkatnya kejahatan tersebut memerlukan penanggulangan dan tindakan agar kejahatan phising dapat berkurang dan pemerintah harus membuat kebijakan agar pengguna smartphone memiliki pengetahuan dan pemahaman terkait hal tersebut. Anti-phishing Working Group mencatat sudah ada 165.772 website phishing yang siap menjaring korban. Selain itu, aturan hukum perlu diperkuat untuk mengantisipasi dan melindungi data pribadi masyarakat dari kejahatan phishing.

PENDAHULUAN

Kejahatan bukanlah konsep baru dalam sejarah peradaban manusia. Sejak manusia diciptakan yang dimulai dengan tindakan pembangkangan iblis terhadap perintah Allah untuk memberi penghornatan terhadap makhluk ciptaan Allah lainnya yang disebut manusia. Pembangkangan ini kemudian dengan janji iblis untuk selalu menggoda manusia hingga akhir zaman. Konflik interest antara manusia dan iblis ini dapat dipandang sebagai embrio kejahat-

an yang kejahatan itu bermula dari perasaan iri, sombong, dan dengki.[1] Pada Perkembangannya, modus operandi kejahatan bergerak maju seiring perkembangan peradaban manusia. Kejahatan dan eksistensi masyarakat menjadi dua sisi mata uang yang saling terkait, sehingga Lacassagne mengatakan bahwa masyarakat mempunyai penjahat sesuai dengan jasanya.[2]

Meningkatnya kejahatan siber, pemerintah melalui penegak hukum berupaya untuk melakukan penegakan hukum. Penegakan hukum merupakan suatu proses, pada hakikatnya merupakan penerapan diskresi yang menyangkut membuat keputusan yang tidak secara ketat diatur oleh kaidah hukum, akan tetapi mempunyai unsur penilaian pribadi. Secara konsepsional, inti dari penegakkan hukum terletak pada kegiatan meyerasikan hubungan nilai-nilai terjabarkan didalam kaidah-kaidah yang mantap dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.[3] Penegakan hukum adalah suatu usaha untuk menanggulangi kejahatan, memenuhi rasa keadilan dan berdaya guna untuk menanggulangi kejahatan terhadap berbagai sarana dan sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa hukum pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya.[4] Menurut Jimly Penegakan hukum merupakan proses dilakukannya upaya untuk tegaknya atau berfungsinya norma-norma hukum secara nyata sebagai pedoman perilaku dalam lalu lintas atau hubungan-hubungan hukum dalam kehidupan bermasyarakat dan bernegara.[5]

Menurut Joseph Goldstein penegakan hukum pidana dapat dibedakan menjadi tiga bagian. Pertama, total *enforcemen*t yaitu dimana ruang lingkup penegakan hukum pidana sebagaimana yang dirumuskan oleh hukum pidana substantif *(substantive law of crimes).* Hukum pidana substantif atau materiil dapat dirumuskan sebagai hukum mengenai delik yang diancam dengan hukum pidana. Ruang lingkup penegakan hukum yang bersifat total tersebut dikurangi area *of no enforcement* selanjutnya muncullah suatu bentuk penegakan hukum pidana yang kedua yaitu *Full Enforcement. Full enforcement* adalah penegakan hukum yang dilakukan secara maksimal oleh

[1] Maskun, *Kejahatan Cyber (Cyber Crime) Suatu Pengantar*, (Jakarta: Kencana Prenada Media Group, 2012), 43.
[2] Agus Raharjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya, 2022), 29-30.
[3] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakkan Hukum*, (Depok: Raja Grafindo Persada, 2019), 5.
[4] Barda Nawawi Arief, *Kebijakan Hukum Pidana*, (Bandung: PT. Citra Aditya Bakti, 2002), 109.
[5] Jimly Asshiddiqie, *Majalah Hukum Nasional, disampaikan pada Badan Pembinaan Hukum Nasional Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia* 48, no. 2 (2018).

aparat penegak hukum. Ketiga, penegakan hukum yang tersisa dan belum dilakukan dalam dua tahap diatas yang disebut *actual enforcement.*

Pertengahan Maret lalu dunia lelang nasional direpotkan oleh sebuah situs bernama lelanginternal.com yang memiliki tampilan dan konten yang sangat mirip dengan situs lelang.go.id bahkan lengkap dengan logo Kementerian Keuangan dan *page title* Direktorat Jenderal Kekayaan Negara 1. Lelang.go.id adalah sebuah situs resmi milik Direktorat Jenderal Keayaan Negara (DJKN). DJKN selaku regulator pelaksanaan lelang di Indonesia sangat menyayangkan dengan masih adanya pihak-pihak yang tidak bertanggung jawab, memanfaatkan nama Kementerian Keuangan cq. DJKN guna mengeruk keuntungan pribadi dengan menipu masyarakat melalui media online. Di dunia online cara-cara penipuan seperti ini dikenal dengan istilah *Phising.*

Selain itu modus kejahatan *phising* melalui *smartphone* yang berekstensi Android Package Kit (APK) juga banyak terjadi diantaranya Penipuan Undangan Pernikahan Online, Penipuan Resi dari Ekspedisi, Penipuan Tagihan PLN, Penipuan Surat Tilang Online, Penipuan Tagihan BPJS, Penipuan dengan Voice Note, Penipuan Catut Nama Direktorat Jenderal Pajak (DJP), dan Penipuan Pendaftaran BI-Fast.[6] Kejahatan tersebut menimbulkan korban yang dialami oleh Silvia Tap asal Lawang, Kabupaten Malang Jawa Timur dengan kerugian uang tabungan sejumlah 1,4 milyar setelah menerima dan menekan undangan pernikahan yang dikirimkan melalui whatsapp.[7]

Phising adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (*username* dan *password*), dan data finansial (informasi kartu kredit, rekening). Istilah resmi *phising* adalah *phising*, yang berasal dari bahasa Inggris fishing yaitu memancing. Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan

[6] Agustinus Rangga Respati dan Aprillia Ika, "Waspada, Ini 8 Modus Penipuan File APK yang Pernah Terjadi di Indonesia", 7 Juli 2023, https://money.kompas.com/read/2023/07/07/075807426/waspada-ini-8-modus-penipuan-file-apk-yang-pernah-terjadi-di-indonesia?page=all.

[7] Agustinus Rangga Respati dan Aprillia Ika, "Penipuan File APK Buat Korban Rugi Rp/ 1,4 Miliar, Simak Ciri-Ciri dan Cara Menghindarinya", 6 Juli 2023, https://money.kompas.com/read/2023/07/06/162921826/penipuan-file-apk-buat-korban-rugi-rp-14-miliar-simak-ciri-ciri-dan-cara.

kejahatan.[8] Phising adalah salah satu jenis kejahatan online yang saat ini harus benar-benar Anda waspadai. Serangan ini masih kerap terjadi dan terus menjadi ancaman bagi siapa saja tanpa pandang bulu. Kalau Anda jadi korbannya, akibatnya pun tak main-main, bahkan bisa berujung pada penipuan atau pencurian data.

Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan kejahatan. Informasi data *phising* yang diperoleh bisa langsung dimanfaatkan untuk menipu korban. Atau, bisa juga dijual ke pihak lain untuk melakukan tindakan tidak bertanggung jawab seperti penyalahgunaan akun. Aksi *cyber* crime ini memang berbahaya. Menurut sebuah laporan**,** 32% pencurian data selalu melibatkan kegiatan phising**.** Bahkan, di awal tahun 2020 saja, Anti *Phishing Working Group* mencatat sudah ada 165.772 website phising yang siap menjaring korban. Dan, sektor finansial masih menjadi sasaran utamanya.

Saat ini sedang marak-maraknya kasus penipuan berkedok paket, undangan, atau tagihan melalui pesan ke gadget melalui sebuah link. Hati-hati dan waspada dengan phising untuk tidak klik tautan tersebut agar melindungi data pribadi kalian. Dikutip dari situs resmi Direktorat Jenderal Kekayaan Negara Kementerian Keuangan (Kemenkeu), istilah *phising* adalah phishing, yang berasal dari bahasa Inggris fishing yaitu memancing. *Phising* adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (*username* dan *password*), dan data finansial (informasi kartu kredit, rekening).

PERLINDUNGAN HUKUM TERHADAP KORBAN *PHISING*

Secara terminologis, perlindungan hukum dapat dijelaskan dari himpunan dua pengertian, yaitu "perlindungan" serta "hukum". KBBI mendefinisikan perlindungan sebagai objek atau tindakan perlindungan. Hukum kemudian dapat dipahami sebagai peraturan atau kebiasaan yang mengikat secara resmi, disahkan oleh otoritas atau pemerintah yang berwenang. Menurut pengertian ini, perlindungan hukum dipahami sebagai usaha untuk memberikan perlindungan

[8] Irfan Fanasafa, "Waspada! Kejahatan Phising Mengintai Anda", 25 Maret 2022, https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html.

berdasarkan aturan yang telah disahkan pihak yang berkuasa atas itu. Secara singkat, melindungi hukum merupakan fungsi dari hukum. Salah satu bentuk kejahatan siber ialah *phising*. Kejahatan ini dilakukan dengan menarik perhatian korban tanpa mengenal batas waktu yang membuat korban lebih mudah terjaring. Hal ini menyebabkan jumlah korban kejahatan phising meningkat. Atas dasar inilah perlindungan hukum diperlukan untuk menjamin kehidupan masyarakat. Tugas ini menjadi bentuk tanggung jawab negara sebagai negara hukum.[9]

Orang sering tidak menyadari bahaya serius yang ditimbulkan terhadap korban kejahatan ini. *Cyber Crime Phising* adalah penipuan yang melibatkan orang lain dengan memanfaatkan email atau situs web palsu untuk mendapatkan informasi pribadi seseorang, seperti User ID, PIN, nomor rekening, nomor kartu kredit, dan sebagainya. Data pengguna sering digunakan untuk mengirimkan email yang tampaknya dilakukan oleh pihak resmi, seperti bank. Menurut studi Pusopskamsinas, email *phising* digunakan dalam sejumlah besar kasus peretasan.[10] Waktu tahun 2020, Pusopskamsinas menemukan sekitar 2.549 email phising (CNBC Indonesia). Teknik rekayasa sosial yang sering digunakan peretas untuk mengelabui korban adalah email phishing. Peretas mengirimi email yang mengundang, biasanya dengan menngunakan sebuah tema keuangan atau pemasaran (hadiah, kupon, diskon, dll.).

Mengetahui cara kerja phishing membuatnya lebih mudah untuk dihindari. Langkah-langkah atau metode *phising* adalah sebagai berikut:

1. Peretas entah bagaimana menipu kita untuk mengklik tautan di situs web palsu, itu bisa berupa gambar yang menarik di jejaring sosial, umpan di *email*, dll.
2. Setelah diklik, tautan tersebut mengarah ke situs web palsu, yang di dalamnya terdapat formulir seperti formulir login Facebook dengan kata-kata pastikan bahwa *Facebook* kita telah keluar dan meminta kita untuk memasukkan kembali nama dan nama pengguna kita. kata sandi. kita yang tidak menganggap situs tersebut hanya palsu akan langsung mengisi username dan password tanpa curiga.

[9] Hukum Online," Pengertian Perlindungan Hukum dan Cara Memperolehnya." Pengertian Perlindungan Hukum dan Cara Memperolehnya", 2022, hukumonline.com.
[10] Khanifah Jannatul Diniyah, "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phising", *Dinamika Jurnal Ilmiah Ilmu Hukum* 28, no. 5 (2022): 3756 -3775.

3. Informasi yang kita masukkan di form akan disimpan di server hacker. Sehingga kita masih memiliki cukup waktu untuk mengganti password yang kita miliki sebelum *hacker* itu melihat *username* & *password* kita di server.
4. Akun kita telah diambil alih. Peretas sepertinya akan menggunakan akun yang kita miliki untuk menyebarkan URL phishing ke teman temen kita, agar mereka bisa menarik lebih banyak korban korban yang terkena phising. Meretas kata sandi menggunakan metode phishing adalah yang paling mudah untuk dipraktikkan. Makanya banyak sekali di dunia maya sehingga bertebaran alamat referral yang mengarahkan browser kita ke alamat email phising atau alamat email palsu.[11]

Kasus *phising* sendiri telah pernah diadili. Salah satunya ialah kasus dalam Putusan PN Pekanbaru No: 958/Pid.Sus/2020/PNPbr. Diketahui bahwa kejahatan ini dilakukan dengan meniru website resmi dan kemudian disebarkan ke alamat e-mail korban. Korban yang mengklik tautan yang dikirimkan ke e-mail maka datanya akan dicuri, seperti id pengguna, kata sandi, hingga alamat dan identitas lainnya. Kejahatan phising ini menargetkan untuk mendapatkan data kartu kredit korban. Setelah memperoleh data tersebut, pelaku menjualnya melalui akun media sosial Facebook. Perbuatannya ini didakwa atas Pasal 32 (2) serta 48 (2) UU ITE. Kejahatannya diancam kurungan 1 tahun 2 bulan serta denda Rp. 20.000.000.[12]

Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) penting dalam menanggulangi phising di Indonesia. UU ini memberikan perlindungan bagi informasi pribadi seseorang serta memberikan sanksi tegas bagi pelaku kejahatan siber, termasuk pelaku phising dan Kemudian, saksi serta korban yang dalam kejahatan ini juga memperoleh perlindungan. Tata cara perlindungannya diatur dalam UU No 31 tahun 2014. UU mengenai perlindungan saksi dan korban ini dijelaskan di pasal (4). Di dalamnya dijelaskan bahwa perlindungan ini dilakukan agar saksi dan korban mampu memberikan keterangan yang dibutuhkan pada proses penegakan hukum.

Perlindungan hukum diberikan untuk saksi dan korban atas kriteria yang telah ditetapkan dalam Pasal 28 UUPSK, yaitu:

[11] Perpus Unusa, "Bahaya Phising Serta Cara Menghindarinya", 29 Januari 2020, https://library.unusa.ac.id/bahaya-phising-serta-cara-menghindarinya/.
[12] Erizka Permatasari, "Jerat Hukum Pelaku Phishing dan Modusnya", 2021, hukumonline.com.

1. Sifat pentingnya keterangan saksi dan/atau korban;
2. Tingkat ancaman yang membahayakan saksi dan/korban;
3. Hasil analisis tin medis atau psikologi terhadap saksi dan/atau korban; dan
4. Rekam jejak kejahatan yang pernah dilakukan oleh saksi dan/atau korban.[13]

Korban *phising* pada dasarnya membutuhkan kompensasi untuk kerugian atas penipuan yang dialaminya. Keberadaan UUPSK memberikan perlindungan kepada saksi maupun korban kejahatan. Bentuk perlindungannya dapat berupa kompensasi, restitusi, serta bantuan. Pengaturan perlindungan ini dinyatakan dalam aturan berikut ini:

1. Pasal 28 D (1) UU 1945 menegaskan "Setiap orang berhak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum."[14]
2. Pasal 40 (2) UU ITE berbunyi "Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan."
3. Pasal 1 (8) UU No 31 Tahun 2014 yang merupakan perubahan atas UU No 13 Tahun 2006 mengenai Perlindungan Saksi dan Korban, menjelaskan "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."[15]

Namun, dari Pasal 45 hingga 52 UU ITE menetapkan bahwa pelaku kejahatan yang melakukan kejahatan yang dilarang berdasarkan UU ini akan dipidana karena melakukan perbuatan yang dilarang dalam UU, yang berarti bahwa mereka akan dikenakan pidana penjara atau denda sebagai bentuk penyelesaian perkara untuk melindungi hak para korban dalam transaksi elektronik/cybercrime. Restitusi adalah pendekatan yang tepat untuk mengurangi kerugian finansial bagi korban phising. Menurut Pasal 1 (11), "Restitusi adalah ganti kerugian

[13] Afiano Pangalilla, "Perlindungan Korban Dalam Proses Penyelesaian Perkara Pidana Berdasarkan Undang-Undang Nomor Tahun 2014", *E Journal Fakultas Hukum Unsrat* 7, no. 8 (2018).
[14] Ardi Saputro Gulo; Lasmadi, Sahuri; Nawawi, Kabib, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik", *PAMPAS: Journal of Criminal* 1, no. 2 (2020).
[15] Cornelis Massie; Rorie, Ronald; Malunsenge, Leticia, "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia", *Lex Crimen* 11, no. 3 (2022).

yang diberikan kepada Korban atau Keluarganya oleh pelaku atau pihak ketiga." Dalam mendapatkan perlindungan melalui LPSK, korban kejahatan harus melewati tahap pengajuan dan mematuhi persyaratan dalam Pasal 21 PP No. 7 Tahun 2018.

PENEGAKAN HUKUM TERHADAP TINDAK PIDANA *PHISING*

Perkembangan teknologi dan perubahan masyarakat telah menyebabkan perubahan gaya hidup masyarakat, sehingga hukum harus mengikutinya. Oleh karena itu juga disyariatkan dalam perkara pidana, khususnya untuk tindak pidana yang kemudian disertai dengan ancaman pidana. Penerapan sanksi dilakukan sesuai dengan ketentuan sanksi yang berlaku sesuai dengan peraturan perundang-undangan yang berlaku. hukuman dimaksudkan untuk menimbulkan penderitaan dan membuat jera pelaku kejahatan, hukuman juga dapat berfungsi sebagai peringatan kepada masyarakat untuk tidak melakukan kejahatan serupa dan untuk tetap waspada dan berhati-hati setiap saat.[16] Soerjono Soekanto menjelaskan penegakan hukum ialah penyelarasan dari isi yang tertuang di aturan perundang-undangan dengan perilaku guna tercipta dan terpeliharanya kehidupan yang aman, damai, serta tertib dalam masyarakat.

Para pelaku kejahatan phising dijatuhkan hukuman sebagaimana pelaku kejahatan lainnya, yakni dengan membatasi kebebasan bergeraknya untuk kemudian dimasukkan ke dalam Lembaga Pemasyarakatan. Para pelaku yang diberi hukuman ini wajib taat pada aturan tata tertib yang ada di dalam penjara dan akan diberikan penertiban apabila melanggarnya.

Meskipun tidak ada undang-undang atau peraturan yang secara khusus mengatur tentang phishing. Namun, pelaku dapat dijerat dengan ketentuan Kitab Undang-Undang Hukum Pidana ("KUHP") dan UU ITE beserta perubahannya, seperti contoh kasus di atas. Penegakan Hukum Terhadap Tindak pidana phising kejahatan dunia maya dapat ditemukan di pasal 378 kuhp. Tindak pidana phishing termasuk dalam tindak pidana penipuan menurut pasal 378 kuhp yang berbunyi: "Barangsiapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau kedaan palsu, baik dengan akal dan tipu muslihat, maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya

[16] Lilis Ekayani dan Djanggih, Hardianto, "Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan", *Jurnal of Lex Philosophy* 4, no. 1 (2023).

memberikan sesuatu barang, membuat utang atau menghapus piutang, dihukum karena penipuan, dengan hukuman penjara selama-lamanya empat tahun."

Selain itu juga ada beberapa pasal-pasal yang telah dijelaskan di atas, pelaku phishing juga bisa dijerat Pasal 40 UU No. 36 tahun 1999 tentang telekomunikasi dengan bunyi: "Bahwa setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun".[17] Pelaku phising yang mengirim e-mail palsu dikenai Pasal 35 jo. Pasal 51 UU ITE, yang isinya berbunyi: "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 dipidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar."

Tindak kejahatan berupa menyebarkan informasi ataupun dokumen elektronik korban maka pelaku dikenai Pasal 32 (2) jo. Pasal 48 (2) UU ITE, yaitu: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak dipidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp3 miliar." Terhadap tindakan kejahatan berupa memasuki sistem elektronik tertentu menggunakan identitas yang dicuri maka akan dikenai Pasal 30 (3) jo. Pasal 46 (3) UU ITE, yakni: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp800 juta."[18]

Berdasarkan unsur phishing dan putusan pengadilan, pengaturan tentang kejahatan dunia maya berupa phishing tercantum dalam Undang-Undang Nomor 1 Republik Indonesia. 11/2008 tentang perubahan atas UU No. 19/2016 tentang informasi dan transaksi elektronik dalam beberapa pasal yang dapat diatur, antara lain:

1. Pasal 28 (1) berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam hal Elektronik." sudah Sebagai ketentuan pidana Pasal 45 ayat 2 disebutkan: "Barang siapa

[17] Undang Undang Nomor 36 tahun 1999 tentang Telekomunikasi.
[18] Diniyah, *Loc.Cit.*

memenuhi keadaan sebagaimana dimaksud dalam Pasal 28, ayat 1 atau ayat 2, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak 1.000.000.000,00 (satu miliar rupiah)".

2. Pasal 35 berbunyi: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengolah, membuat, mengubah, menghapus, memusnahkan data elektronik dan/atau dokumen elektronik dengan maksud agar data elektronik dan/atau dokumen elektronik dianggap asli." sudah Pasal 51 sebagai ketentuan pidana, dimana "Setiap orang yang memenuhi ciri-ciri yang ditentukan dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas milyaran rupiah).[19]

Dari ketentuan tersebut jelas bahwa jenis pemidanaan adalah yang utama, karena dalam KUHP diterapkan pidana penjara dan denda menurut sistem geng maksimum. Pemidanaan yang terjadi dapat berupa pidana penjara maupun pemidanaan denda, yang memiliki arti dan makna yang berbeda untuk pelaku. Kedua pemidanaan tersebut juga agar memberikan efek jera bagi pelaku kejahatan.

KESIMPULAN

Phising merupakan upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran *phising* adalah data pribadi (nama, usia, alamat), data akun (*username* dan *password*), dan data finansial (informasi kartu kredit, rekening). Untuk itu perlu perlindungan dan penegakan hukum yang ekpresif hingga kejahatan *phising* ini dapat diminimilisir agar tidak berdampak luas di Indonesia khususnya bagi pengguna *smarphone.* Tujuan dilakukannya penelitian ini untuk meminimalisir angka kejahatan *phising* dan khusus bagi pengguna *smartphone* untuk mewaspadai modus operandi yang dilakukan oleh oknum baik yang dikirimkan melalui link atau cara lainnya.

[19] Massie, *Loc.Cit.*

DAFTAR PUSTAKA

Agus, Raharjo. *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya, 2022.

Asshiddiqie, Jimly. "Majalah Hukum Nasional". *disampaikan pada Badan Pembinaan Hukum Nasional Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia*. 2018.

Barda, Nawawi Arief. *Kebijakan Hukum Pidana*. Bandung: PT. Citra Aditya Bakti, 2002.

Diniyah, Khanifah Jannatul. "Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phising". *Dinamika Jurnal Ilmiah Ilmu Hukum* 28, no. 5 (2022): 3756 -3775.

Ekayani, Lilis dan Djanggih, Hardianto. "Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan". *Jurnal of Lex Philosophy* 4, no. 1 (2023).

Fanasafa, Irfan. "Waspada! Kejahatan Phising Mengintai Anda". 25 Maret 2022. https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html.

Hukum Online. "Pengertian Perlindungan Hukum dan Cara Memperolehnya". 2022. hukumonline.com.

Maskun. *Kejahatan Cyber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana Prenada Media Group, 2012.

Massie, Cornelis; Rorie, Ronald; Malunsenge, Leticia. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia". *Lex Crimen* 11, no. 3 (2022).

Pangalilla, Afiano. "Perlindungan Korban Dalam Proses Penyelesaian Perkara Pidana Berdasarkan Undang-Undang Nomor Tahun 2014". *E Journal Fakultas Hukum Unsrat* 7, no. 8 (2018).

Permatasari, Erizka. "Jerat Hukum Pelaku Phishing dan Modusnya". 2021. hukumonline.com.

Perpus Unusa. "Bahaya Phising Serta Cara Menghindarinya". 29 Januari 2020. https://library.unusa.ac.id/bahaya-phising-serta-cara-menghindarinya/.

Rangga Respati, Agustinus dan Aprillia Ika. "Penipuan File APK Buat Korban Rugi Rp/ 1,4 Miliar, Simak Ciri-Ciri dan Cara Menghindarinya". 6 Juli 2023.

https://money.kompas.com/read/2023/07/06/162921826/penipuan-file-apk-buat-korban-rugi-rp-14-miliar-simak-ciri-ciri-dan-cara.

Rangga Respati, Agustinus dan Aprillia Ika. “Waspada, Ini 8 Modus Penipuan File APK yang Pernah Terjadi di Indonesia”. 7 Juli 2023. https://money.kompas.com/read/2023/07/07/075807426/waspada-ini-8-modus-penipuan-file-apk-yang-pernah-terjadi-di-indonesia?page=all.

Saputro Gulo, Ardi; Lasmadi, Sahuri; Nawawi, Kabib. “Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik”. *PAMPAS: Journal of Criminal* 1, no. 2 (2020).

Soerjono, Soekanto. *Faktor-Faktor yang Mempengaruhi Penegakkan Hukum*. Depok: Raja Grafindo Persada, 2019.

Sutarli, Fadli; Ananta dan Kurniawan, Shelly. “Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadidalam Menanggulangi Phising di Indonesia”. 3 no. 2 (2023).

Undang Undang Nomor 36 tahun 1999 tentang Telekomunikasi.