Eksekusi: Jurnal Ilmu Hukum dan Administrasi Negara
Volume 3, Nomor 2, Mei 2025
e-ISSN: 2987-7113; p-ISSN: 2987-9124, Hal. 51-71
DOI: https://doi.org/10.55606/eksekusi.v3i2.1815
Available Online at: https://journal-stiayappimakassar.ac.id/index.php/Eksekusi

Perbandingan Penerapan Prinsip Transparansi Antara Indonesia dengan Irlandia dalam Hal Terjadinya Kegagalan Pelindungan Data Pribadi

Marsya Iffah Erisar Raib[1*], Sinta Dewi Rosadi[2], Amelia Cahyadini[3]
[1-3] Fakultas Hukum, Universitas Padjadjaran, Indonesia

Email korespondensi: marsya20002@mail.unpad.ac.id

Abstract*. The implementation of the principle of transparency in personal data protection is a crucial aspect in ensuring data subjects right to information relating to the processing of their data. Indonesia has enacted the Personal Data Protection Law (PDP Law) as a legal framework to protect citizens personal data. However, the implementation of the transparency principle in the PDP Law still faces various challenges, including the lack of notification data breach. This research aims to analyze the implementation of the principle of transparency in the event of personal data breach in Indonesia by taking the practice in Ireland as a benchmark for comparison. Ireland, as part of the European Union that adopted the General Data Protection Regulation (GDPR), has a higher level of a transparency and more rigorous enforcement mechanisms. In this research, the author uses a normative juridical method with a descriptive-analytical approach and collects data through literature study and semi-structured interviews. The results of this research show that although the PDP Law regulates the obligation regarding transparency in the event of a data breach, its implementation has proven to be ineffective due to the lack of awareness of data controllers and the absence of implementing regulations. This contrasts with Ireland, which has a better implementation as it is equipped with several supporting factors, including the existence of an independent authority. Therefore, it is necessary to strengthen regulations, establish independent supervisory institutions, and increase the awareness and compliance of data controllers to achieve a more optimum protection of personal data.*

Keywords*: Personal, Data, Protection, The Principle, of Transparency.*

Abstrak. Penerapan prinsip transparansi dalam pelindungan data pribadi merupakan aspek krusial dalam memastikan hak subjek data atas informasi yang berkaitan dengan pemrosesan data mereka. Indonesia telah mengesahkan Undang-Undang Pelindungan Data Pribadi (UU PDP) sebagai payung hukum dalam melindungi data pribadi masyarakat. Namun implementasi prinsip transparansi dalam UU PDP masih menghadapi berbagai tantangan, termasuk kurangnya notifikasi terkait kegagalan pelindungan data pribadi. Penelitian ini bertujuan untuk menganalisis penerapan prinsip transparansi dalam kegagalan pelindungan data pribadi di Indonesia dengan menjadikan praktik di Irlandia sebagai tolok ukur perbandingan. Irlandia sebagai bagian dari Uni Eropa yang mengadopsi *General Data Protection Regulation* (GDPR), memiliki tingkat transparansi yang lebih tinggi serta mekanisme penegakan hukum yang lebih ketat. Dalam penelitian ini, penulis menggunakan metode yuridis normatif dengan pendekatan deskriptif analitis, serta mengumpulkan data melalui studi kepustakaan dan wawancara semi-terstruktur. Hasil penelitian ini menunjukkan bahwa meskipun UU PDP mengatur kewajiban mengenai transparansi dalam hal adanya kegagalan pelindungan data, implementasinya terbukti belum efektif akibat kurangnya kesadaran pengendali data dan ketiadaan peraturan pelaksana. Hal ini tentu berbeda dengan negara Irlandia yang memiliki implementasi yang lebih baik karena dilengkapi dengan beberapa faktor pendukung, termasuk adanya otoritas independen. Oleh karena itu diperlukan penguatan regulasi, pembentukan lembaga pengawas yang independen, serta peningkatan kesadaran dan kepatuhan pengendali data guna mewujudkan pelindungan data pribadi yang lebih optimal.

Kata Kunci: Pelindungan, Data, Pribadi, Prinsip, Transparansi, Indonesia, Irlandia

1. PENDAHULUAN

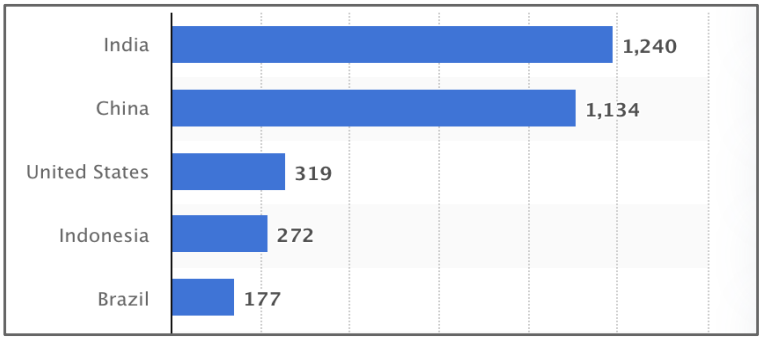
Perkembangan teknologi yang pesat telah membawa peradaban manusia ke dalam babak baru, yakni babak di mana internet hadir dan mengubah pola dan gaya hidup manusia. Layaknya kehidupan manusia yang kian berkembang dari masa ke masa, penggunaan internet juga kian berevolusi seiring dengan berkembangnya zaman. Berawal dari gagasan untuk

Received Februari 10, 2025; Revised Februari 25, 2025; Accepted Maret 11, 2025; Online Available Maret 15, 2025

melakukan pengiriman informasi melalui suatu jaringan (Asa Briggs & Peter Burke, 2000), kini penggunaan internet telah berkembang menjadi pusat akses universal bagi manusia dalam mengolah, memproses, mengakses, serta menghasilkan berbagai bentuk informasi dengan akurat (Munir, 2017).

Salah satu tonggak utama dalam evolusi internet terjadi ketika masyarakat memasuki era Web 2.0, yakni perkembangan generasi kedua dari situs web di mana pengguna tidak hanya menjadi konsumen, melainkan juga menjadi produsen dalam hal pendistribusian informasi (Harris, 2009). Pada era tersebut, evolusi menyebabkan perubahan desain web yang semula hanya bersifat satu arah, menjadi dua arah dengan penambahan fitur baru untuk berkomunikasi serta berbagi informasi (Puspitasari & Irwansyah, 2022). Fitur-fitur tersebut yang banyak digunakan sehingga menarik banyak pengguna hingga saat ini, serta memicu kemunculan berbagai aplikasi dan media sosial lainnya dalam perkembangannya (Facebook, X, dan Instagram). Luasnya jangkauan pengguna yang dapat dicapai tanpa mengenal batas ruang dan waktu, menyebabkan angka penggunaan internet kian meningkat secara signifikan dari waktu ke waktu (Ramli, 2006). Internet telah berkembang menjadi teknologi multidimensi yang menawarkan banyak peluang bagi para penggunanya, sehingga menjadikannya sebagai komponen vital dalam keseharian manusia (Joshi, 2022).

Fenomena tingginya angka penggunaan internet menyebar luas ke seluruh penjuru dunia, termasuk Indonesia. Menurut data yang diperoleh dari hasil survei yang dilakukan oleh Statista pada Desember 2023, negara Indonesia menempati peringkat keempat sebagai negara dengan pengguna internet terbanyak di dunia, dengan total 272 juta pengguna. Sedangkan posisi pertama diperoleh negara India dengan jumlah 1,240 miliar pengguna (Statista, 2023).



Gambar 1. Jumlah Pengguna Internet Tahun 2023

Kenyataan menunjukkan bahwa penggunaan internet telah menjadi bagian integral dari kehidupan sehari-hari masyarakat di Indonesia. Hal ini didukung oleh data yang diperoleh melalui survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), yang menunjukkan bahwa persentase penetrasi internet di Indonesia pada tahun 2024 telah mencapai 79,5% dari

total penduduk Indonesia atau setara dengan 221.563.479 pengguna di Indonesia. Menanggapi fenomena ini, Ketua Umum APJII, Muhammad Arif, mengungkapkan bahwa angka tersebut telah mengalami peningkatan yang signifikan dalam lima tahun terakhir, dengan pandemi COVID-19 yang menjadi salah satu faktor utama pendorong kenaikan angka tersebut di mana mayoritas masyarakat hanya dapat berinteraksi secara virtual.

Dalam beberapa dekade terakhir, kebiasaan masyarakat modern kian bergantung pada internet untuk memenuhi kebutuhan sehari-harinya. Sayangnya, kebiasaan penggunaan internet yang tinggi menimbulkan isu lain seperti terdistorsinya atau terganggunya aspek privasi dari masyarakat itu sendiri. Padahal privasi merupakan bagian dari hak asasi manusia yang tidak dapat diganggu gugat. Bahkan hak tersebut telah dijamin perlindungannya oleh Undang-Undang Dasar 1945 (UUD 1945) yang berbunyi:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi."

Meskipun tidak disebutkan secara eksplisit, pasal tersebut secara implisit mengamanatkan pengakuan dan penghormatan terhadap privasi setiap individu. Namun, kenyataaan menunjukkan bahwa penegakan atas hak asasi tersebut secara perlahan kian tergerus oleh dampak penggunaan internet yang masif seperti saat ini.

Perkembangan teknologi yang pesat membuka ruang yang luas bagi berbagai pihak untuk mengakses beragam bentuk data, yang menimbulkan tantangan baru dalam menjaga hak privasi milik tiap individu. Internet menjadi media yang rentan disalahgunakan dengan ragamnya tindak kejahatan berbasis teknologi atau yang dikenal dengan istilah cybercrime yang terjadi (Tahir, 2010). Dilansir melalui data analisis Badan Siber dan Sandi Negara (BSSN), terdapat beberapa potensi ancaman siber yang diprediksi akan muncul pada tahun 2024, diantaranya *ransomware, phishing, cyber threats based artificial intelligence, web defacement, internet of things attack, dan distributed denial of service* (Direktorat Operasi Keamanan Siber, 2023). Melihat ragamnya potensi ancaman tersebut, dapat dipahami bahwa data pribadi menjadi unsur penting yang rawan dimanfaatkan oleh oknum-oknum yang tidak bertanggung jawab dalam menjalankan cybercrime tersebut.

Pasalnya, banyak platform digital yang mensyaratkan penggunanya untuk memberikan data pribadi mereka demi mengakses layanan tersebut. Bahkan, pengguna platform juga sering kali diminta untuk menyetujui syarat dan ketentuan pada platform yang memuat ketentuan klausula baku mengenai pengelolaan dan pengarsipan data pribadi pengguna guna peningkatan layanan pada platform. Sebab bagi banyak perusahaan, data pribadi yang diperoleh merupakan

aset berharga yang dapat digunakan untuk mengembangkan unit bisnisnya. Sementara di lain sisi, masih banyak pengguna yang tidak menyadari akan potensi hilangnya privasi yang dapat mengancam mereka di kemudian hari.

Terlebih pada era digitalisasi, pemrosesan atas suatu kumpulan data secara masif dan eskalatif atau yang dikenal dengan istilah "Big Data" (Budhijanto, 2022), dapat dilakukan dengan didukung dengan kemajuan teknologi terkini. Perilaku dan preferensi konsumen yang diolah dalam bentuk data, digunakan untuk kepentingan perusahaan dalam menentukan langkah bisnis selanjutnya, serta meningkatkan profit perusahaan kedepannya. Data pribadi saat ini telah menjadi sumber daya bernilai ekonomi tinggi. Bahkan belakangan ini data digadang-gadang telah menggantikan posisi minyak bumi dengan munculnya slogan "*Data is the New Oil*" yang ramai menjadi perbincangan publik.

Meskipun data telah menyumbang kontribusi yang signifikan dalam perkembangan ekonomi digital, tetapi pada waktu yang bersamaan menimbulkan tantangan baru lainnya. Situasi saat ini menunjukkan bahwasannya masih banyak perusahaan yang gagal melindungi data pribadi konsumennya dengan maraknya kebocoran data pribadi yang terjadi. Hal tersebut dibuktikan dengan tingginya angka trafik anomali serangan siber di Indonesia pada yang mencapai jumlah 403.990.813 serangan sepanjang tahun 2023. Oleh sebab itu, perlindungan atas data pribadi merupakan urgensi yang tidak dapat diabaikan dan wajib diupayakan perlindungannya baik oleh pemerintah, perusahaan, serta seluruh komponen masyarakat terkait.

Dalam perspektif hukum positif Indonesia sendiri, pemerintah Indonesia telah berupaya melindungi data pribadi masyarakatnya melalui pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). UU PDP secara resmi disahkan pada tanggal 17 Oktober 2022 sebagai bentuk komitmen pemerintah dalam menjunjung hak privasi masyarakat Indonesia. Meskipun sebelumnya ketentuan mengenai privasi telah diatur oleh beberapa peraturan yang tersebar pada beberapa sektor, namun pembentukan UU PDP menjadi jawaban dari kebutuhan pengaturan yang lebih spesifik atau *sui generis* mengenai perlindungan data pribadi pada era global ini (Rosadi & Pratama, 2018).

Sementara pada prosesnya, perumusan ketentuan dalam UU PDP banyak mengacu pada ketentuan The European Union General Data Protection Regulation (GDPR) sebagai standar global dari regulasi mengenai perlindungan data pribadi. Sejak tahun 2018, GDPR resmi diberlakukan pada negara Uni Eropa yang menggantikan posisi EU Directive sebagai pedoman atas pemrosesan data pribadi. GDPR memuat klausul-klausul yang menekankan pada kontrol data yang dapat dipersonalisasi, sehingga menempatkan pemilik data sebagai pengendali data

serta membatasi kuasa perusahaan atas pemrosesan data (Sczepański, 2020). Secara umum, UU PDP mengadopsi beberapa ketentuan pokok pada GDPR, termasuk diantaranya ketentuan mengenai hak dan kewajiban subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi dalam mewujudkan perlindungan data pribadi.

Dalam hal ini, pembentukan UU PDP tentu tidak lepas dari asas-asas hukum yang berlaku sebagai pedoman dalam penyelenggaraannya. Menurut Satjipto Rahardjo, asas hukum merupakan "jantung" daripada peraturan hukum yang mana perumpamaan tersebut lahir atas dasar fungsi asas hukum sebagai landasan dan alasan lahirnya suatu peraturan hukum (Rokilah & Sulasno, 2021). Hal ini juga berlaku pada pembentukan UU PDP, yang didasarkan atas beberapa asas-asas hukum terkait. Ketentuan pada Pasal 3 UU PDP, menyebutkan penyelenggaraan regulasi tersebut berasaskan beberapa asas, diantaranya asas pelindungan, asas kepastian hukum, asas kepentingan umum, asas kemanfaatan, asas kehati-hatian, asas keseimbangan, asas pertanggungjawaban, dan asas kerahasiaan.

Meskipun demikian, terdapat juga prinsip lain yang tidak disebutkan secara tersurat pada pasal tersebut namun memiliki peran esensial dalam implementasinya, yaitu prinsip transparansi. Transparansi menjadi prinsip yang penting dalam mengupayakan keterbukaan pengendali data mengenai pemrosesan data milik subjek data pribadi. Adapun prinsip ini bertujuan untuk memberikan kontrol yang lebih besar kepada subjek data pribadi atas informasi pribadi mereka serta membangun kepercayaan antara pengendali data dan masyarakat sebagai bagian dari subjek data.

Dalam hal ini, pengendali data memiliki tanggung jawab untuk menerapkan prinsip transparansi ketika melakukan pemrosesan data pribadi milik subjek data. Hal ini selaras dengan ketentuan pada Pasal 27 UU PDP, di mana arti "transparan" dimaknai sebagai berikut:

"Yang dimaksud dengan "transparan" adalah pemrosesan Data Pribadi dilakukan dengan memastikan bahwa Subjek Data Pribadi telah mengetahui Data Pribadi yang diproses dan bagaimana Data Pribadi tersebut diproses, serta setiap informasi dan komunikasi yang berkaitan dengan pemrosesan Data Pribadi tersebut mudah diakses dan dipahami, dengan menggunakan bahasa yang jelas."

Adapun ketentuan tersebut diadopsi melalui ketentuan yang tercantum pada Recital 58 EU GDPR yang menyatakan bahwa pemrosesan data harus dilakukan dengan cara yang transparan, serta hak subjek data untuk memperoleh informasi yang jelas mengenai pemrosesan data pribadi mereka. Dengan demikian, penerapan prinsip transparansi diharapkan dapat mendorong keterbukaan pengendali data pribadi mengenai pemrosesan data pribadi milik subjek data.

Namun pada kenyataannya, penerapan praktik transparansi belum diterapkan secara optimal oleh pengendali data pribadi di Indonesia. Hal ini salah satunya dapat dilihat dari hampir tidak ditemukannya pemberitahuan atas kegagalan pelindungan data pribadi yang disampaikan oleh penyedia layanan digital sebagai pengendali data ketika terjadi indikasi kegagalan pelindungan data pribadi milik pengguna. Padahal, UU PDP telah menetapkan kewajiban bagi pengendali data untuk melakukan notifikasi tertulis kepada subjek data yang terdampak selambat-lambatnya 3 x 24 (tiga kali dua puluh empat) jam. Ketentuan tersebut merupakan salah satu bentuk konkret dari penerapan prinsip transparansi, yang bertujuan untuk memastikan bahwa subjek data memiliki informasi yang jelas mengenai data pribadi mereka.

Sayangnya praktik tersebut tidak hanya ditemukan di Indonesia, tetapi juga di Irlandia. Pada September lalu, Data Protection Comission (DPC) Irlandia baru saja mengenakan denda sebesar €91 juta kepada Meta Platforms Ireland Limited (Meta Irlandia), kantor pusat perusahaan Meta Platforms di Irlandia, atas pelanggaran pelindungan data pribadi yang dilakukan. Dalam putusannya, DPC mengenakan denda tersebut atas beberapa pelanggaran pada ketentuan GDPR, salah satunya ketentuan pada Pasal 33 ayat (1) dan Pasal 33 ayat (5). Ketentuan pada pasal tersebut mengatur kewajiban pengendali data untuk melakukan notifikasi selambat-lambatnya 3 x 24 jam setelah pengendali data mengetahui adanya kegagalan pelindungan data serta kewajiban pengendali data untuk mendokumentasikan mengenai seluruh fakta, dampak, dan tindakan yang diambil dalam hal terjadi kegagalan pelindungan data pribadi milik subjek data.

Peristiwa tersebut bermula dari kelalaian Meta Irlandia selaku pengendali data dalam menyimpan kata sandi milik subjek data dalam bentuk teks biasa (plain text) dalam sistem internal, tanpa disimpan dalam bentuk enkripsi. Setelah menyadari adanya kesalahan tersebut, Meta Irlandia kemudian melakukan notifikasi baik kepada subjek data maupun kepada DPC atas adanya indikasi kegagalan pelindungan data pribadi tersebut. Sayangnya, notifikasi tersebut melewati tenggat waktu yang telah ditentukan.

Melihat adanya peristiwa tersebut, dapat dilihat bahwa praktik transparansi dalam bentuk notifikasi atas kegagalan pelindungan data pribadi belum diterapkan secara maksimal oleh pengendali data di Irlandia. Meskipun demikian, keberadaan DPC sebagai lembaga independen memiliki peran yang esensial dalam mewujudkan pelindungan data pribadi di Irlandia. DPC berperan aktif dalam menangani berbagai bentuk pelanggaran maupun kegagalan atas pelindungan data pribadi serta melindungi subjek data pribadi di Irlandia.

Dalam hal ini, masyarakat Indonesia sebagai salah satu negara dengan tingkat penetrasi internet tertinggi di dunia sudah saatnya memiliki kesadaran yang lebih dalam mewujudkan pelindungan data pribadi di Indonesia. Adapun kesadaran tersebut meliputi seluruh pelaku terkait, selain subjek data, pengendali data dan pemerintah wajib bekerja sama dalam menciptakan ekosistem yang aman dalam hal pengelolaan data pribadi. Selain itu, penerapan ketentuan UU PDP juga perlu diperkuat guna memastikan hak-hak subjek data terlindungi serta mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab.

Berkaitan dengan proses penulisan tugas akhir ini, peneliti telah melakukan penelusuran lebih lanjut mengenai beberapa penulisan tugas akhir yang telah dilakukan oleh peneliti lain. Berdasarkan penelusuran tersebut, peneliti tidak menemukan penelitian yang serupa dengan judul yang telah peneliti ajukan, tetapi terdapat beberapa penelitian lain dengan tema yang berkaitan diantaranya adalah:

1. "Prinsip Transparansi dalam Penggunaan Kecerdasan Artifisial dalam Profiling Data Konsumen pada Marketplace di Indonesia Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan European General Data Protection Regulation" oleh peneliti bernama Raisa Safina dengan NPM 110110200131 pada tahun 2024. Penelitian ini dibuat dalam bentuk skripsi yang membahas mengenai perbandingan penerapan prinsip transparansi pada penggunaan kecerdasan artifisial untuk profiling data konsumen pada marketplace pada ketentuan UU PDP dan GDPR. Melalui penelitian ini, ditemukan bahwa regulasi mengenai kecerdasan artifisial dalam hal pelindungan data pribadi di Indonesia belum komprehensif apabila dibandingkan dengan Uni Eropa.
2. "Pertanggungjawaban Platform Sosial Media Terhadap Kebocoran Data Pribadi Ditinjau dari Hukum Positif Indonesia" yang ditulis oleh peneliti bernama Rieke Puspa Handini dengan NPM 110110180065 pada tahun 2023. Penelitian ini dibuat dalam bentuk skripsi yang membahas mengenai perlindungan dan pertanggungjawaban hukum atas kebocoran data pribadi pengguna platform media sosial yang diatur melalui ketentuan dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan UU PDP. Melalui penelitian ini, ditemukan bahwa hak konsumen belum sepenuhnya terpenuhi yang disebabkan oleh adanya kegagalan dalam melindungi data pribadi yang merupakan bagian dari tanggung jawab penyelenggara sistem elektronik terkait;

Tujuan penelitian ini adalah menganalisis perbandingan penerapan prinsip transparansi antara Indonesia dengan Irlandia dalam hal terjadinya kegagalan pelindungan data pribadi.

2. METODE PENELITIAN

Metode yang digunakan peneliti dalam penelitian ini adalah metode pendekatan yuridis normatif. Lokasi penelelitian yaitu di Perpustakaan Hukum Universitas Padjadjaran dan Perpustakaan Nasional Republik Indonesia. Penelitian ini menggunakan spesifikasi penelitian bersifat deskriptif analitis. Bahan hukum yang digunakan yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier.

Teknik pengumpulan data yang peneliti gunakan dalam penelitian ini adalah studi kepustakaan dan wawancara semi-terstruktur. Penelitian ini menggunakan analisis data dengan metode normatif kualitatif, yakni analisis data penelitian hukum normatif yang kemudian dianalisis secara deskriptif kualitatif untuk memperoleh pemahaman yang mendalam mengenai permasalahan pada penelitian ini.

3. HASIL DAN PEMBAHASAN

Penerapan Praktik Transparansi pada Kegagalan Pelindungan Data Pribadi di Indonesia Berdasarkan Studi Penerapan Praktik Transparansi pada Negara Irlandia

Penegakan penrapan praktik transparansi dalam pemrosesan data pribadi menjadi hal penting di tengah meningkatnya peristiwa kegagalan pelindungan data pribadi yang mengancam privasi masyarakat di Indonesia. Meskipun pengesahan UU PDP diupayakan menjadi kerangka hukum bagi perlindungan subjek data yang lebih kuat, kenyataannya tantangan dalam implementasinya masih sangat nyata. Praktik transparansi belum sepenuhnya diterapkan secara optimal pada pemrosesan data pribadi oleh pengendali data di Indonesia. Padahal hal tersebut merupakan salah satu bentuk dari penerapan prinsip pelindungan data pribadi yang diamanatkan pada Pasal 16 ayat (2) huruf (f) UU PDP yang berbunyi:

"…pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Pelindungan Data Pribadi;"

Berdasarkan bunyi pasal tersebut, dapat dipahami bahwa pemrosesan data pribadi yang dilakukan oleh pengendali data wajib disertakan dengan pemberitahuan mengenai tujuan, aktivitas pemrosesan, serta kegagalan pelindungan data pribadi sebagai bentuk penerapan praktik transparansi yang diatur dalam ketentuan UU PDP. Praktik atas penerapan prinsip transparansi bukan hanya menjadi kewajiban hukum bagi para pengendali data, melainkan juga langkah penting untuk membangun kepercayaan antara pengendali data dan subjek data. Adapun pemberitahuan mengenai tujuan dan aktivitas pemrosesan data pribadi umumnya dicantumkan melalui dokumen kebijakan privasi yang disediakan oleh pengendali data, khususnya pada layanan digital. Melalui dokumen tersebut, subjek data sebagai pengguna

layanan berhak mendapatkan informasi yang jelas dan lengkap mengenai pemrosesan data pribadi mereka oleh pengendali data.

Selain itu, prinsip transparansi juga menuntut pengendali data untuk mengambil langkah proaktif ketika terjadi kegagalan pada pelindungan data pribad milik subjek data. Berdasarkan ayat tersebut, pengendali data wajib memberikan pemberitahuan yang memadai dan tepat waktu kepada subjek data apabila terdapat indikasi kegagalan pelindungan data pribadi, seperti halnya pencurian data atau akses yang tidak sah oleh pihak yang tidak bertanggung jawab. Sebagai kesimpulan, dapat dipahami bahwa penerapan prinsip transparansi mencakup tidak hanya penjelasan rinci mengenai pemrosesan data pribadi milik subjek data, tetapi juga pada responsifitas pengendali data dalam menghadapi insiden yang berpotensi merugikan subjek data.

Transparansi merupakan perwujudan dari implementasi prinsip pelindungan data pribadi yang berlandaskan pada ketentuan dalam UU PDP. Penerapan prinsip transparansi yang efektif mampu menciptakan kejelasan, keamanan, dan kepercayaan di tengah meningkatnya tantangan dalam pelindungan privasi di era ekonomi digital seperti saat ini. Tanpa adanya praktik transparansi yang optimal, perlindungan atas hak-hak privasi milik subjek data akan sulit tercapai.

Di Indonesia, penerapan praktik transparansi dalam pemrosesan data pribadi, khususnya melalui penyertaan kebijakan privasi, telah menunjukkan tingkat kepatuhan yang cukup tinggi. Hal ini dapat dilihat dari banyaknya penyedia layanan digital selaku pengendali data yang mencantumkan kebijakan privasi pada lamannya. Misalnya pada platform layanan digital transportasi milik PT KAI, Access by KAI, yang menyediakan beberapa informasi penting mengenai pemrosesan data pribadi milik subjek data.

Hal serupa juga ditemukan pada platform layanan digital pembayaran pajak milik DJP, M-Pajak, yang menyertakan kebijakan privasi dengan menyediakan informasi penting mengenai pemrosesan data pribadi yang dilakukan. Kebijakan privasi pada kedua platform layanan digital tersebut mencerminkan bentuk penerapan prinsip transparansi PT KAI dan DJP sebagai pengendali data, dengan menjelaskan tujuan dan aktivitas pemrosesan data pribadi subjek data secara jelas. Terlepas dari adanya beberapa rincian informasi yang berbeda, namun kedua kebijakan privasi tersebut memiliki muatan inti yang serupa, diantaranya seperti penjelasan mengenai jenis data yang dikumpulkan, tujuan pemrosesan data, pihak-pihak yang dapat mengakses data, serta masa retensi penyimpanan data.

Adanya bentuk implementasi tersebut menjadi salah satu tolok ukur kepatuhan pengendali data dalam menerapkan prinsip transparansi. Kewajiban ini bertujuan untuk memastikan perlindungan hak-hak subjek data dalam setiap proses pemrosesan data pribadi. Meskipun ketentuan dalam UU PDP tidak merincikan secara spesifik format atau standar bentuk kebijakan privasi yang harus diadopsi, pengendali data tetap wajib untuk memastikan bahwa kebijakan tersebut memuat informasi mengenai tujuan dan aktivitas pemrosesan sebagai bentuk penegakan prinsip-prinsip transparansi yang diamanatkan dalam UU PDP.

Apabila dibandingkan dengan kebijakan privasi milik Facebook yang diberlakukan di Irlandia, terdapat beberapa perbedaan, terutama pada rincian informasi yang dicantumkan. Sebagai contoh, pada informasi mengenai jenis data yang dikumpulkan, PT KAI hanya mencantumkan jenis data yang diproses secara umum, sementara DJP menguraikan secara rinci data yang direkam ketika pengguna menggunakan aplikasi M-Pajak. Meskipun kebijakan privasi DJP lebih spesifik dalam menyajikan informasi mengenai data yang diproses melalui aplikasinya, Facebook tetap memiliki kebijakan privasi yang lebih komprehensif karena mencantumkan rincian dari setiap kategori data, seperti data pengguna, aktivitas pengguna, relasi pengguna pada aplikasi, data perangkat dan aplikasi, serta informasi atau data lainnya yang diperoleh dari pihak ketiga.

Selain itu, pada informasi mengenai tujuan pemrosesan data, Facebook juga memiliki informasi yang lebih komprehensif. Facebook secara eksplisit mencantumkan lima tujuan utama pemrosesan data pribadi milik pengguna, diantaranya adalah untuk menyediakan dan meningkatkan layanan produk, melindungi dan memberikan keamanan pengguna, melakukan analisis layanan bisnis, berkomunikasi dengan pengguna, serta memanfaatkan data sebagai pendukung riset serta inovasi sosial yang relevan. Di Indonesia, kebijakan privasi PT KAI mencantumkan tujuan pemrosesan data pribadi dalam bentuk poin-poin yang lebih merinci dibandingkan dengan DJP. Namun, Facebook tetap unggul dengan menyajikan informasi tersebut dengan lebih terstruktur, yakni dikategorisasikan ke dalam lima kategori besar sebagaimana yang dijelaskan sebelumnya.

Meskipun demikian, perbedaan tersebut juga dapat dipengaruhi oleh kompleksitas fitur yang ditawarkan oleh masing-masing platform. Seperti halnya Facebook, aplikasi milik PT KAI menyediakan layanan yang lebih bervariasi seperti pemesanan tiket, pengecekan jadwal, pengelolaan riwayat perjalanan, hingga notifikasi perjalanan yang memerlukan pengolahan data pengguna secara lebih luas. Sementara itu, M-Pajak milik DJP lebih berfokus pada fungsi utamanya sebagai platform pembayaran pajak, sehingga ruang lingkup pemrosesan datanya lebih terbatas. Meskipun seluruh platform tersebut telah mencantumkan informasi mengenai

tujuan pemrosesan data, tidak dapat dipungkiri bahwa Facebook memiliki elaborasi tujuan yang lebih komprehensif. Facebook tidak hanya mencakup aspek kebutuhan operasional internal, tetapi juga mempertimbangkan kebutuhan pengguna serta kontribusi yang lebih luas terhadap masyarakat.

Selanjutnya, terkait pemberitahuan mengenai kegagalan pelindungan data pribadi dalam pemrosesan data milik subjek data yang juga menjadi aspek yang tak kalah penting pada penerapan prinsip transparansi. Apabila ditelaah melalui kebijakan privasinya, PT KAI secara eksplisit menyatakan bahwa mereka berupaya semaksimal mungkin untuk melindungi data pribadi milik pengguna. Namun, PT KAI juga mengakui bahwa tidak ada jaminan absolut terhadap keamanan data, sehingga data pribadi pengguna tetap berisiko untuk dicegat, diakses, atau diungkapkan oleh pihak ketiga yang tidak berwenang. Sebaliknya, kebijakan privasi M-Pajak sama sekali tidak mencantumkan mengenai risiko kegagalan pelindungan data pribadi maupun komitmen DJP dalam melindungi data pengguna.

Kendati demikian, sayangnya sampai saat ini praktik pemberitahuan tersebut masih sangat jarang ditemukan implementasinya di Indonesia. Di tengah maraknya pemberitaan mengenai kebocoran data di Indonesia, sangat sedikit instansi atau perusahaan yang secara terbuka menyatakan bahwa data mereka telah mengalami kebocoran. Hal ini tentu saja mencerminkan kekhawatiran perusahaan terhadap dampak negatif pada reputasi mereka, sehingga banyak yang enggan secara terbuka mengakui adanya kegagalan pelindungan data. Padahal, transparansi justru menjadi langkah awal untuk membangun kepercayaan publik dan menunjukkan tanggung jawab pengendali data dalam menangani insiden tersebut.

Hal ini berbeda dengan praktik yang terjadi di Irlandia, di mana MPIL secara mandiri melaporkan insiden kegagalan pelindungan data yang dialami kepada DPC sebagai lembaga yang bertanggung jawab dalam menangani permasalahan mengenai pelindungan data pribadi di Irlandia. Meskipun setelah dilakukan investigasi lebih lanjut DPC menemukan bahwa MPIL melakukan beberapa pelanggaran pada ketentuan GDPR, tetapi sikap MPIL yang berinisiatif untuk melakukan pemberitahuan kepada di kepada para pengguna dan DPC merupakan langkah awal yang baik karena menunjukkan komitmen mereka dalam menjaga keamanan data pribadi para penggunanya.

Adanya peristiwa tersebut menunjukkan bahwa kesadaran akan pentingnya pelindungan data pribadi di Irlandia sudah jauh lebih berkembang dibandingan dengan di Indonesia. Seluruh komponen terkait, baik pemerintah, perusahaan, maupun masyarakat memahami betapa pentingnya transparansi dalam mengupayakan pelindungan data pribadi. Hal ini menciptakan ekosistem yang baik di Irlandia, yakni mendorong seluruh pihak terkait

untuk berpartisipasi dalam menangani setiap dugaan kegagalan pelindungan data pribadi secara aktif.

Dalam hal ini, dapat dipahami bahwa kebudayaan menjadi salah satu faktor pendukung pada penegakan hukum di Irlandia. Meskipun demikan terdapat beberapa faktor penting lainnya yang dapat ditelaah dalam memahami efektivitas hukum di Irlandia. Menurut Soerjono Soekanto, terdapat lima faktor penting yang mempengaruhi penegakan hukum, yaitu faktor hukum itu sendiri, faktor penegak hukum, faktor sarana atau fasilitas, faktor masyarakat, dan faktor kebudayaan.

Apabila mengkaji lebih lanjut berdasarkan penerapan praktik transparansi dalam hal penegakan perlindungan data pribadi, terdapat beberapa perbedaan signifikan pada faktor-faktor yang mempengaruhi penegakan hukum di Irlandia dan Indonesia. Dari segi faktor hukum, Irlandia memiliki dasar hukum yang lebih kuat melalui GDPR, yang tidak hanya memberikan panduan yang jelas tetapi juga menetapkan sanksi yang tegas untuk pelanggaran yang terjadi. Sementara itu, di Indonesia, meskipun UU PDP telah disahkan, implementasinya masih dalam tahap awal. Beberapa peraturan turunan yang diperlukan untuk mendukung pelaksanaannya belum tersedia hingga saat ini, sehingga efektivitas hukumnya belum optimal.

Dalam hal faktor penegak hukum, pemerintah Irlandia menunjuk DPC sebagai lembaga independen untuk mengawasi dan menegakkan ketentuan GDPR. Sebaliknya, di Indonesia, hingga saat ini belum ada pembentukan lembaga khusus sebagaimana yang diamanatkan dalam UU PDP untuk menangani pelindungan data secara lebih khusus. Akibatnya, tanggung jawab terkait penegakan hukum dalam pelindungan data pribadi masih berada di bawah Kementerian Komunikasi dan Digital (Kemenkomdigi). Pembentukan lembaga independen oleh pemerintah Indonesia memungkinkan proses penegakan hukum atas perlindungan data pribadi masyarakat Indonesia berjalan lebih efektif dan efisien, tentunya dengan sumber daya yang dialokasikan khusus untuk menangani lingkup tersebut.

Sementara dari sisi faktor sarana atau fasilitas untuk menangani kasus pelindungan data pribadi, Indonesia masih tertinggal apabila dibandingkan dengan Irlandia. Salah satu contohnya adalah dalam hal pelaporan dugaan kegagalan pelindungan data pribadi. Di Irlandia, melalui laman resmi DPC, tersedia serangkaian formulir yang dirancang khusus untuk memudahkan pelaporan insiden pelindungan data pribadi. Menariknya, formulir ini dapat diisi oleh berbagai pihak, termasuk pengendali data, prosesor data, maupun subjek data yang terdampak langsung maupun tidak. Hal ini tentu mencerminkan pendekatan inklusif yang diterapkan Irlandia dalam menangani pelanggaran data pribadi yang terjadi. Di Indonesia, meskipun formulir pelaporan insiden juga tersedia melalui laman

https://komin.fo/formkebocorandatapribadi, namun formulir tersebut hanya dapat diserahkan oleh pengendali data kepada Kemenkomdigi.

Terakhir, dari segi faktor kebudayaan, budaya hukum di Irlandia mencerminkan nilai-nilai transparansi dan akuntabilitas yang telah terinternalisasi hampir di seluruh lapisan masyarakat, baik pemerintah, perusahaan, maupun masyarakat itu sendiri. Di Indonesia, budaya hukum terkait pelindungan data pribadi masih dalam tahap perkembangan. Rendahnya kepatuhan perusahaan terhadap regulasi dan kurangnya perhatian terhadap privasi data menunjukkan bahwa perubahan budaya hukum membutuhkan waktu dan upaya yang konsisten.

Ditambah lagi dengan kurangnya perhatian masyarakat terhadap isu pelanggaran privasi data, yang berdampak pada persepsi yang kurang sensitif terhadap pentingnya perlindungan data pribadi. Sayangnya, anomali yang terjadi adalah perusahaan sering kali lebih khawatir terhadap dampak negatif terhadap reputasi mereka daripada menjalankan tanggung jawab untuk mematuhi regulasi yang berlaku. Hal ini menyebabkan banyak perusahaan di Indonesia yang cenderung menghindari penerapan prinsip transparansi yang oprimal, terutama dalam menghadapi insiden kegagalan pelindungan data pribadi, karena khawatir akan menurunnya reputasi atau hilangnya kepercayaan dari subjek data. Padahal, persepsi seperti ini sudah seharusnya diperbaiki, karena transparansi dalam pelaporan insiden justru akan memperkuat kepercayaan publik dan menunjukkan komitmen perusahaan terhadap pelindungan data pribadi, yang pada akhirnya dapat membangun reputasi yang lebih baik dalam jangka panjang.

Perbandingan penerapan transparansi dalam pemrosesan data pribadi di Indonesia dan Irlandia menunjukkan perbedaan yang signifikan, baik dari segi regulasi, kesiapan lembaga, maupun budaya hukum. Irlandia, dengan dukungan GDPR yang kuat, telah berhasil menciptakan ekosistem transparansi yang komprehensif melalui lembaga independen seperti DPC yang mampu menindaklanjuti pelaporan insiden secara responsif.

Sebaliknya, Indonesia masih menghadapi tantangan besar dalam menegakkan prinsip transparansi, terutama akibat belum disahkannya Rancangan Peraturan Pemerintah (RPP) sebagai peraturan turunan dari UU PDP (RPP PDP). Padahal dalam RPP PDP, terdapat ketentuan mengenai arahan teknis yang lebih mendetail, seperti hal-nya penerapan prinsip transparansi yang mengacu pada Pasal 30 RPP PDP bahwa:

“Dalam rangka penerapan prinsip pemrosesan Data Pribadi dilakukkan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Pelindungan Data Pribadi sebagaimana dimaksud dalam Pasal 24 huruf f, Pengendali Data Pribadi harus:

a. menentukan secara jelas tujuan dari pemrosesan Data Pribadi dan memberitahukan tujuan tersebut kepada Subjek Data Pribadi;
b. menyusun dan menetapkan pemberitahuan Pelindungan Data Pribadi dalam bentuk dokumen;
c. menerapkan pengendalian teknis dan organisasi dalam hal pencegahan kegagalan Pelindungan Data Pribadi;
d. memberikan pemberitahuan tertulis kepada Subjek Data Pribadi dan Lembaga PDP saat terjadi kegagalan Pelindungan Data Pribadi yang paling sedikit memuat informasi terkait:
    1. Data Pribadi yang terungkap;
    2. deskripsi jenis kegagalan Pelindungan Data Pribadi;
    3. waktu dan cara Data Pribadi terungkap;
    4. dampak kegagalan Pelindungan Data Pribadi terhadap Subjek Data Pribadi;
    5. upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi; dan
    6. informasi narahubung.
e. menetapkan dan melaksanakan kebijakan, prosedur, dan/atau pedoman mengenai pencegahan dan penanganan kegagalan Pelindungan Data Pribadi yang paling sedikit memuat:
    1. pembagian peran dan tanggung jawab penanganan kegagalan Pelindungan Data Pribadi;
    2. mekanisme untuk melakukan analisis, klasifikasi, prioritisasi, pemantauan, penanganan, dan penyelesaian kegagalan Pelindungan Data Pribadi, termasuk pasca kejadian;
    3. dokumentasi penanganan kegagalan Pelindungan Data Pribadi dan mekanisme pelaporan kepada Subjek Data Pribadi dan Lembaga PDP; dan
    4. peninjauan dan pembaruan berkala proses penanganan kegagalan Pelindungan Data Pribadi; dan
f. melakukan pemberitahuan kegagalan Pelindungan Data Pribadi terhadap Subjek Data Pribadi dan Lembaga PDP sesuai dengan ketentuan peraturan perundang-undangan."

Namun ketidakpastian pada pengesahan RPP PDP tersebut turut berdampak pada ketidakjelasan berbagai mekanisme implementasi UU PDP, termasuk pembentukan lembaga independen yang bertanggung jawab secara khusus atas pelindungan data pribadi. Sampai saat ini, RPP PDP sebagai peraturan pelaksana UU PDP belum disahkan dan masih dalam proses harmonisasi di bawah Kementerian Hukum dan Hak Asasi Manusia (Kemenkumham).

Padahal, UU PDP seharusnya sudah mulai berlaku efektif pada 17 Oktober 2024 lalu. Namun tanpa adanya peraturan pelaksana yang mendukung, implementasi UU PDP tidak dapat berjalan secara optimal terutama penegakan prinsip transparansi yang sudah seharusnya diimplementasikan secara utuh oleh pengendali data saat ini.

Hal ini selaras dengan tanggapan Ditjen Aptika ketika melakukan sesi wawancara dengan penulis. Dalam sesi wawancara tersebut, Ditjen Aptika juga menyoroti tantangan mengenai kepatuhan pengendali data yang salah satunya disebabkan oleh belum tersedianya ketentuan teknis atas provisi yang diatur dalam UU PDP. Dengan arti lain, bahwa seluruh industri belum memiliki pedoman yang jelas dan pasti mengenai regulasi pelindungan data pribadi yang berlaku. Namun demikian, beliau kembali menekankan bahwa seharusnya ketentuan yang terdapat dalam UU PDP diimplementasikan tanpa harus menunggu pengesahan daripada peraturan pelaksananya, terlebih dengan diberikannya waktu 2 tahun sebagai masa peralihan. Meskipun efektivitas implementasi UU PDP belum dapat sepenuhnya dinilai karena baru mulai berlaku aktif, Beliau menambahkan bahwa seluruh pelaku industri terkait seharusnya menyadari tujuan utama dari kepatuhan tersebut adalah melindungi data pribadi pelanggan, yang pada akhirnya akan membangun kepercayaan dan reputasi yang baik.

Kendati demikian, meskipun Indonesia masih menghadapi tantangan mendasar dibandingkan Irlandia dalam penegakan pelindungan data, seperti salah satunya pada proses pembentukan RPP PDP. Namun, penyusunan rancangan peraturan presiden tersebut mencerminkan komitmen pemerintah untuk membangun sistem perlindungan data yang lebih kuat.

Upaya Hukum Subjek Data Pribadi pada Peristiwa Kegagalan Pelindungan Data Pribadi di Indonesia

Dalam konteks kegagalan pelindungan data pribadi, upaya hukum menjadi aspek penting yang dapat ditempuh oleh subjek data pribadi untuk memastikan perlindungan atas hak-hak mereka. Apabila ditelaah lebih dalam, subjek data pribadi yang dirugikan umumnya memiliki hak untuk menuntut ganti rugi berdasarkan prinsip based on fault, yakni tanggung jawab oleh pengendali data apabila terdapat kesalahan atau kelalaian dalam menjalankan kewajibannya untuk melindungi data milik subjek data pribadi. Selain itu, upaya hukum juga merupakan bentuk kepastian hukum bagi subjek data dalam menuntut hak-haknya di hadapan hukum.

Di Irlandia, terdapat beberapa upaya yang dapat dilakukan oleh subjek data dalam menghadapi kegagalan pelindungan data pribadi. Dalam hal upaya hukum, subjek data dapat meminta ganti rugi kepada pengendali data atas kerugian yang dideritanya dengan mengajukan permohonan ganti rugi kepada pengendali data sesuai dengan ketentuan pada Article 82 (1) GDPR:

"*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*."

Berdasarkan bunyi pasal tersebut, subjek data memiliki hak untuk menerima kompensasi atau ganti rugi atas kerugian materi atau non-materi atas pelanggaran yang dilakukan oleh pengendali dan prosesor data pribadi. Sayangnya, istilah "*non-material damage*" atau kerugian non-material tidak didefinisikan secara tegas dalam regulasi tersebut sehingga membuka ruang interpretasi yang cukup luas.

Kendati demikian, terdapat salah satu contoh kasus gugatan mengenai kerugian non-material yang terjadi di Irlandia pada tahun 2023, yakni kasus Kaminski v. Ballymaguire yang menjadi acuan penting dalam memahami penerapan konsep ganti rugi non-material. Kasus tersebut bermula ketika Kaminski selaku penggugat merupakan karyawan daripada Ballymaguire Foods Limited, sebuah perusahaan produsen makanan siap saji terbesar di Irlandia, menggugat Ballymaguire atas penggunaan rekaman CCTV dirinya tanpa izin sebagai materi pelatihan untuk peningkatan praktik keamanan pangan pada pabrik. Meskipun tergugat berdadlil bahwa wajah penggugat telah disamarkan dalam rekaman tersebut, penggugat merasa tetap dapat dikenali melalui gerakan dan postur fisiknya. Kaminski mengklaim bahwa tindakan tersebut melanggar ketentuan pada GDPR dan Data Protection Act 2018, yang mengakibatkan dirinya mengalami kerugian non-material berupa kecemasan, rasa, malu, penghinaan, serta gangguan tidur akibat komentar kolega setempat yang menyaksikan rekaman tersebut.

Pengadilan kemudian memutuskan bahwa penggugat berhak memperoleh ganti rugi sebesar €2,000 (dua ribu euro) atas kerugian non-material yang dideritanya. Dalam pertimbangannya, Hakim O'Connor merujuk pada putusan Court of Justice European Union (CJEU) atau Mahkamah Hukum Uni Eropa dalam kasus The Austrian Post, yang merupakan putusan pertama terkait kerugian non-material. Selain itu, terdapat beberapa pertimbangan lainnya oleh hakim, di antaranya bahwa "pelanggaran belaka" tidak cukup untuk menjamin pemberian kompensasi. Kerugian non-material harus nyata dan tidak bersifat spekulatif, serta harus didukung dengan bukti yang memadai seperti bukti medis.

Selain upaya hukum, subjek data juga dapat mengajukan upaya administratif melalui DPC sebagai Otoritas Pelindungan Data Pribadi di Irlandia untuk menangani keluhan data pribadi mereka oleh pengendali data. Namun sebelum mengajukan keluhan, subjek data harus terlebih dahulu mencoba menyelesaikan masalah tersebut secara langsung dengan pengendali data terkait. Apabila masalah tersebut tidak dapat diselesaikan, DPC akan menilai keluhan tersebut untuk memastikan apakah masalah tersebut berada dalam ruang lingkup kewenangannya.

Setelah penilaian, DPC akan berupaya untuk menyelesaikan masalah secara musyawarah dengan menghubungkan subjek data dengan pengendali data. Dalam hal pendekatan tersebut gagal, DPC dapat mengambil langkah-langkah lebih lanjut, termasuk memberi saran, mengeluarkan pemberitahuan penagakan, atau bahkan melakukan penyelidikan terhadap praktik pengendali data. Apabila diperlukan, DPC juga dapat mengupayakan tindakan korektif melalui wewenangnya, seperti mengeluarkan peringatan, teguran, dan denda. Dalam kasus pelanggaran serius, seperti pelanggaran besar atau masalah yang bersifat sistemik, DPC dapat melakukan penyelidikan dan mengenakan sanksi yang substansial, termasuk denda administratif hingga €20 juta atau 4% dari omset tahunan pengendali data. Tindakan ini tentu bertujuan untuk memastikan bahwa pengendali mematuhi regulasi pelindungan data dan hak-hak milik subjek data dilindungi dengan baik.

Sementara itu di Indonesia, ketentuan mengenai gugatan dan penerimaan ganti rugi oleh subjek data diatur pada Pasal 12 ayat (1) UU PDP yang berbunyi:

“Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

Sayangnya, pasal tersebut hanya menyebutkan hak subjek data tanpa mengelaborasikan lebih lanjut mengenai mekanisme gugatan dan penerimaan ganti rugi oleh subjek data, melainkan pada ayat berikutnya dijelaskan bahwa rincian mengenai tata cara tersebut diatur lebih lanjut melalui Peraturan Pemerintah terkait.

Meksipun demikian, RPP PDP memuat ketentuan mekanisme gugatan dan penerimaan ganti rugi oleh subjek data dalam hal pelanggaran yang disebabkan oleh kesalahan dan kelalaian pengendali data. Serupa dengan ketentuan dalam GDPR, ganti rugi dalam RPP PDP juga dibagi ke dalam dua bentuk, yaitu ganti rugi material dan ganti rugi non-material. Namun, apabila GDPR tidak memberikan penjelasan lebih lanjut mengenai cakupan dari kerugian tersebut, RPP PDP justru memberikan definisi yang jelas. Berdasarkan Pasal 116 ayat (3), ganti rugi non-material didefinisikan sebagai:

"Ganti rugi non-materiel berupa tindakan pemulihan atau tindakan lain selain pemberian sejumlah uang untuk memulihkan kondisi pelindungan terhadap Data Pribadi Subjek Data Pribadi kepada kondisi sebelum terjadinya pelanggaran pemrosesan Data Pribadi sesuai kewajiban Pengendali Data Pribadi dan/atau Prosesor Data Pribadi pada peraturan perundang-undangan."

Sebaliknya, ganti rugi material didefinisikan pada Pasal 116 ayat (2) sebagai:

"Ganti rugi materiel berupa pemberian sejumlah uang dengan nilai setara kerguian yang diderita oleh Subjek Data Pribadi akibat kegiatan pemrosesan oleh Pengendali Data Pribadi dan/atau Prosesor Data Pribadi"

Berdasarkan ketentuan tersebut, dapat dipahami bahwa RPP PDP dan GDPR memiliki ketentuan yang serupa dalam mengupayakan hak subjek data atas ganti rugi, namun apabila ditelaah lebih lanjut pendekatan daripada kedua kebijakan tersebut cukup berbeda. GDPR mengklasifikasikan "kerugian material" dan "kerugian non-material" untuk merujuk pada bentuk kerugian yang dialami oleh subjek data. Di sisi lain, RPP PDP mengklasifikasikan "ganti rugi material" dan "ganti rugi non-material", yang lebih menekankan pada bentuk kompensasi yang diterima oleh subjek data guna memulihkan kondisi akibat pelanggaran yang terjadi.

Meskipun terlihat serupa, kedua konsep ini memiliki perbedaan. Dalam konteks GDPR, meskipun subjek data menderita kerugian non-material, mereka tetap berhak menerima ganti rugi material, sebagaimana ditunjukkan dalam kasus Kaminski v. Ballymaguire di Irlandia. Sebaliknya, pendekatan dalam RPP PDP cenderung menekankan pada bentuk kompensasi yang sesuai dengan jenis kerugian yang diderita, baik dalam pemulihan secara non-material maupun pembayaran material. Dari kedua pendekatan tersebut, GDPR dapat dikatakan memiliki sifat yang lebih fleksibel namun membuka ruang intepretasi yang luas bagi pengadilan untuk menentukan jenis dan nilai ganti rugi yang sesuai dengan kerugian yang diderita subjek data. Sebaliknya, ketentuan dalam RPP PDP menawarkan kejelasan yang lebih mengenai bentuk kompensasi yang dapat diterima oleh subjek data dalam lingkup sengketa perdata.

RPP PDP mengatur ketentuan subjek data untuk mengajukan permintaan ganti rugi atas pelanggaran pemrosesan data pribadi kepada pengendali dengan menyampaikan beberapa bukti pendukung. Sementara di lain sisi, pengendali data juga diwajibkan untuk menyediakan media komunikasi untuk pengajuan permintaan ganti rugi oleh subjek data. Dalam hal menentukan nilai ganti rugi, para pihak dapat menempuh upaya penyelesaian sengketa melalui pengadilan ataupun di luar pengadilan sesuai dengan kesepakatan yang dicapai.

Dalam hal pengendali data menolak untuk memberikan ganti rugi tidak memenuhi permintaan yang diajukan oleh subjek data, maka subjek data memiliki hak untuk mengajukan permohonan penyelesaian sengketa kepada Lembaga Pelindungan Data Pribadi (Lembaga PDP) untuk memperoleh kesepakatan mengenai bentuk dan besaran ganti rugi atau tindakan tertentu lainnya untuk menjamin hal serupa tidak akan terulang kembali. Lembaga PDP berwenang untuk menyediakan fasilitas penyelesaian sengketa dengan mengutamakan mediasi, kecuali para pihak sepakat untuk menggunakan cara lain.

Proses penyelesaian sengketa melalui Lembaga PDP diawali dengan proses negosiasi antara para pihak yang bersengketa pada pertemuan pertama. Negosiasi ini bertujuan untuk mencapai kesepakatan perdamaian dalam jangka waktu maksimal 14 hari. Apabila dalam waktu tersebut kesepakatan belum tercapai, mediator akan menentukan agenda dan jadwal mediasi pada pertemuan berikutnya bagi para pihak untuk menemukan solusi selanjutnya.

Apabila dalam jangka waktu 30 hari para pihak kembali tidak mencapai kesepakatan, para pihak dapat meminta perpanjangan waktu apabila dirasa perlu yang akan diajukan oleh mediator kepada pimpinan Lembaga PDP. Namun apabila melalui mediasi para pihak tetap tidak mencapai kesepakatan, maka para pihak dapat melanjutkan penyelesaian sengketa melalui jalur arbitrase atau pengadilan, atau bahkan menghentikan proses sengketa. Dengan adanya mekanisme tersebut, penyelesaian sengketa diharapkan dapat berjalan secara efektif, transparan, dan menjamin perlindungan hak-hak dari setiap pihak yang terlibat.

Namun sebagaimana yang telah dijelaskan sebelumnya, bahwa RPP PDP sampai saat ini belum disahkan sehingga belum ada mekanisme yang jelas mengenai pengjuan gugatan dan ganti rugi tersebut di Indonesia. Akibatnya, subjek data yang dirugikan dalam kasus pelanggaran menghadapi kendala dalam memperoleh keadilan dan kepastian hukum. Ketidakjelasan ini juga dapat menghambat upaya penegakan hukum serta menimbulkan keraguan terhadap komitmen negara dalam melindungi data pribadi warga

4. KESIMPULAN

Berdasarkan hasil dan pembahasan diperoleh bahwa pemerintah Indonesia telah mengakomodasi pelindungan data pribadi melalui pengesahan UU PDP sebagai kerangka hukum dalam menjamin hak-hak masyarakat. Sayangnya prinsip transparansi, yang menjadi salah satu prinsip penting dalam mengupayakan pelindungan data pribadi, belum diimplementasikan secara sempurna di Indonesia. Meskipun mayoritas pengendali data telah mencantumkan bagaimana data pribadi milik pengguna diproses dalam kebijakan privasinya, tetapi ketika terjadi kegagalan pelindungan data pribadi, pengakuan atas insiden ini masih

sangat jarang ditemukan. Hal ini sangat berbeda dengan praktik yang terjadi di negara seperti Irlandia, di mana pengendali data lebih transparan dalam mengelola kegagalan tersebut dan juga didukung dengan adanya DPC sebagai otoritas yang berwenang menangani peristiwa tersebut dan memastikan kepatuhan pengendali data terhadap regulasi yang berlaku. UU PDP telah menjamin hak subjek data pribadi untuk mendapatkan ganti rugi apabila terjadi pelanggaran dalam pemrosesan data pribadi oleh pengendali data. Meskipun demikian, UU PDP hanya menyebutkan hak tersebut tanpa mengatur secara rinci mekanisme ganti rugi, dengan menyatakan bahwa ketentuan lebih lanjut mengenai hal ini akan diatur melalui RPP PDP yang saat ini masih belum disahkan. Pada dasarnya RPP PDP memuat ketentuan mengenai ganti rugi yang dibagi ke dalam dua bentuk, yaitu ganti rugi material dan non-material. Selain itu, RPP PDP juga mengatur mengenai prosedur bagi subjek data untuk mengajukan permintaan ganti rugi kepada pengendali data dan penyelesaian sengketa melalui Lembaga PDP. Dalam hal mediasi yang dilakukan melalui Lembaga PDP tidak berhasil mencapai kesepakatan, maka para pihak memiliki opsi untuk melanjutkan proses penyelesaian sengketa melalui jalur arbitrase atau pengadilan, sesuai dengan kesepakatan para pihak.

DAFTAR REFERENSI

Asa Briggs, A., & Burke, P. (2000). A social history of the media: From Gutenberg to the Internet. Polity Press.

Budhijanto, D. (2022). Cybersecurity law: Perlindungan data virtual dan infrastruktur informasi vital (p. 196). Logoz Publishing.

Direktorat Operasi Keamanan Siber BSSN. (2023). Laporan ancaman siber Indonesia 2023. Badan Siber dan Sandi Negara.

Direktorat Operasi Keamanan Siber. (2023). Lanskap keamanan siber Indonesia 2023.

Harris, A. L. (2009). Web 2.0 and virtual world technologies: A growing impact on IS education. Journal of Information Systems Education, 20(2), 137.

Joshi, R. (2022). Internet and integral part of human life in the 21st century: A review. Current Journal of Applied Science and Technology, 41(36), 13.

Munir, N. (2017). Pengantar hukum siber Indonesia. Rajawali Pers.

Puspitasari, K., & Irwansyah. (2022). Fleksibilitas interpretatif teknologi web 2.0 bagi pengelola media sosial instansi pemerintah. Profesi Humas, 6(2), 221.

Rahardjo, S. (2021). Teori hukum: Kajian lintas disiplin. Nusa Media.

Ramli, A. M. (2006). Cyber law dan HAKI dalam sistem hukum Indonesia (p. 1). Refika Aditama.

Rokilah, & Sulasno. (2021). Penerapan asas hukum dalam pembentukan peraturan perundang-undangan. Ajudikasi Jurnal Ilmu Hukum, 5(2), 183.

Rosadi, S. D., & Pratama, G. G. (2018). Perlindungan privasi dan data pribadi dalam era ekonomi digital di Indonesia. Jurnal Hukum Veritas Et Justisia, 4(1), 99.

Sczepański, M. (2020). Is data the new oil? Competition issues in the digital economy (p. 7). Parliamentary Research Service.

Statista. (2023). Number of internet users in selected countries in 2023.

Tahir, A. (2010). Cyber crime (Akar masalah, solusi, dan penanggulangannya) (p. 3). Suka Pers.

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.