(2026), 4 (1): 150–169 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

PERLINDUNGAN HUKUM TERHADAP PENGUNGKAPAN DATA PRIBADI SECARA TIDAK SAH PADA CALON KARYAWAN SWASTA

Shyavara Aisyah[1)]
Universitas 17 Agustus 1945 Jakarta

Correspondence
Email: shyavaraisyah@gmail.com No. Telp: 081289385498
Submitted: 27 Februari 2026 Accepted: 2 Maret 2026 Published: 3 Maret 2026

ABSTRACT

Perkembangan teknologi informasi dan digitalisasi telah meningkatkan intensitas pengumpulan serta pemrosesan data pribadi, termasuk dalam proses rekrutmen calon karyawan swasta. Praktik tersebut menimbulkan risiko pengungkapan data pribadi secara tidak sah yang berpotensi melanggar hak privasi dan merugikan subjek data. Penelitian ini bertujuan untuk menganalisis sejauh mana Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memberikan perlindungan hukum terhadap data pribadi calon karyawan swasta, serta merumuskan reformulasi pengaturan yang lebih efektif dalam mencegah pengungkapan data secara tidak sah. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan perbandingan hukum. Data penelitian diperoleh melalui studi kepustakaan terhadap bahan hukum primer, sekunder, dan tersier, yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa UU PDP telah menyediakan kerangka dasar pelindungan data pribadi, namun masih terdapat kekosongan norma, terutama terkait batas waktu retensi dan mekanisme penghapusan data pribadi calon karyawan. Oleh karena itu, diperlukan reformulasi kebijakan yang lebih tegas guna menjamin kepastian hukum, keadilan, dan pelindungan hak privasi calon karyawan swasta di Indonesia

Kata kunci: pelindungan data pribadi; calon karyawan swasta; pengungkapan data pribadi secara tidak sah; proses rekrutmen; Undang-Undang Pelindungan Data Pribadi

Pendahuluan

Dalam era digitalisasi dan perkembangan teknologi informasi, data pribadi telah menjadi salah satu aset berharga sekaligus rentan terhadap penyalahgunaan. Setiap individu kini hampir tidak dapat dipisahkan dari aktivitas yang melibatkan pemberian data pribadi, baik melalui sistem administrasi negara, pelayanan publik, maupun dalam hubungan kerja dengan perusahaan swasta. Oleh karena itu, pemahaman mengenai konsep "data pribadi" menjadi penting sebagai dasar dalam menganalisis isu pelindungan hukum terhadap pengungkapan data pribadi secara tidak sah atau sering disebut sebagai kebocoran data, khususnya dalam konteks hubungan kerja antara calon karyawan dengan perusahaan.

Secara normatif, berbagai instrumen hukum memberikan definisi yang berbeda namun saling melengkapi mengenai pengertian data pribadi. Dalam konteks hukum nasional, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjelaskan bahwa data pribadi adalah data yang terkait dengan orang perseorangan yang telah diidentifikasi atau dapat diidentifikasi, baik secara individual maupun dalam kombinasi dengan informasi lain melalui sistem elektronik atau non-elektronik secara langsung maupun tidak langsung. (Pasal 1 angka 1)[1]. Definisi ini menegaskan bahwa data pribadi tidak terbatas pada informasi identitas dasar, namun juga mencakup informasi yang secara potensial mengarah

[1] Republik Indonesia, *Undang-Undang Tentang Pelindungan Data Pribadi*, UU No. 27 Tahun 2022, LNRI Tahun 2022 No. 165, Pasal 1 angka 1

pada identifikasi individu tertentu apabila dikombinasikan dengan data lain. UU PDP juga membedakan data pribadi ke dalam dua kategori, yaitu data pribadi bersifat spesifik (misalnya data biometrik, genetika, kesehatan, orientasi seksual, catatan kejahatan, dan data anak) serta data pribadi bersifat umum (seperti nama lengkap, jenis kelamin, agama, dan status perkawinan). Pembagian ini penting karena menentukan tingkat perlindungan dan kewajiban hukum dalam pengelolaannya.

Konsep data pribadi juga diatur oleh instrumen internasional. Salah satunya adalah Peraturan Umum Perlindungan Data Uni Eropa (GDPR), termasuk Inggris Raya, yang mewakili standar global untuk perlindungan data. GDPR mendefinisikan data pribadi sebagai informasi apa pun yang berkaitan dengan individu ("subjek data") yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, terutama dengan merujuk pada identifikasi seperti nama, nomor identifikasi nasional, data lokasi, identifikasi online, atau elemen lain yang berkaitan dengan identitas fisik, fisiologis, genetik, psikologis, ekonomi, budaya, atau sosialnya. (GDPR, Pasal 4 ayat 1)[2]. Definisi ini memberikan cakupan yang lebih luas dengan memasukkan dimensi sosial dan kultural sebagai bagian dari data pribadi sehingga setiap informasi yang memiliki potensi untuk mengungkap identitas seseorang, baik secara individu maupun dalam konteks masyarakat, dianggap sebagai data pribadi yang dilindungi (E-Jurnal Lex Privatum, 2020).

Perkembangan teknologi komunikasi dan informasi membawa konsekuensi pada meningkatnya nilai ekonomi data pribadi, seperti KTP, NIK, dan KK, dalam aktivitas bisnis. Data tersebut sering digambarkan sebagai *digital dossier* atau berkas digital, yaitu sekumpulan informasi pribadi yang tersimpan pada sebagian besar masyarakat. Pengelolaan data pribadi ini biasanya dilakukan melalui internet yang dikelola oleh perusahaan swasta, namun pemanfaatannya tidak jarang menimbulkan ancaman terhadap hak privasi individu.

Pelanggaran terhadap perlindungan data pribadi tidak hanya terjadi dalam lingkup terbatas, melainkan juga melibatkan perusahaan teknologi berskala global. Hal tersebut tercermin dari berbagai sanksi administratif bernilai sangat besar yang dijatuhkan oleh otoritas perlindungan data di Uni Eropa berdasarkan General Data Protection Regulation (GDPR). Salah satu contoh paling signifikan adalah denda terhadap Meta Platforms Ireland Ltd. pada tahun 2023 sebesar €1,2 miliar.[3] Otoritas Perlindungan Data Irlandia (Data Protection Commission/DPC) menyimpulkan bahwa Meta telah melanggar ketentuan GDPR, khususnya yang berkaitan dengan mekanisme transfer data pribadi lintas negara. Pelanggaran tersebut terjadi karena Meta melakukan pemindahan data pribadi pengguna Eropa ke Amerika Serikat dengan mengandalkan klausul kontraktual standar (standard contractual clauses) sejak tahun 2020, tanpa mampu menjamin tingkat perlindungan data yang setara dengan standar Uni Eropa. Padahal, mekanisme tersebut hanya dapat diterapkan apabila negara tujuan transfer menyediakan perlindungan data yang memadai. Kegagalan Meta dalam memenuhi persyaratan tersebut menyebabkan praktik transfer data dinilai bertentangan dengan prinsip-prinsip perlindungan data pribadi sebagaimana diatur dalam GDPR[4]. Selain dijatuhi denda, Meta juga diwajibkan untuk menyesuaikan seluruh proses transfer datanya agar sejalan dengan ketentuan GDPR, meskipun perusahaan menyatakan akan menempuh upaya hukum atas putusan tersebut.

Peristiwa tersebut menunjukkan bahwa pelanggaran dan pengungkapan data pribadi secara tidak sah merupakan persoalan serius yang dapat menimbulkan konsekuensi hukum, ekonomi, dan sosial yang signifikan. Pengenaan sanksi dalam jumlah besar mencerminkan

[2] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Article 4(1).
[3] CMS Law, *GDPR Enforcement Tracker Report: Numbers and Figures 2018–2025*, CMS Legal Services, 2025, diakses pada 10 Januari 2026.
[4] Albina Orlando dan Mario Santoro, "A Semantic Approach to Understanding GDPR Fines: From Text to Compliance Insights," *Computer Law & Security Review*, Vol. 53, 2025, hlm. 1–3.

komitmen negara-negara Uni Eropa dalam menjamin hak atas perlindungan data pribadi sebagai bagian dari hak asasi manusia. Kondisi ini sekaligus menegaskan bahwa tanpa regulasi yang kuat, pengawasan yang efektif, serta kepatuhan dari pengendali data, risiko penyalahgunaan dan kebocoran data pribadi akan terus meningkat, termasuk dalam hubungan antara perusahaan dan individu, seperti calon karyawan dalam proses rekrutmen.

Pada 20 Juni 2024, Pusat Data Nasional (PDN) mengalami insiden serius berupa serangan siber yang mengakibatkan data nasional terkunci oleh peretas yang meminta tebusan *(ransomware*). Peristiwa ini memengaruhi ratusan instansi pemerintah, menimbulkan keresahan masyarakat mengenai perlindungan data pribadi, sekaligus mempertanyakan efektivitas kebijakan keamanan siber yang diterapkan pemerintah Kebocoran. data nasional pada tahun 2024 tersebut bukan sekadar persoalan teknis, melainkan juga menjadi isu sosial dan politik yang menggoyahkan kepercayaan publik terhadap pemerintah.[5] Dampaknya meluas, mulai dari terganggunya pelayanan publik, potensi penyalahgunaan data pribadi, hingga meningkatnya kekhawatiran masyarakat terhadap keamanan digital di tengah era keterbukaan informasi.

Fenomena pengungkapan data pribadi secara tidak sah pada level nasional sebagaimana terjadi pada insiden Pusat Data Nasional tahun 2024 memperlihatkan bahwa kerentanan sistem pengelolaan informasi tidak hanya menjadi persoalan di sektor pemerintahan, tetapi juga berpotensi terjadi dalam lingkup swasta. Salah satu sektor yang rawan adalah proses rekrutmen tenaga kerja. Dalam praktiknya, perusahaan swasta biasanya mengumpulkan berbagai informasi sensitif dari calon karyawan, seperti identitas diri, riwayat pendidikan, pengalaman kerja, hingga data kontak pribadi. Namun, pengumpulan data ini sering kali tidak diimbangi dengan standar keamanan yang memadai, sehingga membuka celah terjadinya kebocoran maupun penyalahgunaan data. Kondisi tersebut tidak hanya merugikan individu yang datanya bocor, melainkan juga berimplikasi pada reputasi perusahaan dan menimbulkan persoalan hukum terkait kewajiban pelindungan data pribadi. Di sinilah letak pentingnya mengkaji pengungkapan data pribadi secara tidak sah calon karyawan swasta dalam perspektif hukum, khususnya setelah disahkannya UU PDP, yang menjadi dasar regulasi utama bagi tata kelola dan perlindungan data di Indonesia.

Pengumpulan data pribadi calon karyawan pada prinsipnya dilakukan untuk kepentingan seleksi serta proses pengambilan keputusan rekrutmen. Data tersebut lazimnya mencakup informasi yang bersifat sensitif, seperti riwayat pendidikan, pengalaman kerja, bahkan hingga nomor identitas kependudukan dan data kontak pribadi. Idealnya, setelah proses rekrutmen berakhir, data tersebut tidak lagi diproses atau disimpan, kecuali terdapat alasan hukum atau persetujuan baru dari pemilik data. Namun dalam praktiknya, banyak perusahaan tetap menyimpan data para pelamar, bahkan menumpuk berkas lamaran untuk kepentingan *talent pool*, tanpa adanya kejelasan mengenai batas waktu retensi maupun permintaan persetujuan ulang. Kondisi ini menimbulkan potensi pelanggaran hak privasi karena semakin lama data disimpan, semakin besar pula risiko penyalahgunaan, kebocoran, atau akses ilegal oleh pihak yang tidak berwenang

UU PDP hadir sebagai instrumen hukum nasional yang mengatur pemrosesan data pribadi secara menyeluruh. UU ini mengedepankan prinsip-prinsip fundamental dalam pengelolaan data, antara lain asas transparansi, pembatasan tujuan, minimalisasi data, pembatasan masa penyimpanan (*storage limitation*), serta akuntabilitas. Salah satu ketentuan penting dalam UU PDP adalah kewajiban pengendali data untuk menghapus data pribadi apabila tujuan awal pengumpulan telah tercapai atau atas permintaan langsung dari subjek data.

[5] Imanuel Toding Bua, & Nur Isdah Idris. "Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024" *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), (2025): 100–114.

Regulasi ini sejatinya sejalan dengan standar internasional, khususnya *General Data Protection Regulation* (GDPR) di negara Uni Eropa khususnya Inggris, yang secara tegas menekankan bahwa data pribadi tidak boleh disimpan lebih lama dari waktu yang diperlukan (*Art. 5(1)(e) GDPR*).

UU PDP tidak secara eksplisit menggunakan istilah "kebocoran data", melainkan mengkualifikasikan peristiwa tersebut sebagai pengungkapan dan/atau akses terhadap data pribadi secara tidak sah, yang secara yuridis termasuk dalam pelanggaran pelindungan data pribadi. Pengungkapan secara tidak sah terjadi apabila pengungkapan data pribadi dilakukan tidak sesuai dengan asas-asas yang tercantum dalam Pasal 3 UU PDP, berupa pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Pengaturan ini menunjukkan bahwa setiap perbuatan yang mengakibatkan terbukanya data pribadi kepada pihak yang tidak berwenang, baik karena kelalaian maupun kesengajaan Pengendali Data Pribadi, dipandang sebagai pelanggaran terhadap kewajiban pelindungan data pribadi sebagaimana diatur dalam UU PDP, sehingga menimbulkan konsekuensi hukum berupa tanggung jawab dan sanksi sesuai ketentuan peraturan perundang-undangan.

UU PDP belum menetapkan batasan waktu yang konkret terkait retensi data, termasuk data pelamar kerja. Kekosongan norma ini memberi ruang interpretasi yang cukup luas bagi perusahaan untuk menentukan secara sepihak lamanya penyimpanan data. Akibatnya, potensi sengketa hukum dapat muncul, misalnya ketika perusahaan enggan menghapus data meskipun telah diminta oleh subjek data, atau ketika penyimpanan dianggap melebihi kepentingan yang sah. Situasi ini menjadi lebih kompleks karena terdapat regulasi sektoral lain, seperti di bidang ketenagakerjaan dan perpajakan, yang mengharuskan penyimpanan dokumen tertentu dalam jangka waktu tertentu, sehingga menimbulkan potensi konflik norma.[6]

Ketiadaan pengaturan spesifik mengenai masa retensi data calon karyawan di Indonesia telah menimbulkan dampak nyata dalam bentuk kasus pengungkapan data pribadi secara tidak sah. Misalnya, pada tahun 2020, Lembaga Riset Siber CISSReC melaporkan kebocoran lebih dari 1,2 juta data pribadi pelamar kerja dari sebuah situs lowongan pekerjaan di Indonesia, yang mencakup nama lengkap, alamat, riwayat pendidikan, hingga nomor telepon.[7] Kasus serupa juga terjadi pada tahun 2021, ketika ditemukan penjualan data pelamar kerja dari sejumlah platform rekrutmen daring di forum *dark web*.[8] Tidak berhenti di situ, pada tahun 2023 muncul kembali laporan pengungkapan data pribadi secara tidak sah dari salah satu platform rekrutmen digital besar di Indonesia, di mana ribuan CV pelamar yang berisi data sensitif seperti alamat rumah, alamat email, serta riwayat pekerjaan diduga diperjualbelikan secara ilegal.

Rangkaian peristiwa tersebut memperlihatkan bahwa retensi data tanpa adanya batasan waktu yang jelas bukan hanya persoalan administratif, melainkan berpotensi menjadi celah serius bagi kejahatan siber yang merugikan privasi, keamanan, serta martabat calon tenaga kerja di Indonesia. Oleh karena itu, urgensi untuk menghadirkan regulasi yang lebih tegas mengenai retensi data, khususnya bagi calon karyawan sektor swasta, menjadi semakin penting agar praktik pengelolaan data pribadi tidak lagi menimbulkan kerugian hukum maupun sosial di masa mendatang.

---

[6] Sihombing, R. "Implikasi Undang-Undang Perlindungan Data Pribadi terhadap Retensi Data dalam Sektor Ketenagakerjaan." *Jurnal Hukum dan Pembangunan*, 53(1), (2023): 77–95.

[7] CISSReC (Communication and Information System Security Research Center), "Laporan Kebocoran Data 2020–2023," Jakarta, 2023.

[8] CNN Indonesia, "Data Pengguna LinkedIn Bocor, Dijual di Dark Web,", https://www.cnnindonesia.com/teknologi/20210630130302-185-661303/data-pengguna-linkedin-bocor-dijual-di-dark-web (cnnindonesia.com, 30 Juni 2021), diakses 2 Oktober 2025.

Metode Penelitian

Penelitian ini merupakan jenis penelitian yuridis normatif yang dalam pelaksanaannya menggunakan data sekunder. Penelitian normatif ini berdefinisi sebagai penelitian tentang sistematika hukum, yaitu penelitian yang tujuan utamanya adalah untuk mengetahui makna atau landasan hukum[9]. Penelitian hukum normatif pada hakikatnya merupakan kegiatan ilmiah yang menelaah hukum positif dari sudut pandang internal sistem hukum itu sendiri. Pendekatan ini berangkat dari pemahaman bahwa hukum dipandang sebagai suatu institusi yang bersifat otonom dan berdiri sendiri, terpisah dari institusi sosial lainnya. Oleh karena itu, permasalahan yang dikaji dalam penelitian hukum normatif dibatasi pada persoalan-persoalan yang bersumber dari norma dan struktur hukum, bukan pada perilaku masyarakat dalam menerapkan ketentuan hukum tersebut. Fokus utama penelitian hukum normatif terletak pada kajian terhadap konsep hukum, asas-asas hukum, serta norma-norma hukum yang berlaku.

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan *(statute approach)* dan metode perbandingan hukum *(comparative law approach*). Menurut Peter Mahmud Marzuki, pendekatan perundang-undangan merupakan metode pendekatan yang dilakukan dengan cara menelaah seluruh peraturan perundang-undangan yang relevan dengan permasalahan hukum yang sedang dikaji. Selain pendekatan perundang-undangan, penelitian ini juga menggunakan pendekatan perbandingan hukum dengan membandingkan pengaturan pelindungan data pribadi di Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dengan General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa. Pendekatan perbandingan hukum bertujuan untuk merumuskan rekomendasi terhadap permasalahan normatif yang timbul akibat kekosongan hukum, ketidakjelasan norma, maupun konflik norma, melalui studi komparatif terhadap praktik hukum di negara lain yang menghadapi permasalahan serupa. Dalam konteks ini, praktik hukum dipahami sebagai penerapan hukum sebagai suatu sistem yang bersifat preskriptif, yaitu memberikan pedoman mengenai apa yang seharusnya dilakukan serta menawarkan solusi ketika terjadi permasalahan hukum, meskipun terdapat perbedaan antara sistem hukum civil law dan common law.

Sumber data yang digunakan dalam penelitian ini adalah sumber data kualitatif yang terdiri dari bahan hukum primer berupa peraturan perundang-undangan yang disusun secara hirarki dan memiliki kekuatan hukum mengikat dan memengaruhi faktor dalam penelitian ini, Bahan hukum sekunder yang memuat bahan hukum yang diperoleh dari buku teks, jurnal-jurnal, pendapat para ahli, kasus-kasus hukum, serta symposium yang dilakukan para pakar.[10] Serta bahan hukum tersier yang berisi bahan hukum yang memberi petunjuk atau penjelasan signifikan untuk bahan hukum utama dan sekunder, datang kamus hukum, ensiklopedi, dll.[11]

Metode pengumpulan data disesuaikan dengan sumber data yang digunakan untuk menunjang penelitian yang dilakukan.[12] Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan *(library research)*. Studi kepustakaan merupakan teknik pengumpulan data yang dilakukan dengan cara menelaah, mengkaji, dan menganalisis berbagai sumber pustaka yang memiliki relevansi dengan topik penelitian yang dibahas. Sumber perpustakaan tersebut dapat berupa buku, artikel ilmiah, jurnal, peraturan perundang-undangan, laporan penelitian, tesis, disertasi, atau dokumen lain yang dapat memberikan informasi dan referensi mendalam mengenai topik yang diteliti.

[9] Bambang Sunggono, *Metodologi Penelitian Hukum*, (Jakarta: Raja Grafindo Persada, 2016), hlm. 93.

[10] Johnny Ibrahim, *Teori & Metodologi Penelitian Hukum Normatif*, (Malang: Bayu Media Publishing, 2012), hlm. 392.

[11] *Ibid*

[12] Rio Christiawan dan Tuti Widyaningrum, *Penelitian Hukum Normatif,* (Depok: Rajawali Pers, 2024), hlm.

Metode analisis data dalam penilitian ini memuat hasil pendeskripsian mengenai cara melakukan analisis terhadap masalah untuk menghasilkan kesimpulan. Metode analisis data yang digunakan yaitu deskriptif kualitatif, yang merupakan pendekatan untuk menganalisis data secara mendalam dan mendeskripsikan fenomena yang terjadi tanpa memfokuskan pada pengujian hipotesis atau angka statistik. Pada analisis deskriptif kualitatif, data yang telah dikumpulkan melalui studi kepustakaan atau sumber lainnya akan dianalisis dengan cara mengidentifikasi pola, tema, atau isu yang muncul, kemudian dijelaskan secara naratif. Peneliti berusaha untuk menggambarkan fenomena yang ada, seperti pengungkapan data pribadi secara tidak sah yang terjadi, dengan memberikan penjelasan yang mendalam berdasarkan dokumen dan referensi yang ada. Tujuannya adalah untuk memberikan pemahaman yang lebih komprehensif dan menyeluruh terhadap masalah yang diteliti

Hasil dan Pembahasan

Perlindungan Hukum Data Pribadi Calon Karyawan Swasta menurut Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

Dalam beberapa dekade terakhir, perkembangan teknologi informasi dan komunikasi membuat munculnya perubahan khususnya tantangan dalam menjaga privasi. Setiap individu memiliki hak asasi manusia yang termasuk hak privasi. Menurut Daniel J. Solovo privasi memiliki dimensi yang luas yang berkaitan erat dengan konsep otonomi pribadi dan kebebasan individu. Privasi dinilai bukan hanya berkaitan dengan kerahasiaan (*secrecy*), tetapi juga mencakup kendali individu terhadap pengumpulan, penyimpanan, dan penyebaran data pribadinya. Artinya, pelanggaran privasi tidak selalu terjadi ketika data dibocorkan saja, namun juga ketika data diproses atau digunakan tanpa dasar hukum yang jelas. Dengan adanya digitalisasi, setiap individu maupun organisasi dapat melakukan inovasi baru dalam pemrosesan informasi, sehingga beberapa informasi yang tidak seharusnya dipublikasi ternyata dipublikasikan tanpa adanya kesadaran dan persetujuan dari pihak yang berkaitan. Hal ini menyebabkan adanya penyalahgunaan data dan pengungkapan data pribadi secara tidak sah yang tentunya merugikan pihak yang berkaitan, terlebih jika informasi yang dipublikasikan merupakan data pribadi. [13]

Pengaturan mengenai pelindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang lahir dari adanya pertimbangan yang tertera pada Undang-Undang Republik Indonesia Tahun 1945 pada Pasal 28G ayat (1) yang menyatakan bahwa, “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.” Berbagai laporan internasional, seperti UNCTAD (2021), menunjukkan bahwa negara berkembang termasuk Indonesia masih memiliki kerangka hukum perlindungan data yang lemah, sehingga meningkatkan kerentanan terhadap penyalahgunaan data. Untuk menjawab tantangan ini, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai regulasi utama yang diharapkan mampu memberikan perlindungan hukum yang kuat terhadap hak-hak privasi warga negara. Data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik (Pasal 1 Ayat 1

[13] Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. Jurnal Multidisiplin Indonesia, 2(3), 654-666.

UU PDP). Setiap individu tentunya memiliki hak untuk melindungi data pribadinya sebab data pribadi merupakan bagian dari hak privasi yang dilindungi oleh hukum. Menurut UU PDP, Pelindungan data Pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. (Pasal 1 Ayat 2 UU PDP).

Pengungkapan data pribadi secara tidak sah dalam skala besar di Indonesia bukan hanya sekadar pelanggaran terhadap hak privasi individu, tetapi juga membawa dampak sosial dan ekonomi yang serius. Kerugian finansial menjadi salah satu akibat paling nyata, baik bagi masyarakat maupun organisasi. Data pribadi yang bocor dapat dimanfaatkan untuk penipuan identitas, pencurian dana, hingga transaksi ilegal yang merugikan korban secara langsung. Hertianto (2021) menekankan bahwa insiden pengungkapan data pribadi secara tidak sah di platform e-commerce maupun lembaga pemerintah seringkali menjadi pintu masuk bagi pelaku kejahatan siber. Sayangnya, penegakan hukum atas kegagalan perlindungan data pribadi masih belum berjalan efektif, sehingga menimbulkan kesan bahwa pelanggaran semacam ini tidak ditindak secara serius.

Selain kerugian materi, organisasi yang mengalami pengungkapan data pribadi secara tidak sah juga harus menanggung dampak reputasi. Ketika publik melihat sebuah perusahaan gagal menjaga keamanan data, kepercayaan konsumen akan menurun. Hal ini bisa berujung pada berkurangnya jumlah pengguna atau pelanggan yang memilih pindah ke layanan lain yang dianggap lebih aman. RSM Indonesia (2024) menunjukkan bahwa pengungkapan data pribadi secara tidak sah tidak hanya merusak citra perusahaan, tetapi juga menghambat pertumbuhan bisnis dan merusak hubungan jangka panjang dengan konsumen.

Pelindungan data pribadi calon karyawan swasta merupakan isu hukum yang semakin relevan seiring dengan meningkatnya penggunaan teknologi informasi dalam proses rekrutmen tenaga kerja. Pada praktiknya, hampir seluruh tahapan rekrutmen, mulai dari pengumpulan curriculum vitae, kartu identitas, ijazah, hingga data pendukung lainnya, dilakukan melalui media elektronik. Kondisi ini menempatkan data pribadi calon karyawan dalam posisi rentan terhadap pengungkapan atau penyalahgunaan oleh pihak yang tidak berwenang. Oleh karena itu, perlindungan hukum terhadap pengungkapan data pribadi secara tidak sah perlu dikaji tidak hanya berdasarkan Undang-Undang Perlindungan Data Pribadi, tetapi juga dengan mengaitkannya pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang berlaku di Indonesia saat ini.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 merupakan regulasi awal yang mengakui dan memberikan perlindungan terhadap data pribadi dalam sistem elektronik. Meskipun UU ITE tidak secara eksplisit menyebut istilah “perlindungan data pribadi” secara komprehensif, pengaturan mengenai data pribadi dapat ditemukan dalam Pasal 26 UU ITE. Pasal tersebut menegaskan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Ketentuan ini menunjukkan bahwa hukum Indonesia telah mengakui data pribadi sebagai bagian dari hak privat (privacy rights) yang melekat pada setiap individu dan harus dilindungi dalam pemanfaatan teknologi informasi.[14]

Dalam penjelasan Pasal 26 UU ITE, perlindungan data pribadi dipahami sebagai bagian dari perlindungan hak asasi manusia, khususnya hak atas kehidupan pribadi, hak untuk

[14] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016, Pasal 26.

berkomunikasi tanpa pengawasan, serta hak untuk mengontrol informasi pribadi yang dimiliki seseorang. Dengan demikian, setiap bentuk pengungkapan data pribadi tanpa persetujuan pemilik data dapat dikategorikan sebagai pelanggaran terhadap hak privasi. Dalam konteks calon karyawan swasta, data yang diserahkan kepada perusahaan dalam proses rekrutmen jelas merupakan data pribadi yang bersifat sensitif, sehingga penggunaannya harus dibatasi hanya untuk kepentingan rekrutmen dan tidak boleh diungkapkan kepada pihak lain tanpa persetujuan subjek data.

UU ITE juga memberikan mekanisme perlindungan hukum bagi pihak yang dirugikan akibat pengungkapan data pribadi secara tidak sah. Pasal 26 ayat (2) UU ITE menyatakan bahwa setiap orang yang dilanggar haknya dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang tersebut. Ketentuan ini membuka ruang bagi calon karyawan yang data pribadinya dibocorkan atau digunakan tanpa izin untuk menuntut pertanggungjawaban secara perdata terhadap pihak yang melakukan pelanggaran. Dalam hal ini, perusahaan swasta yang melakukan pengolahan data calon karyawan melalui sistem elektronik dapat dimintai pertanggungjawaban apabila lalai menjaga kerahasiaan data tersebut.

Selain itu, perubahan UU ITE melalui UU Nomor 19 Tahun 2016 juga memperkenalkan konsep hak untuk dilupakan (right to be forgotten). Ketentuan ini mewajibkan penyelenggara sistem elektronik untuk menghapus informasi elektronik yang tidak relevan atas permintaan subjek data berdasarkan penetapan pengadilan. Meskipun konsep ini lebih sering dikaitkan dengan informasi publik di ruang digital, dalam konteks rekrutmen tenaga kerja, hak untuk dilupakan dapat dimaknai sebagai hak calon karyawan untuk meminta penghapusan data pribadinya setelah proses rekrutmen selesai atau apabila data tersebut sudah tidak lagi relevan. Hal ini penting untuk mencegah penyimpanan dan penggunaan data pribadi secara berlebihan oleh perusahaan.

Meskipun UU ITE dan peraturan pelaksananya memberikan dasar hukum bagi perlindungan data pribadi, pengaturan tersebut masih bersifat umum dan belum mengatur secara rinci mengenai jenis data pribadi, jangka waktu penyimpanan, serta sanksi yang tegas terhadap pengungkapan data pribadi secara tidak sah. Dalam praktiknya, hal ini sering menimbulkan kesulitan pembuktian bagi korban kebocoran data, termasuk calon karyawan yang dirugikan akibat penyalahgunaan data pribadinya. Sejumlah kajian menyatakan bahwa ketentuan Pasal 26 UU ITE belum sepenuhnya efektif dalam memberikan perlindungan hukum yang optimal karena tidak disertai dengan pengaturan teknis dan sanksi administratif maupun pidana yang spesifik.[15]

Dengan demikian, perlindungan hukum terhadap pengungkapan data pribadi calon karyawan swasta tidak dapat dilepaskan dari peran UU ITE sebagai regulasi awal yang mengakui hak atas privasi dalam sistem elektronik. Pengungkapan data pribadi calon karyawan tanpa persetujuan yang sah dapat dikualifikasikan sebagai pelanggaran Pasal 26 UU ITE dan memberikan dasar bagi korban untuk menuntut ganti rugi. Namun, untuk memberikan perlindungan yang lebih efektif dan kepastian hukum yang lebih kuat, keberadaan UU PDP menjadi pelengkap sekaligus penyempurna atas kelemahan pengaturan dalam UU ITE. Oleh karena itu, kajian dalam skripsi ini dapat menempatkan UU ITE sebagai fondasi awal perlindungan data pribadi, yang kemudian diperkuat dan diperluas melalui pengaturan khusus dalam UU Perlindungan Data Pribadi.

[15] Lihat Kompas, *UU ITE Juga Belum Ampuh Lindungi Data Pribadi*, 2021.

Dalam UU PDP dikenal tiga istilah Subjek Data Pribadi, Pengendali Data Pribadi, dan Prosesor Data Pribadi. Subjek Data Pribadi merupakan orang perseorangan yang pada dirinya melekat data pribadi, yang dalam tulisan ini merupakan calon karyawan swasta. Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Dalam hal ini, Pengendali Data Pribadi merupakan perusahaan yang membuka lowongan pekerjaan (*employer*). Prosesor Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama Pengendali Data Pribadi. Prosesor Data Pribadi menfasilitasi penerimaan data, menyimpan, dan meneruskan data kepada Pengendali Data Pribadi. Platform seperti LinkedIn, Indeed, Jobstreet, dan platform rekrutmen lain umumnya merupakan bagian dari Prosesor Data Pribadi. Perbedaan antara Pengendali Data Pribadi dan Prosesor Data Pribadi terletak pada peran dan kendalinya. Dalam aspek penetapan tujuan dan alasan pemrosesan data, Pengendali Data Pribadi menentukan "apa" dan "mengapa" data diproses (misalnya untuk pelayanan, kontrak, persetujuan, dll), sedangkan Prosesor data pribadi hanya melaksanakan instruksi dan tidak menetapkan tujuan sendiri. Selain itu, dalam aspek hubungan langsung dengan Subjek Data Pribadi, Pengendali Data Pribadi umumnya berhubungan langsung untuk menentukan tujuan pemrosesan data, sedangkan Prosesor data pribadi tidak berhubungan langsung dan hanya bertindak atas nama pengendali. Pengendal Data Pribadi memegang kendali atas pemrosesan, menetapkan kebijakan, sistem, keamanan, retensi, dan pemberitahuan subjek data. Di lain sisi, Prosesor Data Pribadi tidak memiliki kendali penuh dan hanya melakukan pemrosesan sesuai arahan pengendali.

Berdasarkan uraian di atas, kewajiban perusahaan (*employer*) sebagai Pengendali Data Pribadi berupa:

1. Memastikan adanya dasar hukum sebelum memproses data (misalnya persetujuan, kontrak, kepentingan sah, pelayanan publik, dan lain-lain)
2. Memberikan informasi kepada Subjek Data Pribadi tentang tujuan, jenis data, retensi, jangka waktu, dan hak-hak subjek data.
3. Menjaga keamanan, kerahasiaan, akursi, konsistensi data, serta mencegah akses tidak sah.

Kewajiban Platform Rekrutmen sebagai Prosesor Data Pribadi berupa:

1. Melakukan pemrosesan data hanya berdasarkan perintah Pengendali Data Pribadi.
2. Jika melibatkan sub-prosesor lain (prosesor tambahan), harus ada persetujuan tertulis dari Pengendali Data Pribadi
3. Tetap ikut menerapkan standar keamanan dan kerahasiaan sesuai kontrak dengan pengendali

Pemberian informasi kepada calon karyawan seperti yang dijelaskan di atas merupakan salah satu kewajiban dari perusahaan (*employer*), namun dalam praktiknya, banyak perusahaan swasta yang menyimpan data pelamar dalam jangka waktu sangat Panjang tanpa dasar hukum yang memadai. Hali ini disebabkan karena UU PDP tidak mengatur secara spesifik mengenai berapa lama retensi data dapat dilakukan dalam konteks rekrutmen. UU PDP hanya mengatur retensi secara normatif, tanpa memberikan batas waktu yang pasti. Pasal 16 ayat (1) huruf c UU No. 27 Tahun 2022 menyatakan bahwa Pengendali Data Pribadi wajib: "menetapkan jangka waktu pemrosesan data pribadi sesuai tujuan pemrosesan." Sementara itu, Pasal 18 ayat (2) menyatakan bahwa data pribadi harus dimusnahkan: "setelah tujuan pemrosesan tercapai atau jangka waktu retensi berakhir." Namun, kedua pasal tersebut tidak menentukan berapa

lama retensi yang dianggap wajar bagi sektor tertentu, termasuk sektor ketenagakerjaan. Implikasinya, perusahaan sebagai Pengendali Data Pribadi memiliki keleluasaan yang besar dalam menentukan sendiri jangka waktu retensi dan data pelamar sebagai Subjek Data Pribadi disimpan tanpa batas jelas.

Sebagai Subjek Data Pribadi, calon karyawan swasta memiliki sejumlah hak yang wajib dijamin oleh perusahaan (*employer*) sebagai Pengendali Data Pribadi. Hak-hak ini tidak hanya bersumber dari UU PDP, tetapi juga berkaitan dengan perlindungan umum dalam UU Ketenagakerjaan/UU Cipta Kerja terkait martabat, privasi, dan perlakuan adil bagi pekerja dan calon pekerja. UU PDP memberikan hak yang luas, antara lain hak untuk memperoleh informasi lengkap mengenai pemrosesan data (Pasal 5), hak akses dan memperoleh salinan data (Pasal 7), hak mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data (Pasal 8), hak untuk menarik persetujuan (Pasal 9), serta hak untuk dihapuskan datanya setelah tidak relevan atau masa retensi berakhir (Pasal 16 ayat (2) huruf g). Selain itu, calon karyawan juga berhak mendapatkan perlakuan yang adil dan tidak diskriminatif dalam proses rekrutmen sebagaimana diatur dalam UU Ketenagakerjaan dan peraturan turunannya.

Dari perspektif implementasi, sejumlah studi hukum menunjukkan bahwa meskipun UU PDP sudah menjadi tonggak penting dalam perlindungan data pribadi di Indonesia, masih terdapat tantangan signifikan dalam penerapan aturan tersebut. Rinjani & Firmansyah dalam penelitian mereka menyatakan bahwa kendala utama adalah lemahnya penegakan hukum dan akuntabilitas, serta rendahnya kesiapan kelembagaan untuk mengawasi pelaksanaan UU PDP. Hal ini menunjukkan bahwa norma yang baik sekalipun bisa tidak efektif apabila tidak didukung oleh pengawasan dan mekanisme penegakan yang kuat. [16]

Salah satu masalah besar dalam pelaksanaan UU PDP adalah tidak adanya lembaga pengawas independen. Akibatnya, penegakan hukum sering berjalan tanpa arah yang jelas, tidak terkoordinasi, dan kehilangan fokus kelembagaan. Padahal dalam sistem hukum modern, keberadaan otoritas pengawas sangat penting untuk memastikan aturan dipatuhi sekaligus menjamin hak-hak korban bisa dipulihkan.

Selain itu, aturan teknis mengenai cara melaporkan pelanggaran, bagaimana investigasi dilakukan, hingga mekanisme pemberian sanksi masih belum jelas. Hal ini membuat banyak pihak ragu apakah UU PDP benar-benar efektif. Memang, undang-undang sudah mencantumkan ancaman pidana maupun sanksi administratif, tetapi tanpa aturan pelaksana yang konkret dan bisa dijalankan, ketentuan tersebut berisiko hanya menjadi hiasan belaka sekadar "aturan di atas kertas" tanpa daya paksa nyata. Situasi ini menunjukkan adanya kesenjangan yang cukup lebar antara rancangan normatif yang tertulis dalam undang-undang dengan praktik di lapangan. Dengan kata lain, pelindungan data pribadi masih menghadapi tantangan serius: bagaimana menjembatani idealisme hukum dengan realitas implementasi agar masyarakat benar-benar terlindungi.

Kekurangan lain dari UU PDP adalah belum adanya pengaturan teknis yang cukup rinci tentang jangka waktu retensi data pribadi bagi calon karyawan swasta dan bagaimana data tersebut harus dimusnahkan secara nyata. Meskipun secara prinsip UU PDP mengharuskan penyimpanan data hanya selama diperlukan, belum terdapat contoh konkret atau praktik yang terdokumentasi secara hukum di Indonesia di mana perusahaan telah memusnahkan data pribadi calon karyawan sesuai ketentuan UU PDP. Kondisi ini mengindikasikan bahwa aspek retensi dan pemusnahan data masih menjadi area abu-abu dalam implementasi hukum.

[16] Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70-83.

Selanjutnya, kajian penegakan hukum oleh Bachtiar dkk. juga menyoroti bahwa norma dalam UU PDP masih menyisakan ketidakjelasan, termasuk dalam standar teknis perlindungan data serta belum terbentuknya lembaga pengawas yang independen yang memiliki kewenangan besar untuk memastikan kepatuhan perusahaan.[17]

Selain itu, sejumlah kajian menegaskan bahwa UU PDP belum sepenuhnya menjamin kepastian hukum terutama dalam pemulihan hak korban pelanggaran data pribadi. Hasil penelitian menunjukkan bahwa meskipun UU PDP memberikan sanksi administratif dan pidana, mekanisme perlindungan substantif terhadap hak subjek data masih perlu penguatan, termasuk untuk kasus di mana data pribadi disimpan tanpa dasar hukum yang kuat atau disalahgunakan setelah periode retensi berakhir.

Pengungkapan data pribadi secara tidak sah dalam proses rekrutmen tenaga kerja swasta merupakan persoalan yang sangat serius karena dapat menimbulkan berbagai bentuk ancaman terhadap calon pekerja sebagai pemilik data tersebut. Dalam praktik perekrutan di Indonesia, perusahaan biasanya mengumpulkan beragam informasi pribadi dari pelamar kerja. Informasi ini mencakup data identitas dasar seperti nama lengkap, nomor induk kependudukan (NIK), serta alamat domisili. Selain itu, perusahaan juga menghimpun data pendidikan berupa ijazah, transkrip nilai, dan sertifikat keahlian, serta data riwayat pekerjaan dan informasi kontak. Tidak jarang pula perusahaan meminta dokumen tambahan seperti Surat Keterangan Catatan Kepolisian (SKCK), surat keterangan sehat dari fasilitas kesehatan, hingga foto pribadi pelamar. Keseluruhan data tersebut secara hukum dikategorikan sebagai data pribadi sebagaimana diatur dalam Pasal 1 angka 1 UU PDP. Oleh karena itu, data tersebut wajib mendapatkan perlindungan yang ketat sejak tahap pengumpulan, penyimpanan, pemrosesan, hingga pemusnahannya.

ancaman pengungkapan data pribadi secara tidak sah juga semakin diperburuk apabila perusahaan tidak dikenakan sanksi yang tegas dan efektif atas pelanggaran yang dilakukan. UU PDP memang telah mengatur adanya sanksi administratif maupun pidana bagi Pengendali Data Pribadi yang melanggar kewajiban, sebagaimana tercantum dalam Pasal 57 hingga Pasal 67 UU PDP[18]. Namun, lemahnya implementasi dan penegakan hukum dapat mengurangi efek jera bagi perusahaan. Akibatnya, calon karyawan swasta berada dalam posisi yang rentan dan belum memperoleh perlindungan hukum yang optimal. Kondisi ini menegaskan urgensi penguatan mekanisme pengawasan serta penerapan sanksi secara konsisten guna menjamin pelindungan Data Pribadi dalam proses rekrutmen.

Kurangnya contoh praktik pemusnahan data yang sesuai dengan UU PDP juga menjadi masalah serius. Hingga saat ini, belum banyak perusahaan yang secara terbuka menunjukkan kepatuhan terhadap kewajiban pemusnahan data pribadi pelamar kerja. Dalam praktiknya, data pelamar sering kali tetap tersimpan dalam sistem internal perusahaan atau bahkan dialihkan kepada pihak ketiga yang menyediakan jasa outsourcing rekrutmen. Hal ini tidak hanya menimbulkan ketidakpastian hukum bagi calon karyawan, tetapi juga memperbesar kemungkinan data pribadi mereka digunakan untuk tujuan lain yang tidak sesuai dengan maksud awal pengumpulan. Tanpa adanya pedoman teknis yang rinci dan contoh praktik yang dapat dijadikan acuan, perusahaan cenderung mengabaikan kewajiban pemusnahan data, sehingga perlindungan yang dijanjikan UU PDP menjadi tidak efektif.

[17] Rizki Bachtiar, F., Ardytia, W., & Brian Wicaksono, D. (2025). Analisis Penegakan Hukum Data Pribadi Pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia. *AMAR*, *3*(2), 101–110.
[18] Republik Indonesia*, Undang-Undang Tentang Pelindungan Data Pribadi*, UU No. 27 Tahun 2022, LNRI Tahun 2022 No. 165, Pasal 57-67.

Lebih jauh lagi, tantangan dalam penegakan dan pengawasan juga memperlihatkan kelemahan implementasi UU PDP. Meskipun UU PDP memberikan kewenangan kepada otoritas pelindungan data untuk melakukan pengawasan, dalam praktiknya mekanisme pengawasan terhadap perusahaan swasta masih belum berjalan optimal. Hal ini disebabkan oleh keterbatasan sumber daya, kurangnya koordinasi antar lembaga, serta belum adanya sistem pelaporan yang transparan mengenai kepatuhan perusahaan terhadap UU PDP. Akibatnya, banyak pelanggaran yang terjadi tidak terdeteksi atau tidak ditindaklanjuti secara serius. Kondisi ini membuat perusahaan tidak memiliki insentif yang cukup kuat untuk mematuhi ketentuan UU PDP, sehingga perlindungan terhadap data pribadi calon karyawan swasta menjadi lemah.

Selain faktor-faktor tersebut, terdapat pula tantangan budaya organisasi dan kesadaran hukum yang rendah di kalangan perusahaan swasta. Banyak perusahaan masih memandang data pribadi pelamar kerja hanya sebagai dokumen administratif yang dapat disimpan dan digunakan secara bebas, tanpa memperhatikan aspek hukum dan etika pelindungan data.[19] Rendahnya kesadaran ini diperparah oleh minimnya sosialisasi dan edukasi mengenai UU PDP di sektor ketenagakerjaan. Akibatnya, perusahaan tidak memiliki kebijakan internal yang memadai untuk melindungi data pribadi pelamar, dan calon karyawan swasta menjadi pihak yang paling dirugikan.

Dengan mempertimbangkan seluruh kelemahan tersebut, dapat disimpulkan bahwa meskipun UU PDP secara normatif telah memberikan kerangka perlindungan hukum yang penting bagi calon karyawan swasta sebagai subjek data pribadi, perlindungan tersebut belum sepenuhnya melindungi calon karyawan dari sisi implementasi praktis. Kekosongan dalam pengaturan teknis retensi data, kurangnya contoh praktik pemusnahan data yang sesuai UU PDP, tantangan dalam penegakan dan pengawasan, rendahnya kesadaran hukum perusahaan, ketidakjelasan tanggung jawab pihak ketiga, serta kesulitan pembuktian hukum menunjukkan bahwa perlindungan hukum yang dijanjikan oleh UU ini masih perlu diperkuat melalui peraturan pelaksana yang lebih rinci dan pemantauan kepatuhan perusahaan yang efektif. Dengan demikian, dapat ditegaskan bahwa saat ini UU PDP belum sepenuhnya mampu melindungi data pribadi calon karyawan swasta dari pengungkapan data pribadi secara tidak sah.

Reformulasi Aturan Pelindungan Data Pribadi yang Dapat Memberikan Perlindungan Hukum bagi Calon Karyawan Swasta

Perlindungan hukum adalah salah satu konsep penting dalam ilmu hukum karena berkaitan langsung dengan upaya menjamin hak dan kepentingan setiap orang sebagai subjek hukum. Satjipto Rahardjo, merujuk pada pemikiran Fitzgerald tentang tujuan hukum, menjelaskan bahwa hukum berfungsi untuk menyatukan dan mengoordinasikan berbagai kepentingan dalam masyarakat. Fungsi ini diwujudkan melalui aturan yang melindungi kepentingan tertentu, sekaligus membatasi kepentingan lain agar tidak menimbulkan ketidakadilan atau penyalahgunaan kekuasaan.[20] Dengan demikian, hukum tidak hanya dipahami sebagai kumpulan norma tertulis, tetapi juga sebagai sarana yang memberi perlindungan dan rasa aman bagi manusia dalam kehidupan bermasyarakat.

[19] OECD, *Data Protection in Employment Sector*, 2023.
[20] Satjipto Rahardjo, *Ilmu Hukum*, (Bandung: PT Citra Aditya Bakti, 2014), hlm. 53.

Lebih jauh, Satjipto Rahardjo memandang perlindungan hukum sebagai upaya melindungi kepentingan seseorang dengan memberikan hak atau kekuasaan yang diakui oleh hukum, sehingga ia dapat bertindak untuk mempertahankan kepentingannya. Perlindungan hukum erat kaitannya dengan pengakuan dan jaminan hak asasi manusia, sebab tanpa perlindungan yang efektif, hak-hak tersebut tidak bisa dijalankan secara optimal. Pandangan ini sejalan dengan pemikiran Philipus M. Hadjon yang menekankan bahwa perlindungan hukum bertujuan memberi rasa aman dan kepastian hukum bagi rakyat, terutama dari tindakan sewenang-wenang penguasa atau pihak lain yang memiliki posisi lebih kuat.[21] Konsep perlindungan hukum menjadi sangat relevan jika dikaitkan dengan hubungan antara calon karyawan swasta dan pemberi kerja, khususnya dalam tahap rekrutmen. Pada tahap ini, calon karyawan biasanya diminta menyerahkan data pribadi seperti identitas, riwayat pendidikan, pengalaman kerja, hingga informasi lain yang bersifat sensitif. Dalam praktiknya, posisi calon karyawan sering kali lebih lemah dibandingkan pemberi kerja, sehingga rentan mengalami pelanggaran terhadap hak-hak pribadinya. Tanpa aturan hukum yang jelas dan tegas, data pribadi tersebut bisa disalahgunakan, misalnya dikumpulkan secara berlebihan, diproses tanpa persetujuan, atau digunakan di luar tujuan rekrutmen.

UU PDP hadir sebagai instrumen hukum yang secara khusus mengatur hak subjek data dan kewajiban pengendali data. Namun, masih perlu ditelaah lebih jauh apakah ketentuan dalam UU PDP sudah cukup memberikan perlindungan hukum bagi calon karyawan swasta, dan apakah pengaturannya mencerminkan prinsip perlindungan hukum sebagaimana dikemukakan oleh Satjipto Rahardjo. Analisis ini penting sebagai dasar untuk menilai perlunya reformulasi aturan perlindungan data pribadi agar hukum benar-benar mampu memberikan perlindungan optimal bagi calon karyawan swasta dalam proses rekrutmen.

UU PDP dapat dipandang sebagai langkah maju dalam sistem hukum Indonesia karena berusaha menjamin hak-hak subjek data, termasuk calon karyawan swasta. Namun, untuk menilai apakah aturan ini benar-benar efektif dan cukup kuat dalam memberikan perlindungan hukum, penting dilakukan perbandingan dengan regulasi lain yang sudah lebih mapan dan diakui secara internasional. Dalam hal ini, General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa sering dijadikan acuan karena dianggap sebagai standar global dalam perlindungan data pribadi.[22]

Secara prinsip, UU PDP dan GDPR memiliki banyak kesamaan. Keduanya menekankan pentingnya persetujuan yang jelas dari pemilik data, transparansi dalam proses pengumpulan dan pengolahan data, serta pengakuan atas hak-hak subjek data seperti hak untuk mendapatkan informasi, hak akses, dan hak untuk menolak pemrosesan data pribadi. Kesamaan ini menunjukkan bahwa UU PDP secara konseptual sudah mengadopsi nilai-nilai universal yang berkembang dalam hukum internasional, sehingga secara substansi memiliki potensi untuk memberikan perlindungan hukum yang memadai bagi calon karyawan swasta.

Meski begitu, ada perbedaan penting yang perlu diperhatikan, terutama dalam hal kelembagaan dan mekanisme pengawasan. GDPR secara tegas mewajibkan adanya otoritas pengawas independen di setiap negara anggota Uni Eropa, yang kemudian dikoordinasikan melalui European Data Protection Board (EDPB). Lembaga ini memiliki kewenangan nyata untuk menerima pengaduan, melakukan pemeriksaan, hingga menjatuhkan sanksi administratif kepada pihak yang melanggar.[23] Keberadaan lembaga pengawas independen inilah yang

[21] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia*, (Surabaya: PT Bina Ilmu, 1987), hlm. 38.
[22] European Commission, *Data Protection in the EU*, European Union, 2023
[23] European Commission, *General Data Protection Regulation (GDPR)*, 2023.

membuat penerapan GDPR lebih efektif. Sebaliknya, meskipun UU PDP telah mengamanatkan pembentukan Otoritas Perlindungan Data Pribadi (OPDP), hingga kini lembaga tersebut belum benar-benar beroperasi.

Dalam kerangka General Data Protection Regulation (GDPR), sanksi administratif dirancang sebagai instrumen hukum untuk memastikan kepatuhan para Pengendali Data Pribadi, termasuk divisi sumber daya manusia (HR) yang memiliki peran langsung dalam mengelola data pribadi calon tenaga kerja sejak tahap awal rekrutmen. Regulasi ini memberikan otoritas penuh kepada lembaga pengawas untuk menjatuhkan denda administratif dengan nilai yang sangat signifikan, yakni hingga 4% dari total pendapatan tahunan global perusahaan atau maksimal 20 juta euro, bergantung pada jumlah yang lebih besar. Ketentuan tersebut menegaskan bahwa pengelolaan data pribadi pelamar kerja meliputi curriculum vitae, data identitas, riwayat pekerjaan, serta dokumen pendukung lainnya merupakan tanggung jawab hukum yang tidak dapat dianggap sepele. Ancaman sanksi dengan nominal besar tersebut mendorong perusahaan untuk menerapkan prinsip kehati-hatian, pembatasan tujuan pemrosesan, serta pengamanan data yang ketat dalam setiap tahapan rekrutmen dan penyimpanan data oleh unit HR.

Ketegasan pengaturan sanksi dalam GDPR tercermin dari praktik penegakan hukum di kawasan Eropa. Salah satu contoh yang menonjol adalah kasus Google LLC pada tahun 2019, di mana perusahaan tersebut dijatuhi denda sebesar 50 juta euro oleh otoritas perlindungan data Prancis (CNIL).[24] Sanksi tersebut dijatuhkan karena adanya kekurangan transparansi serta tidak adanya dasar hukum yang sah dalam pemrosesan data pribadi. Walaupun kasus ini tidak secara langsung berkaitan dengan proses rekrutmen, prinsip yang dilanggar tetap relevan dengan praktik HR, khususnya kewajiban perusahaan untuk memberikan informasi yang jelas dan transparan kepada calon karyawan mengenai tujuan, dasar hukum, serta jangka waktu penyimpanan Data Pribadi sejak awal proses rekrutmen.

Lebih lanjut, meskipun UU PDP telah mengenal adanya instrumen berupa denda administratif, undang-undang ini tidak secara eksplisit menetapkan besaran maksimum denda dalam batang tubuhnya. Sebaliknya, pengaturan mengenai besaran denda tersebut diserahkan lebih lanjut kepada peraturan pelaksana (Pasal 57 UU PDP).[25] Ketiadaan kepastian mengenai besaran denda ini menimbulkan persoalan serius dalam hal daya paksa sanksi administratif. Tanpa adanya angka yang jelas mengenai batas maksimum denda, perusahaan tidak dapat memperhitungkan secara konkret konsekuensi hukum yang akan dihadapi apabila terjadi kebocoran data pribadi calon karyawan. Akibatnya, potensi efek jera yang diharapkan dari penerapan sanksi administratif menjadi berkurang, karena perusahaan cenderung menilai risiko pelanggaran sebagai sesuatu yang masih dapat ditoleransi dibandingkan dengan biaya kepatuhan yang harus mereka keluarkan untuk memperkuat sistem pelindungan data pribadi.

Dalam praktik hukum administrasi di Indonesia, efektivitas sanksi administratif sangat bergantung pada tiga aspek utama, yaitu kepastian hukum, proporsionalitas sanksi, dan konsistensi penegakan. Kepastian hukum diperlukan agar subjek hukum mengetahui secara jelas konsekuensi dari setiap pelanggaran yang dilakukan. Proporsionalitas sanksi memastikan bahwa hukuman yang dijatuhkan sebanding dengan tingkat kesalahan dan dampak yang ditimbulkan. Sedangkan konsistensi penegakan menjadi faktor penting agar sanksi tidak hanya

[24] Commission Nationale de l'Informatique et des Libertés (CNIL), *Délibération SAN-2019-001 prononçant une sanction pécuniaire à l'encontre de la société Google LLC*, 21 Januari 2019.
[25] Republik Indonesia, *Undang-Undang Tentang Pelindungan Data Pribadi*, UU No. 27 Tahun 2022, LNRI Tahun 2022 No. 165, Pasal 57.

berlaku di atas kertas, tetapi benar-benar diterapkan secara nyata terhadap setiap pelanggaran. Tanpa adanya standar pengenaan sanksi yang jelas dan konsisten, sanksi administratif dalam UU PDP berisiko menjadi sekadar formalitas normatif yang tidak memiliki daya tekan nyata terhadap perusahaan. Kondisi ini dapat menimbulkan persepsi bahwa UU PDP hanya memberikan kerangka hukum yang bersifat deklaratif, tetapi tidak mampu menghadirkan perlindungan yang efektif bagi subjek data pribadi, khususnya calon karyawan swasta yang menyerahkan data pribadinya dalam proses rekrutmen.

Dari perspektif hukum perusahaan, badan hukum diperlakukan sebagai subjek hukum yang berdiri sendiri dan memiliki hak serta kewajiban yang terpisah dari pengurusnya. Prinsip ini sejalan dengan doktrin *separate legal personality* yang diakui secara universal dan juga diatur dalam Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas (UU PT).[26] Doktrin tersebut menegaskan bahwa perseroan terbatas sebagai badan hukum memiliki kepribadian hukum yang berbeda dari para pemegang saham maupun pengurusnya. Oleh karena itu, ketika UU PDP menetapkan sanksi administratif terhadap Pengendali Data Pribadi, maka yang menjadi subjek sanksi adalah perusahaan sebagai badan hukum, bukan individu pengurus atau karyawan yang secara operasional terlibat dalam pengelolaan data pribadi.

Namun demikian, pengaturan yang menempatkan badan hukum sebagai satu-satunya subjek sanksi administratif berpotensi menimbulkan persoalan efektivitas. Dalam praktik, kerugian akibat denda administratif akan dibebankan pada keuangan perusahaan, sehingga dampaknya lebih bersifat institusional.Individu pengambil keputusan, seperti pejabat HR atau manajer yang bertanggung jawab atas pengelolaan data, tidak selalu menanggung konsekuensi langsung dari pelanggaran yang terjadi. Kondisi ini dapat mengurangi insentif bagi pejabat internal perusahaan untuk memastikan kepatuhan terhadap prinsip pelindungan data pribadi, karena mereka merasa tidak akan terkena dampak pribadi meskipun terjadi pelanggaran. Dengan kata lain, beban sanksi administratif yang hanya ditujukan kepada badan hukum berisiko menciptakan *moral hazard*, di mana pengurus perusahaan tidak memiliki dorongan yang cukup kuat untuk menjalankan kewajiban hukum secara optimal.

Dalam hukum perusahaan Indonesia, konsep pertanggungjawaban pengurus sebenarnya telah dikenal dengan baik, khususnya melalui prinsip *fiduciary duty* dan *duty of care* sebagaimana diatur dalam Pasal 92 dan Pasal 97 UU PT.[27] Direksi sebagai organ perseroan bertanggung jawab penuh atas pengurusan perusahaan dan dapat dimintai pertanggungjawaban secara pribadi apabila terbukti lalai atau melakukan kesalahan dalam menjalankan tugasnya. Prinsip ini memberikan dasar hukum bahwa pengurus tidak dapat berlindung sepenuhnya di balik badan hukum apabila kelalaiannya menimbulkan kerugian bagi perseroan[28]. Namun, keterkaitan antara prinsip pertanggungjawaban pengurus dalam UU PT dengan pelanggaran pelindungan data pribadi dalam UU PDP belum diatur secara eksplisit. Akibatnya, terdapat ruang abu-abu dalam penegakan hukum, di mana sanksi administratif hanya dikenakan kepada perusahaan sebagai badan hukum, sementara individu pengurus yang secara nyata mengambil keputusan terkait pengelolaan data pribadi tidak tersentuh oleh mekanisme pertanggungjawaban.

[26] Republik Indonesia, Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas, Pasal 3.
[27] Munir Fuady, *Hukum Perseroan Terbatas: Paradigma Baru*, Citra Aditya Bakti, Bandung, 2020, hlm. 3–5.
[28] Siti Anisah Dhan, Wenny Franciska, dan Andi Fitrian, "Perlindungan Hukum terhadap Pemegang Saham atas Pelanggaran Prinsip Fiduciary Duty oleh Direksi dalam Perseroan Terbatas," *ARMADA: Jurnal Penelitian Multidisiplin*, Vol. 2, No. 9, 2024, hlm. 740–742.

Kekosongan pengaturan ini menimbulkan pertanyaan mengenai efektivitas sistem sanksi dalam UU PDP. Apabila hanya badan hukum yang dikenai sanksi, maka terdapat kemungkinan bahwa perusahaan akan menganggap pelanggaran pelindungan data pribadi sebagai risiko finansial biasa yang dapat ditoleransi, bukan sebagai pelanggaran serius yang harus dicegah. Padahal, dalam konteks pelindungan data pribadi, keterlibatan individu pengurus sangat menentukan kualitas kepatuhan perusahaan. Tanpa adanya mekanisme yang memungkinkan penjatuhan sanksi langsung kepada pengurus atau pejabat yang lalai, maka tujuan UU PDP untuk menciptakan efek jera dan meningkatkan standar kepatuhan perusahaan berpotensi tidak tercapai.

Walaupun UU PDP telah resmi diberlakukan dan dimaksudkan sebagai pijakan utama dalam sistem hukum Indonesia untuk melindungi data pribadi, kenyataannya hingga saat ini belum tersedia peraturan pelaksana berupa Peraturan Pemerintah yang secara resmi ditetapkan untuk menjabarkan ketentuan-ketentuan di dalamnya. Ketiadaan aturan turunan ini membuat banyak norma dalam UU PDP masih bersifat umum dan normatif, sehingga belum bisa diterapkan secara maksimal dalam praktik sehari-hari. Pemerintah memang telah menyusun Rancangan Peraturan Pemerintah sebagai tindak lanjut dari UU PDP yang diharapkan dapat mengatur secara teknis berbagai aspek penting, mulai dari mekanisme pemrosesan dan penghapusan data pribadi, pelaksanaan hak-hak subjek data, pengenaan sanksi administratif, hingga penilaian dampak perlindungan data pribadi. Namun, hingga pertengahan tahun 2025, rancangan tersebut masih berada dalam tahap harmonisasi dan pembahasan lintas kementerian dan lembaga, sehingga belum memiliki kekuatan hukum yang mengikat.[29] Kondisi ini berimplikasi langsung pada terbatasnya implementasi UU PDP di lapangan, termasuk dalam konteks pelindungan data pribadi calon karyawan swasta, karena belum ada pedoman operasional yang jelas bagi pengendali data maupun mekanisme perlindungan yang efektif bagi subjek data.

Ketiadaan aturan turunan juga berdampak pada lemahnya kepastian hukum. Walaupun UU PDP sudah mengatur hak dan kewajiban secara normatif, tanpa adanya peraturan pelaksana, penerapan ketentuan tersebut bergantung pada penafsiran masing-masing pihak. Situasi ini berpotensi menimbulkan ketidaksamaan penerapan di berbagai sektor, serta membuka peluang terjadinya pelanggaran data pribadi tanpa mekanisme penegakan hukum yang jelas. Dalam konteks calon karyawan swasta, kondisi ini menempatkan mereka pada posisi yang rentan, karena data pribadi yang diserahkan dalam proses rekrutmen belum sepenuhnya dijamin perlindungannya melalui mekanisme hukum yang operasional. Oleh sebab itu, keberadaan Peraturan Pemerintah sebagai aturan turunan UU PDP merupakan kebutuhan mendesak untuk memastikan perlindungan hukum yang efektif, konsisten, dan berkeadilan.

Jika dilihat dari keseluruhan analisis mengenai teori perlindungan hukum, pengaturan dalam UU PDP, perbandingan dengan General Data Protection Regulation (GDPR) di Uni Eropa, serta belum optimalnya implementasi akibat ketiadaan aturan turunan, maka jelas diperlukan reformulasi pengaturan perlindungan data pribadi. Reformulasi ini harus berorientasi pada penguatan perlindungan hukum bagi subjek data, khususnya calon karyawan swasta. Reformulasi tersebut mencakup tiga aspek utama: kelembagaan, sanksi, dan mekanisme pengawasan, agar perlindungan data pribadi tidak berhenti pada tataran normatif, tetapi benar-benar dapat dijalankan secara nyata.

[29] Direktorat Jenderal Peraturan Perundang-undangan Kementerian Hukum dan HAM, *Status Harmonisasi RPP PDP*, 2025

Dalam aspek kelembagaan, reformulasi harus menekankan percepatan pembentukan Otoritas Perlindungan Data Pribadi (OPDP) yang bersifat independen sebagaimana diamanatkan UU PDP.[30] Lembaga ini harus memiliki kedudukan yang jelas, kewenangan yang kuat, serta bebas dari intervensi pihak mana pun agar mampu menjalankan fungsi pengawasan dan penegakan hukum secara efektif. Keberadaan otoritas independen sangat penting jika dikaitkan dengan teori perlindungan hukum Satjipto Rahardjo, yang menekankan bahwa hukum harus memberikan pengayoman nyata bagi subjek hukum. Tanpa lembaga pengawas independen, perlindungan hukum terhadap data pribadi calon karyawan swasta berpotensi tidak berjalan optimal, karena tidak ada institusi yang secara khusus bertanggung jawab menerima pengaduan, melakukan pemeriksaan, dan menindak pelanggaran. Oleh karena itu, reformulasi kelembagaan harus diarahkan pada pembentukan dan penguatan OPDP dengan struktur, kewenangan, dan mekanisme kerja yang jelas serta mudah diakses oleh masyarakat.

Dalam aspek sanksi, reformulasi perlu memastikan efektivitas sanksi administratif dan pidana sebagaimana diatur dalam UU PDP. Walaupun UU PDP sudah memuat ketentuan sanksi, ketiadaan peraturan pelaksana membuat sanksi tersebut belum bisa diterapkan secara optimal.[31] Reformulasi harus menjamin bahwa sanksi yang diatur bersifat proporsional, tegas, dan memiliki efek jera, terutama bagi pengendali data yang memiliki posisi dominan, seperti perusahaan swasta dalam proses rekrutmen tenaga kerja. Dalam hal ini, pengalaman penerapan GDPR dapat dijadikan rujukan, khususnya terkait pemberlakuan sanksi administratif yang signifikan untuk mendorong kepatuhan. Sanksi yang efektif tidak hanya berfungsi sebagai alat penghukuman, tetapi juga sebagai sarana pencegahan pelanggaran data pribadi calon karyawan swasta.

Selain itu, reformulasi juga harus mencakup mekanisme pengawasan yang jelas dan terintegrasi. Mekanisme pengawasan harus meliputi prosedur pengaduan yang mudah diakses oleh subjek data, tata cara pemeriksaan dan investigasi pelanggaran, serta transparansi dalam penanganan perkara perlindungan data pribadi. Dalam konteks calon karyawan swasta, mekanisme pengawasan yang efektif akan memberikan jaminan bahwa setiap dugaan pelanggaran data pribadi dapat ditindaklanjuti secara adil dan profesional. Pengawasan yang kuat juga sejalan dengan tujuan hukum untuk mengoordinasikan berbagai kepentingan, sebagaimana dikemukakan oleh Fitzgerald dan dikembangkan oleh Satjipto Rahardjo, agar kepentingan pemberi kerja tidak mengorbankan hak-hak calon karyawan sebagai subjek data.

Reformulasi aturan perlindungan data pribadi harus dipahami sebagai upaya menyeluruh untuk memperkuat perlindungan hukum, bukan sekadar perubahan normatif. Reformulasi yang mencakup penguatan kelembagaan, efektivitas sanksi, dan mekanisme pengawasan yang jelas akan memastikan bahwa hak calon karyawan swasta atas perlindungan data pribadi benar-benar terlindungi. Hal ini sejalan dengan prinsip perlindungan hukum yang menempatkan hukum sebagai sarana pengayoman dan penjamin hak asasi manusia, sehingga perlindungan data pribadi dapat diwujudkan secara nyata dalam praktik ketenagakerjaan di Indonesia.

[30] Pasal 58 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

[31] Hertianto, "Tantangan Implementasi Undang-Undang Pelindungan Data Pribadi," *Jurnal Legislasi Indonesia*, 2021.

Kesimpulan

1. Berdasarkan hasil pembahasan dalam penelitian ini, dapat disimpulkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) belum memberikan perlindungan hukum kepada calon karyawan swasta karena belum memberikan pengaturan yang rinci mengenai jangka waktu penyimpanan data pribadi calon karyawan, standar retensi data, mekanisme pemusnahan data setelah proses rekrutmen berakhir, lemahnya perlindungan dalam praktik, serta belum adanya otoritas pelindungan data pribadi sebagai pengawas. UU PDP secara normatif telah membentuk fondasi hukum yang penting dalam menjamin pelindungan data pribadi sebagai bagian dari hak asasi manusia dengan telah mengakui keberadaan subjek data pribadi, menetapkan prinsip-prinsip pemrosesan data pribadi, serta meletakkan kewajiban hukum kepada Pengendali dan Prosesor Data Pribadi untuk menjaga keamanan dan kerahasiaan data pribadi. Dalam konteks ketenagakerjaan, pengakuan bahwa calon karyawan swasta merupakan subjek data pribadi meskipun hubungan kerja belum terbentuk menunjukkan adanya perluasan cakupan perlindungan hukum yang bersifat preventif. Namun demikian, hasil analisis menunjukkan bahwa perlindungan hukum terhadap data pribadi calon karyawan swasta masih menghadapi berbagai keterbatasan dalam tataran implementasi. Dalam praktik rekrutmen tenaga kerja swasta di Indonesia, perusahaan secara rutin mengumpulkan dan menyimpan data pribadi calon karyawan dalam jumlah besar, baik melalui sistem internal maupun melalui platform rekrutmen daring dan pihak ketiga. Sayangnya, UU PDP belum memberikan pengaturan yang rinci. Kekosongan pengaturan ini membuka ruang bagi perusahaan untuk menyimpan data pelamar kerja tanpa batas waktu yang jelas, sehingga meningkatkan risiko kebocoran dan pengungkapan data pribadi secara tidak sah.
2. Dari sisi sanksi, penelitian ini juga menemukan bahwa dominasi sanksi administratif dalam UU PDP belum sepenuhnya mampu menciptakan efek jera bagi perusahaan swasta. Ketentuan sanksi administratif yang belum disertai kejelasan besaran denda, serta kecenderungan penjatuhan sanksi yang hanya diarahkan kepada badan hukum tanpa menyentuh tanggung jawab personal pengurus perusahaan, berpotensi melemahkan daya paksa norma hukum. Perbandingan dengan rezim General Data Protection Regulation (GDPR) menunjukkan bahwa ketegasan sanksi administratif, besaran denda yang signifikan, serta keberadaan otoritas pengawas independen memainkan peran penting dalam memastikan kepatuhan dan memberikan perlindungan efektif bagi subjek data, termasuk calon karyawan. Dengan demikian, reformulasi UU PDP harus mencakup tiga aspek utama yaitu: kelembagaan, sanksi, dan mekanisme pengawasan. Kesenjangan antara norma hukum dan implementasi, ketiadaan pengaturan teknis yang spesifik dalam konteks rekrutmen, serta lemahnya penegakan dan pengawasan menunjukkan bahwa perlindungan hukum terhadap data pribadi calon karyawan swasta masih bersifat belum optimal dan memerlukan penguatan lebih lanjut melalui reformulasi regulasi dan mekanisme penegakan yang efektif.

Referensi

Christiawan, R. & Widyaningrum, T. (2024). *Penelitian Hukum Normatif*. Depok: Rajawali Pers.

Fuady, M. (2020). *Hukum Perseroan Terbatas: Paradigma Baru*. Bandung: Citra Aditya Bakti.

Hadjon, P.M. (1987). *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: PT Bina Ilmu.

Ibrahim, J. (2012). *Teori & Metodologi Penelitian Hukum Normatif*. Malang: Bayu Media Publishing.

Rahardjo, S. (2014). *Ilmu Hukum*. Bandung: PT Citra Aditya Bakti.

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

Dhan, S.A., Franciska, W., & Fitrian, A. (2024). Perlindungan Hukum terhadap Pemegang Saham atas Pelanggaran Prinsip Fiduciary Duty oleh Direksi dalam Perseroan Terbatas. ARMADA: Jurnal Penelitian Multidisiplin, 2 (9), 740-742.

Hertianto. (2021). Tantangan Implementasi Undang-Undang Pelindungan Data Pribadi. Jurnal Legislasi Indonesia.

Orlando, A. & Santoro, M. (2025). A Semantic Approach to Understanding GDPR Fines: From Text to Compliance Insights. Computer Law & Security Review, 53, 1-3.

Rinjani, M.A. & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum, 8 (1), 70-83.

Rizki Bachtiar, F., Ardytia, W., & Wicaksono, D.B. (2025). Analisis Penegakan Hukum Data Pribadi pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi di Indonesia. AMAR, 3 (2), 101-110.

Sihombing, R. (2023). Implikasi Undang-Undang Perlindungan Data Pribadi terhadap Retensi Data dalam Sektor Ketenagakerjaan. Jurnal Hukum dan Pembangunan, 53 (1), 77-95.

Toding Bua, I. & Idris, N.I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan, 2 (2), 100-114.

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. Jurnal Multidisiplin Indonesia, 2 (3), 654-666.

CISSReC (Communication and Information System Security Research Center). (2023). Laporan Kebocoran Data 2020-2023. Jakarta.

CNN Indonesia. (2021). Data Pengguna LinkedIn Bocor, Dijual di Dark Web. CNN Indonesia, 30 Juni 2021.

CMS Law. (2025). GDPR Enforcement Tracker Report: Numbers and Figures 2018-2025. CMS Legal Services.

Direktorat Jenderal Peraturan Perundang-undangan Kementerian Hukum dan HAM. (2025). Status Harmonisasi RPP PDP.

European Commission. (2023). Data Protection in the EU. European Union.

European Commission. (2023). General Data Protection Regulation (GDPR). European Union.

Kompas. (2021). UU ITE Juga Belum Ampuh Lindungi Data Pribadi.

OECD. (2023). Data Protection in Employment Sector.

Commission Nationale de l'Informatique et des Libertés (CNIL). (2019). Délibération SAN-2019-001 prononçant une sanction pécuniaire à l'encontre de la société Google LLC, 21 Januari 2019.

Republik Indonesia. (2007). Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas.

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

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

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

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.