UNES LAW REVIEW
+62 813 6511 8590
+62 813 6511 8590
https://review-unes.com/
uneslawreview@gmail.com

DOI: https://doi.org/10.31933/unesrev.v5i4
Diterima: 27/07/2023, Diperbaiki: 22/08/2023, Diterbitkan: 23/08/2023

ANALISIS YURIDIS PENANGGULANGAN PENYALAHGUNAAN DATA PRIBADI DALAM BENTUK *PHISING* YANG DILAKUKAN OLEH *PAID VERIFIED ACCOUNT* DI MEDIA SOSIAL MENURUT UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI

Dewana Saputra[1], Zaid Alfauza Marpaung [2]

1)Universitas Islam Negeri Sumatera Utara, Sumatera Utara, Indonesia.
Email: dewanasaputra17@gmail.com

2)Universitas Islam Negeri Sumatera Utara, Sumatera Utara, Indonesia.
Email: zaidalfauzamarpaung@uinsu.ac.id

***Corresponding Author*: Dewana Saputra**

ABSTRACT

This research discusses the handling of personal data abuse in the form of phishing carried out by paid verified accounts on social media according to Law Number 27 of 2022 concerning Personal Data Protection. The problem raised in this study is the rampant phishing crime against personal data abuse on social media. The research method used in this study is juridical-normative with sources of legal materials, namely: Laws, previous legal research results, opinions of legal experts, works from legal experts and other sources of information that are useful for this study. The results of this study reveal that the Personal Data Abuse Law in tackling phishing crime against personal data abuse, by strengthening personal data protection through several efforts, such as imposing sanctions, establishing a special authority agency, encouraging the government to strengthen cyber security and increasing digital literacy for the community as a form of participation. with the aim of minimizing the possibility of personal data abuse, such as phishing on social media by paid verified accounts. The handling of personal data abuse through the Personal Data Protection Law is good if it is fully implemented, but it would be even better if various modus operandi of personal data abuse could be explicitly or clearly written in it, so that there are no gaps for violators to escape from the articles of the Personal Data Protection Law. Then regarding the Personal Data Protection Authority Agency must stand independently and independently, so that there is no conflict of interest that can injure and disrupt the enforcement of personal data protection in Indonesia.

Keywords: *Phising, Social Media, Paid Verified Account, Personal Data, Protection, Misues*

ABSTRAK

Penelitian ini membahas tentang penanggulangan penyalahgunaan data pribadi dalam bentuk *phising* yang dilakukan oleh *paid verified account* di media sosial menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Permasalahan yang diangkat pada penelitian ini adalah maraknya kejahatan *phising* terhadap penyalahgunaan data pribadi di media sosial. Metode penelitian yang dipergunakan pada penelitian ini adalah yuridis-normatif dengan sumber bahan hukum, yaitu: Undang-Undang, hasil penelitian hukum terdahulu, pendapat ahli hukum, hasil karya dari kalangan ahli hukum dan sumber informasi lainnya yang berguna bagi penelitian ini. Hasil penelitian ini mengungkapkan bahwa Undang-Undang Penyalahgunaan Data Pribadi dalam menanggulangi kejahatan *phising* terhadap penyalahgunaan data pribadi, dengan cara memperkuat perlindungan data pribadi melalui beberapa upaya, seperti pemberian sanksi, pembentukan lembaga otoritas khusus, mendorong pemerintah untuk memperkuat keamanan siber dan meningkatkan literasi digital masyarakat sebagai bentuk partisipasi masyarakat, dengan maksud untuk meminimalisir kemungkinan terjadinya tindak penyalahgunaan data pribadi, seperti *phising* di media sosial oleh *paid verified account*. Penanggulang penyalahgunaan data pribadi melalui Undang-Undang Perlindungan Data Pribadi sudah baik jika diimplementasikan seluruhnya, namun akan lebih baik lagi jika berbagai modus operandi penyalahgunaan data pribadi dapat tertulis secara eksplisit atau jelas di dalamnya, agar tidak adanya celah bagi para pelanggar untuk lolos dari jeratan pasal-pasal Undang-Undang Perlindungan Data Pribadi. Lalu perihal Lembaga Otoritas Perlindungan Data Pribadi haruslah berdiri secara mandiri dan independen, agar tidak terjadi sebuah konflik kepentingan yang dapat mencederai dan mengganggu penegakan perlindungan data pribadi di Indonesia.

Kata Kunci: *Phising*, Media Sosial, Akun Terverifikasi Berbayar, Data Pribadi, Perlindungan, Penyalahgunaan

PENDAHULUAN

Perkembang teknologi yang terjadi di dunia dari masa ke masa semakin mengalami peningkatan yang pesat, khususnya di bidang teknologi informasi dan telekomunikasi. Dengan perkembangan teknologi informasi dan telekomunikasi yang begitu pesat, maka tentunya hal ini didukung pula dengan akses internet yang semakin luas dan semakin terjangkau pula biaya aksesnya. Dengan semakin luas dan murahnya akses internet yang didapatkan, maka manusia semakin banyak yang menggunakannya dan membuat manusia memiliki ketergantungan terhadap teknologi-teknologi yang ada. Fenomena tersebut tentunya dapat merubah kebiasaan dan kehidupan manusia di berbagai belahan dunia. Contoh yang paling dapat disaksikan secara kasat mata adalah ketergantungan manusia terhadap penggunaan *gadget*, salah satunya adalah *smartphone*.[1] Tentunya penggunaan *smartphone* atau ponsel pintar dapat mempermudah kehidupan manusia, karena di dalam perangkat smartphone tersebut terdapat aplikasi yang tak terhingga jumlahnya, mulai dari aplikasi media sosial, pemutar *multimedia*, peramban bahkan juga *video game*. Penggunaan smartphone tersebut telah merubah kebiasaan hidup manusia, salah

[1] Thiara Dewi dan Abdurrakhman Alhakim, Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi di Indonesia, Journal Komunitas Yustisia Universitas Pendidikan Ganesha, Vol. 4 No. 3, (2021), hal. 1057

satunya ada pada penggunaan media sosial yang telah mengubah aktivitas dan kebiasaan hidup manusia.

Media sosial atau *social media* adalah suatu wadah atau media yang diakses oleh para penggunanya secara daring yang mendukung berbagai jenis kegiatan interaksi sosial. Interaksi para pengguna media sosial dengan cara mengisi, berbagi dan berpartisipasi dalam jejaring media sosial dan dunia virtual.[2] Di Indonesia sendiri tercatat pada Januari 2023, setidaknya terdapat 167 juta pengguna media sosial. Dengan demikian dari total penduduk Indonesia yang berjumlah sekitar 276,4 juta jiwa, maka pengguna media sosial memiliki presentase 60,4 persen dari total populasi penduduk Indonesia.[3] Dengan begitu besarnya persentase pengguna media sosial di Indonesia dari total populasi penduduk, maka dengan demikian membuktikan bahwasannya mayoritas penduduk Indonesia sudah menggunakan media sosial dan penduduk Indonesia sudah hidup di dalam dunia maya dalam kesehariannya. Hal ini juga berarti sudah banyak data-data pribadi dari para pengguna media sosial Indonesia yang sudah terdaftar dan berada di dalam *database* atau *cloud storage* dari pihak pengelola dan penyedia layanan media sosial, karena untuk dapat menggunakan media sosial tentu harus diikuti dengan memasukkan data-data identitas sebagai syarat pendaftaran akun. Selain itu pula dalam penggunaan media sosial, pengguna dengan sukarela mengunggah konten bermuatan tulisan ataupun media, seperti gambar, pesan suara, dan video. Konten-konten yang diunggah oleh pengguna dapat dilihat oleh pengguna lainnya tersebut juga termasuk data pribadi. Walaupun dengan secara sukarela, bukan berarti konten tersebut bebas dari resiko para pelaku kejahatan di dunia maya atau digital. Hal ini cukup begitu mengkhawatirkan karena berjuta-juta data Warga Negara Indonesia memiliki resiko untuk diretas ataupun dicuri oleh pihak yang tidak bertanggungjawab. Resiko tercurinya atau bocornya data pribadi yang ada pada media sosial juga semakin diperparah dengan pola pikir sebagian masyarakat yang menilai bahwa data pribadi tersebut tidaklah penting.[4] Walaupun demikian, Pemerintah sebagai penyelenggara negara harus membuat sebuah tindakan untuk menjamin dan melindungi data pribadi para warga negaranya.

Pemerintah memiliki sebuah kewajiban untuk menjamin dan melindungi data pribadi para penduduk agar senantiasa aman, karena mendapatkan sebuah perlindungan dan jaminan keamanan atas data pribadi merupakan salah satu bentuk hak asasi manusia yang harus dilindungi, karena data pribadi masuk kedalam hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi. Perlindungan data pribadi juga merupakan sebuah amanah konstitusi, hal tersebut tertuang pada Pasal 28G Ayat (1) UUD 1945 yang berbunyi: *"setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dikuasainya, serta berhak atas*

[2] Tongkotow Liedfray, Fonny J. Waani dan Jouke L Lasut, Peran Media Sosial Dalam Mempererat Antar Keluarga Di Desa Esandom Kecamatan Tombantu Timur Kabupaten Minahasa Tenggara, Jurnal Ilmiah Society, Vol.2 No.1, (2022), hal. 2

[3] Raihan Hasya, "*Whatsapp Teratas, Ini 7 Media Sosial Paling Banyak Digunakan Warganet Indonesia Sepanjang 2022*" (https://goodstats.id/article/whatsapp-teratas-ini-7-media-sosial-paling-banyak-digunakan-warganet-indonesia-sepanjang-2022-iJklw), diakses pada 17 April 2023, Pukul 14.00 WIB.

[4] Muhammad Arvy C A dan Hari Soeskandi, Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE dan UU PDP, Bureaucracy Journal: Indonesia Journal of Law and Social-Politic Governance, Vol. 3 No. 1, (2023), hal. 561-562

rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".[5]

Sebagai respon untuk mengatasi permasalahan tersebut, pemerintah menerbitkan sebuah Undang-Undang yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik atau UU ITE. Walaupun lebih banyak berfokus memuat tentang transaksi elektronik, terdapat 1 pasal yang bermuatan tentang perlindungan data pribadi yaitu pada Pasal 26yang berbunyi:

1) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan;
2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini".[6]

Lalu kemudian terdapat pembaruan pada UU ITE, yang tertuang pada Undang-Undang Nomor 19 Tahun 2016. Pada pembaruan tersebut terdapat tambahan di Pasal 26. Pembaruan pada Pasal 26 menambahkan jumlah ayat pada pasal tersebut, yang awalnya berjumlah 2 ayat kemudian menjadi 5 ayat dengan 3 ayat tambahan, 3 ayat tambahan tersebut berbunyi:

1. Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan;
2. Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan;
3. Ketentuan mengenai tata cara penghapusan Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah".[7]

Hal tersebut membuktikan bahwa perhatian pemerintah terhadap perlindungan data pribadi sedikit mengalami kemajuan. Selama bertahun-tahun UU ITE dipakai sebagai salah satu dalil dalam permasalahan perlindungan data pribadi, lalu pada 17 Oktober 2022 telah disahkan sebuah Undang-Undang yang dikhususkan untuk perlindungan data pribadi, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Dengan bergesernya gaya hidup manusia akibat dari teknologi yang berkembang pesat, hal ini juga berlaku bagi pelaku kejahatan. Berkembangnya teknologi dan bergesernya gaya hidup manusia ke era digital yang membuat manusia banyak bergantung dan menghabiskan kehidupannya di dunia virtual media sosial, maka ikut bergeser juga para pelaku kejahatan ke dunia virtual media sosial dengan modus-modus tindak kejahatannya. Berbagai macam modus kejahatan dikonversi ke dunia digital yang biasa disebut *Cyber Crime* atau Kejahatan Siber. Salah satu bentuk kejahatan digital yang sering ditemui salah satunya adalah *Phising*.

[5] Undang-Undang Dasar Tahun 1945
[6] Undang-Undang Nomor 11 Tahun 2008
[7] Undang-Undang Nomor 19 Tahun 2016

Phising merupakan sebuah tindakan pengelabuan untuk mendapatkan informasi atau data-data dari seseorang. Data-data yang dijadikan sasaran dari pelaku *phising* adalah data-data yang bersifat memuat informasi pribadi atau rahasia seperti informasi perihal identitas, *username* dan *password* akun media sosial, *file-file* media pribadi dan data-data perbankan atau yang bernilai materil seperti informasi akun bank, nomor kartu kredit, dan nomor pin akun bank.[8] Dari segi kebahasaan, *Phising* berasal dari kata *Fishing* yang jika diterjemahkan dari Bahasa Inggris ke dalam Bahasa Indonesia memiliki arti memancing. Sama seperti artinya tindakan *phising* menggunakan teknik atau cara untuk mengelabui korbannya menggunakan umpan, korban pun tidak menyadari bahwa korban telah terperangkap di dalam jebakannya. Pelaku *phising* disebut dengan sebutan *Phisher*, para *Phisher* biasanya akan menyamar atau berpura-pura menjadi suatu entitas yang mempunyai reputasi baik, resmi dan terpercaya di Internet, seperti Bank, BUMN, Perusahaan/Brand. *Phisher* akan berkomunikasi dengan baik sampai korbannya tidak sadar, yang kemudian *Phisher* akan mengirimkan *link address* yang kemudian akan dialihkan ke halaman *web* palsu yang dibuat dengan semirip mungkin yang berisikan formulir yang harus diisi korban, tampilan *web* tersebut sangat mirip dengan tampilan *web* aslinya, hal ini dimaksudkan agar korban tidak sadar dan dengan harapan korban terjebak mau mengisi formulir tersebut.

Selain teknik atau modus memberikan *link address web* berisikan formulir, ada juga *Phisher* yang mengirimkan *file malware* kepada korban. *Malware* atau *Malicious Software* merupakan *software* atau perangkat lunak yang digunakan untuk menyusup, merusak atau membahayakan perangkat[9]. *Phisher* mengirimkan *malware* dengan membuat file tersebut seolah-olah hanya berupa gambar ataupun file dokumen. *Phisher* mengintruksikan korban untuk membuka *file malware* atau virus tersebut, setelah korban telah membukanya maka secara otomatis *file malware* tersebut akan terinstal di *smartphone* atau ponsel pintar korban. Ketika *malware* tersebut telah terinstal maka smartphone korban pun telah berhasil tersadap dan segala aktivitas yang dilakukan di smartphone tersebut dapat diketahui oleh *Phisher*. Contohnya ketika korban membuka aplikasi perbankan, maka *Phisher* dapat mengetahui akun dan kata sandi yang dimasukkan oleh korban pada saat membuka aplikasi perbankan tersebut.[10]

Melihat begitu berbahayanya modus kejahatan *phising* sebagai tindak kejahatan siber di era digital, jika tidak berhati-hati dan cermat dalam berselancar di internet, siapa saja bisa menjadi korban *phising*. Hal ini bisa diperparah dengan munculnya layanan verifikasi akun berbayar oleh pihak pengelola media sosial. Awalnya langkah pembuatan layanan verfikasi akun berbayar ini digagas oleh pemilik Twitter, Elon Musk. Twitter meluncurkan sebuah layanan verifikasi akun berbayar yang dinamakan Twitter Blue. Dengan membayar biaya langganan Twitter Blue, maka pelanggan dapat merasakan fitur-fitur yang ditawarkan salah satunya adalah lencananya centang

[8] Ananta Fadli S dan Shelly Kurniawan, Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phising* di Indonesia, INNOVATIVE: Journal of Social Science Research, Vol. 3 No. 2 (2023), hal. 3

[9] Julian Dwi N, Avon Budiono, Ahmad Almaarif, Jurnal Rekayasa Sistem Dan Industri: Analisis *Malware* Berdasarkan *API CALL MEMORY* Deangan Metode Deteksi *Signature-Based*, Vol. 6 No. 2, (2019), hal. 78

[10] Mia Haryati W dan Nur Fatimah, JOEICT (Jurnal of Education and Informative Communication Technology): Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime, Vol. 1 No. 1, (2017), hal. 3

pada akun.[11] Melihat layanan verifikasi berbayar telah banyak mendapatkan uang, tidak berselang lama Meta yang merupakan induk perusahaan pemilik Facebook dan Instagram juga ikut membuat hal yang sama. Perusahaan yang diketuai oleh Mark Zuckerberg tersebut membuat hal yang serupa di media sosialnya. Meta membuat layanan verifikasi akun berbayar yang diberi nama Meta Verified. Pada Meta Verified menyediakan layanan verifikasi akun berbayar atau berlangganan di 2 *Platform* media sosial, yaitu Instagram dan Facebook. Sama seperti dengan Twitter Blue, Meta Verified juga menawarkan fitur-fitur ekslusif bagi pelanggannya dan menyediakan lencana centang biru layaknya seperti akun terverifikasi yang didapatkan tanpa berlangganan. [12]

Akibat dari layanan verifikasi akun berbayar atau centang biru berbayar di media sosial, marak muncul akun-akun palsu yang terverifikasi atau memiliki lencana centang biru. Hal ini tentunya mempermudah para pelaku tindak pidana siber untuk melakukan *phising*, karena masyarakat sulit membedakan antara akun asli yang terverifikasi dengan akun palsu yang terverifikasi. Masyarakat terpaksa harus cermat agar tidak masuk ke dalam perangkap para pelaku kejahatan siber *phising*, dengan memperhatikan detail-detail kecil yang membedakan akun terverifikasi asli dengan akun terverifikasi berbayar. Hal ini telah mengubah fungsi awal dari lencana akun centang biru, yang mana awalnya diperuntukkan untuk validasi sebuah akun bagi para pengguna yang bersifat ekslusif untuk menjauhkan dari duplikasi atau pemalsuan akun oleh pihak yang tidak bertanggungjawab, yang dapat berakibat timbulnya hal-hal yang tidak diinginkan. Kebijakan pemberlakuan verifikasi akun berbayar atau berlangganan, dimana membuat siapa saja bisa mendapatkan akun terverifikasi hanya dengan membayarkan tarif yang ditentukan, tanpa harus melalui serangkaian proses verifikasi khusus dan ketat. Ini berarti telah terjadi ketidakcermatan dalam verifikasi sehingga memunculkan fenomena pemalsuan akun dan penipuan melalui akun terverifikasi berbayar (Febby Risti, 2023).[13]

METODE PENELITIAN

Pada penelitian tentang "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk *Phising* Yang Dilakukan oleh *Paid Verified Account* di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi" menggunakan metode penelitian hukum yuridis-normatif atau penelitian hukum kepustakaan (*Library Reseach*). Penelitian ini menggunakan sumber data sekunder, yang mana berasal dari Undang-Undang, bahan hukum primer, hasil penelitian terdahulu, hasil karya terdahulu dari para kalangan hukum dan sumber informasi lainnya yang dapat membantu permasalahan yang termuat di dalam penelitian ini.[14]

[11] Intan Rakhmayamti D, "*Warga RI Kebagian Juga, Twitter Centang Biru Bayar Segini*" (https://www.cnbcindonesia.com/tech/20230209130838-37-412434/warga-ri-kebagian-juga-twitter-centang-biru-bayar-segini), diakses pada 20 April 2023, Pukul 15.00 WIB

[12] Dina Karina, "*Meta Jual Centang Biru Facebook dan Instagram, Harganya Rp100.000 per Bulan" (https://www.kompas.tv/ekonomi/428763/meta-jual-centang-biru-facebook-dan-instagram-harganya-rp100-000-per-bulan),* diakses pada 26 Juli 2023, Pukul 22.00 WIB

[13] Rafli Noer K, "Banjir Akun Palsu Centang Biru Twitter, Begini Pandangan Dosen UNAIR" (https://unair.ac.id/banjir-akun-palsu-centang-biru-twitter-begini-pandangan-dosen-unair/), diakses pada 25 Maret 2023, Pukul 12.00 WIB

[14] Muhammad Siddiq A, Penentuan Metode dan Pendekatan Penelitian Hukum, (Banda Aceh, Lembaga Kajian Konstitusi Indonesia, 2022), hal. 8

HASIL DAN PEMBAHASAN

Modus Operandi Phising oleh *Paid Verified Account* menurut Undang-Undang Perlindungan Data Pribadi

Di era digital yang kebanyakan manusia di dunia sudah akrab dan bergantung pada smartphone atau ponsel pintar-nya, juga mengakibatkan terjadinya modus kejahatan dengan variasi baru. Pada dasarnya hal-hal tersebut tidaklah benar-benar baru, hanya aja modus kejahatan tersebut mengalami konversi dari dunia nyata ke dunia maya, atau biasa disebut dengan kejahatan siber atau *cyber crime*. Sudah banyak modus kejahatan siber di dunia maya, salah satunya adalah *phising*. *Phising* jika diterjemahkan ke dalam bahasa Indonesia menjadi sebuah kata yaitu pengelabuan. Menurut Kamus Besar Bahasa Indonesia, pengelabuan memiliki arti proses, cara perbuatan mengelabui.[15] Dapat dimaknai bahwasannya kata mengelabui memiliki makna sebuah perbuatan yang dilakukan dengan sengaja untuk membuat seseorang tidak menyadari hal yang sebenarnya telah dilakukan kepada seseorang tersebut.

Phising adalah sebuah tindak kejahatan berupa sebuah upaya yang dilakukan kepada seseorang menggunakan teknik pengelabuan dengan maksud untuk mendapatkan data atau informasi dari seseorang yang telah dikelabui. Data atau informasi yang diambil biasanya yang berhubungan dengan keuangan, contohnya informasi perbankan.[16] Pada era dengan tingginya aktivitas dunia maya di sosial media, hal tersebut membuat para pelaku *phising* menjadikan media sosial sebagai lading tempat menjalankan aksinya. Apalagi sekarang di media sosial terdapat layanan *paid verified accoun*t (verfikasi akun berbayar) atau biasa dikenal dengan centang biru berbayar. Layanan ini membuat para pelaku phising menjadi lebih mudah menjalankan aksinya, karena dengan layanan tersebut para pengguna media sosial jika tidak teliti maka tak akan bias membedakan antara akun asli yang terverifikasi atau akun palsu yang terverifikasi secara berbayar. Karena terdapat kesamaan tampilan yang membuat susah untuk dibedakan, hal ini tentunya mempermudah para pelaku *phising* dalam menjalankan aksinya.

Pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, tidak terdapat sebuah aturan khusus atau secara eksplisit yang mengatur atau menyebutkan tentang *Phising*. Hal ini dikarenakan Undang-Undang Perlindungan Data Pribadi tidak secara khusus mengatur lingkup data pribadi yang bersifat *person to person* seperti halnya perbuatan *phising*. *Person to person* dalam komukasi merupakan komunikasi antar dua orang dalam lingkup tertutup atau *private.* [17] Meskipun demikian, *phising* dengan menggunakan *paid verified account* masih tetap dijerat dengan Undang-Undang Perlindungan Data Pribadi. Hal tersebut dapat dilihat pada Pasal 65 ayat 1 dan 3, dengan ketentuan pidana yang ada di Pasal 67 ayat 1 dan 3. Penggunaan akun palsu yang terverifikasi secara berbayar juga dapat dijerat pada Pasal 66, karena modus *phising* menggunakan *verified account* termasuk kedalam perbuatan pemalsuan data pribadi yang

[15] Kamus Besar Bahasa Indonesia
[16] Suryadi Kurniawan, "Phising: Pengertian, Cara Kerja dan Langkah Mengatasinya", (https://www.niagahoster.co.id/blog/mengatasi-phishing/), diakses pada 26 Maret 2023, Pukul 17.00 WIB
[17] Restia Moegiono, "Phising: Kejahatan dalam Lingkup Perlindungan Data Pribadi yang Tidak Diatur dalam UU PDP", (https://kliklegal.com/phising-kejahatan-dalam-lingkup-pelindungan-data-pribadi-yang-tidak-diatur-dalam-uu-pdp/), diakses pada 26 Maret 2023, Pada Pukul 15.00 WIB

menguntungkan diri sendiri dan merugian orang lain. Hal tersebut diikuti dengan ketentuan pidananya yang terdapat pada Pasal 68. Walaupun perbuatan phising menggunakan akun palsu terverifikasi atau bercentang biru dapat dijerat oleh Undang-Undang Perlindungan Data Pribadi, bahkan dapat dijatuhi pasal berlapis. Namun ada baiknya kita tetap waspada, teliti dan berhati-hati dalam berselancar di media sosial.

Penanggulangan *Phising* Oleh *Paid Verified Account* Ditinjau Menurut Undang-Undang Perlindungan Data Pribadi

Pada dasarnya hukum memiliki sebuah definisi sebagai nilai untuk mencapai suatu keidealan, dengan menata serta menjawab permasalahan masyarakat, sehingga terciptalah representasi dari sebuah keadilan. Secara prinsip, hukum memiliki sifat universal yang senantiasa berkembang dapat menyesuaikan dinamika masyarakat mengikuti tatanan permasalahan manusia seiring berkembangnya pergaulan manusia. Selain itu hukum telah menjadi suatu yang tak terpisahkan dari kehidupan manusia.[18] Begitu pula dengan Undang-Undang Perlindungan Data Pribadi dengan keamanan perlindungan kehidupan aktivitas dunia maya di Indonesia melalui peraturan-peraturannya.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai sumber hukum formil memiliki peranan penting dalam upaya penanggulangan phising di Indonesia. Undang-Undang Perlindungan Data Pribadi memiliki peranan sebagai bentuk perlindungan data pribadi dan pemberian sanksi tegas terhadap para pelanggarnya, khususnya para pelaku kejahatan siber. Pada Undang-Undang ini juga termuat tentang penanggulangan atau cara preventif mengatasi penyalahgunaan data pribadi termasuk phising.

Dijelaskan pada Undang-Undang Perlindungan Data Pribadi di Pasal 58, akan terdapat suatu lembaga yang dibentuk dan ditugaskan oleh Presiden sebagai kepala pemerintah Lembaga otoritas ini juga akan betanggungjawab kepada Presiden sebagai Kepala Negara, yang bernama Lembaga Otoritas Perlindungan Data Pribadi atau LOPDP. Lembag otoritas tersebut ditugaskan untuk melindungi data pribadi warga negara Indonesia dan menjalankan amanat yang tertuang pada Undang-Undang Data Pribadi.[19] Walaupun lembaga tersebut dipilih dan dibawahi oleh Presiden, namun diharapkan agar lembaga otoritas tersebut memiliki indepedensi atau kemandirian dalam menjalankan tugas dan amanat dari Undang-Undang Perlindungan Data Pribadi, agar terciptanya *fairness* atau keadilan pada saat penegakkan Undang-Undang Perlindungan Data Pribadi tersebut yang membuktikan bahwa pemerintah tidak dilindungi pada saat pihak pemerintah melanggar peraturan yan termuat dalam Undang-Undang Perlindungan Data Pribadi.[20]

Lalu pada Pasal 59 dan 60 Undang-Undang Perlindungan Data Pribadi tertuang tugas dan wewenang dari Lembaga Otoritas Perlindungan Data Pribadi, walaupun demikian pada Pasal 61 menjelaskan tugas dan wewenang dari Lembaga tersebut lebih lanjut akan tercantum pada

[18] Yati Nurhayati, Pengantar Ilmu Hukum, (Bandung, Penerbit Nusa Media, 2020), hal. 2
[19] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
[20] Ernest, Rian. "Sidang: Mampukah UU PDP Jadi Juru Selamat Data Pribadi Kita?" Youtube, diunggah oleh Asumsi

Peraturan Pemerintah dengan menjadikan Pasal 59 dan 60 Undang-Undang Perlindungan Data Pribadi sebagai acuan. Berikut di bawah ini merupakan gambaran dari tugas dan wewenang Lembaga Otoritas Perlindungan Data Pribadi dengan menjadikan Pasal 59 dan 60 sebagai acuannya.

1. Tugas dari Lembaga Otoritas Perlindungan Data Pribadi:
   a) Membuat pengembangan kebijakan yang memiliki hubungan dengan perlindungan data pribadi, supaya semakin memastikan bahwa data pribadi individu dapat terlindungi dengan baik.
   b) Memberikan sanksi administratif kepada para pihak yang melanggar ketentuan perlindungan data pribadi. Hal ini bertujuan agar timbulnya efek jera sehingg dapat mendorong kepatuhan terhadap undang-undang.
   c) Melakukan kolaborasi atau kerja sama dengan aparat penegak hukum untuk membantu dalam penanganan tindak pidana yang melibatkan data pribadi.
   d) Melakukan penilaian terhadap pemenuhan persyaratan yang berkaitan dengan transfer data pribadi ke luar wilayah hukum Indonesia. Mereka menjadi pihak yang memastikan bahwa *transfer* data pribadi dilakukan dengan memperhatikan perlindungan yang memadai.
2. Wewenang dari Lembaga Otoritas Perlindungan Data Pribadi:
   a) Melakukan pemeriksaan terhadap organisasi dan perusahaan yang diduga melanggar peraturan perlindungan data pribadi, dan memberikan sanksi administratif dan denda yang sesuai.
   b) Menghentikan penggunaan atau pengolahan data pribadi yang tidak sah atau tidak diizinkan kepada individu, organisasi atau perusahaan.
   c) Melakukan investigasi secara independen dan memberikan laporan kepada publik mengenai pelanggaran dan pelaksanaan perlindungan data pribadi.
   d) Memberikan nasihat kepada pemerintah dan lembaga terkait mengenai kebijakan perlindungan data pribadi di internasional.[21]

Untuk semakin menguatkan tindak penanggulangan atau pencegahan tindak kejahatan siber, salah satunya *phising* yang mengancam data pribadi masyarakat. Dengan amanat dari pembentukan Undang-Undang Perlindungan Data Pribadi, pemerintah menjalankan amanat tersebut dengan cara memperkuat kerja sama atau sinergitas antara lembaga-lembaga yang memiliki wewenang di bidang keamanan siber, seperti POLRI, Badan Intelejen Indonesia, Badan Siber dan Sandi Negara (BSSN) dan Kemenkominfo.[22]

Walaupun dengan sanksi pidana dan sanksi administrasi yang dimiliki oleh Undang-Undang Perlindungan Data Pribadi, serta penguatan keamanan siber antar lembaga yang bersinggungan dengan permasalahan kejahatan siber. Hal tersebut merupakan sebuah cara penanggulangan yang masih mimiliki celah yang besar. Celah yang besar ini terdapat pada user atau pengguna internet dalam hal ini pengguna media sosial yang rawan terjebak dalam kejahatan

[21] Opcit. Ananta Fadli S, hal. 9-10
[22] Adhitya Prananda, Yusuf dan Rudy A.G Gultom, Sinergi Lembaga Intelejen dalam Menghadapi Ancaman Siber di Indonesia, Jurnal Peperangan Asimetris, Vol 7 No 1, (2021), hal. 60

phising. Masyarakat di Indonesia secara garis besar masih belum mampu mengenali ancaman dari kejahatan *phising* di media sosial.[23] Melihat fakta tersebut tentunya harus segera diperbaiki mengingat bahwa para pelaku *phising* menggunakan akun terverifikasi berbayar dalam menjalankan aksinya yang mengakibatkan korban semakin mudah untuk terjebak dalam modusnya. Dengan mempertimbangkan amanat dari Undang-Undang Perlindungan Data Pribadi, pemerintah harus melakukan sosialisasi mengenai data pribadi kepada masyarakat. Selain itu masyarakat juga harus mendorong peningkatan literasi dgital kepada masyarakat, sebagai salah satu bentuk penanggulangan terhadap permasalahan penyalahgunaan data pribadi, seperti *phising*. Tentunya implementasi dari Undang-Undang Perlindungan Data Pribadi harus dibarengi dan sejalan dengan literasi digital yang baik, agar pelaksanaannya menjadi lebih baik lagi.[24] Dengan meningkatkan literasi digital pada seluruh lapisan masyarakat, hal tersebut dapat meningkatkan kepedulian, kewaspadaan masyarakat ketika di dunia maya sehingga modus-modus seperti phising yang dilakukan oleh akun terverifikasi berbayar atau aun centang biru dapat dicegah atau dihindari. Hal ini juga sebagai penerapan tentang Partisipasi Masyarakat yang terdapat di Undang-Undang Perlindungan Data Pribadi pada Pasal 63.

KESIMPULAN

Perkembangan yang begitu pesat pada bidang informasi dan teknologi berdampak terhadap beberapa aspek. Seperti bagaimana manusia di zaman sekarang memiliki ketergantungan terhadap penggunaan media sosial. Mayoritas manusia menghabiskan lebih banyak waktu di media sosial dibandingkan di dunia nyata. Ketika manusia hidup berpindah ke dunia maya, maka menjadi sebuah keharusan bahwa data-data yang mereka miliki juga akan ter-*digitalize* atau berubah menjadi digital. Data-data tersebut akan tersimpan di dalam penyimpanan masing-masing penyedia atau pengelola layanan media sosial. Tentunya data-data yang tersimpan tersebut memiliki resiko untuk diretas oleh pihak yang tidak bertanggungjawab. Dengan terjadinya pergeseran kebiasaan hidup manusia, dari dunia nyata ke dunia maya. Tentu hal yang ditimbulkan tidak selamanya hanya berdampak baik saja. Dengan terjadinya pergesaran kebiasaan manusia, maka mau tidak mau tindak kejahatan juga ikut bergeser dan ikut masuk ke dalamnya. Akibat dari pergeseran tersebut maka banyak modus-modus kejahatan yang berhubungan dengan dunia maya, salah satunya adalah *phising*. Phising merupakan tindak pengelabuan yang dilakukan seseorang kepada orang lain dengan maksud seseorang yang melakukan pengelabuan tersebut berhasil mendapatkan data atau informasi yang diincarnya, data yang diincar biasanya data atau informasi yang dapat menyebabkan keuntungan bagi pelaku dan kerugian bagi korban. Tidak sampai di situ, modus phising dapat terus berkembang sesuai dengan bagaimana keadaan dunia maya. Terjadi perubahan pada modus phising dikarenakan munculnya sebuah layanan yang mengakibatkan terjadinya sebuah kebingungan dan rasa ambigu atas keaslian sebuah akun, karena terdapat fitur

[23] Nunu Vadila dan Ahmad R. Pratama, Analisis Kesadara Keamanan Terhadap Ancaman Phising, AUTOMATA Deseminasi Tugas Akhir Mahasiswa, Vol. 2 No. 2, (2021), hal. 4

[24] Heri Purwata, "Kehadiran UU PDP Wajib Dibarengi Peningkatan Literasi Digital Masyarakat", (https://jurnal.republika.co.id/posts/180049/kehadiran-uu-pdp-wajib-dibarengi-peningkatan-literasi-digital-masyarakat), diakses pada 10 Juni 2023, pukul 12.00 WIB.

yang sedari awal bersifat ekslusif sebagai pembuktian atas keaslian sebuah akun. Kini fitur tersebut malah dibeli dengan gampangnya. Tentu hal tersebut membuat para pengguna untuk membedakan antara akun asli atau akun palsu.

Sebagai penyelenggara negara, pemerintah sudah seharusnya senantiasa melindungi hak-hak pada masyarakatnya. Termasuk data pribadi yang dimiliki oleh para masyarakat yang menggunakan media sosial tersebut. Untuk mengatasi permasalahan tersebut pemerintah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai jawaban atas permasalahan ini. Undang-Undang Perlindungan Data Pribadi dapat berperan besar dalam penanggulangan kejahatan siber atau permasalahan penyalahgunaan data pribadi, seperti *phising* yang dilakukan oleh paid verified account. Dengan cara-cara yang preventif yang ada pada Undang-Undang Perlindungan Data Pribadi, diharapkan dapat menekan angka kasus kejahatan siber atau penyalahgunaan data pribadi seperti *phising.* Beberapa solusi penanggulangan atau pencegahan penyalahgunaan data pribadi menurut Undang-Undang Perlindungan Data Pribadi, yaitu: ancaman dan sanksi bagi para pelaku atau pelanggar, dibentuknya lembaga otoritas khusus dan idependen untuk mengatasi permasalahan data pribadi, terjadinya kerja sama atau sinegritas antar lembaga yang berhubungan dengan keamanan siber dan yang terakhir adalah peningkatan literasi digital masyarakat sebagai bentuk partisipasi masyarakat dalam melindungi data pribadi.

DAFTAR PUSTAKA

Arvy, M. C. A. dan Soeskandi, H. (2023). *Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE dan UU PDP*, Bureaucracy Journal: Indonesia Journal of Law and Social-Politic Governance, 3 (1), (2023); 561-562

Dewi, T. dan Alhakim. (2021). *Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi di Indonesia*. Journal Komunitas Yustisia Universitas Pendidikan Ganesha, 4 (3); 1057.

Dina Karina, "*Meta Jual Centang Biru Facebook dan Instagram, Harganya Rp100.000 per Bulan" (https://www.kompas.tv/ekonomi/428763/meta-jual-centang-biru-facebook-dan-instagram-harganya-rp100-000-per-bulan),* diakses pada 26 Juli 2023, Pukul 22.00 WIB

Dwi, J. N., Budiono, A., dan Almaarif, A. (2019). *Analisis Malware Berdasarkan API CALL MEMORY Deangan Metode Deteksi Signature-Based.* Jurnal Rekayasa Sistem Dan Industri, 6 (2); 78

Ernest, Rian. "Sidang: Mampukah UU PDP Jadi Juru Selamat Data Pribadi Kita?" Youtube, diunggah oleh Asumsi

Fadli, A. S. dan Kurniawan. Shelly. (2023). *Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia*. INNOVATIVE: Journal of Social Science Research, 3 (2); 3-10

Haryati, M., W. dan Fatimah, N. (2017). *Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime*. JOEICT (Jurnal of Education and Informative Communication Technology), 1 (1); 3

Heri Purwata, "Kehadiran UU PDP Wajib Dibarengi Peningkatan Literasi Digital Masyarakat", (https://jurnal.republika.co.id/posts/180049/kehadiran-uu-pdp-wajib-dibarengi-peningkatan-literasi-digital-masyarakat), diakses pada 10 Juni 2023, pukul 12.00 WIB.

Intan Rakhmayamti D, "*Warga RI Kebagian Juga, Twitter Centang Biru Bayar Segini*" (https://www.cnbcindonesia.com/tech/20230209130838-37-412434/warga-ri-kebagian-juga-twitter-centang-biru-bayar-segini), diakses pada 20 April 2023, Pukul 15.00 WIB

Liedfray, T., Fonny J. W. dan Jouke L Lasut. (2022). *Peran Media Sosial Dalam Mempererat Antar Keluarga Di Desa Esandom Kecamatan Tombantu Timur Kabupaten Minahasa Tenggara*. Jurnal Ilmiah Society, 2 (1); 2

Nuhayati, Y. (2020). *Pengantar Ilmu Hukum*. Bandung: Penerbit Nusa Media.

Prananda, A., Yusuf dan Rudy A.G Gultom. (2021). *Sinergi Lembaga Intelejen dalam Menghadapi Ancaman Siber di Indonesia*. Jurnal Peperangan Asimetris, 7 (1), (2021); 60

Rafli Noer K, "Banjir Akun Palsu Centang Biru Twitter, Begini Pandangan Dosen UNAIR" (https://unair.ac.id/banjir-akun-palsu-centang-biru-twitter-begini-pandangan-dosen-unair/), diakses pada 25 Maret 2023, Pukul 12.00 WIB

Raihan Hasya, "*Whatsapp Teratas, Ini 7 Media Sosial Paling Banyak Digunakan Warganet Indonesia Sepanjang 2022*" (https://goodstats.id/article/whatsapp-teratas-ini-7-media-sosial-paling-banyak-digunakan-warganet-indonesia-sepanjang-2022-iJklw), diakses pada 17 April 2023, Pukul 14.00 WIB.

Restia Moegiono, "Phising: Kejahatan dalam Lingkup Perlindungan Data Pribadi yang Tidak Diatur dalam UU PDP", (https://kliklegal.com/phising-kejahatan-dalam-lingkup-pelindungan-data-pribadi-yang-tidak-diatur-dalam-uu-pdp/), diakses pada 26 Maret 2023, Pada Pukul 15.00 WIB

Suryadi Kurniawan, "Phising: Pengertian, Cara Kerja dan Langkah Mengatasinya", (https://www.niagahoster.co.id/blog/mengatasi-phishing/), diakses pada 20 Maret 2023, Pukul 17.00 WIB

Undang-Undang Dasar Tahun 1945

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Pembaruan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Vadila, N. dan Ahmad R. P., (2021). *Analisis Kesadara Keamanan Terhadap Ancaman Phising*. AUTOMATA Deseminasi Tugas Akhir Mahasiswa, 2 (2); 4