

SANKSI HUKUM TERHADAP PELANGGARAN PRIVASI KARYAWAN DALAM LINGKUNGAN KERJA DIGITAL**Dimas Hariseno¹, Sidi Ahyar Wiraguna²**^{1, 2} Fakultas Ilmu Hukum, Hukum, Universitas Esa Unggul, Jakarta Indonesia

Alamat: Jl. Arjuna Utara No.9, Kebon Jeruk, Jakarta Barat 11510

Dimashariseno@gmail.com**Abstract (English)**

The protection of employee privacy in the digital workplace has become an increasingly important issue with the rapid advancement of information technology. Law No. 27 of 2022 on Personal Data Protection provides a clear legal framework regarding employees' rights to protection over their personal data. This study aims to analyze the legal sanctions that can be imposed for violations of employee privacy and to assess the effectiveness of the protection provided by the law. The methodology employed in this research is a normative approach with qualitative analysis of legislation, as well as interviews with legal experts and practitioners in the field of personal data protection. The expected outcome of this research is a deeper understanding of employees' rights in the context of personal data protection, along with recommendations to enhance the implementation of legal sanctions against privacy violations. This study is anticipated to contribute to the development of personal data protection policies in Indonesia and to raise awareness of the importance of employee privacy in the digital era.

Article History

Submitted: 21 Mei 2025

Accepted: 24 Mei 2025

Published: 25 Mei 2025

Key Words

Privacy, Personal Data Protection, Legal Sanctions, Employee Rights, PDP Law

Abstrak (Indonesia)

Perlindungan privasi karyawan dalam lingkungan kerja digital menjadi isu yang semakin penting seiring dengan pesatnya perkembangan teknologi informasi. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum yang jelas mengenai hak karyawan untuk mendapatkan perlindungan atas data pribadi mereka. Penelitian ini bertujuan untuk menganalisis sanksi hukum yang dapat dikenakan terhadap pelanggaran privasi karyawan dan menilai efektivitas perlindungan yang diberikan oleh undang-undang tersebut. Metodologi yang digunakan dalam penelitian ini adalah pendekatan normatif dengan analisis kualitatif terhadap peraturan perundang-undangan, serta wawancara dengan ahli hukum dan praktisi di bidang perlindungan data pribadi. Hasil yang diharapkan dari penelitian ini adalah pemahaman yang lebih mendalam mengenai hak-hak karyawan dalam konteks perlindungan data pribadi, serta rekomendasi untuk meningkatkan implementasi sanksi hukum terhadap pelanggaran privasi. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan perlindungan data pribadi di Indonesia dan meningkatkan kesadaran akan pentingnya privasi karyawan dalam era digital.

Sejarah Artikel

Submitted: 21 Mei 2025

Accepted: 24 Mei 2025

Published: 25 Mei 2025

Kata Kunci

Privasi, Perlindungan Data Pribadi, Sanksi Hukum, Hak Karyawan, UU PDP

PENDAHULUAN

Perkembangan pesat teknologi informasi dan komunikasi telah membawa dampak transformasional di berbagai sektor, tidak terkecuali dalam dunia kerja. Salah satu wujud nyata dari perubahan ini adalah terbentuknya ekosistem kerja berbasis digital, yang memungkinkan kegiatan operasional perusahaan dilakukan secara daring dengan dukungan perangkat lunak dan infrastruktur digital (Sri Mulyati, 2025). Transformasi ini tidak hanya meningkatkan efisiensi dan fleksibilitas kerja, tetapi juga memunculkan tantangan baru, khususnya terkait perlindungan terhadap data pribadi pekerja.

Lingkungan kerja digital mensyaratkan adanya pengumpulan, penyimpanan, dan pemrosesan berbagai jenis data pribadi milik karyawan, mulai dari data identitas, riwayat pendidikan, informasi kesehatan, hingga aktivitas kerja yang tercatat secara elektronik. Data-data ini menjadi sangat bernilai sekaligus rentan disalahgunakan, baik karena lemahnya sistem

keamanan data maupun karena kurangnya kesadaran hukum dari pihak pengelola data (Muryani Verina Dwi, 2025).

Privasi karyawan, dalam konteks tersebut, tidak sekadar menyangkut hak untuk merahasiakan informasi pribadinya dari pihak ketiga, melainkan juga merupakan bagian integral dari perlindungan terhadap martabat dan integritas individu dalam relasi kerja. Penghormatan terhadap privasi menjadi elemen penting dalam membangun hubungan industrial yang sehat, berlandaskan kepercayaan dan keadilan antara pekerja dan pemberi kerja.

Namun demikian, masih terdapat celah besar dalam praktik perlindungan privasi karyawan di lingkungan kerja digital di Indonesia. Banyak kasus yang menunjukkan bagaimana data pribadi karyawan digunakan tanpa persetujuan, diakses oleh pihak yang tidak berwenang, atau bahkan dibocorkan ke publik, baik secara sengaja maupun karena kelalaian. Hal ini menimbulkan pertanyaan mengenai sejauh mana hukum yang berlaku dapat melindungi hak privasi karyawan secara efektif (Muryani Verina Dwi, 2025).

Sebagai respons terhadap kompleksitas tersebut, pemerintah Indonesia menerbitkan **Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)** yang bertujuan untuk memberikan kerangka hukum yang jelas dan terstruktur dalam menjaga keamanan data pribadi. Undang-undang ini merupakan langkah progresif dalam menyelaraskan regulasi nasional dengan praktik internasional mengenai hak atas privasi dan perlindungan informasi pribadi (Fauzi & Radika Shandy, 2022).

Dalam UU PDP, terdapat pengaturan yang komprehensif mengenai hak-hak subjek data, seperti hak untuk mengetahui, mengakses, memperbaiki, menghapus, dan menolak pemrosesan data pribadi. Di sisi lain, undang-undang ini juga menetapkan tanggung jawab bagi pengendali data (data controller) dan pemroses data (data processor), termasuk kewajiban menerapkan prinsip keamanan dan akuntabilitas dalam pengelolaan data (Reysha Aurelia Shabilla, 2025).

Khusus dalam konteks hubungan kerja, perlindungan data pribadi karyawan harus ditempatkan sebagai bagian dari kewajiban hukum perusahaan. Ketidakpatuhan terhadap ketentuan UU PDP dapat mengakibatkan sanksi administratif hingga pidana, tergantung pada tingkat pelanggaran yang dilakukan. Hal ini penting mengingat posisi karyawan sering kali tidak seimbang dalam hubungan kerja, sehingga hukum harus hadir sebagai pelindung hak mereka (Wahyuni, 2021).

Namun, meskipun kerangka hukum telah tersedia, dalam praktiknya masih ditemukan berbagai tantangan implementatif. Banyak perusahaan belum memahami secara utuh kewajiban mereka, sementara karyawan juga belum sepenuhnya menyadari hak-haknya atas data pribadi. Selain itu, penegakan hukum terhadap pelanggaran privasi masih bersifat sporadis dan belum mencerminkan efek jera yang memadai.

Atas dasar itu, tulisan ini bertujuan untuk melakukan kajian mendalam terhadap **sanksi hukum yang diatur dalam UU No. 27 Tahun 2022** berkaitan dengan pelanggaran privasi di tempat kerja digital. Fokus utama penelitian ini adalah untuk menganalisis pasal-pasal yang relevan, jenis sanksi yang dapat dikenakan, serta bagaimana penerapan sanksi tersebut dilakukan dalam praktik hukum di Indonesia.

Melalui kajian normatif terhadap peraturan perundang-undangan, literatur hukum, serta pandangan para ahli, penelitian ini diharapkan mampu memberikan kontribusi ilmiah terhadap pengembangan wacana perlindungan data pribadi di sektor ketenagakerjaan. Selain itu, tulisan ini juga bertujuan menyusun rekomendasi kebijakan yang bersifat aplikatif guna memperkuat penegakan hukum dan menjamin perlindungan hak privasi karyawan dalam ekosistem kerja digital yang terus berkembang (Rizki, Brahmana, Iskandar, An, & Susanto, 2022).

METODE PENELITIAN

Penelitian ini dilaksanakan dengan menggunakan pendekatan **yuridis normatif** yang berpadu dengan metode **analisis kualitatif** (Sidi Ahyar, 2025). Pemilihan pendekatan yuridis

normatif dilandasi oleh fokus utama kajian yang menelaah sistem norma hukum tertulis, khususnya mengenai perlindungan data pribadi dan pemberlakuan sanksi hukum atas pelanggaran privasi di lingkungan kerja berbasis digital. Hal ini sejalan dengan upaya memahami penerapan **Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)** sebagai pijakan utama dalam pembentukan regulasi perlindungan hak privasi individu, termasuk karyawan.(P, Esfandiari, & Wasis, 2023)

Sumber data dalam penelitian ini bersifat **data sekunder**, yang diperoleh melalui studi kepustakaan (*library research*). Bahan hukum yang dikaji meliputi peraturan perundang-undangan nasional, khususnya UU PDP, serta perangkat hukum lain yang relevan seperti **Undang-Undang Ketenagakerjaan** dan **UU ITE**. Selain itu, penelitian ini turut memanfaatkan literatur ilmiah berupa buku teks, jurnal hukum, hasil penelitian terdahulu, serta pendapat para pakar hukum data pribadi dan ketenagakerjaan yang memiliki otoritas dalam bidangnya (Djumrianti & Rizkiawan Rizkiawan, 2024).

Proses analisis dilakukan secara **deskriptif-kualitatif**, di mana data dianalisis dengan cara menginterpretasikan muatan normatif dari peraturan yang berlaku, mengidentifikasi isu hukum yang timbul, serta mengevaluasi relevansi dan efektivitas norma tersebut dalam konteks dunia kerja digital. Penelitian ini juga mempertimbangkan perkembangan teknologi serta praktik pelanggaran privasi yang terjadi dalam relasi industrial, untuk mengaitkannya dengan sistem penegakan hukum yang tersedia (Putri & Elmina Martha, 2022).

Dengan pendekatan tersebut, penelitian ini tidak hanya bertujuan untuk memetakan kerangka hukum yang mengatur perlindungan data pribadi karyawan, tetapi juga untuk mengulas bentuk-bentuk pelanggaran yang potensial terjadi serta **konsekuensi yuridis** yang dapat dikenakan kepada pihak yang bertanggung jawab. Harapannya, kajian ini mampu memberikan pemahaman yang lebih mendalam dan menyeluruh mengenai tantangan serta kebutuhan regulatif dalam menjaga hak privasi di era digitalisasi ketenagakerjaan Indonesia.

HASIL DAN PEMBAHASAN

Bentuk Pelanggaran Privasi dalam Lingkungan Kerja Digital

Transformasi digital yang pesat dalam dunia kerja telah menghadirkan beragam inovasi dalam sistem pengelolaan sumber daya manusia. Perusahaan kini dapat dengan mudah mengakses teknologi pemantauan yang bertujuan untuk meningkatkan efisiensi dan produktivitas. Namun di balik kemudahan tersebut, terdapat potensi pelanggaran terhadap hak-hak privasi karyawan yang tak jarang luput dari perhatian atau bahkan dilakukan secara sengaja oleh pihak pemberi kerja (Ramadhani & Nugroho, 2022).

Dalam kerangka hukum perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022, setiap aktivitas pengumpulan, pemrosesan, dan penyimpanan data pribadi harus memenuhi prinsip-prinsip legalitas, transparansi, dan akuntabilitas. Kegagalan dalam mematuhi prinsip-prinsip tersebut dapat menyebabkan terjadinya pelanggaran privasi yang berdampak hukum (Shafa Salsabila, 2025). Berikut ini adalah beberapa bentuk pelanggaran privasi yang kerap dijumpai dalam praktik ketenagakerjaan digital:

I. Pengawasan Aktivitas Digital Karyawan Tanpa Informasi atau Persetujuan

Sering kali perusahaan melakukan monitoring terhadap email kantor, aktivitas browsing, hingga penggunaan aplikasi kerja milik karyawan tanpa pemberitahuan yang jelas atau persetujuan eksplisit dari individu yang bersangkutan. Meskipun perangkat yang digunakan adalah milik perusahaan, intervensi terhadap komunikasi pribadi atau pemantauan perilaku digital tanpa dasar hukum yang sah bertentangan dengan prinsip transparansi dalam Pasal 20 ayat (1) UU PDP. Ketentuan ini mengharuskan pengendali data untuk memberikan pemberitahuan tertulis mengenai tujuan dan dasar hukum pengolahan data.

II. **Penanganan Data Biometrik yang Tidak Sesuai Prosedur**

Banyak perusahaan menggunakan data biometrik, seperti sidik jari atau pengenalan wajah, sebagai bagian dari sistem presensi dan kontrol akses. Data jenis ini termasuk dalam kategori data pribadi yang bersifat spesifik dan sensitif sebagaimana dijelaskan dalam Pasal 4 ayat (2) huruf a UU PDP. Perlakuan terhadap data biometrik menuntut kehati-hatian ekstra karena sifatnya yang tidak dapat diubah seperti kata sandi. Penyimpanan data ini tanpa proteksi memadai—misalnya tanpa enkripsi—atau penggunaannya untuk kepentingan lain di luar fungsi utama dapat dianggap sebagai pelanggaran serius yang berimplikasi hukum.

III. **Pemasangan Kamera Pengawas (CCTV) Tanpa Transparansi**

Keberadaan kamera pengawas di area kerja memang dapat menunjang aspek keamanan. Namun, pemasangannya kerap dilakukan tanpa kejelasan mengenai area pengawasan, durasi penyimpanan data, serta tujuan penggunaannya. Hal ini bertentangan dengan prinsip kejelasan tujuan dan pembatasan ruang lingkup pengumpulan data yang tercantum dalam Pasal 3 huruf a dan b UU PDP. Rekaman visual yang kemudian digunakan untuk menilai performa kerja atau dijadikan dasar sanksi tanpa persetujuan karyawan dapat dikategorikan sebagai penyalahgunaan data.

IV. **Ilustrasi Nyata: Studi Kasus Pelanggaran Privasi dalam Relasi Kerja**

Untuk menggambarkan potensi pelanggaran secara nyata, dapat dikaji sebuah kasus di mana perusahaan melakukan pemantauan aktivitas karyawan melalui perangkat digital, lalu menggunakan data tersebut sebagai dasar untuk melakukan Pemutusan Hubungan Kerja (PHK) secara sepihak. Dalam kasus ini, karyawan tidak diberi tahu bahwa aktivitas mereka sedang dipantau dan data yang dikumpulkan kemudian digunakan untuk menilai loyalitas atau produktivitas, tanpa adanya prosedur transparan. Sengketa pun terjadi karena pelanggaran terhadap hak atas privasi dan penggunaan data tanpa dasar hukum. Contoh lain yang relevan adalah kebocoran data biometrik yang terjadi akibat kelalaian pihak ketiga, yaitu vendor penyedia sistem absensi digital. Data yang bocor—seperti rekaman sidik jari dan wajah karyawan—kemudian tersebar di internet akibat lemahnya sistem keamanan vendor. Insiden ini menimbulkan dampak serius, baik secara psikologis maupun materiil bagi karyawan yang terdampak, dan mencerminkan kegagalan dalam menerapkan prinsip keamanan data sebagaimana dipersyaratkan dalam peraturan perundang-undangan.

V. **Penegakan Hukum dan Urgensi Kepatuhan terhadap UU PDP**

Berbagai bentuk pelanggaran tersebut menegaskan pentingnya kesadaran hukum dalam dunia ketenagakerjaan digital. UU PDP bukan sekadar instrumen hukum, melainkan juga fondasi perlindungan atas martabat dan integritas individu dalam relasi kerja. Perusahaan sebagai pengendali data wajib menyusun kebijakan internal yang sejalan dengan ketentuan hukum serta memberikan pelatihan kepada seluruh pemangku kepentingan untuk menghindari praktik-praktik pengolahan data yang melanggar hukum (Andriansyah, 2023).

Implikasi Hukum atas Pelanggaran Data Pribadi dalam Hubungan Kerja Berdasarkan UU PDP

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam pengaturan hak atas privasi di Indonesia, termasuk dalam konteks ketenagakerjaan. Dalam hubungan industrial, pemberi kerja memegang posisi strategis sebagai pengendali data pribadi karyawan, sehingga memiliki tanggung jawab hukum untuk mengelola data secara sah, terbatas, dan proporsional. Ketidakpatuhan terhadap ketentuan tersebut dapat mengakibatkan konsekuensi hukum yang signifikan, baik dalam bentuk sanksi administratif maupun pidana. Ketentuan dalam UU PDP menegaskan bahwa setiap

pelanggaran atas prinsip-prinsip pengolahan data pribadi tidak boleh dibiarkan tanpa pertanggungjawaban. Hukum memberikan instrumen sanksi yang bertujuan tidak hanya untuk menghukum, tetapi juga untuk mencegah terulangnya pelanggaran dan memastikan pemulihan bagi subjek data yang dirugikan (Rika Widianita, 2023).

Berdasarkan Pasal 57 ayat (1) UU PDP, pengendali data yang melanggar ketentuan dapat dikenai berbagai bentuk sanksi administratif. Sanksi ini bersifat bertingkat dan dapat dikenakan satu atau lebih secara bersamaan, tergantung pada derajat pelanggaran dan dampaknya terhadap subjek data. Jenis-jenis sanksi administratif mencakup teguran tertulis, penghentian sementara pemrosesan data, penghapusan atau pemusnahan data pribadi, kewajiban untuk membayar ganti rugi, pembekuan sebagian atau seluruh kegiatan usaha, serta pengenaan denda administratif.

Pemberlakuan sanksi administratif umumnya menjadi opsi pertama dalam penegakan hukum, khususnya untuk pelanggaran yang bersifat teknis atau administratif, seperti kegagalan memberikan pemberitahuan kebocoran data kepada karyawan, pengumpulan data tanpa kejelasan tujuan, atau kelalaian dalam penerapan protokol keamanan. Pengawasan dan penerapan sanksi administratif dilaksanakan oleh lembaga independen yang dibentuk khusus untuk menangani perlindungan data pribadi, sebagaimana diatur dalam Pasal 58 UU PDP. Untuk pelanggaran yang lebih serius, UU PDP mengatur ketentuan sanksi pidana yang bersifat represif. Bab XIII UU PDP (Pasal 67–73) secara eksplisit merinci ancaman pidana bagi individu maupun entitas hukum yang secara sengaja melakukan penyalahgunaan data pribadi.

Misalnya, Pasal 67 menetapkan bahwa setiap orang yang secara melawan hukum mengakses atau mengumpulkan data pribadi milik orang lain dapat dipidana dengan penjara hingga lima tahun atau denda maksimal sebesar Rp5 miliar. Selanjutnya, Pasal 68 dan 69 mengatur sanksi bagi pihak yang menyebarkan data pribadi tanpa persetujuan, yang ancaman hukumannya mencapai enam tahun penjara dan/atau denda sebesar Rp6 miliar (Junaedi, Said, & Tahir, 2023).

Bagi korporasi yang melanggar ketentuan, Pasal 70 hingga 73 memberikan ruang bagi penerapan sanksi berat, termasuk denda administratif hingga 2% dari total pendapatan tahunan, perampasan keuntungan hasil pelanggaran, pembekuan izin usaha, dan dalam kasus ekstrem, pembubaran badan hukum. Sanksi pidana ini mencerminkan keseriusan negara dalam melindungi data pribadi sebagai hak fundamental. Penerapan sanksi pidana lazimnya diberikan pada pelanggaran yang berdampak sistemik dan membahayakan subjek data, seperti praktik penjualan data pribadi karyawan untuk kepentingan komersial, kebocoran data dalam jumlah besar yang digunakan untuk pemerasan, atau pemanfaatan data untuk diskriminasi dan PHK semena-mena (Junaedi, 2022).

Untuk memahami perbedaan antara kedua jenis sanksi ini, penting menilik tujuan dan karakteristik penegakan hukumnya. Sanksi administratif bertujuan korektif dan bersifat preventif, diberikan kepada pelaku yang melakukan pelanggaran prosedural atau teknis tanpa unsur kesengajaan. Otoritas yang berwenang menjatuhkan sanksi ini adalah lembaga pengawas perlindungan data pribadi. Sebaliknya, sanksi pidana memiliki fungsi represif dan bertujuan memberikan efek jera. Ia diterapkan pada pelanggaran yang disengaja, berdampak besar, serta mengandung unsur pelanggaran etika dan hukum yang serius. Penegak hukum seperti kepolisian, kejaksaan, dan pengadilan memiliki wewenang untuk menindak pelanggaran ini.

Tanggung Jawab Perusahaan sebagai Pengendali Data

Perusahaan yang beroperasi dalam ekosistem kerja digital memiliki kedudukan yang strategis sebagai pengendali data pribadi (data controller), khususnya atas data karyawan yang dikumpulkan dan diproses selama berlangsungnya hubungan kerja. Kedudukan hukum ini ditegaskan dalam **Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)**, yang menyatakan bahwa pengendali data pribadi

adalah setiap subjek hukum yang memiliki kewenangan untuk menentukan tujuan serta cara pemrosesan data pribadi.

Sebagai entitas yang menentukan arah dan ruang lingkup pengolahan data, perusahaan berkewajiban untuk menjalankan pengelolaan data karyawan secara sah, akuntabel, dan sesuai prinsip perlindungan data. Setiap penyimpangan dari kewajiban tersebut dapat menimbulkan pertanggungjawaban hukum, baik dalam bentuk administratif maupun pidana.

1. Persetujuan yang Sah sebagai Dasar Pemrosesan

Salah satu kewajiban fundamental perusahaan dalam kapasitasnya sebagai pengendali data adalah mendapatkan **persetujuan yang sah dan eksplisit dari karyawan** sebelum melakukan aktivitas pengumpulan atau penggunaan data pribadi. Hal ini menjadi prinsip utama yang diatur dalam **Pasal 20 ayat (1) UU PDP**, yang mensyaratkan adanya persetujuan sebelum data dapat diproses, kecuali terdapat pengecualian yang secara jelas diatur oleh peraturan perundang-undangan. Persetujuan dimaksud harus didasarkan pada prinsip *informed consent*, yaitu diberikan secara bebas, spesifik, berdasarkan informasi yang memadai, dan secara sadar oleh subjek data. Informasi tersebut mencakup jenis data yang dikumpulkan, tujuan dari pemrosesan, jangka waktu penyimpanan, hingga kemungkinan akses oleh pihak ketiga. Oleh karena itu, perusahaan tidak dapat mengklaim kepatuhan hukum hanya dengan menyisipkan klausul umum dalam kontrak kerja; harus ada bentuk persetujuan yang eksplisit dan terdokumentasi. Dalam praktik ketenagakerjaan, pemrosesan data karyawan yang tergolong sensitif—seperti data kesehatan, informasi biometrik, lokasi, atau penggunaan perangkat kerja—memerlukan tingkat kehati-hatian yang tinggi. Tanpa dasar hukum atau persetujuan yang sah, pemrosesan atas data tersebut dapat dianggap sebagai pelanggaran terhadap hak privasi individu.

2. Kewajiban Menjalankan Prinsip Transparansi dan Akuntabilitas

UU PDP juga menuntut perusahaan untuk menjalankan prinsip **transparansi** dalam memberikan informasi terkait pengolahan data pribadi. Transparansi ini mengharuskan perusahaan untuk menyampaikan secara terbuka dan mudah dipahami mengenai mekanisme pengumpulan, penggunaan, penyimpanan, dan penghapusan data pribadi. Hal ini diatur secara spesifik dalam **Pasal 22 UU PDP**, yang memberikan jaminan hak informasi kepada subjek data. Selain transparansi, prinsip **akuntabilitas** menjadi standar penting dalam penegakan tata kelola data. Perusahaan harus mampu menunjukkan bukti kepatuhan atas seluruh tahapan pemrosesan data, termasuk menyusun dokumentasi proses, melakukan audit internal secara berkala, dan memiliki kebijakan tertulis yang menjelaskan perlakuan atas data pribadi. Kegagalan memenuhi prinsip ini dapat memicu tanggung jawab hukum, sebagaimana diatur dalam **Pasal 46 UU PDP**, termasuk jika perusahaan lalai dalam menginformasikan terjadinya insiden kebocoran data dalam jangka waktu yang ditentukan. Dengan demikian, pelaksanaan prinsip transparansi dan akuntabilitas bukan hanya kewajiban moral atau etis, melainkan bagian dari sistem penegakan hukum yang dapat digunakan sebagai dasar evaluasi kepatuhan dan pertanggungjawaban.

3. Tanggung Jawab Korporasi dari Perspektif Hukum Pidana dan Kepatuhan Internal

Dalam kajian hukum pidana korporasi, tanggung jawab perusahaan sebagai subjek hukum semakin mendapat tempat, khususnya ketika pelanggaran dilakukan oleh pengurus atau individu dengan jabatan strategis yang bertindak untuk dan atas nama perusahaan. **Prof. Hikmahanto Juwana** berpendapat bahwa badan hukum dapat dimintai pertanggungjawaban pidana apabila unsur pelanggaran hukum dilakukan oleh pihak internal yang memiliki otoritas, dan tindakan tersebut membawa keuntungan bagi perusahaan secara langsung maupun tidak langsung. Selaras dengan itu, **Prof. R. Benny Riyanto** menekankan bahwa tanggung jawab korporasi tidak hanya dilihat dari

sisi represif, tetapi juga dalam kerangka **preventif**, yaitu dengan menerapkan kebijakan kepatuhan internal yang komprehensif. Langkah ini mencakup penyusunan Standar Operasional Prosedur (SOP), kode etik pemrosesan data, serta pelatihan reguler kepada seluruh personel mengenai perlindungan data pribadi. Apabila suatu pelanggaran dilakukan oleh karyawan tanpa sepengetahuan perusahaan, maka korporasi dapat terbebas dari tanggung jawab pidana selama mampu menunjukkan bahwa sistem pengawasan internal telah berjalan dengan wajar dan memadai. Konsep ini dikenal dengan istilah *due diligence defense*, yang telah lama menjadi bagian dari doktrin dalam hukum korporasi global.

4. Membangun Budaya Perlindungan Data sebagai Bentuk Tanggung Jawab Berkelanjutan

Kepatuhan terhadap UU PDP bukan sekadar kewajiban hukum, melainkan juga refleksi dari integritas dan tanggung jawab sosial perusahaan dalam melindungi hak asasi manusia, khususnya hak atas privasi. Oleh sebab itu, tanggung jawab sebagai pengendali data harus dijalankan secara proaktif dengan membangun **budaya perlindungan data pribadi** di seluruh lini organisasi. Langkah-langkah strategis yang dapat diambil mencakup pembentukan satuan kerja khusus perlindungan data (Data Protection Officer), integrasi prinsip-prinsip privasi sejak awal perancangan sistem (privacy by design), hingga evaluasi berkala atas kebijakan data yang berlaku. Semua ini berkontribusi dalam menciptakan ekosistem kerja yang aman, transparan, dan bertanggung jawab terhadap hak-hak digital karyawan. Dalam era transformasi digital yang ditandai oleh pemanfaatan teknologi berbasis data, komitmen perusahaan terhadap perlindungan data pribadi menjadi tolok ukur penting dalam membangun kepercayaan, kredibilitas, dan reputasi korporasi. Tanggung jawab hukum yang melekat pada peran sebagai pengendali data bukan hanya bersifat normatif, melainkan juga strategis dalam menjawab tantangan tata kelola data masa depan (Susanto, 2023).

Kekosongan Regulatif dan Tantangan dalam Implementasi UU Pelindungan Data Pribadi di Lingkungan Kerja Digital

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah memberikan kerangka hukum yang solid dalam mengatur pemrosesan data pribadi, termasuk dalam konteks hubungan industrial modern. Namun, dalam praktik implementasinya, terdapat berbagai celah dan hambatan yang memperlihatkan ketidaksesuaian antara norma hukum yang bersifat ideal dengan realitas faktual di lapangan. Kondisi ini menimbulkan tantangan serius dalam menjamin perlindungan hak privasi karyawan di era digitalisasi ketenagakerjaan. Salah satu kendala utama yang menghambat efektivitas penerapan UU PDP dalam lingkungan kerja adalah ketiadaan kebijakan internal yang terstruktur dan seragam di kalangan pelaku usaha. Banyak perusahaan, terutama yang bergerak di sektor informal atau tergolong dalam kategori Usaha Mikro, Kecil, dan Menengah (UMKM), belum memiliki sistem kebijakan tertulis mengenai tata kelola data pribadi karyawan. Hal ini meliputi ketiadaan prosedur terkait perolehan persetujuan pemrosesan data, penyimpanan yang aman, serta pembatasan penggunaan data untuk tujuan tertentu (Riyadi & Toto Tohir Suriaatmadja, 2023).

Kekosongan kebijakan internal ini tidak hanya menunjukkan lemahnya kepatuhan administratif, tetapi juga menimbulkan kekaburan hukum bagi pekerja yang datanya digunakan tanpa dasar yang jelas. Bahkan di sektor formal, beberapa korporasi besar masih menggunakan pedoman pengelolaan data yang belum selaras dengan prinsip-prinsip baru yang ditetapkan dalam UU PDP, seperti akuntabilitas, pembatasan tujuan (*purpose limitation*), dan keamanan pemrosesan (*data security*). Hal ini menyebabkan implementasi UU PDP di tempat kerja bersifat parsial, tidak konsisten, dan tidak memiliki kekuatan eksekutorial yang memadai. Padahal, keberadaan regulasi internal yang terstandar menjadi fondasi penting dalam menumbuhkan budaya kepatuhan hukum terhadap perlindungan data pribadi.

Tantangan lainnya yang cukup krusial adalah masih rendahnya tingkat pemahaman hukum di kalangan pemberi kerja maupun pekerja terkait dengan pentingnya perlindungan data pribadi. Banyak pekerja belum menyadari bahwa data yang mereka serahkan kepada perusahaan—seperti rekam medis, data biometrik, atau aktivitas daring melalui platform kerja digital—termasuk dalam kategori data pribadi yang dijamin perlindungannya oleh hukum. Kurangnya literasi ini menjadikan karyawan rentan terhadap eksploitasi data, karena mereka tidak mengetahui hak-hak hukum yang dimiliki, termasuk hak untuk menarik persetujuan, meminta penghapusan data, atau mengajukan keberatan atas penggunaan data mereka. Di sisi lain, pengusaha atau manajemen sering kali masih melihat data pribadi hanya sebagai bagian dari aset operasional tanpa memahami dimensi yuridis dan etisnya. Ketidaktahuan ini berdampak pada minimnya kontrol internal atas praktik pemrosesan data. Banyak perusahaan melakukan pengumpulan data secara luas tanpa memperhatikan prinsip-prinsip dasar perlindungan data seperti *lawfulness*, *data minimization*, dan *storage limitation*. Akibatnya, praktik yang tidak etis dan melanggar hukum terus berlangsung tanpa koreksi dan sering kali tidak dilaporkan, karena korban tidak memahami bentuk pelanggaran yang terjadi atau mekanisme pengaduannya (Nugroho, 2022).

UU PDP sejatinya telah merancang pembentukan suatu lembaga pengawas independen yang bertugas mengawasi, menangani sengketa, serta menegakkan norma perlindungan data pribadi. Namun, dalam implementasinya, lembaga ini belum beroperasi secara fungsional karena terkendala pada aspek kelembagaan, seperti belum tersusunnya struktur organisasi yang definitif, pembagian kewenangan teknis, dan sistem pelaporan yang dapat diakses publik secara efektif. Selain itu, tidak adanya petunjuk pelaksanaan dan teknis yang rinci mengenai tata cara penegakan hukum terhadap pelanggaran data di sektor ketenagakerjaan menyebabkan kekaburan hukum dalam menangani kasus. Aparat penegak hukum, dalam banyak kasus, kesulitan menindak pelanggaran karena kurangnya regulasi pelengkap yang menjabarkan secara operasional norma-norma yang terdapat dalam UU PDP.

Lebih jauh, tantangan yang tidak kalah penting adalah pada aspek pembuktian digital. Pelanggaran privasi di lingkungan kerja sering kali dilakukan melalui sistem internal perusahaan, seperti penggunaan perangkat lunak pelacak, rekaman kamera pengawas (CCTV), atau pengawasan aktivitas daring, yang tidak disertai dengan sistem audit yang terbuka dan dapat diverifikasi. Bukti atas pelanggaran tersebut sering kali bersifat tertutup, tersembunyi, atau bahkan telah dihapus oleh pelaku yang memiliki akses ke sistem. Tanpa kehadiran teknologi *digital forensics* yang terjangkau dan infrastruktur investigasi siber yang kuat, pembuktian menjadi lemah dan menimbulkan keraguan dalam proses hukum. Terbatasnya jumlah penyidik yang memiliki keahlian dalam menelusuri jejak digital, serta belum adanya kolaborasi yang kuat antara otoritas perlindungan data dengan instansi ketenagakerjaan dan kepolisian, semakin memperparah kondisi ini.

Melihat kompleksitas tantangan di atas, maka perlu dilakukan reformasi struktural yang mencakup harmonisasi regulasi antar sektor, pembentukan sistem pelaporan yang mudah diakses publik, serta edukasi hukum yang sistematis di tingkat korporasi dan pekerja. Pemerintah perlu mempercepat implementasi lembaga pengawas independen yang profesional, memiliki otoritas penuh, serta dilengkapi dengan perangkat teknis dan sumber daya manusia yang memadai. Di sisi lain, perusahaan juga didorong untuk mengembangkan program pelatihan internal terkait perlindungan data pribadi yang tidak hanya bersifat administratif, tetapi juga menyentuh aspek etika dan tanggung jawab sosial. Pelibatan serikat pekerja, LSM, dan media dalam mengawal penerapan UU PDP juga menjadi elemen penting dalam menciptakan ekosistem perlindungan data yang inklusif dan berkeadilan (Junaedi et al., 2023).

SIMPULAN

Transformasi digital dalam dunia ketenagakerjaan telah menciptakan dinamika baru yang berdampak langsung terhadap aspek perlindungan data pribadi karyawan. Dalam era di mana pengumpulan dan pemrosesan data dilakukan secara masif dan terotomatisasi, hak privasi pekerja menjadi isu yang semakin penting dalam relasi industrial. Dalam konteks ini, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) merupakan langkah maju yang signifikan dalam membangun sistem hukum yang menjamin hak atas data pribadi sebagai bagian dari hak asasi manusia.

UU PDP memberikan kerangka normatif yang jelas dan terstruktur mengenai kewajiban pengendali dan prosesor data—termasuk pelaku usaha atau perusahaan—dalam mengelola informasi pribadi secara sah, terbatas, dan bertanggung jawab. Pengaturan mengenai hak-hak subjek data, mulai dari hak akses, hak untuk memperbaiki, hingga hak untuk menghapus data, memperkuat posisi individu dalam relasi hukum dengan pihak pengendali data. Selain itu, ketentuan sanksi administratif dan pidana sebagaimana diatur dalam Pasal 57 serta Pasal 67 hingga 73 menunjukkan bahwa UU PDP tidak hanya bersifat deklaratif, tetapi juga represif terhadap pelanggaran yang terjadi. Namun demikian, penerapan norma-norma tersebut dalam praktik masih menghadapi berbagai hambatan yang signifikan. Tantangan utama terletak pada lemahnya kapasitas penegakan hukum dan belum berfungsinya lembaga pengawas secara optimal. Di samping itu, rendahnya pemahaman pelaku usaha terhadap prinsip-prinsip perlindungan data, serta kurangnya kesadaran pekerja akan hak privasi mereka, menciptakan ruang yang cukup besar bagi terjadinya pelanggaran tanpa pertanggungjawaban.

Fenomena pengawasan digital yang dilakukan secara sepihak tanpa persetujuan eksplisit, pemrosesan data biometrik tanpa dasar hukum yang kuat, serta penggunaan sistem pelacakan karyawan yang invasif terhadap ruang pribadi, memperlihatkan adanya ketimpangan antara norma hukum yang diidealkan oleh UU PDP dan praktik faktual di lingkungan kerja digital. Hal ini diperparah oleh belum adanya integrasi yang memadai antara kebijakan perlindungan data pribadi dan regulasi ketenagakerjaan yang telah lebih dahulu eksis, seperti Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan. Oleh karena itu, diperlukan langkah-langkah strategis untuk menyelaraskan UU PDP dengan instrumen hukum ketenagakerjaan, baik dalam bentuk harmonisasi regulasi maupun pengembangan kebijakan sektoral yang lebih spesifik. Sinkronisasi ini menjadi penting agar perlindungan hak karyawan dapat dilakukan secara menyeluruh dan berkelanjutan, serta tidak terfragmentasi antara satu kerangka hukum dengan kerangka hukum lainnya.

Penelitian ini menyimpulkan bahwa meskipun landasan hukum untuk perlindungan data pribadi telah tersedia secara normatif, efektivitas implementasinya sangat bergantung pada tiga aspek utama: pertama, penguatan kelembagaan penegak hukum dan lembaga pengawas yang independen dan profesional; kedua, peningkatan literasi hukum di kalangan pelaku usaha dan pekerja mengenai hak-hak privasi dan kewajiban hukum dalam pemrosesan data; dan ketiga, pembangunan sistem kebijakan internal perusahaan yang sejalan dengan prinsip-prinsip perlindungan data pribadi. Pelindungan data pribadi karyawan bukan semata-mata merupakan kewajiban negara, tetapi juga menjadi tanggung jawab kolektif seluruh entitas korporasi sebagai pengendali data. Dalam ekosistem kerja digital yang terus berkembang, partisipasi aktif semua pemangku kepentingan menjadi kunci untuk memastikan bahwa hak privasi individu tetap terlindungi dan tidak tergerus oleh kepentingan efisiensi dan produktivitas semata.

SARAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disusun sejumlah rekomendasi strategis guna memperkuat perlindungan data pribadi karyawan di tengah maraknya transformasi digital dalam dunia kerja. Upaya-upaya berikut ini diharapkan dapat memperkecil kesenjangan antara norma hukum dan realitas implementatif yang selama ini menjadi tantangan utama dalam perlindungan privasi tenaga kerja di Indonesia.

Perusahaan, baik skala besar maupun pelaku usaha mikro, kecil, dan menengah (UMKM), perlu menetapkan dan menerapkan kebijakan internal yang secara sistematis mengatur tata kelola data pribadi karyawan. Kebijakan tersebut idealnya mencakup seluruh siklus pemrosesan data, mulai dari tahap pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data, dengan berpedoman pada prinsip-prinsip utama yang tercantum dalam UU Pelindungan Data Pribadi (UU PDP). Prinsip-prinsip seperti legalitas, persetujuan eksplisit, pembatasan tujuan, akuntabilitas, integritas data, dan keamanan pemrosesan wajib dijadikan fondasi dalam penyusunan pedoman internal. Dalam rangka memastikan pelaksanaan yang berkelanjutan, perusahaan juga disarankan untuk mengangkat petugas khusus yang memiliki tanggung jawab terhadap perlindungan data pribadi (Data Protection Officer/DPO), guna menjamin adanya pengawasan institusional secara menyeluruh dan berkelanjutan.

Pemerintah, khususnya melalui koordinasi antara Kementerian Komunikasi dan Informatika (Kominfo) serta Kementerian Ketenagakerjaan, perlu memperluas cakupan program literasi dan edukasi hukum mengenai perlindungan data pribadi. Kampanye ini seyogianya tidak hanya bersifat seremonial, melainkan dirancang sebagai upaya jangka panjang melalui pelatihan intensif, penyediaan modul edukatif, dan bimbingan teknis bagi pelaku usaha serta pekerja. Sosialisasi harus menargetkan kelompok strategis di tempat kerja seperti manajemen sumber daya manusia (HRD), serikat buruh, dan karyawan secara umum, terutama di sektor-sektor yang rentan terhadap pelanggaran privasi akibat rendahnya pemahaman hukum yang memadai. Edukasi semacam ini juga penting untuk menanamkan nilai-nilai etis dalam pengelolaan data, sehingga prinsip perlindungan data pribadi tidak hanya menjadi kewajiban legal, tetapi juga bagian dari budaya organisasi.

Urgensi untuk segera membentuk lembaga pengawas independen sesuai mandat UU PDP menjadi semakin mendesak, mengingat kebutuhan akan mekanisme pengaduan dan penegakan hukum yang efektif di bidang perlindungan data. Lembaga ini harus dilengkapi dengan kewenangan investigatif yang kuat, prosedur penanganan laporan yang transparan, serta wewenang untuk menjatuhkan sanksi administratif maupun pidana secara proporsional. Di samping itu, diperlukan pula penyusunan standar operasional prosedur (SOP) yang mengatur penggunaan sistem pemantauan digital di tempat kerja. Instrumen pengawasan seperti kamera CCTV, sistem absensi berbasis biometrik, serta perangkat pelacakan aktivitas daring harus dikendalikan melalui SOP yang menjamin keterbukaan, perlindungan hak privasi, dan kejelasan batas kewenangan. SOP ini juga harus mencakup kewajiban pemberitahuan kepada karyawan, pembatasan ruang lingkup pemantauan, serta jangka waktu penyimpanan data hasil pemantauan (Putri & Elmina Martha, 2022).

DAFTAR PUSTAKA

- Djumrianti, D., & Rizkiawan Rizkiawan, E. K. (2024). *KONSEP DAN TEORI E-BUSINESS & E-COMMERCE*. Bandung: CV. Widina Media Utama.
- Muryani Verina Dwi, W. S. (2025). EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENJAWAB TANTANGAN KEAMANAN SIBER DI INDONESIA. *Causa: Jurnal Hukum dan Kewarganegaraan*, 81-90.
- Reysa Aurelia Shabilla, S. A. (2025). Oversharing di Kalangan Remaja dan Mahasiswa serta Ancaman terhadap Privasi Menurut UU Pelindungan Data Pribadi. *INLAW (Indonesian Journal of Law)*, 68-77.
- Shafa Salsabila, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 145-157.

- Sidi Ahyar, w. (2025). EKSPLORASI METODE PENELITIAN DENGAN PENDEKATAN NORMATIF DAN EMPIRIS DALAM PENELITIAN HUKUM DI INDONESIA. *Lex Jurnalica*, 66-72.
- Sri Mulyati, S. A. (2025). PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL. *Causa: Jurnal Hukum dan Kewarganegaraan*, 91-100.
- Andriansyah, Y. (2023). *Perlindungan Data Pribadi di Era Digital: Tinjauan terhadap UU No. 27 Tahun 2022*. Jakarta: Rajawali Pers.
- Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, 7(3), 445–461. <https://doi.org/10.20885/jlr.vol7.iss3.art1>
- Junaedi, J. (2022). Criminal Penalty for Employees Who Leave Company Confidential According To the Electronic Information and Transaction Law. *International Journal of Social Science*, 2(2), 1565–1570. <https://doi.org/10.53625/ijss.v2i2.3426>
- Junaedi, Said, T. G., & Tahir, M. (2023). Criminal for Leaking Administs Data of PDDIKTI and PSD-PTU According to Law Number 19 Year 2016 Concerning ITE. *East Asian Journal of Multidisciplinary Research*, 2(2), 691–704. <https://doi.org/10.55927/eajmr.v2i2.3026>
- Nugroho, H. P. (2022). Hak atas Privasi sebagai Bagian dari Hak Asasi Manusia dalam Konteks Digital. *Jurnal HAM*, 13(1), 54–68.
- P, A. A. W., Esfandiari, F., & Wasis, W. (2023). Juridical Analysis of Legal Protection of Personal Data in terms of Legal Certainty. *Indonesia Law Reform Journal*, 3(1), 96–108. <https://doi.org/10.22219/ilrej.v3i1.23840>
- Putri, E. P., & Elmina Martha, A. (2022). The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage. *Varia Justicia*, 17(3), 287–303. <https://doi.org/10.31603/variajusticia.v17i3.6231>
- Ramadhani, M., & Nugroho, S. (2022). Perlindungan Hukum Terhadap Data Biometrik di Era Digitalisasi Ketenagakerjaan. *Jurnal Hukum Digital Indonesia*, 5(1), 45–62.
- Riyadi, G. A., & Toto Tohir Suriaatmadja. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Bandung Conference Series: Law Studies*, 3(1). <https://doi.org/10.29313/bcsls.v3i1.4945>
- Rizki, R., Brahmana, H., Iskandar, J., An, Y., & Susanto, S. (2022). Tinjauan Yuridis Perlindungan Hak Privasi Dalam Transaksi Elektronik Pada Era Disrupsi Teknologi. *Journal of Education, Humaniora and Social Sciences (JEHSS)*, 4(4), 2234–2246. <https://doi.org/10.34007/jehss.v4i4.1044>
- Susanto, D. (2023). Protection of Personal Data in Business: An Overview of the Perspective of Business Ethics and Its Implications for Regulatory Compliance. *Indonesian Journal of Contemporary Multidisciplinary Research*, 2(2), 109–120. <https://doi.org/10.55927/modern.v2i2.3459>
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). Pemerintah Republik Indonesia.
- Wahyuni, S. (2021). Tanggung Jawab Hukum Pengendali Data dalam Sistem Elektronik. *Jurnal Hukum & Teknologi*, 5(2), 123–137.