LEGAL: Journal of Law
Vol. 3 No. 1, Mei 2024, 18-29 / ISSN 2829-6672

Tanggung Jawab Pelaksana Sistem Elektronik dalam Melindungi Informasi Pemakai Media Sosial Menurut Undang-undang Nomor 19 Tahun 2016 Mengenai Informasi dan Transaksi Elektronik

Andi Wahyuddin Nur[1], Besse Muqita Dewi Mentari Rijal[2],
Dewi Wahyuni Mustafa[3], Nelvi[4]

[1,2,3,4] Institut Ilmu Hukum dan Ekonomi Lamaddukelleng

Abstrak
Teknik pengumpulan data dalam penelitian ini dilakukan dengan cara studi dokumen atau kepustakaan yang pada dasarnya mengkaji berbagai informasi tertulis mengenai hokum, baik yang dipublikasikan atau tidak dipublikasikan secara umum tetapi boleh diketahui oleh pihak tertentu. Hasil penelitian menunjukkan bahwa Tanggung jawab penyelenggara sistem elektronik terhadap data pengguna bukan hanya merupakan kewajiban etis, tetapi juga memiliki implikasi hukum yang signifikan. Di Indonesia, implikasi hukum tersebut telah di atur dalam berbagai bentuk produk perundang-undangan. Mulai dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya yakni Undang-undang No 19 Tahun 2016 Mengenai Informasi dan Transaksi Elektronik. Sementara apabila pengguna merasa dirugikan oleh tindakan penyelenggara sistem elektronik, mereka memiliki opsi untuk mengajukan keluhan kepada Menteri Komunikasi dan Informatika. Namun, menurut Pasal 32 dari Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, jika usaha untuk menyelesaikan perselisihan melalui perundingan atau alternatif lain belum berhasil mengatasi masalah perlindungan data pengguna di platform media sosial, maka pengguna berhak untuk mengambil langkah lebih lanjut dengan mengajukan tuntutan perdata sesuai dengan ketentuan hokum yang berlaku.

Kata Kunci: *pelaksana sistem elektronik, pemakai media sosial, informasi dan transaksi elektronik*

PENDAHULUAN

Setiap masyarakat di suatu negara memiliki hak-hak yang dijamin oleh Hukum Konstitusional. Melalui hak-hak ini, negara memiliki tanggung jawab untuk melindungi seluruh warganya. Peran konstitusional negara ini diatur dalam Pembukaan Alinea Ke 4 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDRI 1945), yang menegaskan bahwa negara wajib menjaga kesejahteraan umum bagi seluruh bangsa Indonesia, mendorong pendidikan yang lebih baik, serta mempromosikan perdamaian dan keadilan sosial dalam tatanan dunia yang merdeka.

Hak-hak konstitusional yang diatur dalam Undang-Undang Dasar Negara Republik Indonesia tahun 1945 mencakup 40 hak bagi warga negara, termasuk hak atas proteksi diri pribadi. Hak ini dijelaskan dalam Pasal 28G Ayat (1) yang secara garis besar menyatakan bahwa setiap masyarakat negara memiliki hak untuk dilindungi

dalam hal proteksi diri pribadi, keluarga, martabat, derajat, dan harta benda yang berada di bawah kekuasaannya. Pasal ini menegaskan bahwa hak-hak individu diakui sebagai hak milik yang harus dihormati.

Dengan perkembangan teknologi informasi dan komunikasi, penting untuk menganggap hak individu bukan hanya sebagai hak milik, tetapi juga sebagai hak privasi. Hak privasi memiliki dimensi yang lebih sensitif dan mencakup hak-hak pribadi tersebut. Hak pribadi mencakup hal-hal yang bersifat pribadi dan sensitif, termasuk informasi pribadi dan identitas seseorang seperti Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Paspor, Kartu Keluarga (KK), Nomor Pokok Wajib Pajak (NPWP), nomor rekening, sidik jari, ciri khas individu, dan lain sebagainya.

Kini, Indonesia telah memasuki zaman Revolusi Industri 4.0, dimana segala hal bisa dikendalikan dari berbagai tempat melalui jaringan internet dan perangkat terhubung. Keterhubungan di era ini sangat penting ketika teknologi digital menjadi bagian dari kehidupan sehari-hari masyarakat. Contohnya, teknologi ini dapat meningkatkan daya produksi kerja, membentuk ikatan sosio-ekonomi, serta membantu mempermudah berbagai aspek kehidupan. (Syaifuddin, 2020). Perkembangan pesat teknologi informasi dan komunikasi berbasis komputer telah mempengaruhi masyarakat secara signifikan. Hal ini telah membawa kemudahan bagi masyarakat. (R Aswandi, 2020)

Kemajuan teknologi sistem informasi dan komunikasi elektronik telah menjadi bahasa komunikasi terkini dalam masyarakat. Perkembangan ini telah mengubah perilaku masyarakat Indonesia. Tidak dapat disangkal bahwa perkembangan teknologi telah membawa dampak yang tak terduga sebelumnya bagi manusia. Saat ini, hampir setiap aspek kehidupan masyarakat telah dipengaruhi oleh sistem informasi dan komunikasi elektronik. Ini menciptakan pasar baru yang mendorong pergeseran dari model ekonomi konvensional yang berpusat pada industri manufaktur menuju ekonomi digital yang berpusat pada informasi, kreativitas intelektual, dan ilmu pengetahuan, atau yang disebut sebagai ekonomi kreatif.

Pada tahun 2019, data dari Asosiasi Pengguna Jasa Internet Indonesia (APJII) menunjukkan bahwa sebanyak 196,71 juta orang di Indonesia telah menggunakan internet. Jumlah tersebut mencakup 73,7% dari total penduduk Indonesia yang berjumlah 270 juta jiwa. Pulau Jawa menjadi wilayah dengan jumlah pengguna internet terbanyak, mencapai 55,7% dari total pengguna internet di Indonesia. Dengan adanya penggunaan teknologi ini, masyarakat menjadi lebih mudah dalam berbagai aktivitas, seperti berkomunikasi, bertransportasi, dan melakukan transaksi secara digital. (Informatika, 2021).

Revolusi digital sudah menciptakan suatu inovasi terkini pada kapasitas guna mendapatkan, menaruh, memanipulasi serta mentransmisikan daya muat informasi dengan cara jelas *(real time)*, luas serta kompleks. Oleh karenanya revolusi digital kerapkali dikira identik dengan revolusi data. Kemajuan tersebut sudah mendesak pengumpulan bermacam informasi, tidak lagi terkait dalam pertimbangan data apa yang bisa jadi bermanfaat di era depan.

Kehadiran teknologi digital sebagai sarana komunikasi telah mengubah cara interaksi kita melalui internet. Saat ini, masyarakat berinteraksi melalui platform media sosial yang dikembangkan oleh perusahaan teknologi. Media sosial telah menjadi bagian tak terpisahkan dari gaya hidup masyarakat, bahkan berperan sebagai pasar di mana pelaku usaha dan konsumen saling berhubungan dan bertransaksi.

Di platform media sosial, pihak ketiga yang mendapatkan izin khusus memiliki

akses terhadap data pengguna. Pihak ketiga yang dimaksud bisa mencakup otoritas hukum seperti penyidik kepolisian, atau bahkan staf internal dari penyedia layanan. Meskipun izin ini telah diberikan, potensi penyalahgunaan data dapat muncul saat pengguna berinteraksi di media sosial. Situasi ini mungkin terjadi ketika informasi atau data yang diposting oleh pengguna dalam jejaring sosial digunakan oleh pihak lain untuk maksud yang dianggap mengganggu, berbahaya, atau bahkan mengancam orang lain.

Penggunaan teknologi internet berarti kita harus berhati-hati terhadap risiko rentannya data pribadi pengguna. Berbagai layanan aplikasi memerlukan data pribadi seperti nama lengkap, e-mail, bahkan nomor rekening untuk memverifikasi identitas pengguna dan menyediakan layanan dengan tepat. Namun, tidak ada jaminan bahwa data pribadi tersebut tidak akan disalahgunakan. Oleh karena itu, pemilik platform media sosial membuat kebijakan privasi yang menjelaskan siapa yang selain pengguna akun dapat melihat atau mengetahui data dan informasi pengguna.

Berdasarkan survei dari Direktur Jenderal Aplikasi Informatika, bahwa aplikasi media sosial yang digunakan di Indonesia cukup beragam. Aplikasi yang paling banyak digunakan belakangan ini adalah whatsApp (WA) dengan presentase 89,2%, youtube 72,3% dan facebook 70,2%. Menyusul instagram 60,1%, tiktok 33,5%, telegram 32,9%, twitter 23,0%, line 7,8% dan linkedin 7,3%. (Direktur Jenderal Aplikasi Informatika, 2021: 17). Aplikasi media sosial yang digunakan kebanyakan masyarakat, mengharuskan mencantumkan data diri pada tahapan penginstalan aplikasi.

Beberapa kasus telah ditemukan adanya kebocoran data. Kebocoran data ini kemudian berlanjut pada kasus penyalahgunaan data pribadi yang merugikan masyarakat. Kerugian yang paling marak terjadi adalah beberapa orang yang tidak dikehendaki mengetahui data pribadi orang lain. Beberapa masyarakat juga mengaku sering mendapat teror atau dihubungi oleh orang yang tidak dikenal dan tidak dikehendaki. Selain itu adapula yang mengaku bahwa akun media sosial mereka dibajak dan digunakan untuk penipuan. (Informatika, 2021).

Perlindungan data pribadi menjadi sangat penting karena secara langsung terkait dengan Hak Asasi Manusia, termasuk hak untuk mengakses, menghapus, membatasi, mengumpulkan, dan mentransfer data. Kebocoran-kebocoran data seperti yang diungkapkan, tentunya harus menjadi perhatian. Terlebih dampak kerugian yang diakibatkan sudah terpampang nyata terjadi di tengah-tengah masyarakat. Hal tersebut juga tentu tidak terlepas dari orang-orang dibalik layar aplikasi media sosial yang seharusnya menjaga data pribadi pengguna aplikasinya.

Tingkat kepercayaan dalam dunia maya *(online trust)* sangat dipengaruhi oleh perlindungan privasi dan data pribadi. Kurangnya perlindungan dapat mengakibatkan data privasi tersebar ke tangan pihak yang tidak bertanggung jawab, yang berpotensi menyebabkan kerugian finansial bahkan mengancam keselamatan pemilik data tersebut. Maka dari itu tanggung jawab dari penyelenggara sistem elektronik atau aplikasi elektronik penting untuk dipertanyakan. Selain itu upaya apa yang mesti ditempuh oleh pengguna aplikasi yang menderita kebocoran data juga tidak kalah pentingnya untuk dipertanyakan dan diketahui.

METODE PENELITIAN

Berdasarkan penjelasan yang diberikan, riset yang dilakukan adalah tipe riset pustaka *(library research)* atau juga dikenal sebagai studi pustaka. Riset ini melibatkan aktivitas pengumpulan informasi dari berbagai sumber pustaka, seperti buku, jurnal

ilmiah, artikel, dan sumber-sumber lainnya yang relevan dengan topik penelitian. (Zed, 2014) Pengumpulan informasi pada riset hukum normatif dilakukan dengan cara penelitian dokumen ataupun kepustakaan yang pada dasarnya menelaah bermacam data tercatat perihal hukum, baik yang diterbitkan ataupun tidak diterbitkan secara umum namun bisa diketahui oleh pihak tertentu. Dengan kata lain studi dokumen merupakan bermacam aktivitas mengakumulasi serta mengecek dan menelusuri dokumen-dokumen ataupun kepustakaan yang bisa memberikan data ataupun penjelasan yang diperlukan oleh periset. (Syamsuddin, 2007)Metode analisa data pada riset ini dilakukan dengan cara kualitatif, maksudnya menjelaskan informasi dengan cara bermutu serta menyeluruh dalam bentuk perkataan yang teratur, masuk akal, tidak tumpang tindih serta efisien, alhasil mempermudah uraian serta pemahaman informasi. (Ishaq, 2017).

PEMBAHASAN

Tanggung Jawab Penyelenggara Sistem Elektronik Melindungi Data Konsumen

Pasal 1 Ayat (6) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mendefinisikan "Penyelenggaraan Sistem Elektronik" sebagai penggunaan Sistem Elektronik oleh penyelenggara negara, individu, badan usaha, dan atau masyarakat. Artinya, ketika seseorang atau suatu entitas menggunakan sistem elektronik untuk keperluan tertentu, termasuk dalam hal penyelenggaraan negara atau kegiatan oleh individu, badan usaha, atau masyarakat, maka itu disebut sebagai "Penyelenggaraan Sistem Elektronik."

Sedangkan menurut Pasal 1 Ayat (5) Undang-Undang yang sama, "Sistem Elektronik" didefinisikan sebagai serangkaian perangkat dan prosedur elektronik yang memiliki fungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan atau menyebarkan Informasi Elektronik. Artinya, sistem elektronik mencakup segala macam perangkat dan prosedur yang digunakan dalam memproses informasi elektronik, mulai dari penyimpanan hingga pengumuman dan pengiriman informasi.

Berdasarkan penjelasan kedua pasal tersebut, dapat dipastikan bahwa individu, institusi, atau masyarakat yang mengoperasikan suatu platform dengan cara mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan atau menyebarkan Informasi Elektronik dianggap sebagai penyelenggara sistem elektronik. Dengan kata lain, ketika seseorang atau suatu entitas melakukan aktivitas tersebut dalam penggunaan sistem elektronik, mereka dianggap sebagai penyelenggara sistem elektronik sesuai dengan definisi dalam Undang-Undang tentang Informasi dan Transaksi Elektronik.

Penulis memberikan contoh tentang aplikasi Facebook yang sebagian besar pendapatannya berasal dari iklan. Facebook mengolah data informasi pengguna dengan cermat untuk membuat pengguna menjadi target iklan bagi mitra Facebook. Mitra-mitra ini berkolaborasi dengan Facebook dan memanfaatkan Fitur Facebook Business, yang merupakan bagian dari rangkaian produk Facebook. Fitur ini membantu berbagai pihak seperti pemilik situs web, penerbit, pengembang, pengiklan, mitra bisnis, dan entitas lainnya untuk berintegrasi, menggunakan, dan berbagi informasi dengan Facebook. Melalui fitur ini, Facebook memungkinkan mitra-mitra tersebut untuk mencapai target audiens tertentu dan mengoptimalkan efektivitas kampanye iklan mereka.

Dalam Undang-Undang Informasi dan Transaksi Elektronik, Pasal 15 mengatur tentang kewajiban bagi Penyelenggara Sistem Elektronik, seperti Facebook, untuk

menjalankan sistemnya secara andal. Artinya, Facebook memiliki tanggung jawab untuk memastikan bahwa platformnya berfungsi dengan baik, handal, dan tidak mengalami gangguan yang dapat menghambat penggunaan dan akses pengguna. Facebook harus berusaha untuk menjaga kualitas layanan dan memastikan bahwa sistemnya berjalan sesuai dengan standar keamanan dan kualitas yang ditetapkan oleh hukum. Kewajiban ini bertujuan untuk melindungi hak-hak dan kepentingan pengguna serta memastikan keberlangsungan layanan yang baik bagi pengguna platform tersebut.

Kewajiban yang dimuat dalam Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah dirubah menjadi Undang-undang No 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik, bahwa: Setiap penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem elektronik sebagaiman mestinya; Penyelenggara Sistem Elektronik bertanggung jawab terhadap penyelenggaraan Sistem Elektronik; Ketentuan sebagaimana dimaksud pada Ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/ atau kelalaian pihak pengguna Sistem Elektronik.

Berdasarkan penjelasan dari Pasal 15 ayat 1, istilah "andal" merujuk pada sistem elektronik yang sesuai dengan kebutuhan penggunanya. Istilah "aman" mengacu pada sistem elektronik yang terlindungi baik secara fisik maupun non-fisik. Sedangkan frasa "beroperasi sebagaimana mestinya" menunjukkan bahwa sistem elektronik berfungsi sesuai dengan spesifikasinya. Pada Pasal 15 ayat 2, istilah "bertanggung jawab" merujuk kepada subjek hukum yang bertanggung jawab secara hukum atas penyelenggaraan sistem elektronik tersebut.

Dengan demikian, penulis mencontohkan penyelenggara sistem elektronik di Indonesia seperti Facebook, maka dari penjelasan pasal tersebut, sebagai penyelenggara sistem elektronik, Facebook memiliki tugas untuk memastikan bahwa sistemnya dapat dipercaya oleh pengguna. Selain itu, Facebook juga harus bertanggung jawab atas segala hal yang terjadi dalam sistem mereka.

Namun, di sisi lain Undang-undang Pasal 15 ayat 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah dirubah menjadi Undang-undang No 19 Tahun 2016, memberikan pengecualian apabila terjadi kelalaian, kesalahan, atau keadaan memaksa yang bukan sepenuhnya disebabkan oleh Penyelenggara Sistem Elektronik. Dalam hal ini, jika terjadi kegagalan atau masalah dalam sistem yang disebabkan oleh kelalaian atau kesalahan pihak pengguna atau karena keadaan memaksa, maka tanggung jawab Penyelenggara Sistem Elektronik dapat dikecualikan sejauh tidak ada kesalahan atau kelalaian dari pihak mereka sendiri.

Hal tersebut sesuai dengan tuntutan atau kewajiban yang diatur dalam Pasal 27 Peraturan Menteri Komunikasi dan Informatika, yang mengharuskan pengguna untuk: Menjaga kerahasiaan data pribadi yang diperoleh, dikumpulkan, diproses, dan dianalisis; Memanfaatkan data pribadi hanya sesuai dengan kebutuhan pengguna; Menjaga data pribadi dan dokumen yang dari tindakan yang mengandung penyalahgunaan; dan Bertanggung jawab atas penyalahgunaan data pribadi yang dimilikinya, baik secara organisasi maupun individu.

Singkatnya, perlindungan data pribadi bukan hanya tanggung jawab beberapa pihak. Pemerintah, penyelenggara sistem elektronik, dan pengguna semua memiliki tanggung jawab yang besar untuk melindungi data pribadi.

Dalam praktiknya, hubungan antara penyelenggara sistem elektronik dan pengguna harus didasari oleh perjanjian atau perikatan yang menetapkan hak dan

kewajiban masing-masing pihak. Perikatan ini terbentuk ketika pengguna mendaftarkan diri atau menggunakan sistem elektronik tertentu, seperti Facebook, Instagram, atau sistem elektronik lainnya.

Dalam perjanjian tersebut, penyelenggara sistem elektronik akan menetapkan persyaratan penggunaan platform mereka, termasuk mengenai akses, penggunaan data, dan perlindungan data pribadi pengguna. Di sisi lain, pengguna juga memiliki tanggung jawab untuk mematuhi ketentuan yang telah ditetapkan oleh penyelenggara sistem elektronik, termasuk mengenai keamanan dan kerahasiaan data pribadi mereka sendiri.

Menurut Pasal 1233 Kitab Undang-Undang Hukum Perdata, perikatan dapat terbentuk melalui persetujuan antara pihak-pihak yang terlibat atau berdasarkan Undang-Undang. Dalam hubungan antara pengguna dan penyelenggara sistem elektronik, perikatan terbentuk berdasarkan persetujuan. Hal ini berarti bahwa kedua belah pihak (pengguna dan penyelenggara sistem elektronik) memiliki kewajiban untuk memberikan sesuatu, melakukan sesuatu, atau tidak melakukan sesuatu sesuai dengan kesepakatan yang telah dibuat. Penjelasan mengenai jenis perikatan ini dapat ditemukan dalam Pasal 1314 Kitab Undang-Undang Hukum Perdata.

Dalam perjanjian antara kedua belah pihak tersebut, penyelenggara sistem elektronik memiliki kewajiban untuk menyampaikan informasi kepada pengguna sesuai dengan ketentuan yang dijelaskan dalam Pasal 25 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menerangkan bahwa sekurang-kurangnya, penyelenggara Sistem Elektronik harus memberikan informasi kepada pengguna Sistem Elektronik tentang:

1. Identitas Penyelenggara Sistem Elektronik
   Identitas lengkap dari penyelenggara Sistem Elektronik harus disediakan kepada pengguna. Informasi yang mencakup nama perusahaan, alamat kantor pusat, nomor kontak, dan alamat situs web harus diberikan secara terbuka dan mudah diakses oleh pengguna. Dengan memberikan identitas yang jelas, pengguna dapat mengenali dan memverifikasi keaslian penyelenggara, serta dapat menghubungi pihak penyelenggara sistem elektronik jika diperlukan.
2. Objek yang Ditransaksikan
   Penyelenggara Sistem Elektronik harus menjelaskan dengan rinci mengenai jenis barang atau jasa yang dapat ditransaksikan melalui platform tersebut.
3. Kelayakan atau Keamanan Sistem Elektronik
4. Penyelenggara harus memberikan penjelasan tentang kemampuan dan keamanan Sistem Elektronik yang disediakan. Ini termasuk informasi tentang teknologi yang digunakan, langkah-langkah keamanan yang diadopsi untuk melindungi data pengguna, dan keandalan sistem dalam menghadapi potensi ancaman keamanan. Hal ini akan memberikan keyakinan kepada pengguna bahwa Sistem Elektronik yang digunakan telah memenuhi standar keamanan yang tepat dan dapat diandalkan dalam transaksi mereka.
5. Tata Cara Penggunaan Perangkat
   Penyelenggara harus menyediakan panduan yang jelas dan mudah dipahami tentang cara menggunakan perangkat atau platform Sistem Elektronik. Pengguna harus diberikan petunjuk langkah demi langkah tentang bagaimana cara berinteraksi dengan sistem. Informasi ini akan membantu pengguna yang mungkin tidak terlalu familiar dengan teknologi atau platform sejenis untuk dapat menggunakan Sistem Elektronik dengan lancar.
6. Syarat Kontrak

Informasi mengenai syarat dan ketentuan yang berlaku saat menggunakan Sistem Elektronik harus disampaikan secara terperinci kepada pengguna. Hal ini bisa meliputi ketentuan pembayaran, kebijakan pengembalian, batasan tanggung jawab, hak dan kewajiban pengguna, serta hak dan kewajiban penyelenggara. Pengguna harus secara jelas memahami peraturan dan aturan yang mengikat selama menggunakan Sistem Elektronik tersebut.

7. Prosedur Mencapai Kesepakatan
   Penjelasan yang komprehensif mengenai langkah-langkah atau prosedur yang harus diikuti oleh pengguna untuk mencapai kesepakatan dalam transaksi menggunakan Sistem Elektronik perlu diberikan. Ini mencakup informasi tentang proses pemesanan, konfirmasi, pembayaran, pengiriman barang atau jasa, dan langkah-langkah lain yang relevan. Pengguna harus memahami seluruh alur proses transaksi untuk memastikan bahwa mereka dapat mengikuti langkah-langkah dengan benar.
8. Jaminan Privasi dan atau perlindungan Data pribadi
   Dalam era digital yang semakin maju, perlindungan privasi dan data pribadi menjadi sangat penting. Penyelenggara harus menjelaskan dengan jelas bagaimana data pribadi pengguna akan dikelola, disimpan, dan digunakan oleh Sistem Elektronik. Pengguna harus diberikan kepastian bahwa data mereka akan dijaga kerahasiaannya dan tidak akan disalahgunakan oleh pihak lain. Informasi mengenai kebijakan privasi, penggunaan cookie, serta hak dan pilihan pengguna dalam mengatur data pribadi mereka harus tersedia dengan transparan.

Menurut Pasal 12 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Kewajiban penyelenggara sistem elektronik adalah untuk memastikan; Ketersediaan kontrak tingkat layanan; Tersedianya kesepakatan yang berkaitan dengan keamanan data terhadap layanan teknologi informasi yang digunakan dan Penyediaan sarana komunikasi internal dan keamanan data.

Penyelenggara Sistem Elektronik yang disebutkan pada Ayat (1) bertanggung jawab untuk memastikan bahwa setiap komponen dan integrasi seluruh Sistem Elektronik berfungsi dengan baik.

Terkait dengan perlindungan informasi pengguna sistem elekronik di Indonesia, penulis menilai bahwa penyelenggara sistem elektronik telah berkomitmen untuk menjaga informasi-informasi pribadi pengguna. Sebagai contoh penyelenggara sistem elektronik di Indonesia adalah facebook. Pada praktiknya, facebook menyediakan perjanjian tingkat layanan untuk memastikan bahwa data pengguna aman.

Kebijakan data Facebook, yang mencakup kebijakan privasi Facebook, mengatur perlindungan data pengguna dan mengatur penyebaran informasi tersebut. Ketentuan layanan mencakup: Jenis informasi yang dikumpulkan oleh penyelenggara sistem elektronik Facebook terhadap pengguna; Penggunaan informasi yang dikumpulkan dan diolah oleh Facebook; Bagaimana informasi yang diperoleh disebarluaskan; Cara perusahaan-perusahaan Facebook bekerja sama dalam mengelola informasi; Cara mengelola dan menghapus informasi pengguna di platform Facebook; Bagaimana Facebook menanggapi hukum atau mencegah bahaya terkait data pengguna; Bagaimana data dioperasikan dan ditransfer sebagai bagian dari layanan global Facebook; Kebijakan pemberitahuan tentang perubahan kebijakan Facebook; Bagaimana cara pengguna dapat mengajukan pertanyaan atau memberikan umpan balik kepada Facebook.

Pengguna Facebook yang memiliki akun media sosial menyetujui perjanjian yang

disebut *"Statement of Rights and Responsibilities"* dengan Facebook sebagai penyelenggara sistem elektronik yang menangani data pribadi. Pengguna setuju untuk memberikan izin terkait hak intelektual sesuai dengan pengaturan "Privasi dan Pengaturan Penggunaan". Pengguna juga setuju untuk memberikan izin lisensi yang Non-Eksklusif, berdasarkan Kebijakan Privasi, *Transferable, Sub-Licensable*, Tanpa Royalti, dan Berlaku di Seluruh Dunia untuk menggunakan semua konten yang diposting oleh pengguna (Lisensi IP).

Lisensi IP ini berakhir ketika pengguna menghapus konten yang dimaksud (IP Content) atau menghapus akun mereka, kecuali jika konten tersebut telah dibagikan di akun orang lain dan belum dihapus oleh mereka. Ini berarti bahwa Facebook tidak perlu meminta izin atau membayar royalti untuk menampilkan konten yang terkait hak intelektual tersebut ketika Facebook menggunakannya, selama konten tersebut diposting untuk konsumsi publik.

Menurut kebijakan privasi Facebook, data dibagi menjadi dua kategori: data pribadi dan data publik. Data pribadi hanya dapat dilihat oleh sejumlah pengguna tertentu; data publik dapat dilihat oleh orang lain jika pengguna memberikan izin, tetapi izin tersebut harus memenuhi persyaratan tertentu, seperti menjaga kerahasiaan data.

Jenis data atau informasi yang diterima Facebook, termasuk data yang dikumpulkan untuk mengelola akun dan melacak aktivitas pengguna di media sosial, dijelaskan dalam kebijakan privasi Facebook. Pada saat pengguna memberikan izin kepada Facebook untuk menggunakan informasi mereka, pengguna selalu memiliki akses penuh kepada data prbadinya. Dalam Privacy Policy, Facebook menyatakan bahwa tidak akan membagikan data atau informasi pengguna, kecuali dalam situasi-situasi berikut:

1. Atas persetujuan pengguna. Facebook dapat membagikan data atau informasi pengguna jika pengguna memberikan izin atau persetujuan secara eksplisit untuk tujuan tertentu. Pengguna memiliki kendali atas izin ini dan dapat memilih untuk memberikannya atau tidak.
2. Memberikan pemberitahuan. Sebelum membagikan data atau informasi pengguna, Facebook akan memberikan pemberitahuan kepada pengguna mengenai tindakan tersebut, terutama jika ada perubahan dalam kebijakan privasi yang berdampak pada cara data pengguna diolah atau digunakan.
3. Menyamarkan identitas. Dalam beberapa situasi, Facebook dapat menyamarkan identitas pengguna ketika membagikan data atau informasi, misalnya dengan menggunakan kode unik atau data anonim untuk melindungi privasi dan keamanan pengguna. Hal ini dilakukan untuk mencegah penyalahgunaan informasi oleh pihak lain.

Apabila terjadi keselahan dalam melindungi privasi pengguna, maka, hal tersebut merupakan tanggung jawab penyelenggara sistem elektronik. Cara bertanggung jawab oleh penyelenggara sistem elektronik harus sesuai dengan ketentuan yang tercantum dalam Pasal 28 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik bahwa jika terjadi kebocoran data pribadi dalam sistem elektronik yang dikelola oleh penyelenggara, beri tahu pemilik data pribadi secara tertulis dengan mengikuti persyaratan berikut:

1. Harus Menyertakan Alasan Kegagalan Perlindungan Data Pribadi
   Dalam pemberitahuan, penyelenggara sistem elektronik harus menjelaskan secara rinci alasan atau penyebab terjadinya kegagalan perlindungan data pribadi yang

mengakibatkan kerahasiaan data tersebut terlampaui.

2. Pengumpulan dan perolehan data pribadi dapat dilakukan secara elektronik jika pemilik data pribadi telah memberikan persetujuan untuk itu pada saat prosesnya. Jika Pemilik Data Pribadi telah memberikan persetujuan tertulis untuk menerima pemberitahuan secara elektronik, penyelenggara sistem elektronik dapat mengirimkan pemberitahuan tersebut melalui media elektronik yang diizinkan.
3. Pastikan Pemilik Data Pribadi menerimanya jika kegagalan mengakibatkan kerugian bagi pihak yang bersangkutan. Penyelenggara sistem elektronik harus memastikan bahwa pemberitahuan telah diterima oleh Pemilik Data Pribadi, terutama jika kegagalan perlindungan data tersebut berpotensi menyebabkan kerugian bagi Pemilik Data.
4. Pemilik Data Pribadi menerima pemberitahuan secara tertulis dalam waktu 14 (empat belas) hari. Pemberitahuan tertulis mengenai kegagalan perlindungan data pribadi harus segera dikirimkan kepada Pemilik Data Pribadi dalam waktu maksimal 14 hari sejak adanya kegagalan tersebut diketahui oleh penyelenggara sistem elektronik.

Tanggung jawab penyelenggara sistem elektronik dalam melindungi data konsumen sangatlah penting. Penyelenggara sistem elektronik dalam menjalankan sistemnya diwajibkan bertanggung jawab atas beroperasinya sistem elektronik tersebut. Regulasi mengenai hal tersebut telah diatur dalam berbagai peraturan perundangan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah dirubah menjadi Undang-undang No 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik, Peraturan Menteri dan Peraturan Pemerintah.

Upaya Hukum yang Dapat Dilakukan Pengguna Apabila Penyelenggara Sistem Elektronik Gagal dalam Melindungi Data Pengguna

Jika pengguna merasa bahwa penyelenggara sistem elektronik gagal melindungi data mereka, ada opsi untuk mengajukan keluhan kepada Menteri Komunikasi dan Informatika. Dalam menghadapi sengketa ini, dapat digunakan mekanisme alternatif penyelesaian sengketa sesuai dengan Pasal 29 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, sebagai berikut:

Setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik memiliki hak untuk mengajukan pengaduan kepada Menteri terkait pelanggaran perlindungan kerahasiaan Data Pribadi.

Pengaduan yang disebutkan dalam ayat (1) bertujuan untuk mencari penyelesaian sengketa melalui jalur musyawarah atau metode alternatif lainnya.

Pengaduan yang dimaksudkan dalam ayat tersebut diajukan berdasarkan alasan: Jika Penyelenggara Sistem Elektronik tidak memberikan pemberitahuan tertulis kepada Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lain yang terkait dengan Data Pribadi, dapat diajukan pengaduan; atau Meskipun pemberitahuan tertulis telah diberikan, pengaduan dapat diajukan jika Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lain yang terkait mengalami kerugian sebagai akibat dari kegagalan perlindungan kerahasiaan Data Pribadi.

Untuk menindaklanjuti pengaduan sesuai dengan yang disebutkan dalam Ayat (1), menteri dapat bekerja sama dengan pimpinan Instansi Pengawas dan Pengatur Sektor.

Sesuai dengan ketentuan yang tercantum dalam Ayat (1) Pasal 36 Peraturan

Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016, sanksi administratif akan dikenakan jika Menteri menerima pengaduan dan terbukti bahwa penyalahgunaan data pengguna dilakukan oleh individu atau organisasi non-badan hukum. Sanksi tersebut meliputi: Peringatan lisan; Peringatan Tertulis; Penghentian sementara Kegiatan; Pengumuman di situs dalam jaringan *(website online).*

Menurut Pasal 84 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, sanksi administratif dapat dikenakan jika penyelenggara sistem elektronik terbukti bersalah. Sanksi yang dimaksud dapat terdiri dari: Teguran tertulis; Denda administratif; Penghentian sementara; dan/atau Dikeluarkan dari daftar sebagaimana dimaksud dalam Pasal 5 Ayat (4), Pasal 37 Ayat (2), Pasal 62 Ayat (1), dan Pasal 65 Ayat (4).

Sanksi-sanksi administratif tersebut bertujuan untuk memberikan efek jera dan mendorong para pelaku sistem elektronik untuk mematuhi ketentuan peraturan yang berlaku serta melindungi data pribadi pengguna dengan baik dan benar.

Apabila perbandingan yang dipilih adalah Regulasi Perlindungan Data Umum) Eropa, maka kesimpulannya bahwa penyelenggara sistem elektronik yang gagal melindungi data pengguna di Indonesia akan menerima sanksi yang lebih ringan daripada sanksi yang diberikan oleh hukum Eropa. pengguna dapat dikenakan Sanksi hingga dua puluh juta euro atau setara dengan 4% (empat persen) dari pendapatan perusahaan secara global. (Juanda, 2019).

Perbedaan besar ini menunjukkan bahwa Eropa memiliki pendekatan yang lebih tegas dan memberikan sanksi yang lebih berat terhadap pelanggaran privasi dan keamanan data pribadi. Dengan Sanksi sebesar itu, Eropa berusaha mendorong para penyelenggara sistem elektronik untuk sangat berhati-hati dalam mengelola dan melindungi data pengguna.

Sementara itu, di Indonesia, Sanksi Administratif yang dijatuhkan kepada penyelenggara sistem elektronik yang gagal melindungi data pengguna terbilang lebih ringan dan lebih fleksibel. Meskipun Sanksi Administratif ini tetap bertujuan untuk memberikan efek jera dan mendorong kepatuhan terhadap peraturan, namun jumlahnya tidak sebesar yang diberlakukan di Eropa.

Perlu diingat bahwa perbedaan ini dapat disebabkan oleh banyak faktor, termasuk perbedaan kondisi ekonomi dan keuangan antara Eropa dan Indonesia, serta perbedaan dalam pendekatan hukum dan regulasi di masing-masing wilayah. Meskipun demikian, perlindungan data pribadi tetap menjadi isu yang penting dan menjadi perhatian di seluruh dunia, termasuk di Indonesia, dan diharapkan para penyelenggara sistem elektronik tetap mengutamakan keamanan dan privasi data pengguna.

Jika upaya penyelesaian sengketa melalui musyawarah atau metode penyelesaian sengketa lainnya tidak berhasil menyelesaikan perselisihan karena kegagalan untuk melindungi kerahasiaan data pengguna, pihak yang terdampak dapat mengajukan gugatan perdata sesuai dengan undang-undang yang berlaku. Pengguna yang data pribadinya disalahgunakan dapat meminta pertanggungjawaban hukum dalam kasus penyalahgunaan data jika mereka memenuhi empat persyaratan yang disebutkan dalam pasal 1365 dari KUH Perdata, meliputi:

1. Adanya perbuatan melawan hukum. Unsur pertama yang harus terpenuhi adalah adanya perbuatan yang melanggar hukum atau dikenal sebagai perbuatan melawan hukum. Artinya, tindakan atau tindakan yang dilakukan oleh pihak lain harus bertentangan dengan hukum atau tidak sah menurut hukum yang berlaku.
2. Adanya kerugian. Unsur kedua adalah adanya kerugian atau kerugian yang dialami

oleh pihak yang terdampak akibat perbuatan melawan hukum tersebut. Kerugian dapat berupa kerugian materiil, seperti kerugian finansial atau kehilangan pendapatan, maupun kerugian immateriil, seperti reputasi yang rusak atau emosi yang terganggu.

3. Adanya hubungan sebab-akibat. Unsur ketiga adalah adanya hubungan sebab-akibat antara perbuatan melawan hukum dan kerugian yang dialami oleh pihak yang terdampak. Artinya, perbuatan melawan hukum tersebut harus menjadi penyebab langsung dari kerugian yang diderita oleh pihak yang terdampak.
4. Adanya kesalahan. Unsur terakhir adalah adanya kesalahan atau kelalaian dari pihak yang melakukan perbuatan melawan hukum. Pihak yang melakukan tindakan tersebut harus bertanggung jawab atas perbuatannya dan dianggap salah atau keliru dalam tindakannya.

Jika keempat unsur tersebut terpenuhi, maka pengguna yang data pribadinya disalahgunakan memiliki dasar hukum untuk mengajukan gugatan perdata dan meminta pertanggungjawaban hukum dari pihak yang bertanggung jawab atas penyalahgunaan data tersebut. Gugatan perdata ini harus diajukan sesuai dengan ketentuan perundang-undangan yang berlaku dan melalui jalur hukum yang sah. Dalam proses gugatan, pengadilan akan melakukan penilaian berdasarkan fakta dan bukti yang ada untuk memutuskan apakah pengguna berhak mendapatkan pertanggungjawaban hukum atas penyalahgunaan data yang dialaminya.

SIMPULAN

Tanggung jawab penyelenggara sistem elektronik terhadap data pengguna bukan hanya merupakan kewajiban etis, tetapi juga memiliki implikasi hukum yang signifikan. Di Indonesia, implikasi hukum tersebut telah di atur dalam berbagai bentuk produk perundang-undangan. Mulai dari Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya yakni Undang-undang No 19 Tahun 2016 Mengenai Informasi dan Transaksi Elektronik. Apabila pengguna merasa dirugikan oleh tindakan penyelenggara sistem elektronik, mereka memiliki opsi untuk mengajukan keluhan kepada Menteri Komunikasi dan Informatika. Namun, menurut Pasal 32 dari Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, jika usaha untuk menyelesaikan perselisihan melalui perundingan atau alternatif lain belum berhasil mengatasi masalah perlindungan data pengguna di platform media sosial, maka pengguna berhak untuk mengambil langkah lebih lanjut dengan mengajukan tuntutan perdata sesuai dengan ketentuan hukum yang berlaku.

Sudah semestinya, pengguna media sosial menggunakan plafform media dengan mengutamakan prinsip kehatian-hatinya. Utamanya kehati-hatian dalam penggunaan data pribadi. Selain itu kepada penyelenggara media sosial, sudah semestinya bertanggung jawab secara penuh terhadap data pribadi pengguna (konsumen) media sosial.

DAFTAR PUSTAKA

Informatika, D. J. (2021). *Persepsi Masyarakat atas Perlindungan Data Pribadi*. t.tp: Direktur Jenderal Aplikasi Informatika.

Ismail Ali, & Andi Sumangelipu. (2023). *Pengantar Hukum Bisnis.* Sengkang: CV Mange.

Ismail Ali, Besse Muqita Dewi, Andi Wahyuddin Nur, & Andi Wira Saputra. (2023). Tinjauan Sosio Yuridis Terhadap Penerapan Sistem Digital Id Berbasis Aplikasi

Pada Dinas Kependudukan Dan Pencatatan Sipil Kabupaten Wajo. *Legal Journal of Law*, 2(2), 25–35. Retrieved from https://jurnal.lamaddukelleng.ac.id/index.php/legal/article/view/70.

Juanda, F. M. (2019). *Tanggungjawab Penyelenggara Sistem Elektronik terhadap Perlindungan Data Pengguna Media Sosial menurut Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*. Jakarta: Uin Syarif Hidayatullah.

R Aswandi, P. R. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS). *Legislatif*, 167-190.

Syaifuddin, A. (2020). Perlindungan Hukum terhadap Para Pihak di dalam Layanan Financial Technology Berbasis Peer to Peer (P2P) Lending (Studi Kasus PT Pasar Dana Pinjaman Jakarta). *Dinamika*, 408-421.

Syamsuddin, M. (2007). *Operasionalisasi Penelitian Hukum*. Jakarta: Raja Grapindo Persada.

Zed, M. (2014). *Metode Penelitian Pustaka*. Jakarta: Yayasan Pustaka Obot.