PERLINDUNGAN HUKUM TERHADAP KORBAN PENYALAGUNAAN DATA PRIBADI MELALUI PENGIRIMAN UNDANGAN PALSU DI MEDIA SOSIAL

LEGAL PROTECTION FOR VICTIMS OF PERSONAL DATA MISUSE THROUGH SENDING FAKE INVITATIONS ON SOCIAL MEDIA

Elen Josefina
Universitas Sriwijaya
elenjosefina10@gmail.com

Henny Yuningsih
Universitas Sriwijaya
hennyyuningsih@gmail.com

Abstrak

Penelitian ini diberi judul Perlindungan Hukum Terhadap Korban Penyalagunaan Data Pribadi Melalui Pengiriman Undangan Palsu di Media Sosial. Metode yang digunakan dalam penelitian ini adalah metode hukum yuridis normatif. Bahan hukum yang diperoleh dari bahan hukum primer dan sekunder, bahan tersebut akan dianalisis dengan analisis kualitatif dan akan ditarik kesimpulan dengan cara induktif. Berdasarkan hasil penelitian dapat disimpulkan bahwa hasil penelitian menunjukkan bahwa meskipun regulasi sudah ada, penerapan hukum terhadap kejahatan ini masih menghadapi kendala seperti keterbatasan bukti digital, kurangnya kesadaran hukum, dan kompleksitas yurisdiksi. Oleh karena itu, diperlukan sinergi antara aparat penegak hukum, regulator, platform digital, dan masyarakat untuk memperkuat perlindungan korban serta menjaga integritas ruang digital. Penelitian ini memberikan kontribusi penting dalam pengembangan kebijakan dan strategi penegakan hukum yang adaptif terhadap dinamika kejahatan siber di Indonesia. Serta untuk korban penyalahgunaan data pribadi dapat menempuh jalur administratif, pidana, dan perdata untuk mendapatkan perlindungan, pemulihan hak, dan ganti rugi, sehingga memberikan perlindungan yang menyeluruh sekaligus efek jera bagi pelaku.

Kata Kunci: Perlindungan Korban, Undangan Palsu, Media Sosial

Abstract

This research is entitled "Legal Protection for Victims of Personal Data Misuse Through Sending Fake Invitations on Social Media." The method used in this research is normative juridical law. Legal materials obtained from primary and secondary legal sources will be analyzed qualitatively, and conclusions will be drawn inductively. Based on the research results, it can be concluded that despite existing regulations, the implementation of the law against this crime still faces obstacles such as limited digital evidence, lack of legal awareness, and jurisdictional complexity. Therefore, synergy is needed between law

enforcement officials, regulators, digital platforms, and the public to strengthen victim protection and maintain the integrity of the digital space. This research provides an important contribution to the development of adaptive law enforcement policies and strategies to address the dynamics of cybercrime in Indonesia. Victims of personal data misuse can also pursue administrative, criminal, and civil legal channels to obtain protection, rights restoration, and compensation, thus providing comprehensive protection and a deterrent effect for perpetrators.

Keywords : *Victim Protection, Fake Invitations, Social Media*

A. Pendahuluan

Perkembangan teknologi merupakan titik awal dari munculnya revolusi industri 4.0. Perkembangan ini tidak hanya membawa dampak positif dengan memperluas peluang interaksi manusia, tetapi juga menyebabkan perubahan signifikan dalam berbagai aspek kehidupan.[1] Perubahan ini pertama kali dirasakan dalam bidang ekonomi, yang kemudian memicu fenomena disrupsi, terutama dalam konteks bisnis.[2]

Memasuki era globalisasi, di mana Teknologi Informasi dan Komunikasi (TIK) berkembang dengan sangat pesat. Jarak dan waktu kini bukan lagi hambatan dalam berkomunikasi, memungkinkan orang di pulau atau negara yang berbeda untuk berhubungan dengan mudah. Berbagai perangkat elektronik seperti televisi, ponsel, dan laptop telah menjadi hal yang lazim dalam kehidupan masyarakat. Perkembangan TIK semakin cepat dengan hadirnya alat-alat yang lebih canggih. Meskipun kemajuan ini membawa dampak positif, tidak dapat dipungkiri bahwa ada juga dampak negatif yang dirasakan oleh penggunanya.[3] Meningkatnya aktivitas transaksi elektronik telah memicu tantangan baru dengan munculnya berbagai tindak kejahatan berbasis siber di ruang kegiatan virtual. Kejahatan siber ini dilakukan oleh pihak-pihak yang berusaha mengeksploitasi kelemahan sistem dan kurangnya kesadaran pengguna terhadap

[1] Chakim, M. H. R. 2023. Kemajuan Teknologi di Abad 21: Perubahan Perspektif. ADI Pengabdian Kepada Masyarakat, 4(1), hlm. 40.

[2] Aprilia, N. 2022. Perkembangan Teknologi. Pena Media. hlm. 5.

[3] Hendri Diansah., Usman, & Monita, Y. 2022. Kebijakan Hukum Pidana Terhadap Tindak Pidana Carding. Pampas: Journal of Criminal, 3(1), hlm. 16. diakses pada web: https://online journal.unja.ac.id/Pampas/article/view/17704, pada tanggal 05 Agustus 2025, pada pukul 11:51 WIB.

keamanan sistem informasi.[4] Di Indonesia, kejahatan berbasis siber ini dikenal dengan istilah *cybercrime*, dengan pelakunya disebut sebagai *frauder*. Salah satu bentuk kejahatan siber yang kini marak adalah *fraud phising*. *Fraud* merujuk pada kejahatan penipuan, yaitu Tindakan kesengajaan yang menyebabkan kerugian materiil maupun immateriil bagi individu atau perusahaan.[5]

Indonesia kini dipandang sebagai negara dengan indeks keamanan siber terburuk di Asia dan dunia. Penilaian ini merupakan hasil penelitian oleh Reboot Digital PR Service yang berbasis di Inggris. Mereka menganalisis statistik keamanan siber, termasuk unduhan *drive-by*, *phising*, *hosting malware,* serta komputer yang disusupi. Indonesia menempati peringkat teratas dengan skor 82,8 dari 100, dengan 643 komputer terkontaminasi virus, 1.080 insiden *phising*, dan 1.040 kasus *malware.*[6]

Perkembangan teknologi informasi dan komunikasi (TIK) pada era digital telah mengubah pola interaksi sosial secara cepat dan masif. Selain memudahkan pertukaran informasi, platform media sosial juga membuka ruang baru bagi kegiatan kriminal berbasis teknologi, termasuk modus- modus rekayasa sosial seperti phishing, spoofing, dan penyebaran malware melalui konten yang tampak kredibel. Salah satu variasi modus tersebut adalah pengiriman "undangan palsu" (fake invitations) kepada pengguna media sosial, yang pada permukaan tampak sebagai undangan resmi untuk sebuah acara tetapi dirancang untuk memperoleh data pribadi, kredensial akses, atau menyebabkan korban mengunduh perangkat lunak berbahaya. Modus ini memanfaatkan kepercayaan sosial, kecenderungan berbagi informasi, dan kebiasaan pengguna untuk menerima undangan dari jaringan mereka.

Fenomena undangan palsu memiliki beberapa karakteristik yang membahayakan: *pertama*, sifatnya yang tampak personal atau relevan sehingga

[4] Rahmad, N. 2019. Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online. Jurnal Hukum Ekonomi Syariah, 3(2), hlm. 105. diakses pada web: https://journal.unismuh.ac.id/index.php/jhes/article/view/2419/235, pada tanggal 05 Agustus 2025, pada pukul 13:01 WIB.

[5] Hartanto. 2022. Karakteristik Penipuan Sebagai Kejahatan Siber Tertinggi Di Indonesia. Jurnal Ilmu Hukum, 10(2), hlm. 220. diakses pada web: https://diktum.upstegal.ac.id/index.php/diktum/article/download/210/61/, pada tanggal 04 Agustus 2025, pada pukul 20:07 WIB.

[6] Ekayani, L., & Djanggih, H. 2023. Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. Journal of Lex Philosophy (JLP), 4(1), hlm. 22.

menurunkan kecurigaan penerima; *kedua*, penggunaan teknik rekayasa sosial untuk meminta informasi sensitif (misal NIK, nomor telepon, nomor rekening, atau detail kartu kredit) dengan dalih verifikasi pendaftaran; *ketiga*, integrasi tautan atau lampiran berbahaya yang dapat mengunduh *malware* atau mengarahkan korban ke situs *phishing* yang meniru layanan resmi; dan *keempat*, kemampuan pelaku untuk menyebarkan materi ini secara massal melalui *bot* atau jaringan akun palsu sehingga dampaknya meluas dengan cepat Salah satu yang paling marak di Indonesia adalah *Phising*. *Phising* adalah metode kejahatan online yang mencuri data untuk keuntungan pribadi, merugikan korbannya. Teknik ini melibatkan pengelabuan untuk memperoleh informasi pribadi seperti nama, usia, alamat; data akun seperti username dan password; serta informasi finansial seperti detail kartu kredit dan rekening bank. *Phising* dapat terjadi di berbagai platform, termasuk media sosial, situs web, dan aplikasi. Saat ini, banyak orang menggunakan *WhatsApp* untuk bertukar pesan dan Instagram untuk berbagi foto dan video. Sayangnya, platform populer ini juga dimanfaatkan oleh pelaku kejahatan. Misalnya, di *WhatsApp*, penjahat siber sering mengirim pesan ke nomor tertentu dengan tujuan mencuri informasi pribadi.

Phising adalah kejahatan di mana korban diarahkan untuk membuka *Link* (tautan) yang tampak sah tetapi sebenarnya berbahaya. Setelah membuka tautan tersebut, korban mengikuti instruksi yang disediakan dan diminta untuk memberikan data pribadi, seperti nomor KTP, nomor rekening, rincian kartu kredit, dan kata sandi. Hal ini menyebabkan korban mengalami penipuan dan kerugian finansial. Penjahat siber memanfaatkan rasa penasaran pengguna, yang kemudian mengirimkan tautan tersebut kepada orang lain dengan keyakinan bahwa informasi yang dijanjikan benar adanya. Akibatnya, pengguna lain juga terjebak untuk mengklik tautan tersebut, yang dapat mengandung virus atau mengarahkan mereka ke situs berbahaya yang mengancam keamanan mereka Konteks hukum nasional Indonesia telah mengalami perkembangan signifikan dalam beberapa tahun terakhir untuk mengantisipasi ancaman siber dan pelanggaran privasi. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) mengalami perubahan berulang, dan pembaruan terakhir melalui Undang-Undang Nomor 1 Tahun 2024 memperkuat beberapa aspek penegakan hukum terkait informasi elektronik. Sementara itu, pengesahan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menandai tonggak penting dalam memberikan landasan hukum bagi perlindungan hak subjek data di Indonesia. Kombinasi antara UU ITE yang mengatur penggunaan informasi elektronik dan UU PDP yang mengatur pemrosesan data pribadi menciptakan kerangka hukum yang berpotensi efektif untuk menjerat pelaku penyalahgunaan lewat undangan palsu, namun implementasinya memerlukan harmonisasi norma, kesadaran penegak hukum, serta mekanisme pelaporan dan remediasi yang memadai.

Berdasarkan laporan lembaga yang menangani keamanan siber menunjukkan peningkatan insiden *phishing* dan *social engineering* yang menargetkan pengguna media sosial dan aplikasi pesan singkat. Insiden-insiden tersebut tidak selalu dilaporkan ke pihak berwenang, dan ketika dilaporkan, penanganannya seringkali menemui kendala terkait bukti elektronik yang mudah hilang, keterbatasan kemampuan forensik digital, serta adanya hambatan yurisdiksi jika infrastruktur pelaku berada di luar negeri. Selain itu, korban sering kali mengalami kesulitan mengklaim ganti rugi atau mendapat bantuan pemulihan atas kerugian non-moneter seperti kerusakan reputasi atau trauma psikologis yang disebabkan oleh penyalahgunaan data pribadi.

Dari perspektif kepentingan publik, modus undangan palsu tidak hanya menimbulkan kerugian individual tetapi juga mengancam kepercayaan publik terhadap ekosistem digital. Ketika pengguna kehilangan kepercayaan pada platform komunikasi, dampaknya meluas ke aspek ekonomi dan sosial: transaksi elektronik menjadi berisiko, partisipasi publik dalam ruang digital berkurang, dan biaya untuk mengendalikan risiko meningkat. Oleh karena itu, perlindungan hukum terhadap korban bukan sekadar soal menjerat pelaku, melainkan juga soal memelihara kepercayaan publik terhadap infrastruktur digital dan memastikan pemulihan yang efektif bagi korban.

Analisis terhadap undangan palsu memerlukan perspektif interdisipliner: aspek teknis (forensik digital, arsitektur platform), aspek hukum (pidana, perdata, administratif), dan aspek sosial (literasi digital, perilaku pengguna). Misalnya, pengukuran dampak kerugian ekonomi akibat undangan palsu memerlukan data empiris yang akurat terkait jumlah insiden, skala kerugian rata-rata per korban, serta biaya remediasi. Di sisi lain, kajian yuridis perlu menilai apakah norma yang ada sudah memadai untuk menutupi celah praktik baru yang sebelumnya tidak

terbayangkan saat undang-undang disusun.

Meskipun regulasi hukum terkait kejahatan siber sudah ada, kejahatan ini tetap merajalela. Oleh karena itu, diperlukan penelitian untuk memahami bagaimana tindak pidana ini dapat diatasi dan bagaimana pandangan hukum pidana ekonomi terhadap kejahatan ini. Penelitian ini penting untuk mengidentifikasi strategi efektif dalam penegakan hukum serta pendekatan yang lebih komprehensif dalam melindungi masyarakat dari ancaman kejahatan siber.

Praktik penegakan di pengadilan memperlihatkan kecenderungan penggunaan kombinasi norma: pasal pidana terkait penipuan, akses ilegal, atau perusakan sistem elektronik seringkali digabungkan dengan klaim perdata atas perbuatan melawan hukum, serta pengaduan administratif atas pelanggaran perlindungan data. Walaupun demikian, preseden yang spesifik mengenai undangan palsu sebagai modus secara eksplisit masih relatif terbatas, sehingga diperlukan pengembangan interpretasi hukum oleh hakim, jaksa, dan penasihat hukum untuk membentuk yurisprudensi yang konsisten.

Berdasarkan penjelasan di atas, penelitian ingin menegaskan urgensi kajian mengenai maraknya penggunaan undangan palsu sebagai modus penyalahgunaan data pribadi menuntut respons hukum yang adaptif, berbasis bukti, dan terkoordinasi antara lembaga penegak hukum, regulator, platform, dan masyarakat sipil. Penelitian ini diharapkan dapat memberikan kontribusi teoretis dan praktis, baik untuk pembuat kebijakan, penegak hukum, maupun akademisi dalam upaya memperkuat perlindungan korban serta menjaga integritas ekosistem digital di Indonesia.

B. Metode Penelitian

Metode yang digunakan dalam penelitian ini yaitu penelitian normatif dengan menggunakan pendekatan perundang-undangan, konseptual, dan kasus. Metode ini digunakan untuk memecahkan masalah yang diselidiki dengan menganalisis permasalahan menggunakan peraturan perundang-undangan terkait. Penelitian ini menekankan pada implementasi ketentuan hukum normatif dalam penerapannya di setiap peristiwa hukum tertentu yang terjadi dalam suatu masyarakat. Setelah data yang dibutuhkan terkumpul kemudian menuju kepada identifikasi masalah yang pada akhirnya menuju pada penyelesaian masalah.

C. Pembahasan

1. Perlindungan Hukum Terhadap Korban Penyalagunaan Data Pribadi Melalui Pengiriman Undangan Palsu

di Media Sosial.

Hak asasi manusia banyak macam bentuknya, mulai dari hak untuk hidup, hak kesehatan, hak untuk berpendapat, hak pribadi, serta masih banyak hak-hak yang lainnya. Hak pribadi merupakan hak yang mengandung unsur diri pribadi seperti data pribadi. Bila didefinisikan secara lebih umum, data pribadi merupakan suatu bahan baku berbentuk informasi atau sebuah keterangan ataupun bahan yang masih berupa suatu bahan mentah yang didalamnya berisi simbol, angka, huruf atau bahkan kata- kata dan sebagainya yang bersifat rahasia dan pribadi.

Bentuk perlindungan hukum terdiri dari dua macam jenis, yaitu perlindungan hukum secara preventif dan perlindungan hukum secara represif. Perlindungan hukum preventif merupakan perlindungan hukum dimana rakyat diberikan kesempatan untuk mengajukan keberatan atau pendapatnya sebelum suatu keputusan pemerintah mendapat bentuk definitif. Dengan ini, perlindungan hukum preventif artinya bertujuan untuk mencegah terjadinya suatu sengketa Sedangkan perlindungan hukum represif, bertujuan untuk menyelesaikan sengketa yang sedang terjadi. Dalam hal ini sengketa yang dimaksud adalah perkara pidana dimana bila terjadi Orang menjadi korban tindak kejahatan pengaksesan tanpa izin dan penyebaran data pribadi tanpa izin yang menjadi korban kejahatan siber. Di Indonesia mengenai peraturan perundang-undangan yang ada hubungannya dengan soal data pribadi di media elektronik terdapat dalam Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik yang mengatur tentang data pribadi sebagai berikut: Berdasarkan pada Pasal 26 Ayat (1) UU ITE, menyebutkan bahwa: "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".

Pada bagian yang terdapat dalam Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dijelaskan secara lebih lanjut mengenai apa yang dimaksud dengan perlindungan data pribadi dalam kaitannya pemanfaatan tentang teknologi informasi. Terkait dengan perlindungan data pribadi dari pengguna tanpa izin, isi Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik tersebut menyatakan bahwa pengguna setiap pemilik data pribadi dalam sebuah media elektronik harus mendapatkan izin dari pemilik data yang bersangkutan. Data pribadi adalah salah satu bagian dari hak asasi yakni hak

pribadi. Selanjutnya, diuraikan bahwa data pribadi merupakan salah satu bagian dari hak pribadi (Privacy Rights) yang memiliki pengertian sebagai berikut.

a) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Konstitusi Indonesia tidak secara eksplisit mengatur tentang perlindungan data didalam Undang-Undang Dasar Tahun 1945, meskipun UUD 1945 menyatakan dengan tegas mengenai perlindungan hak asasi manusia. Menyangkut suatu privasi setiap orang, Undang-Undang Dasar Republik Indonesia Tahun 1945 dalam Pasal 28 G Ayat (1) menyatakan bahwa "Setiap Orang berhak perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Dalam Pasal tersebut menjelaskan bahwa data pribadi masuk dalam kaitannya dengan hak pribadi yang merupakan salah satu dari hak asasi manusia yang dilindungi, dihormati, dan dijaga kerahasiaannya. Pada intinya, setiap penggunaan data pribadi seseorang haruslah dengan izin atau persetujuan orang pemilik data tersebut.

Beberapa Undang-Undang telah mengatur mengenai bentuk-bentuk hukum yang diberikan kepada pelaku untuk dapat dijerat yakni Undang- Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik lewat beberapa pasal sebagai berikut Pasal 45 dan Pasal 46 UU ITE. Ketentuan pidana tersebut sedikit membantu dalam penanganan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik karena dipasal tersebut dijelaskan secara rinci bagaimana proses pengunaan seperti apa, maka dari itu penulis berpendapat bahwa untuk menjerat pelakunya dengan mendakwa pelaku tersebut terlebih dahulu dengan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik dimana sebelum proses penggunan informasi tersebut, terlebih dahulu dilakukan proses pengaksesan informasi atau data pribadi tersebut dengan tanpa hak melawan hukum mengakses perangkat komputer atau sistem elektronik dengan sengaja.

Pengiriman undangan palsu melalui media sosial sering kali melibatkan penggunaan data pribadi korban, seperti nama, foto, nomor telepon, atau jabatan, tanpa persetujuan atau dasar

hukum yang sah. Tindakan ini bukan hanya melanggar privasi, tetapi juga dapat merugikan korban secara reputasi, psikologis, maupun materiil. Dalam konteks hukum Indonesia, perbuatan tersebut dapat dilihat dari dua instrumen utama, yaitu Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)23 dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

Undang-Undang ITE mengatur larangan penyebaran informasi elektronik yang mengandung muatan yang menyesatkan, merugikan, atau merendahkan kehormatan orang lain, termasuk informasi palsu atau hoaks yang disebarkan melalui media sosial. Ketentuan ini dapat menjerat pelaku yang membuat dan menyebarkan undangan palsu dengan menggunakan data pribadi korban yang menimbulkan kerugian, baik secara langsung maupun tidak langsung. Sementara itu, UU PDP memberikan perlindungan hukum yang lebih spesifik terhadap hak-hak subjek data pribadi, termasuk hak untuk mendapatkan pemberitahuan, memberikan persetujuan, meminta penghapusan data, dan menuntut ganti rugi jika data pribadi digunakan tanpa dasar hukum yang sah Dalam praktiknya, korban dapat menempuh langkah administratif dengan mengajukan permintaan penghapusan atau penonaktifan informasi kepada pengendali data pribadi atau penyelenggara sistem elektronik, sesuai dengan mekanisme yang diatur dalam UU PDP dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Selain itu, korban juga dapat menempuh jalur pidana melalui pelaporan kepada kepolisian jika undangan palsu mengandung unsur pencemaran nama baik, penipuan, atau pemalsuan identitas. Dalam hal terdapat tujuan untuk memperoleh keuntungan secara melawan hukum, pelaku dapat dikenakan Pasal 378 Kitab Undang- Undang Hukum Pidana (KUHP).26

Kombinasi penerapan UU ITE dan UU PDP memberikan payung hukum yang cukup komprehensif bagi korban. UU ITE berfungsi sebagai instrumen represif untuk menindak pelaku penyebaran informasi palsu dan merugikan, sedangkan UU PDP berfungsi sebagai instrumen preventif dan kuratif melalui pengaturan hak-hak subjek data dan kewajiban pengendali data pribadi. Dengan demikian, korban penyalahgunaan data pribadi melalui pengiriman undangan palsu di media sosial memiliki landasan hukum yang kuat

untuk menuntut perlindungan, pemulihan, dan ganti rugi atas kerugian yang dialaminya.

2. Upaya Hukum Yang Dapat Ditempuh Oleh Korban Yang Data Pribadinya Disalahgunakan.

Upaya hukum yang berlaku agar mendapatkan kembali rasa keadilan yang semestinya didapat. Upaya hukum adalah suatu upaya dilakukan oleh pihak yang berkepentingan dalam suatu kejadian yang dialami. Di dalam Kitab Undang-Undang Hukum Acara Pidana, ada dua upaya hukum yang diberikan, yakni Upaya Hukum Biasa dan Upaya Hukum Luar Biasa. Upaya hukum biasa termasuk di dalamnya banding dan kasasi, sedangkan dalam upaya hukum luar biasa terdapat kasasi demi kepentingan hukum dan peninjauan kembali.

Upaya hukum biasa terdiri dari banding dan kasasi. Banding atau lembaga banding berguna untuk memberi kesempatan kepada terdakwa atau jaksa untuk memohon pemeriksaan ulang pada Pengadilan Tinggi dengan suatu harapan agar putusan Pengadilan Tinggi itu membawa kepuasan bagi pemohon yang melakukan banding.28 Kasasi berdasarkan Pasal 244 Kitab Undang-Undang Hukum Acara Pidana terdakwa atau jaksa penuntut umum dapat mengajukan permintaan pemeriksaan kasasi kepada Mahkamah Agung kecuali terhadap putusan bebas. Terdakwa mengajukan permintaan pemeriksaan kasasi kepada Mahkamah Agung adalah karena merasa kurang atau tidak puas terhadap putusan yang dijatuhkan oleh Pengadilan Tinggi.

Upaya hukum luar biasa memuat tentang kasasi demi kepentingan hukum yakni mengenai pengajuan untuk dilakukan pemeriksaan tingkat kasasi demi kepentingan hukum hanyalah putusan-putusan yang sudah memperoleh keputusan hukum yang tetap akan tetapi bukan putusan dari Mahkamah Agung, sehingga termasuk didalamnya putusan Pengadilan Negeri dan Pengadilan Tinggi Serta peninjauan kembali putusan pengadilan yang telah memperoleh kekuatan hukum tetap dapat ditempuh baik melalui jalur administratif, pidana, maupun perdata. Secara administratif, korban dapat menggunakan hak-hak yang diberikan oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), antara lain hak untuk mengajukan permintaan penghapusan, pemutakhiran, atau pemblokiran data pribadi yang diproses tanpa persetujuan atau dasar hukum yang sah. Permintaan ini dapat disampaikan langsung kepada pengendali data pribadi atau melalui mekanisme pengaduan yang diatur dalam Peraturan Menteri Komunikasi dan

Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Secara pidana, korban dapat melaporkan pelaku kepada pihak kepolisian berdasarkan ketentuan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), apabila penyalahgunaan data pribadi tersebut dilakukan untuk menyebarkan informasi yang menyesatkan, mencemarkan nama baik, atau digunakan untuk melakukan penipuan. Jika terbukti terdapat unsur penipuan untuk memperoleh keuntungan secara melawan hukum, pelaku dapat dijerat dengan Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP).

Secara perdata, korban dapat mengajukan gugatan ganti rugi berdasarkan ketentuan perbuatan melawan hukum (onrechtmatige daad) di pengadilan negeri, serta menggunakan hak untuk menuntut kompensasi sebagaimana diatur dalam UU PDP[2]. Kombinasi dari jalur administratif, pidana, dan perdata ini memberikan perlindungan yang komprehensif bagi korban dalam menuntut pemulihan dan keadilan atas penyalahgunaan data pribadi yang dialaminya.

Penyebaran data pribadi di dunia maya masih terbilang belum terlalu banyak, akan tetapi dampak yang dirasakan akibat tindakan tersebut sangat besar efeknya. Modus operandi penyebaran data pribadi di dunia maya ini berbeda dengan tindak kejahatan yang konvensional. Hal yang paling mencolok adalah mengenai locus delicti atau kejadian perkaranya karena perkara ini terjadi lewat lintas sistem dan jaringan. Media sosial merupakan suatu bagian dari pekembangan teknologi yang baru di era modern tempat para pengguna (user) berekspresi di dunia maya. Media sosial tidak pernah lepas dari terkoneksinya jaringan internet.

Pertama, pencarian data : pelaku mencari data yang kira-kira dapat diakses dengan tanpa izin, menentukan ruang lingkup wilayah dimana akan dilakukan serangan, menyeleksi jaringan dan mengintai jaringan. Kedua, adalah pemilihan sasaran. Disini pelaku mulai meraba-raba dimana letak kelemahan sistemnya tersebut. Pelaku mencari sistem mana yang bisa ditembus dan diakses dengan tepat sasaran. Ketiga, pencarian data mengenai sasaran yang dituju. Hal ini sudah bersifat sangat mengganggu terhadap suatu sistem. Disini pelaku dapat mencari mengenai nama akun, password akunkorban, isi percakapan maupun transaksi data-data berupa foto/video, file

dokumen, phonesex antara korban dengan lawan interaksi di sistem tersebut. Keempat, akses secara ilegal telah ditetapkan atau ditentukan. Yang Kelima adalah menaikkaan atau mengamankan suatu posisi, mengansumsikan bahwa penyerang atau pelaku sudah memiliki log-on access pada sistem tersebut sebagai pengguna biasa. Selanjutnya setelah pelaku mendapatkan akses dan mendapatkan data pribadi pengguna tersebut, pelaku mulai melakukan penyebaran data pribadinya

D. Kesimpulan

Penyalahgunaan data pribadi melalui media sosial, khususnya dalam bentuk pengiriman undangan palsu, merupakan pelanggaran serius terhadap hak privasi dan keamanan informasi yang secara tegas dilindungi oleh Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Tindakan ini tidak hanya "Modus Operandi Tindak Pidana Cracker Menurut Undang- Undang Informasi dan Transaksi Elektronik",berimplikasi pada kerugian materiil dan immateriil yang dialami korban, seperti kerugian finansial, pencemaran nama baik, dan tekanan psikologis, tetapi juga menimbulkan dampak luas terhadap rasa aman masyarakat dalam menggunakan layanan digital. Selain itu, maraknya modus penyalahgunaan data pribadi di ruang siber dapat meruntuhkan kepercayaan publik terhadap integritas penyelenggara sistem elektronik dan keberlangsungan ekosistem digital yang sehat.

Korban yang data pribadinya disalahgunakan memiliki berbagai jalur upaya hukum yang dapat ditempuh untuk memperoleh perlindungan dan pemulihan hak. Secara administratif, korban dapat mengajukan pengaduan resmi kepada Kementerian Komunikasi dan Informatika atau otoritas perlindungan data pribadi untuk menuntut penghapusan dan pemblokiran data yang disalahgunakan. Secara pidana, korban dapat melaporkan pelaku kepada aparat penegak hukum agar diproses berdasarkan ketentuan sanksi pidana dalam UU ITE dan UU PDP, yang mencakup pidana penjara dan denda bagi pelaku. Secara perdata, korban berhak mengajukan gugatan ganti kerugian kepada pengadilan untuk memperoleh kompensasi atas kerugian yang dialami. Pendekatan hukum yang terpadu ini diharapkan mampu memberikan perlindungan yang komprehensif, memulihkan kerugian korban, sekaligus menciptakan efek jera yang efektif bagi pelaku dan pihak-pihak yang berpotensi melakukan pelanggaran

serupa di masa mendatang.

Daftar Pustaka

Buku

Agus Raharjo. 2002. *CyberCrime*. Bandung: Citra Adi Karya.

Aprilia, N. 2022. Perkembangan Teknologi. Pena Media.

Bambang Waluyo. 2002. *Penelitian Hukum dalam Praktek*. Jakarta: Sinar Grafika.

C. Djisman Samosir. 2013. *Segenggam Tentang Hukum Acara Pidana*. Bandung: Nuansa Aulia.

M. Nazir. 2003. *Metode Penelitian*. Jakarta: Ghealia Indonesia, cetakan ke-5.

Karya Ilmiah

Chakim, M. H. R. 2023. Kemajuan Teknologi di Abad 21: Perubahan Perspektif. ADI Pengabdian Kepada Masyarakat, 4(1).

Ekayani, L., & Djanggih, H. 2023. Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) di Lingkungan Perbankan. Journal of Lex Philosophy (JLP), 4(1).

Hartanto. 2022. Karakteristik Penipuan Sebagai Kejahatan Siber Tertinggi di Indonesia. Jurnal Ilmu Hukum, 10(2).

Hendri Diansah, Usman, & Monita, Y. 2022. Kebijakan Hukum Pidana Terhadap Tindak Pidana Carding. Pampas: Journal of Criminal, 3(1).

Hutasoit, K. 2018. Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Dalam Perspektif Hukum Pidana di Indonesia. Jurnal Fakultas Hukum Universitas Sumatera Utara, 3(1).

Kaimuddin, Arfan. 2019. Perlindungan Hukum Terhadap Tenaga Kerja Anak Dalam Perundang-Undangan di Indonesia. Jurnal Yurispruden, 2.

Nur Khalimatus. 2017. Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi dan Transaksi Elektronik. Jurnal Hukum Universitas Wijaya Kusuma Surabaya, 20.

Rahmad, N. 2019. Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online. Jurnal Hukum Ekonomi Syariah, 3(2).

Saragih, L. K., Budhijanto, D., & Somawijaya, S. 2020. Perlindungan

Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial Berdasarkan Undang-Undang Republik Indonesia Nomor 19 tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jurnal Hukum De'Rechtsstaat, 6(2).

Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. 2023. Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau dari KUHP dan UU ITE. Lex Veritatis, 2(01).

Peraturan Perundang – Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana.

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Sumber Lainnya

Hendri Diansah, Usman, & Monita, Y. 2022. Kebijakan Hukum Pidana Terhadap Tindak Pidana Carding. Pampas: *Journal of Criminal*, 3(1), hlm. 16. Diakses dari: https://online-journal.unja.ac.id/Pampas/article/view/17704.

Rahmad, N. 2019. Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online. *Jurnal Hukum Ekonomi Syariah*, 3(2), hlm. 105. Diakses dari: https://journal.unismuh.ac.id/index.php/jhes/article/view/2419/2357.

Hartanto. 2022. Karakteristik Penipuan Sebagai Kejahatan Siber Tertinggi di Indonesia. *Jurnal Ilmu Hukum*, 10(2), hlm. 220. Diakses dari: https://diktum.upstegal.ac.id/index.php/diktum/article/download/210/61/.