INNOVATIVE: Journal Of Social Science Research
Volume 3 Nomor 2 Tahun 2023 Page 4208-4221
E-ISSN 2807-4238 and P-ISSN 2807-42468
Website: https://j-innovative.org/index.php/Innovative

Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phising* di Indonesia

Ananta Fadli Sutarli[1]✉, Shelly Kurniawan[2]
Fakultas Hukum, Universitas Kristen Maranatha
Email: ananta.fadli@gmail.com[1]✉

Abstrak

Undang-Undang Nomor 27 tahun 2022 Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) adalah instrumen hukum yang melindungi data pribadi masyarakat Indonesia dari penyalahgunaan, termasuk praktik phising. Penulisan ini bertujuan untuk mengetahui sejauh mana efektivitas peran pemerintah dalam menanggulangi phishing di Indonesia melalui UU PDP. Penelitian ini akan menganalisis implementasi UU PDP dalam menanggulangi praktik phishing dengan menggunakan metode hukum normatif. Hasilnya menunjukkan bahwa UU PDP tahun 2022 melindungi data pribadi, termasuk informasi secara merinci yang menjadi target phising. Lembaga Otoritas Perlindungan Data Pribadi akan bertanggung jawab dalam pelaksanaan UU PDP, memberikan sanksi administratif, mendukung penegak hukum, dan menilai persyaratan transfer data pribadi ke luar Indonesia. Sanksi pidana termasuk penjara atau denda diterapkan untuk menanggulangi phising, serta sanksi administratif seperti pencabutan izin usaha dan/atau pembekuan kegiatan usaha sebagai efek jera. UU PDP tahun 2022 penting dalam melindungi data pribadi dari phising, tetapi perlu perkuat pelaksanaan dan kerja sama antara lembaga pemerintah terkait agar efektivitasnya meningkat, sehingga masyarakat merasa aman dalam transaksi online dan menjaga data pribadi mereka.

Kata Kunci: *Data Pribadi; Pemerintah; Phishing; Regulasi*

Abstract

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a legal instrument that protects the personal data of Indonesian citizens from misuse, including phishing practices. This paper aims to assess the effectiveness of the government's role in combating phishing in Indonesia through the PDP Law. The study analyzes the implementation of the PDP Law in addressing phishing practices using a normative legal method. The results indicate that the PDP Law of 2022 safeguards personal data, including detailed information that is targeted by phishing. The Personal Data Protection Authority is responsible for enforcing the PDP Law, imposing administrative sanctions, supporting law enforcement agencies, and assessing the requirements for transferring personal data outside Indonesia. Criminal sanctions, such as imprisonment and/or fines, are applied to combat phishing, while administrative penalties, such as revoking business licenses or suspending business activities, serve as deterrents. The PDP Law of 2022 plays a crucial role in protecting personal data from phishing, but efforts should be made to strengthen its implementation and foster cooperation among relevant government institutions to enhance its effectiveness, ensuring that individuals feel secure in conducting online transactions and safeguarding their personal data.
Keywords: *Government; Phishing; Regulation.*

PENDAHULUAN

Perkembangan teknologi internet yang semakin cepat telah mengakibatkan dampak yang sangat signifikan bagi masyarakat dunia. Perkembangan tersebut telah mengubah banyak metode konvensional dan gaya hidup masyarakat menjadi lebih modern di berbagai bidang, seperti sosial, budaya, ekonomi, militer, administrasi, dan bidang lainnya. Adanya perkembangan teknologi dan kemudahan akses informasi membuat peluang dan persaingan di masyarakat semakin meningkat. Oleh karena itu, masyarakat saat ini diharuskan untuk hidup lebih modern dan mengikuti perkembangan tersebut jika tidak ingin ketinggalan dalam persaingan (Wahyudi & Sukmasari, 2014)

Internet adalah media informasi dan komunikasi elektronik yang menyediakan berbagai aktivitas, seperti *e-commerce, e-education, e-health, e-government, e-payment,* transportasi, pariwisata, dan cloud computing. Salah satu kemajuan dalam teknologi informasi dan komunikasi adalah pengumpulan, penyimpanan, pembagian, dan analisis data secara efisien dan efektif antara perusahaan atau masyarakat (Dewi, 2016). Banyak masyarakat Indonesia juga memanfaatkan teknologi internet. Menurut hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia pada tahun 2016, terdapat 132,7 juta pengguna internet di Indonesia, dimana sebagian besar pengguna internet berada di wilayah Jawa yaitu sebanyak 86,3 juta orang. Pemanfaatan teknologi internet tersebut sangat beragam, dimana dari 132,7

juta pengguna internet tersebut, 97,4% diantaranya menggunakan internet untuk media sosial, 96,8% untuk hiburan, 96,4% untuk mengakses berita, 93,8% untuk kebutuhan pendidikan, 93,1% untuk komersial, dan 91,6% diantaranya juga menggunakan internet untuk layanan publik Indonesia (Dewi, 2016).

Dengan semakin majunya zaman dan teknologi yang semakin canggih, kejahatan siber (*cybercrime*) telah berkembang dan menghasilkan berbagai jenis kejahatan baru dengan metode baru. Bentuk-bentuk kejahatan siber (*cybercrime*) terus berkembang dan tidak hanya terbatas pada *hacking*, *cracking*, atau *carding*, namun juga mencakup jenis-jenis kejahatan yang lebih spesifik seperti *probe* (upaya untuk mendapatkan akses ke suatu sistem), *scan* (probe dalam jumlah besar), *account compromise* (penggunaan akun secara ilegal), *root compromise* (account compromise dengan hak akses bagi pelaku penyusup), *denial of service* atau *DoS* (membuat jaringan tidak berfungsi karena terlalu banyak lalu lintas), penyalahgunaan nama *domain*, dan masih banyak lagi (Ekawati, 2018). Data pribadi yang bocor dapat menjadi awal munculnya berbagai aktivitas mengganggu seperti spam pada email dan SMS, serta kejahatan siber lainnya yang merugikan masyarakat. Oleh karena itu, perlindungan data pribadi menjadi sangat penting dalam era digitalisasi saat ini. Data pribadi, seperti nama, nomor identitas, alamat, nomor telepon, dan lain-lain, merupakan bagian integral dari identitas seseorang. Pelaku kejahatan siber seringkali memanfaatkan data pribadi tersebut melalui metode phishing, yang merupakan tindakan kejahatan untuk memperoleh informasi rahasia dari korban (Mia Haryati Wibowo, 2017). Oleh karena itu, penting bagi pemerintah untuk menjaga keamanan data pribadi masyarakat melalui Undang-Undang Perlindungan Data Pribadi.

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. Kejahatan *phising* menggunakan teknik rekayasa sosial untuk menipu orang dan memperoleh informasi pribadi atau data sensitif seperti username, password, dan rincian kartu kredit. Pelaku kejahatan phising disebut sebagai *Phisher*, dan mereka cenderung menyamar sebagai entitas yang terpercaya atau sah dalam sebuah komunikasi elektronik, seperti bank, perusahaan, atau situs web populer. *Phisher* akan menggunakan berbagai taktik untuk membuat korban mereka percaya dan terdorong untuk membagikan informasi pribadi mereka, seperti mengirim email palsu atau membuat situs web palsu yang terlihat sangat mirip dengan situs web asli. Setelah mendapatkan informasi pribadi korban, phisher dapat menggunakannya untuk melakukan kejahatan, seperti pencurian identitas, penipuan kartu kredit, dan penipuan keuangan lainnya.

Kejahatan Siber *Phising* melalui *WhatsApp* terus menjadi ancaman yang harus diwaspadai oleh masyarakat. Salah satu skema penipuan terbaru yang ditemukan adalah Rediroff.ru. Para penipu menggunakan rekayasa sosial untuk mendapatkan akses ke data pengguna *WhatsApp*, termasuk informasi keuangan seperti rincian akun bank dan kartu. Para penipu mengirimkan tautan kepada pengguna *WhatsApp* yang mengklaim bahwa mereka memenangkan hadiah dan diminta untuk mengikuti survei. Setelah pengguna menjawab pertanyaan, mereka diarahkan ke situs web lain yang meminta pengguna untuk mengisi informasi pribadi seperti nama, usia, alamat, informasi bank, dan data pribadi lainnya.

Informasi yang diperoleh tersebut dapat digunakan untuk melakukan penipuan atau digunakan untuk keuntungan para pelaku kejahatan siber. Selain itu, penjahat dunia maya dapat memanfaatkan informasi ini untuk mengirimkan spam dan email berbahaya kepada korban, serta menginstal aplikasi yang tidak diinginkan di perangkat pengguna. Situs web phishing ini juga menggunakan taktik untuk menyesuaikan skema penipuan sesuai dengan lokasi pengguna. Oleh karena itu, penting bagi pengguna WhatsApp untuk melaporkan tautan spam seperti Rediroff.ru sebagai spam dan menghapusnya segera. Jika pengguna secara tidak sengaja mengklik tautan tersebut, mereka harus memindai perangkat mereka dengan antivirus untuk mencari malware atau aplikasi yang tidak diinginkan.

Maka dari itu, penting bagi masyarakat untuk memahami dan waspada terhadap tindak-tindak kejahatan phising agar data pribadi mereka tidak jatuh ke tangan yang tidak bertanggung jawab. Untuk itu, masyarakat harus berhati-hati dan memperhatikan tanda-tanda phising seperti email atau pesan yang tidak dikenal, tautan yang tidak dikenal, atau permintaan informasi pribadi yang tidak biasanya diberikan. Dengan melakukan hal-hal tersebut, masyarakat dapat melindungi data pribadi mereka dari tindak kejahatan phising.

Perlindungan data pribadi menjadi hal yang sangat penting untuk diterapkan dalam era digital saat ini. Pemerintah berperan penting dalam melindungi data pribadi dengan Undang-Undang Perlindungan Data Pribadi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disingkat UU PDP) adalah peraturan baru yang mengatur bagaimana data pribadi harus dilindungi dan diproses di Indonesia. Ini merupakan langkah penting untuk menjamin privasi dan hak-hak individu dalam hal pengumpulan, penggunaan, dan pembagian data pribadi. Undang-Undang ini membatasi bagaimana data pribadi harus ditangani dan dilindungi, termasuk catatan, persetujuan, akses, keamanan, penyalahgunaan, hukum, dan lembaga otoritas.

Meskipun undang-undang ini telah diterbitkan, masih banyak individu maupun organisasi yang belum memahami sepenuhnya tentang Undang-Undang Perlindungan Data Pribadi dan bagaimana tindakan preventif yang harus diterapkan dalam melindungi data pribadi. Mengingat undang-undang ini masih baru, pemerintah perlu melakukan sosialisasi secara menyeluruh di seluruh wilayah agar semua lembaga pemerintah, badan hukum, dan masyarakat dapat memahami hak dan kewajibannya serta mengetahui cara untuk melaporkan tindakan pengambilan data secara tidak sah oleh pihak lain. Dengan era digital saat ini, data pribadi sangat berharga dan seringkali disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Dengan demikian, UU PDP merupakan langkah penting untuk memastikan privasi dan hak-hak individu dalam hal pengumpulan, penggunaan, dan pembagian data pribadi.

Dalam tulisan ini, Penulis akan membahas bagaimana peranan pemerintah melalui Undang-Undang Perlindungan Data Pribadi dalam menanggulangi kejahatan Phising di Indonesia. Tulisan ini akan menjelaskan bagaimana undang-undang tersebut dapat membantu menjamin privasi dan hak-hak individu, dan bagaimana tindakan preventif dapat diterapkan untuk melindungi data pribadi dari tindak kejahatan phising. Perlu diperhatikan bahwa penulisan ini berfokus pada peran pemerintah melalui undang-undang perlindungan data pribadi dalam menanggulangi phishing, pada penulisan "*Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik* (Gulo dkk., 2020) memfokuskan pada undang-undang yang lebih spesifik, yaitu Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ITE memberikan dasar hukum bagi penegakan hukum terhadap tindakan *cybercrime*, termasuk *phising*. Dalam penulisan tersebut menjelaskan bahwa UU ITE mengatur tindakan yang dianggap sebagai kejahatan di dunia maya dan sanksi yang dapat dikenakan bagi pelakunya, acuan penulisan tersebut dijadikan sebagai refrensi dalam pembahasan pengaturan perlindungan data di indonesia. Kedua penulisan ini memiliki tema yang sama, yaitu phishing, namun fokusnya berbeda. Penulisan tentang "*Peranan pemerintah melalui Undang-Undang Perlindungan Data Pribadi dalam menanggulangi kejahatan Phising di Indonesia*" lebih menekankan pada upaya pemerintah dalam melindungi data pribadi masyarakat dari praktik phishing melalui UU PDP yang baru saja disahkan pada tahun 2022, sedangkan penulisan tentang "*Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik*." lebih menekankan pada sanksi yang dapat diberikan kepada pelaku tindak pidana phishing. Kedua penulisan ini dapat saling melengkapi dan memberikan pemahaman yang lebih baik tentang phishing dan upaya pencegahannya di Indonesia. Penulis

berharap tulisan ini akan memberikan wawasan dan informasi yang berguna bagi masyarakat dan organisasi dalam menjaga privasi dan hak-hak data pribadi dalam era digital saat ini.

METODE PENELITIAN

Penulisan "*Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia*" menggunakan metode penelitian hukum normatif. Metode ini melibatkan analisis terhadap norma hukum yang berlaku dalam masyarakat, baik yang tercantum dalam peraturan perundang-undangan maupun yang berdasar pada etika dan moral yang berlaku (Suggono, 2016). Dalam hal ini, penelitian dilakukan dengan mengumpulkan data dan informasi mengenai peraturan hukum dan regulasi yang terkait dengan perlindungan data pribadi, seperti undang-undang perlindungan data pribadi, dan membandingkannya dengan praktik-praktik yang ada dalam menanggulangi phising.

Penelitian ini bertujuan untuk mengetahui sejauh mana peran pemerintah melalui undang-undang perlindungan data pribadi dalam mengatasi masalah phising di Indonesia dan bagaimana implementasi undang-undang tersebut dalam praktiknya. Oleh karena itu, metode penelitian hukum normatif sangat sesuai untuk digunakan dalam hal penulisan ini untuk menemukan solusi atau jawaban terhadap masalah yang ada.

HASIL DAN PEMBAHASAN

Peraturan Perlindungan Data Pribadi di Indonesia

Perkembangan teknologi dan informasi pada era digitalisasi yang semakin luas menjadikan informasi privasi seseorang dapat diakses dengan mudah oleh orang yang tidak bertanggung jawab. Kepentingan pengaturan perlindungan data menjadi sangat penting bagi masyarakat Indonesia. Dengan adanya perlindungan hukum preventif yaitu suatu upaya pemerintah untuk mencegah terjadinya pelanggaran hukum sebelum terjadi. Perlindungan ini diatur dalam peraturan perundang-undangan dengan tujuan memberikan pedoman dan batasan dalam menjalankan kewajiban tertentu. Mekanisme perlindungan hukum preventif memberikan kesempatan bagi subyek hukum untuk menyampaikan keberatan atau pendapat sebelum keputusan pemerintah menjadi final, dengan tujuan mencegah terjadinya sengketa. Perlindungan hukum preventif juga sangat penting untuk tindakan pemerintahan yang didasarkan pada kebebasan bertindak, karena pemerintah akan lebih berhati-hati dalam mengambil keputusan dengan mengandalkan perlindungan hukum preventif (Raharjo, 2000). Sebelum adanya UU PDP, indonesia telah mempunyai beberapa regulasi mengenai data regulasi yang belum spesifik namun telah mencerminkan perlindungan data pribadi.

Salah satu undang-undang yang mengatur tentang hal ini adalah UU Nomor 36 Tahun 2009 tentang Kesehatan, yang mengatur bahwa setiap orang memiliki hak atas privasi dan perlindungan data pribadi mereka. Pasal 57 ayat 1 UU Nomor 36 Tahun 2009 menentukan bahwa setiap orang berkewajiban untuk melindungi data pribadi orang lain. Sebagai tambahan, UU Nomor 23 Tahun 2006 tentang Administrasi Kependudukan juga memiliki beberapa pasal yang berkaitan dengan perlindungan data pribadi. Pasal 1 ayat 22 UU Nomor 23 Tahun 2006 menentukan bahwa data pribadi harus dilindungi dan tidak boleh digunakan untuk tujuan yang tidak sah. Pasal 2 huruf C dan F UU Nomor 23 Tahun 2006 juga menentukan bahwa setiap orang berkewajiban untuk melindungi data pribadi orang lain dan tidak boleh menyalahgunakannya.

Untuk menunjang upaya perlindungan data pribadi, pemerintah juga memiliki peraturan tambahan melalui Peraturan Menteri Komunikasi dan Informatika RI Nomor 19 Tahun 2016. Namun, di dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), tidak terdapat definisi yang jelas mengenai "data pribadi". Pasal 26 dalam penjelasannya hanya menyebutkan bahwa perlindungan data pribadi merupakan bagian dari hak pribadi yang mencakup tiga pengertian, yaitu: pertama, hak untuk menikmati kehidupan pribadi dan bebas dari gangguan; kedua, hak untuk berkomunikasi dengan orang lain tanpa disadap; dan ketiga, hak untuk mengawasi akses informasi tentang kehidupan dan data seseorang (Yuniarti, 2019).

Sebenarnya, selain beberapa pasal dalam peraturan perundang-undangan yang telah disebutkan, ada beberapa undang-undang lain yang mengatur hal-hal terkait data pribadi. Namun, pengaturan perlindungan data pribadi dalam peraturan perundang-undangan tersebut masih bersifat umum dan tidak memberikan perlindungan yang menyeluruh. Selain itu, ada kelemahan lain dari tidak adanya undang-undang yang menjamin pemulihan bagi korban jika hak privasinya dilanggar. Hal ini menunjukkan bahwa perlindungan data pribadi masih belum terpenuhi secara menyeluruh (Rizal, 2019).

UU PDP merupakan peraturan yang memastikan hak masyarakat atas perlindungan data pribadi yang sangat krusial (Manurung & Thalib, 2022). Melalui peraturan ini, pemerintah memiliki tanggung jawab untuk melindungi data pribadi masyarakat. Berbagai pasal dalam Undang-Undang ini memberikan petunjuk bagi pemerintah dan masyarakat mengenai hal-hal terkait perlindungan data pribadi, seperti pasal 7 UU PDP yang menyatakan hak setiap orang untuk meminta perlindungan data pribadinya. Selain itu, pasal-pasal lain juga memberikan bimbingan bagi pemerintah dalam melakukan tindakan untuk melindungi data pribadi. Pasal 12 UU PDP misalnya, yang menyatakan bahwa pemerintah wajib menyediakan mekanisme perlindungan data pribadi yang efektif dan menjamin bahwa data pribadi tidak akan digunakan

untuk kepentingan yang tidak semestinya.

Kementerian Komunikasi dan Informatika (Kemenkominfo) Republik Indonesia telah mengakui manfaat dari transaksi elektronik, yang telah menginspirasi lahirnya alternatif baru dalam penyelenggaraan berbagai kegiatan di dunia siber, mulai dari kegiatan bisnis, pendidikan, pendaftaran, pembelian, pembayaran, jasa perbankan, hingga semua kegiatan elektronik lainnya yang digunakan untuk memenuhi kebutuhan sehari-hari (Yustitiana, 2021). Kemenkominfo secara tegas berpendapat bahwa dengan adanya teknologi, informasi, dan komunikasi yang terintegrasi melalui kegiatan berbasis elektronik, maka di masa depan akan terbuka peluang yang baik bagi pertumbuhan penduduk Indonesia, baik dari segi ilmu pengetahuan maupun ekonomi.

Faktanya, kegiatan transaksi elektronik dianggap memiliki dua sisi yang berbeda, yaitu memberikan dampak positif bagi pengguna, tetapi juga membawa dampak negatif. Tidak dapat dipungkiri bahwa transaksi elektronik dapat menjadi sarana yang efektif dan efisien bagi masyarakat untuk melakukan tindakan melawan hukum. Masyarakat yang memiliki niat buruk dalam menggunakan transaksi elektronik dapat memanfaatkannya sebagai media untuk melakukan kejahatan. Jenis kejahatan yang terjadi di dunia siber ini disebut sebagai *cyber crime* (Yustitiana, 2021).

Perlu diingat bahwa selain dikenal dengan istilah hacking atau hacker, kejahatan siber juga dapat dikenal dengan istilah *cracking* atau *cracker*. Meskipun terdapat beberapa persamaan antara *hacking* dan *cracking*, keduanya juga memiliki perbedaan. Salah satu bentuk kejahatan yang dilakukan oleh *cracking* atau *cracker* adalah phising. Kejahatan ini bertujuan untuk menguntungkan diri sendiri dan merugikan pihak lain yang menjadi korban dari *cyber crime* dalam bentuk phising (Gulo dkk., 2021). Dalam konteks keamanan komputer, *Phishing* merupakan salah satu bentuk kejahatan elektronik yang menggunakan penipuan untuk mendapatkan informasi sensitif, seperti username, password, dan detail kartu kredit. Proses *Phishing* dilakukan dengan meniru sebagai entitas yang terpercaya atau organisasi yang sah, dan biasanya berkomunikasi secara elektronik (Rachmawati, 2014).

Peran Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising di Indonesia

Pada umumnya, hukum adalah sekumpulan aturan atau peraturan yang mempengaruhi perilaku manusia dalam suatu masyarakat atau negara. Sumber hukum dapat ditentukan oleh berbagai faktor, termasuk faktor yang mempengaruhi bentuk hukum itu sendiri. Sumber hukum dapat berasal dari sumber material dan immaterial. Sumber hukum material terdiri dari berbagai

aturan hukum yang telah ditetapkan oleh badan-badan legislatif atau lembaga lain yang memiliki kewenangan untuk membuat peraturan, sementara sumber hukum immaterial meliputi faktor-faktor seperti budaya hukum dan penegak hukum yang mempengaruhi cara di mana hukum diterapkan dalam masyarakat. Dengan memperhatikan faktor-faktor ini, kita dapat menentukan sumber hukum yang baik untuk suatu wilayah atau negara (Confido, 2019).

Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) penting dalam menanggulangi phising di Indonesia. UU PDP memberikan perlindungan bagi data pribadi seseorang dan memberikan sanksi tegas bagi pelaku kejahatan siber, termasuk pelaku phising. Pemerintah memiliki tanggung jawab untuk memastikan bahwa peraturan dalam UU PDP diterapkan dan diikuti dengan baik untuk melindungi data pribadi masyarakat.

Sebagai upaya pencegahan dan penindakan terhadap pelaku phising, pemerintah juga berperan dalam menegakkan UU PDP ini. Hal ini dilakukan dengan memperkuat kerja sama antara lembaga pemerintah yang memiliki tugas dan wewenang dalam bidang keamanan siber, seperti Kepolisian Negara Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), serta Komisi Perlindungan Anak Indonesia (KPAI). Selain itu, pemerintah juga bertanggung jawab untuk memberikan sanksi bagi pelaku-pelaku yang melakukan kejahatan phising. Sanksi yang diberikan oleh pemerintah diharapkan bisa memberikan dampak yang signifikan bagi pelaku dan memastikan bahwa mereka tidak akan melakukan kejahatan yang sama lagi di masa mendatang. Sanksi yang diterapkan oleh pemerintah juga harus memastikan bahwa masyarakat merasa aman dan nyaman dalam melakukan transaksi *online* dan menjaga data pribadi mereka.

Pasal 58 UU PDP menyebutkan lembaga yang bertanggung jawab dalam pelaksanaan UU PDP adalah Lembaga Otoritas Perlindungan Data Pribadi (LOPDP) yang dibentuk oleh pemerintah, dan lembaga yang bertanggung jawab dalam melaksanakan hal tersebut ditetapkan oleh Presiden dan diatur lebih lanjut dengan Peraturan Presiden. LOPDP memiliki tugas dan wewenang yang penting dalam upaya melindungi data pribadi individu. Berikut adalah gambaran tentang tugas dan wewenang yang mungkin akan dimiliki LOPDP berdasarkan UU PDP:

1. Tugas LOPDP:
    a) Mengembangkan kebijakan yang berkaitan dengan perlindungan data pribadi untuk memastikan bahwa data pribadi individu terlindungi dengan baik. Mereka bertanggung jawab untuk merumuskan kebijakan yang memenuhi perkembangan teknologi dan bisnis.

b) Menjatuhkan sanksi administratif terhadap pihak-pihak yang melanggar ketentuan perlindungan data pribadi. Hal ini bertujuan untuk memberikan efek jera dan mendorong kepatuhan terhadap undang-undang.
c) Bekerja sama dengan aparat penegak hukum untuk membantu dalam penanganan tindak pidana yang melibatkan data pribadi. Mereka memberikan bantuan dan dukungan yang diperlukan dalam penyelidikan dan penuntutan pelanggaran data pribadi.
d) Memiliki tugas untuk melakukan penilaian terhadap pemenuhan persyaratan yang berkaitan dengan transfer data pribadi ke luar wilayah hukum Indonesia. Mereka memastikan bahwa transfer data pribadi dilakukan dengan memperhatikan perlindungan yang memadai.

2. Wewenang LOPDP:
   a) Memeriksa organisasi dan perusahaan yang diduga melanggar peraturan perlindungan data pribadi, dan memberikan sanksi administratif dan denda yang sesuai.
   b) Memberikan perintah untuk 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.

Dalam menjalankan tugas dan wewenangnya, lembaga otoritas perlindungan data pribadi harus memiliki independensi, keahlian yang memadai, dan transparansi. Lembaga ini harus memastikan tugas dan wewenangnya tidak tumpang tindih dengan kelembagaan pemerintah lainnya di Indonesia dan bekerja sama dengan lembaga pemerintah lainnya. LOPDP juga harus mematuhi ketentuan hukum yang berlaku dan batas wewenang yang telah ditetapkan oleh undang-undang, agar dapat bekerja secara efektif dan efisien dalam menjalankan tugasnya. Selain itu, lembaga tersebut juga diharapkan bisa bekerja sama dengan lembaga atau otoritas perlindungan data pribadi di negara lain untuk memperkuat kerjasama internasional dalam bidang perlindungan data pribadi. Hal ini penting untuk melindungi data pribadi pengguna yang tidak hanya berada di dalam wilayah Indonesia, tetapi juga di seluruh dunia.

UU PDP memberikan sanksi administratif dan pidana bagi pelaku kejahatan siber yang melanggar ketentuan perlindungan data pribadi, termasuk phising. Sanksi administratif yang dapat diberikan antara lain teguran, peringatan, denda administratif, pencabutan izin usaha, dan/atau pembekuan kegiatan usaha. Pelaku kejahatan siber yang melakukan phising dapat dikenai sanksi pidana sesuai dengan Pasal 67 UU PDP, dengan ancaman pidana penjara maksimal 5 tahun dan/atau denda maksimal 5 miliar rupiah. Phising merupakan suatu tindakan penipuan daring (*online*) yang dilakukan dengan memalsukan identitas atau data pribadi seseorang, dengan maksud untuk memperoleh keuntungan atau data pribadi korban. Jika tindakan phising tersebut mengumpulkan atau memperoleh data pribadi korban yang bukan milik pelaku dengan cara melawan hukum, maka dapat dianggap sebagai suatu tindakan yang melanggar Pasal 67 Undang-undang Perlindungan Data Pribadi Tahun 2022.

Jika tindakan pidana dilakukan oleh perusahaan, maka pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau perusahaan itu sendiri dapat dikenai pidana. Selain pidana penjara dan/atau denda, pidana tambahan seperti perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari tindak pidana dan pembayaran ganti rugi juga dapat dijatuhkan. Terpidana memiliki waktu satu bulan setelah putusan untuk membayar pidana denda, dan jika tidak membayar dalam waktu yang ditentukan, harta kekayaan atau pendapatan terpidana dapat disita dan dilelang oleh jaksa.

Adanya UU PDP dan Lembaga Otoritas Perlindungan Data Pribadi, diharapkan pemerintah dapat lebih aktif dalam menanggulangi kejahatan siber seperti phising di Indonesia. Pelaku kejahatan siber akan dihukum secara tegas sesuai dengan sanksi administratif dan pidana yang telah ditetapkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam era digital saat ini, keamanan data pribadi menjadi semakin penting terutama dengan adanya ancaman kejahatan siber seperti phising melalui media sosial seperti *WhatsApp*, *Instagram*, *Line*, dan media sosial lainnya. Oleh karena itu, Lembaga Otoritas Perlindungan Data Pribadi diharapkan bisa berkomunikasi dan bekerjasama dengan perusahaan swasta, untuk pelaku usaha marketplace, *e-commerce*, dan ekspedisi untuk meningkatkan perlindungan data pribadi agar masyarakat terhindar dari kejahatan siber tersebut. Dalam hal ini, peran media massa juga sangat penting untuk memberikan edukasi kepada masyarakat mengenai bahaya phising dan bagaimana cara mencegahnya. Secara keseluruhan, Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi dan upaya pemerintah dalam menegakkan undang-undang ini sangat penting dalam menanggulangi praktik phising di Indonesia. Dengan adanya perlindungan data pribadi yang kuat, kerjasama antara lembaga pemerintahan maupun organisasi dan perusahaan dengan

sosialisasi yang tepat, masyarakat akan lebih waspada dan berhati-hati dalam melindungi data pribadinya, sehingga praktik phising dapat dihindari dan ditekan. UU PDP di Indonesia memberlakukan kewajiban pada perusahaan yang mengumpulkan, memproses, menyimpan, atau mengirimkan data pribadi, dan memberikan sanksi bagi penanganan data pribadi yang salah. Meskipun belum ada informasi yang jelas mengenai dampak pada kasus phishing di Indonesia, dengan adanya UU PDP ini diharapkan dapat membantu mengurangi jumlah kasus phishing dari waktu ke waktu. Undang-undang tersebut juga diharapkan memiliki dampak yang signifikan pada keamanan siber di Indonesia karena mencakup ketentuan untuk sanksi bagi pengungkapan dan penggunaan data pribadi yang melanggar hukum, serta menyediakan kerangka kerja untuk perlindungan data dan keamanan siber bagi organisasi dan individu.

SIMPULAN

Berdasarkan penulisan-penulisan diatas dapat disimpulkan bahwa perkembangan teknologi dan informasi telah mempermudah akses orang yang tidak bertanggung jawab terhadap informasi pribadi seseorang. Meskipun Indonesia memiliki beberapa regulasi terkait perlindungan data pribadi sebelum adanya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun regulasi tersebut belum cukup spesifik. UU PDP memberikan perlindungan bagi data pribadi seseorang dan memberikan sanksi tegas bagi pelaku kejahatan siber, termasuk pelaku phising. Pemerintah memiliki peran penting dalam melaksanakan UU PDP, termasuk memberikan sanksi bagi pelaku kejahatan siber, memperkuat kerja sama antara lembaga pemerintah dalam bidang keamanan siber, dan memberikan rasa aman dan nyaman bagi masyarakat dalam melakukan transaksi online dan menjaga data pribadi mereka. Lembaga Otoritas Perlindungan Data Pribadi dibentuk pemerintah untuk merumuskan kebijakan dan mengawasi perlindungan data pribadi serta memberikan sanksi administratif dan membantu penegak hukum dalam menangani tindak pidana data pribadi. UU PDP dan tindakan pemerintah yang terkait diharapkan dapat meminimalisir praktik phising dan melindungi data pribadi masyarakat Indonesia.

Menurut pandangan penulis, ada beberapa saran yang dapat diberikan terkait perlindungan data pribadi. Pertama, penting bagi pemerintah dan masyarakat untuk memahami pentingnya melindungi data pribadi dan menerapkan Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi dengan tepat untuk menjamin hak privasi masyarakat. Kedua, perlu dilakukan kesadaran dan edukasi terhadap masyarakat oleh pemerintah untuk melindungi data pribadi mereka dan juga orang lain. Ketiga, pemerintah dan lembaga legislatif harus melakukan evaluasi berkala terhadap peraturan-peraturan yang berkaitan dengan

perlindungan data pribadi dan melakukan perubahan jika diperlukan. Terakhir, pemerintah juga harus meningkatkan pemahaman tentang teknologi dan memberikan dukungan yang memadai untuk menegakkan hukum terkait kejahatan siber seperti Phising.

DAFTAR PUSTAKA

Satjipto Raharjo, "*Ilmu hukum",* (Bandung: Pt. Citra Aditya Bakti, 2000).

Bambang Sunggono, "*Metodologi Penelitian Hukum*" (Jakarta: Raja Grafindo Persada, 2016).

Hendro Setyo Wahyudi, Mita Puspita Sukmasari. "Teknologi dan Kehidupan Masyarakat" Jurnal Analisa Sosiologi, Volume 3, Nomor 1, (2014).

Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia.", Yustisia Jurnal Hukum, Volume 5, Nomor 1 (2016).

Margareta Rosa Anjani dan Budi Santoso. "Urgensi Rekonstruksi Hukum E-commerce di Indonesia", Jurnal Law Reform, Volume 14, Nomor 1, (2018).

Dian Ekawati, "Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan.", UNES Law Review, Volume 1, Nomor 2 (2018)

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime", Journal of Education and Information Communication Technology, Volume 1, Nomor 1, (2017).

Siti Yuniarti, "Perlindungan Hukum Data Pribadi di Indonesia", Jurnal Becoss, Volume 1, Nomor 1, (2019).

Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia." Jurnal Cakrawala Hukum, Volume 10, Nomor 2, (2019).

Evelyn Angelita Pinondang Manurung, dan Emmy Febriani Thalib. "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022." Jurnal Hukum Saraswati (JHS), Volume 4, Nomor 2, (2022).

Rhesita Yustitiana "Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian Dari Upaya Penegakan Hukum Di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum" Jurnal Hukum Visio Justisia Volume 1 Nomor 1, (2021).

Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nabawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik.", PAMPAS: Journal Of Criminal, Volume 1, Nomor 2, (2020)

Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," Jurnal

Saintkom, Volume 13, Nomor 3, (2014)

Confido, Jemy Vestius. Urgensi hukum bagi penyelenggara platform e-commerce di Indonesia. Diss. Universitas Pelita Harapan, (2019).

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan.

Peraturan Menteri Komunikasi dan Informatika RI Nomor 20 Tahun 2016.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

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

N.P. Singh "Online Frauds in Banks with Phishing," Journal of Internet Banking and Commerce 12, no. 2 (2007): 4 https://www.icommercecentral.com/open-access/online-frauds-in-banks-with-phishing.php?aid=38493

Tim, CNBC Indonesia, "Jangan Klik Pesan WhatsApp ini atau Data Kamu Dirampok!", https://www.cnbcindonesia.com/tech/20220103090734-37-303996/jangan-klik-pesan-whatsapp-ini-atau-data-kamu-dirampok

DPR RI, "Sampaikan Penjelasan di Sidang Uji Materi UU PDP, Supriansa: Perlu Adanya Sosialisasi Agar Tidak Salah Tafsir" https://www.dpr.go.id/berita/detail/id/42974/t/Sampaikan+Penjelasan+di+Sidang+Uji+Materi+UU+PDP%2C+Supriansa%3A+Perlu+Adanya+Sosialisasi+Agar+Tidak+Salah+Tafsir