Abdurrauf Science and Society
Vol. 1, No. 4, 2025, pp. 800~811
ISSN: 3090-093X; DOI: 10.70742/asoc.v1i4.283

Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana *Phising* Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia

Criminal Law Policy for Combating Phishing Crimes Through the Personal Data Protection Act: Comparative Study of Indonesia and Malaysia

Rohmah Dwi Cahyaningsih[1]*, Anis Fauzan[2], Saupi Hasbi[3], Atik Winanti[4]
[1,2,3,4]Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
Email: fazajusticia@gmail.com

ARTICLE INFO

Article history:

Received 30-05-2025
Accepted 24-06-2025
Published 25-06-2025

Keywords:

Phising;
Personal Data Protection;
Criminal Policy

Corresponding Email:

fazajusticia@gmail.com

Competing interest:
The author(s) have declared that no competing interests exist

ABSTRACT

Phishing is a digital crime that targets victims' sensitive information or data via email, social media posts, or text messages. This research on phishing focuses on the criminal law policies regulated in Indonesia and Malaysia as a preventive effort against phishing. In order to examine these issues, this study employs a normative research method with a statute-based approach, a conceptual approach, and a comparative approach. The legal comparison is conducted on personal data protection regulations applicable in Indonesia and Malaysia, namely Indonesia's Law No. 27 of 2022 on Personal Data Protection (UU PDP) and Malaysia's Personal Data Protection Act (PDPA) 2010 (Act 709) as amended by the Personal Data Protection (Amendment) Act 2024 (Act A1727). The objectives of this study are to analyze the criminal policies of Indonesia and Malaysia in addressing phishing crimes and to identify gaps in existing regulations. The findings indicate that criminal sanctions under personal data protection law in Indonesia are more severe than in Malaysia. Violations of the Indonesian PDP Law carry a maximum prison sentence of 4 to 6 years and a fine between IDR 4,000,000,000 and IDR 6,000,000,000. In contrast, Malaysia stipulates lighter criminal sanctions, with a maximum prison term of 1 to 3 years, and the 2024 amendments to the PDPA (Act A1727) impose a maximum fine of RM 1 million. Moving forward, policy responses to address phishing crimes must emphasize three key aspects: first, institutional strengthening of the body responsible for enforcing personal data protection in Indonesia; second, enhanced international cooperation in law enforcement; and third, the establishment of victim protection mechanisms through compensation frameworks.

Citation: Cahyaningsih, R. D., Fauzan, A., Hasbi, S., & Winanti, A. (2025). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia. *Abdurrauf Science and Society*, *1*(4), 800–811. https://doi.org/10.70742/asoc.v1i4.283

ABSTRAK

Phishing adalah kejahatan digital yang menargetkan informasi atau data sensitif korban melalui email, unggahan media sosial, atau pesan teks. Penelitian tentang phising ini difokuskan pada kebijakan hukum pidana yang diatur di Indonesia dan Malaysia sebagai upaya pencegahan phising. Dalam rangka mengkaji mengenai hal tersebut penelitian ini menggunakan metode penelitian normatif dengan pendekatan perundang- undangan (*statute approach*), pendekatan konsep (*conseptual approach*), dan pendekatan perbandingan. Perbandingan hukum dilakukan pada regulasi perlindungan data pribadi yang berlaku di Indonesia dan Malaysia yaitu dalam UU Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan *Personal Data Protection Act* (PDPA) 2010 (*Act* 709) serta Akta A1727 Akta Perlindungan Data Peribadi (Pindaan) 2024. Tujuan dari penelitan ini untuk menganalisis kebijakan kriminal Indonesia dan Malaysia dalam menanggulangi tindak pidana phising. Selain itu, untuk mengidentifikasi kesenjangan dalam regulasi yang ada. Hasil penelitian menemukan sanksi pidana dalam undang-undang perlindungan pribadi di Indonesia lebih tinggi daripada di Malaysia. Sanksi pidana terhadap pelanggaran UU PDP adalah penjara maksimum 4 s.d.6 tahun dan denda maksimum antara Rp4.000.000.000,-s.d. Rp6.000.000.000,-. Malaysia mengatur sanksi pidana yang lebih rendah yaitu maksimum 1 s.d. 3 tahun, sedangkan berdasarkan Amandemen *Personal Data Protection Act* (PDPA) 2010 (Act 709) tahun 2024 yang tercantum Akta A1727 Akta Perlindungan Data Peribadi (Pindaan) 2024 pidana denda menjadi RM 1 Juta. Kebijakan dalam penanggulangan tindak pidana phishing pada masa yang akan datang perlu menekankan pada tiga aspek yaitu, kelembagaan yang bertanggung jawab dalam pelaksanaan perlindungan data pribadi di Indonesia, kerjasama Internasional dalam penegakkan hukum, dan mekanisme perlindungan korban melalui ganti rugi.

Kata kunci: Phising; Perlindungan Data Pribadi; Kebijakan Pidana

PENDAHULUAN

Transformasi digital memberikan kemudahan bagi aktivitas masyarakat. Lebih dari itu transformasi digital telah menghilangkan batas teritorial negara sehingga memberikan kemudahan dalam transaksi perdagangan maupun komunikasi. Di era digital orang-orang semakin banyak berbagi informasi pribadi terutama melalui media sosial. Kemajuan bidang teknologi informasi seperti laiknya mata uang yaitu di satu sisi mengatasi hambatan waktu dan jarak, namun disisi lain transfer data pribadi menimbulkan masalah bagi hak privasi individu.

Dunia digital berkembang dan berevolusi dengan cepat, dan penjahat di dunia maya bertransformasi dengan cara baru yaitu mengandalkan penggunaan data digital secara illegal terutama informasi pribadi untuk menimbulkan kerugian pada individu (Alkhalil et al., 2021). Perubahan yang signifikan dalam bidang teknologi informasi memicu kejahatan berbasis siber (*cybercrime*). Peter Stephenson sebagaimana dikutip Muhammad Agus Fajar Syaefudin berpendapat bahwa, *Cybercrime* adalah *The easy definition of cybercrime is crimes directed at a computer or a computer system. Then nature of cybercrime however, is far more complex. As we will see later, cybercrime can take the form of simple snooping into a computer system for which we have no authorizon. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system*. "Definisi dari Kejahatan dunia maya (*cybercrime*) adalah yang dikendalikan dari komputer atau sistem komputer, tetapi bentuk asli dari *cybercrime* jauh lebih rumit. Seperti yang akan kita lihat nanti, kejahatan dunia maya dapat berupa pengintaian sederhana ke dalam sistem komputer yang tidak memiliki izin. Kejahatan tersebut dapat membuat virus komputer lebih liar. Bisa jadi itu sebuah kejahatan perusakan oleh ketidakpuasan karyawan atau mungkin tindakan pencurian data, uang, atau informasi penting menggunakan sistem data" (Syaefudin et al., 2021).

Pada tahun 2024 Indonesia mengalami serangan siber pada sektor pemerintahan maupun bisnis yang berdampak luas. Dua kasus serangan siber yang menjadi perhatian publik pada tahun lalu adalah serangan *ransomware* pada sistem Bank Syariah Indonesia dan Pusat Data Nasional yang mengancam kebocoran data pada kedua entitas tersebut. Salah satu bentuk serangan di dunia siber yang marak saat ini adalah *phising*. Badan Siber dan Sandi Negara mencatat sepanjang tahun 2024 telah terjadi aktivitas yang diindikasikan sebagai phishing di Indonesia sebanyak 26.771.610 aktivitas (Badan Siber dan Sandi Negara, 2024). *Phishing* adalah salah satu bentuk ancaman siber yang dilakukan dengan cara membuat tampilan atau sistem yang menyerupai sistem asli untuk menipu korban. Melalui serangan ini, pelaku berusaha mencuri data kredensial, seperti *username* dan *password*, atau informasi sensitif lainnya dengan menggunakan komunikasi yang tampak sah, seperti *email*, situs web, atau pesan instan yang mengancam (Badan Siber dan Sandi Negara, 2024).

Pesatnya perkembangan pengguna internet di Asia Tenggara tidak hanya berdampak pada kemajuan ekonomi kawasan, namun menimbulkan potensi serangan siber. Negara-negara Asia Tenggara menghadapi ancaman kejahatan siber karena menjadi target operasi penjahat mayantara. Laporan Kaspersky, sebuah perusahaan keamanan siber dan privasi digital global, menyebutkan adanya upaya phishing keuangan yang menargetkan bisnis di wilayah Asia Tenggara terdeteksi di Thailand (247.560), Indonesia (85.908), dan Malaysia (64.779) (Purnama, 2025). Serangan siber ini tidak hanya menimbulkan kerugian secara individu, namun berpotensi menimbulkan kerugian secara ekonomi. Kementerian Komunikasi dan Informatika menyebutkan perkiraan kerugian secara global akibat serangan siber diperkirakan mencapai US$9,5 triliun atau sekitar Rp156.018 triliun (dengan asumsi kurs Rp16.423) (Anggraeni, 2024). Malaysia mengalami kerugian yang cukup besar akibat *cybercrime* pada tahun 2024 mencapai RM1.57 *bilion* (Azil, 2025).

Kemudahan mengakses internet tidak diiringi dengan kesadaran pengguna untuk melakukan perlindungan data pribadinya. Para pengguna media sosial bahkan cenderung tidak peduli untuk mengungkapkan informasi sensitif mereka di internet. Belum ada kesadaran mengenai informasi yang dibagikan melalui internet terutama di media sosial, sedangkan tindakan yang dilakukan memiliki risiko terkena pelanggaran data atau pencurian. Pengguna mengunggah gambar mereka ke media sosial seperti *Facebook*, *WhatsApp* dan mayoritas menganggap dapat diterima untuk memberi label pada gambar dengan nama mereka, nama teman maupun tempat pengambilan gambar (Ananthan & Zolkipli, 2022). Saat ini media sosial memiliki daya tarik bagi semua golongan masyarakat, sehingga menimbulkan terekspos nya data pribadi tanpa sepengetahuan pemilik akun. Berbagai bentuk serangan siber terutama phising menimbulkan kebutuhan akan regulasi yang efektif dalam melindungi data pengguna di dunia maya semakin mendesak.

Kejahatan siber merupakan fenomena sosial yang akan terus berkembang mengikuti kemajuan teknologi. Penanggulangan kejahatan siber diperlukan untuk membangun sistem penanggakan hukum yang responsif terhadap kemajuan zaman. Tidak dapat dipisahkan antara pemidanaan terhadap pelaku tindak pidana berbasis siber dengan kebijakan perlindungan sosial. Hakikatnya pembuatan undang-undang pidana merupakan bagian integral dari usaha perlindungan sosial (Arief, 2010). Lebih lanjut Barda Nawawi Arief, upaya penanggulangan *cybercrime*, dapat dilihat dari bererapa prespektif hukum pidana antara lain aspek pertanggungjawaban pidana atau

pemidanaan (termasuk aspek pembuktian), aspek kriminalisasi yang berkaitan dengan formulasi perbuatan dan aspek kewenangan dalam mengadili (Nur et al., 2023).

Penelitian-penelitian sebelumnya digunakan sebagai dasar pijakan untuk memberikan pembaharuan dalam penelitian ini. Penelitian terkait perlindungan data pribadi yang ditulis oleh Ananta Fadli Sutarli dan Shelly Kurniawan, pada 2023 dengan judul Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi *Phising* di Indonesia. Penelitian ini menjelaskan mengenai ketentuan-ketuan dalam Undang-Undang Perlindungan Data Pribadi untuk memberikan perlindungan dari tindak pidana phising. Berbeda dengan penelitian Ananta Fadli Sutarli, penelitin ini menggunakan pendekatan perbandingan dengan *Personal Data Protection Act* (PDPA) 2010 (*Act* 709).

Penelitian lain yang menjadi rujukan adalah penelitian dengan judul 'Urgensi Penguatan Implementasi terkait Pelindungan Data Pribadi bagi Pemodal Sektor Jasa Keuangan *Equity Crowdfunding* di Indonesia (Studi Komparas terhadap Negara Malaysia)'. Penelitian yang dibuat oleh Salwa Naya Syakirah dan Haipa Nisrina Sayyida, membandingkan Undang-Undang Perlindungan Data Pribadi Indonesia dan Malaysia. Penelitian ini memiliki obyek yang berbeda yaitu mengenai kebijakan kriminal yang terkait tindak pidana *phising*, sedangkan penelitian Salwa Naya Syakirah yang dimuat di Padjadjaran *Law Review* memfokuskan pada sektor jasa keuangan.

Penelitian ini bertujuan untuk menganalisis kebijakan kriminal Indonesia dan Malaysia dalam menanggulangi tindak pidana phising. Selain itu juga untuk mengidentifikasi kesenjangan dalam regulasi yang ada. Dengan menganalisis regulasi antara Indonesia dan Malaysia, penelitian ini akan memberikan pemahaman yang komprehensif dalam menghadapi tantangan dalam implementasi pelindungan data pribadi dan rekomendasi yang dapat memperkuat kebijakan kriminal di era digital.

METODE

Mendasarkan pada kondisi tersebut diatas, penelitian ini menggunakan metode penelitian normatif yang mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan atau putusan pengadilan serta norma-norma yang hidup dan berkembang dalam masyarakat. Dari segi pendekatan penelitian hukum, dalam penelitian hukum normatif umumnya meliputi pendekatan perundang- undangan (*statute approach*), pendekatan konsep (*conseptual approach*), dan pendekatan perbandingan. Pendekatan konsep digunakan untuk memahami konsep-konsep pernormaan dalam suatu peraturan perundang-undangan apakah telah sesuai dengan ruh yang terkandung dalam konsep hukum yang mendasarinya (Irwansyah, 2022).

Sumber bahan hukum yang digunakan berupa bahan hukum primer diperoleh dari risalah perundang-undangan, naskah akademik, dan undang-undang. Bahan hukum sekunder yaitu data yang diperoleh dari dokumen-dokumen resmi, hasil-hasil penelitian dalam bentuk jurnal. Bahan hukum tersier adalah petunjuk atau penjelasan mengenai bahan hukum primer ataupun bahan hukum sekunder yang berasal dari berita, majalah, surat kabar. Adapun untuk melakukan analisisnya akan dilakukan dengan pendekatan deduktif-induktif yaitu dengan cara menarik kesimpulan dari suatu permasalahan yang bersifat umum terhadap suatu permasalahan yang secara spesifik menjadi obyek suatu penelitian. Selain menganalisis secara analisis preskriptif bahan hukum yang diperoleh akan dilakukan untuk memberikan rekomendasi langkah kedepannya.

Metode penelitian yang digunakan dalam penulisan ini adalah penelitian normatif dengan pendekatan yaitu pendekatan undang-undang dengan menelaah terhadap

regulasi dan asas serta teori terkait isu yang dihadapi. Penelitian ini juga menganalisis bahan-bahan hukum berupa bahan hukum primer dan bahan hukum sekunder dengan menggunakan pendekatan deduktif-induktif yaitu dengan cara menarik kesimpulan dari suatu permasalahan yang bersifat umum terhadap suatu permasalahan yang secara spesifik menjadi obyek suatu penelitian.

HASIL DAN PEMBAHASAN

Pengaturan Sanksi Pidana dalam Undang-Undang Perlindungan Data Pribadi di Indonesia dan Malaysia

Serangan siber dalam bentuk *phishing* bertujuan untuk mengambil data kredensial atau informasi sensitif milik penggunan internet. Pelaku memodifikasi media sosial atau *website* sehingga mudah untuk pelaku mengambil data privasi pengguna *platform* digital. Guna melancarkan aksinya pelaku menggunakan *link* ataupun *icon*. *Phishing* sering terjadi pada *platform* media sosial *WhatsApp* dan *Facebook* yang digunakan dengan mengatasnamakan instansi resmi dan seolah-olah bertindak dari pegawai instansi tersebut, sehingga tanpa disadari pemilik akun mengikuti perintah pelaku (Putra et al., 2023).

Sebelum UU PDP disahkan, pelaku *phishing* dikenakan Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Secara eksplisit pengaturan data pribadi dalam UU ITE diatur dalam Pasal 26 ayat (1) Undang-Undang ITE yang mensyaratkan persetujuan pemilik data pribadi apabila informasi yang terdapat dalam media elektronik akan digunakan. Dalam penegakan hukum terhadap kasus *phising* digunakan Pasal 35 UU ITE, dalam beberapa kasus mengenai *phishing* (Y., 2021). Pasal ini mengandung unsur dengan sengaja dan tanpa hak atau melawan hukum Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan, Informasi Elektronik dan/atau Dokumen Elektronik yang bertujuan Informasi Elektronik dan/atau Dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Pengaturan mengenai perlindungan data pribadi di Indonesia baru disahkan pada tahun 2022 dengan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dibandingkan negara di kawasan Asia Tenggara, Indonesia tertinggal dalam memberikan "payung" hukum bagi penganturan data pribadi. UU PDP telah mengakui subjek hukum tidak hanya perorangan, namun juga korporasi. Regulasi ini tidak hanya mengatur perbuatan-perbuatan yang dilarang dan mempertegas dengan dengan ketentuan sanksi pidana. Pembentuk undang-undang memformulasikan adanya saksi tidak hanya untuk memberikan efek jera, namun untuk mengedukasi perilaku masyarakat agar lebih menghargai hak privasi atas data pribadi.

UU PDP mengatur perbuatan yang dilarang dalam menggunakan data pribadi yaitu (Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022):

1. memperoleh atau mengumpulkan data pribadi yang bukan miliknya;
2. mengungkapkan data pribadi yang bukan miliknya;
3. menggunakan data pribadi yang bukan miliknya;
4. membuat data pribadi palsu atau memalsulkan.

Formulasi perbuatan yang dilarang terkait dengan data pribadi telah diatur secara eksplisit dalam regulasi ini. Secara eksplisit sanksi pidana dalam UU PDP, sebagai berikut:

Tabel 1. Rumusan Perbuatan dan Sanksi Pidana dalam UU PDP

Pasal	Rumusan Perbuatan	Pidana
Pasal 67 ayat (1)	Dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.	Pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
Pasal 67 ayat (2)	dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya.	pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).
Pasal 67 ayat (3)	dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya.	paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000,00 (lima miliar rupiah)
Pasal 68	dengan sengaja membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain	pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah)

Pelaku yang melakukan perbuatan yang dilarang dalam UU PDP dapat dikenai sanksi tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh atau merupakan hasil tindak pidana, serta kewajiban untuk membayar ganti kerugian Secara khusus UU PDP mengatur pidana yang dapat dikenakan kepada korporasi yang melakukan pelanggaran terhadap undang-undang ini yaitu pidana denda dengan ketentuan maksimum 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan. Pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasinya. Tidak hanya pidana denda, korporasi dapat dijatuhi pidana tambahan berupa (Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022):

a. perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
b. pembekuan seluruh atau sebagian usaha Korporasi;
c. pelarangan permanen melakukan perbuatan tertentu;
d. penutupan seluruh atau sebagian tempat usaha dan/ atau kegiatan Korporasi;
e. melaksanakan kewajiban yang telah dilalaikan;
f. pembayaran ganti kerugian;
g. pencabutan izin; dan/atau
h. pembubaran Korporasi.

pemidanaan merupakan upaya yang signifikan dalam penegakan perlindungan data pribadi, mengingat potensi dampak yang sangat besar bagi individu dan masyarakat jika hak tersebut dilanggar.

Malaysia telah memiliki Undang-Undang Perlindungan Data Pribadi sejak tahun 2010, namun diberlakukan pada Desember 2013. Berbeda dengan UU PDP Indonesia yang berlaku pada sektor publik, *Personal Data Protection Act* (PDPA) 2010 (*Act* 709)

hanya berlaku pada sektor komersil. Selain terbatas pada transaksi komersial, bahkan tidak berlaku untuk transaksi yang membantu fungsi regulasi (Aw & Lai, 2024). Ruang lingkup keberlakukan PPDA berbeda dengan UU PDP Indonesia yang menetapkan bahwa undang-undang ini berlaku bagi setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum di wilayah hukum Indonesia atau yang menimbulkan akibat hukum di Indonesia, termasuk pengolahan data pribadi di sektor publik maupun swasta. Pembatasan ini berpotensi menciptakan celah dalam perlindungan data pribadi warga negara, terutama dalam memastikan standar perlindungan data yang komprehensif di Malaysia (Sukerta & Sutrisno, 2024). PDPA mengatur Prinsip Perlindungan Data Pribadi antara lain Prinsip Perlidungan Data Peribadi, Prinsip Am, Prinsip Notis dan Pilihan, Prinsip Penzahiran, Prinsip Keselamatan, Prinsip Penyimpanan, Prinsip Integriti Data, dan Prinsip Akses.

Personal Data Protection Act (PDPA) mengatur adanya sanksi berupa denda dan pidana penjara bagi setiap orang yang melanggar ketentuan perlindungan data pribadi. Dalam PDPA terdapat beberapa ketentuan pidana yang mengatur pelanggaran data pribadi. Misalnya, pelanggaran terhadap prinsip perlindungan data pribadi sebagaimana diatur dalam Seksyen 5 ayat (3) dapat dikenakan sanksi denda hingga tiga ratus ribu ringgit atau pidana penjara selama tidak lebih dari dua tahun, atau keduanya. Selain itu, memproses data pribadi tanpa sertifikat pendaftaran sesuai Seksyen 16 ayat (4) dapat dikenai denda maksimal lima ratus ribu ringgit atau pidana penjara hingga tiga tahun, atau keduanya.

Praktik ketidakpatuhan terhadap peraturan bagi pengguna data diatur dalam Seksyen 29, dengan sanksi berupa denda tidak melebihi seratus ribu ringgit atau pidana penjara sampai satu tahun, atau keduanya. Penolakan untuk mematuhi permintaan koreksi data sebagaimana diatur dalam Seksyen 37 ayat (4) juga dapat dikenakan denda hingga seratus ribu ringgit atau pidana penjara selama satu tahun, atau keduanya. Penarikan persetujuan untuk memproses data pribadi diatur dalam Seksyen 38 ayat (4) dengan sanksi serupa.

Pengolahan data pribadi yang sensitif diatur dalam Seksyen 40 ayat (3), dengan ancaman denda hingga dua ratus ribu ringgit atau pidana penjara hingga satu tahun, atau keduanya. Menghalangi pemrosesan yang dapat menyebabkan kerusakan atau kesusahan diatur dalam Seksyen 42, dengan sanksi denda hingga dua ratus ribu ringgit atau pidana penjara hingga dua tahun, atau keduanya. Hak untuk mencegah pemrosesan data untuk tujuan pemasaran langsung diatur dalam Seksyen 43 ayat (4) dengan sanksi yang sama.

Ketidakpatuhan terhadap pemberitahuan penegakan hukum diatur dalam Seksyen 108 ayat (8), dengan ancaman denda hingga dua ratus ribu ringgit atau pidana penjara sampai dua tahun, atau keduanya. Menghalangi petugas yang berwenang diatur dalam Seksyen 120, dengan sanksi pidana penjara hingga satu tahun, denda hingga sepuluh ribu ringgit, atau keduanya. Pemindahan data pribadi ke luar Malaysia tanpa izin sesuai ketentuan Menteri diatur dalam Seksyen 129 ayat (5), dengan ancaman denda hingga tiga ratus ribu ringgit atau pidana penjara hingga dua tahun, atau keduanya.

Pengumpulan data pribadi yang melanggar hukum diatur dalam Seksyen 130 ayat (7), dengan sanksi denda hingga lima ratus ribu ringgit atau pidana penjara hingga tiga tahun, atau keduanya. Terakhir, pembantuan dan percobaan tindak pidana diatur dalam Seksyen 131 ayat (1) dan (2), di mana pelaku percobaan dihukum sesuai dengan perbuatan yang dilanggar, sedangkan pelaku pembantuan dapat dikenai sanksi setengah dari pidana maksimum.

Malaysia saat ini telah melakukan amandemen PPDA pada tahun 2024 dengan disahkannya Akta A1727 Akta Perlindungan Data Peribadi (Pindaan) 2024. Amandemen PPDA akan mulai berlaku pada bulan Juni 2025. Undang-undang baru ini mengubah ketentuan denda dalam pelanggaran terhadap prinsip-prinsip perlindungan pribadi menjadi 1 juta ringgit dari maksimum sebelumnya 300.000 ringgit.

UU PDP dan PPDA memiliki perbedaan dalam formulasi pemidaan terutama dalam lamanya pidana penjara. Hukum Malaysia mengatur pidana penjara antara dua-tiga tahun artinya lebih rendah dari Indonesia yang mencapai maksimum enam tahun. Dilihat dari aspek denda, denda yang dapat dikenakan juga lebih tinggi daripada Malaysia. Namun dengan Amandemen PPDA tahun 2024 yang tercantum Akta A1727 Akta Perlindungan Data Peribadi (Pindaan) 2024 pidana denda mengalami kenaikan yang cukup signifikan menjadi RM 1 juta atau dapat dikatakan pemerintah Malaysia serius menggunakan hukum pidana sebagai upaya penanggulangan pelanggaran data pribadi. Tidak cukup menaikkan denda, Malaysia perlu memperbaiki celah penegakan hukum perlindungan data pribadi dengan penerapan denda maksimum yang lebih ketat yang didasarkan pada persentase omzet perusahaan, seperti di Uni Eropa (Aw & Lai, 2024).

Penjatuhan pidana kepada pelaku tindak pidana harus sepadan dengan tindak pidananya. Andrew von Hirsh sebagaimana dikutip Muhammad Ainul Syamsul, kesepadanan bertujuan memenuhi prinsip keadilan. *The principle of proportionalty that sanctions be proportionate in their severity to gravity of offence-appears to be requirement of justice*. Ketidaksepadanan antara pidana dan ancaman pidana dapat menghilangkan fungsi kecaman (*censure*) yang terkandung dalam pidana (Syamsu, 2015). Perumusan pada sanksi pidana dalam suatu peraturan perundang-undangan dipengaruhi oleh politik hukum penyusunan regulasi. Di Indonesia ancaman pidana penjara maksimum enam tahun yang di atur dalam UU PDP sudah cukup tinggi. Tidak mengabaikan fungsi kecaman dalam pidananya, namun jika dilihat dari naskah akademik UU PDP, pembentuk undang-undang memformulasikan pemidanaan tidak hanya untuk penjeraan terhadap pelaku. Tujuan lain yang hendak dicapai dari UU PDP adanya perubahan perilaku masyarakat agar lebih peduli dengan data pribadi.

Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana *Phising* pada Masa Yang Akan Datang

Pada tahun 2022 sebuah studi yang dilakukan oleh ISEAS – Institut Yusof Ishak menganalisa regulasi perlindungan pribadi di negara-negara Asia Tenggara. Berdasarkan riset tersebut ditemukan kualitas hukum perlindungan data pribadi di negara-negara Asia Tenggara belum merata. Regulasi perlindungan data pribadi yang baik memiliki substansi persyaratan yang mengatur pengumpulan, penggunaan, pengungkapan, dan perawatan data pribadi di suatu negara. Hal ini bertujuan untuk melindungi data pribadi individu, disisi lain sektor publik dan swasta dapat mengumpulkan, menggunakan, atau mengungkapkan data pribadi untuk tujuan yang sah dan wajar (Suvannaphakdy, 2022). Negara ASEAN yang telah menerapkan regulasi perlindungan data pribadi yang komprehensif adalah Filipina.

Perbaikan terhadap kerangka regulasi secara berkesinambungan diperlukan untuk mengantisipasi modus baru serangan siber. Kejahatan siber khusunya *phishing* menimbulkan kerugian ekonomi negara jika dibiarkan tanpa perhatian khusus. Perilaku *Phisher* yang menyamar sebagai entitas yang terpercaya atau sah dalam sebuah komunikasi elektronik, seperti situs pemerintah, perbankan, perusahaan, atau situs web populer dapat menurunkan kepercayaan publik (Sutarli & Kurniawan, 2023). Oleh karena

itu perlu diperlukan penegakkan hukum yang menyeluruh tidak hanya dari segi substansi, namun juga dari aspek kelembagaan, dan kerjasama internasional.

Pertama, dari aspek kelembagaan UU PDP telah mengamanatkan pembentukan lembaga yang bertanggung jawab dalam pelaksanaan perlindungan data pribadi di Indonesia yaitu Lembaga Otoritas Perlindungan Data Pribadi (LOPDP). Lembaga ini memiliki tugas antara lain:

1. perumusan dan penetapan kebijakan dan strategi Pelindungan Data Pribadi yang menjadi panduan bagi ' Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Fribadi;
2. pengawasan terhadap penyelenggaraan Pelindungan Data Pribadi;
3. penegakan hukum administratif terhadap pelanggaran Undang-Undang ini; dan
4. fasilitasi penyelesaian sengketa di luar pengadilan.

Pembentukan lembaga ini menjadi kunci dalam melakukan penegakkan kepatuhan standar dan kewajiban PDP, dari pengendali dan prosesor data. Sampai saat ini kelembagaan pengawas perlindungan data di Indonesia masih dalam tahap pembentukan, masih menunggu keputusan Presiden untuk dapat beroperasi secara resmi. Berbeda dari Indonesia Malaysia telah membentuk *Personal Data Protection Department* (JPDP) sejak 2011, yang berkedudukan berada di bawah Kementerian Digital. PDPA turut mengamanatkan adanya pembentukan Komite Penasihat PDP, hal ini dimuat dalam *Part IV Personal Data Protection Advisory Comittee*. Komisi ini dikenal juga dengan sebutan *Personal Data Protection Comission* (PDPC), sebagai jabatan yang diisi orang perseorangan. Komisi ini bertugas dalam penegakan ketentuan PDPA dengan tugas memberi nasihat kepada Komisaris perihal pelindungan data pribadi,penegakan administrasi dan undang-undang, dan memberi nasihat pada Komisaris terhadap perihal yang dirujuk kepada Komisi Penasihat Perlindungan Data Pribadi (Syakirah & Sayyidah, 2024). Lembaga Perlindungan Data Pribadi memiliki yang strategis, sebaiknya dibentuk lembaga independen dan tidak dibawah lembaga lain.

Kedua, aspek kerjasama Internasional dalam penegakkan hukum. *Phishing* sebagai salah satu bentuk kejahatan siber memiliki tantangan dalam penegakkan hukumnya karena kejahatan siber dapat dilakukan lintas negara. Hal ini menimbulkan persoalan mengenai yuridiksi untuk menuntut pelaku. Kerjasama regional ditingkat Asia Tenggara di tingkat internasional, terutama dalam mendukung proses pembuktian dan ekstradisi. Negara-negara seperti Amerika Serikat dan Uni Eropa telah mengadopsi kebijakan keamanan siber yang komprehensif yaitu melalui *Cybersecurity Information Sharing Act* (CISA) di Amerika Serikat dan *General Data Protection Regulation* (GDPR) di Uni Eropa (Arafat & Wirasto, 2024). Kedua regulasi tersebut memberikan perlindungan data secara ketat dan mendorong kerja sama antarinstansi. Indonesia khususnya dan ASEAN dapat mengambil contoh dari praktek baik yang dilakukan Amerika Serika dan Uni Eropa untuk menjalin kerjasama internasional dalam menanggulangi kejahatan siber dan meningkatkan keamanan siber secara global.

Negara ASEAN telah membentuk ASEAN Regional Forum (ARF) dan ASEAN *Political-Security Community* (APSC) sebagai upaya untuk meningkatan kerjasama dalam hal ancaman non tradisional, yang memfokuskan pada persoalan kejahatan transnasional dan lintas batas. Pada tahun 2006 ARF membentuk ARF *on cybersecurity initiatives* terkait pembahasan kejahatan siber di ASEAN yang dituangkan dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime* (Rosy, 2020). Kerjasama ditingkat regional ini membawa keuntungan bagi Indonesia berupa kontak poin (*point*

of contact) dengan negara-negara di luar anggota yang bekerjasama melalui kerangka kerja ARF. Kerjasama ini akan memberikan kemudahan diplomasi siber Indonesia, termasuk dalam pencegahan dan penegakkan hukum terhadap tindak pidana *phising*.

Ketiga, mekanisme perlindungan korban melalui ganti rugi atau restitusi. Dalam undang-undang perlindungan data pribadi Indonesia dan Malaysia tidak mengatur secara eksplisit ganti rugi atau restitusi kepada korban. Untuk mengakomodasi perlindungan terhadap korban, baik di Malaysia maupun di Indonesia, terdapat beberapa aspek yang diatur dalam perundang-undangan terkait mekanisme ganti rugi atau restitusi. Kedua negara memiliki pendekatan yang berbeda, tetapi ada kesamaan dalam tujuan untuk memberikan perlindungan hukum kepada korban kejahatan atau pelanggaran. Di Malaysia, perlindungan terhadap korban salah satunya diatur dalam Undang-Undang Perlindungan Korban Kejahatan (*Victim Protection Act*) dan Restitusi. Mekanisme restitusi di Malaysia melibatkan pengadilan yang memutuskan nilai kompensasi yang harus diberikan oleh pelaku kepada korban. Akta Perlindungan Korban (*Victim Protection Act 2009*) memberikan perlindungan kepada korban dari intimidasi dan pembalasan dari pelaku. Beberapa putusan pengadilan mengenai kejahatan kekerasan atau yang menimbulkan kerugian finansial, pengadilan dapat memerintahkan pelaku untuk memberikan restitusi langsung kepada korban.

Hukum Malaysia tidak hanya mengatur ganti rugi dari pelaku, tetapi memberikan kewajiban bagi negara memberikan ganti rugi kepada korban kejahatan. Hal ini dimungkinkan jika korban tidak dapat mendapatkan ganti rugi dari pelaku. Korban dapat mengajukan permohonan untuk mendapatkan kompensasi dari negara. Skema pembayaran ganti rugi oleh negara merupakan bentuk dukungan terhadap korban yang menderita kerugian akibat tindakan kriminal, namun pelaku tidak dapat atau tidak mampu membayar.

Di Indonesia, mekanisme perlindungan korban dan restitusi juga diatur dalam undang-undang. Restitusi diatur dalam Pasal 14 Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, yang memberikan hak kepada korban untuk meminta restitusi (ganti rugi) dari pelaku tindak pidana. Pelaku yang tidak mampu membayar, negara dapat memberikan bantuan melalui program yang disediakan. Korban berhak mengajukan permohonan restitusi melalui pengadilan apabila ia menderita kerugian akibat tindak pidana. Jika pelaku tidak mampu membayar, negara dapat menanggung sebagian dari ganti rugi tersebut.

Skema ganti rugi oleh negara, mekanisme untuk memberikan restitusi kepada korban jika pelaku tidak dapat memberikan ganti rugi. Pengajuan restitusi diajukan melalui Lembaga Perlindungan Saksi dan Korban (LPSK). LPSK memberikan dukungan kepada korban, termasuk dalam hal kompensasi finansial, meskipun hal ini terbatas pada jenis kejahatan tertentu, seperti kejahatan terorganisir atau korupsi.

Perbedaan mendasar mekanisme restitusi antara Indonesia terletak pada jenis kejahatannya. Ganti rugi di Malaysia lebih sering diterapkan pada kejahatan kekerasan fisik atau kerugian finansial langsung, dan pengadilan dapat menentukan besaran ganti rugi. Di Indonesia, mekanisme restitusi dan perlindungan korban lebih terintegrasi dengan lembaga negara seperti LPSK yang memberikan bantuan langsung, termasuk bantuan finansial untuk korban yang tidak mendapatkan ganti rugi dari pelaku.

Pengembangan sistem perlindungan yang mengakomodir perlindungan terhadap korban di kedua negara, beberapa langkah yang bisa dipertimbangkan meliputi:

1. Peningkatan akses korban terhadap restitusi dengan memperluas jangkauan restitusi sehingga lebih banyak korban yang bisa memperoleh ganti rugi, bahkan jika pelaku tidak dapat membayar.
2. Pendidikan dan Penyuluhan untuk meningkatkan pemahaman korban tentang hak-hak mereka dan bagaimana cara mengajukan klaim restitusi.
3. Koordinasi antar Lembaga untuk mengoptimalkan koordinasi antara lembaga yang berperan dalam perlindungan korban, seperti lembaga perlindungan saksi dan korban, pengadilan, serta polisi, untuk mempercepat proses restitusi.

Dengan penguatan mekanisme ini, baik di Malaysia maupun Indonesia, korban dapat lebih mudah memperoleh hak-hak mereka, dan rasa keadilan bagi mereka dapat lebih tercapai.

KESIMPULAN

Pengaturan sanksi pidana mengenai perlindungan data pribadi memiliki perbedaan dalam pengenaan minimum sanksi pidana penjara dan denda. Di Indonesia perbuatan yang melanggar Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dapat dipidana dengan pidana penjara maksimum 4 s.d.6 tahun dan denda maksimum antara Rp4.000.000.000-s.d. Rp6.000.000.000,-. Dibandingkan Indonesia, Malaysia mengatur sanksi pidana yang lebih rendah yaitu maksimum 1 s.d. 3 tahun. Amandemen Personal Data Protection Act (PDPA) 2010 (Act 709) pada tahun 2024 yang tercantum Akta A1727 Akta Perlindungan Data Peribadi (Pindaan) 2024 pidana denda mengalami kenaikan yang cukup signifikan dari RM 300.000 menjadi RM 1 juta.

Kebijakan hukum pidana dalam penanggulangan tindak pidana phishing pada masa yang akan datang perlu menekankan pada tiga aspek. Pertama, kelembagaan UU PDP telah mengamanatkan pembentukan lembaga yang bertanggung jawab dalam pelaksanaan perlindungan data pribadi di Indonesia yaitu Lembaga Otoritas Perlindungan Data Pribadi (LOPDP). Kedua, aspek kerjasama Internasional dalam penegakkan hukum. Selanjutnya aspek ketiga, mekanisme perlindungan korban melalui ganti rugi atau restitusi.

DAFTAR PUSTAKA

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*.

Ananthan, T. R., & Zolkipli, M. F. (2022). The Challenges and Issues in Implementing Personal Data Protection. *International Journal of Recent Contributions from Engineering, Science & IT (IJES)*.

Anggraeni, R. (2024, June 27). *Kemenkominfo: Kerugian Serangan Siber Global Ditaksir Rp156 Triliun pada 2024*. Teknologi.Bisnis.Com.

Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. *Equality: Journal of Law and Justice*, *1*(2), 220–241.

Arief, B. N. (2010). *Bunga Rampai Kebijakan hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru)*. Kencana.

Aw, C., & Lai, B. (2024, August 6). *Malaysia Pushes Out Groundbreaking Amendment to Personal Data Protection Act – Impact on Businesses*. Natlawreview.Com.

Azil, F. (2025, January 19). *AISSE' 25: Lebih RM1.22b kerugian akibat jenayah siber, rentas sempadan dicatat pada 2024 – TKSU KDN*. Astroawani.Com.

Badan Siber dan Sandi Negara. (2024). *Lanskap Keamanan Siber Indonesia 2024*. Badan Siber dan Sandi Negara.

Irwansyah. (2022). *Penelitian Hukum Pilihan Metode & Praktik Penulisan Artikel (Edisi Revisi)*. Mirra Buana Media.

Nur, M. S., Puluhuwa, F., & Wantu, F. M. (2023). Kebijakan Penegakan Hukum Dalam Upaya Menangani Cyber Crime Yang Dilakukan Oleh Polri Virtual Di Indonesia. *The Juris*, *7*(2), 464–470.

Purnama, B. E. (2025, March 11). *Lebih dari 500 ribu Serangan Phishing Targetkan Bisnis di Asia Tenggara Selama 2024*. Media Indonesia.

Putra, I. K. O. K., Darmawan, I. M. A., & Juliana, I. P. G. (2023). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phishing. *Cyber Security Dan Forensik Digital*, *5*(2), 77–82.

Rosy, A. F. (2020). Kerjasama internasional Indonesia: memperkuat keamanan nasional di bidang keamanan siber. *Journal of Government Science (GovSci): Jurnal Ilmu Pemerintahan*, *1*(2), 118–129.

Sukerta, P. A. D., & Sutrisno, A. (2024). Perlindungan Data Pribadi di ASEAN: Perbandingan Kritis antara Kerangka Hukum Indonesia dan Malaysia. *Jurnal Constitusional Law Review*, *3*(2).

Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadidalam Menanggulangi Phishing di Indonesia. *Innovative: Journal Of Social Science Research*, *3*(2), 4208–4221.

Suvannaphakdy, S. (2022). *Better Safeguards Needed for Trusted Data Use in ASEAN Countries*. ISEAS-Yusof Ishak Institute.

Syaefudin, M. A. F., Sudewo, F. A., & Rizkianto, K. (2021). *Hukum Siber: Perbandingan Indonesia dan Malaysia*. Penerbit NEM.

Syakirah, S., & Sayyidah, H. (2024). Urgensi Penguatan Implementasi terkait Pelindungan Data Pribadi bagi Pemodal Sektor Jasa Keuangan Equity Crowdfunding di Indonesia (Studi Komparas terhadap Negara Malaysia). *Padjadjaran Law Review*, *12*(1), 109–122.

Syamsu, M. A. (2015). *Penjatuhan Pidana & Dua Prinsip Dasar Hukum Pidana*. Kencana.

Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).

Y., V. F. P. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurnal Juris-Diction*, *4*(6).