HUKUM DINAMIKA EKSELENSIA

https://journalversa.com/s/index.php/hde Volume 07, No. 2, Juni 2025

PERLINDUNGAN DATA PRIBADI : TANTANGAN DAN SOLUSI DI ERA BIG DATA YANG BERKAITAN DENGAN HUKUM TELEMATIKA

Ratna Wulan Valentina[1], Rina Arum Prastiyanti[2]
[1,2]Universitas Duta Bangsa Surakarta
ratnavalentina0514@gmail.com[1], rin_arum@udb.ac.id[2]

***ABSTRACT**; Personal data protection is becoming an increasingly crucial issue in the Big Data era, where the volume, speed, and variety of data collected by various parties are increasing significantly. This article aims to explore the legal challenges faced in protecting personal data amidst the rapid development of Big Data technology and to provide legal solutions to overcome these challenges. The main focus of this article is two problem formulations: first, what are the legal challenges that arise in protecting personal data in the Big Data era? Second, what legal solutions can be applied to overcome these challenges? Through an analysis of existing personal data protection regulations, including a comparison with policies implemented in various countries such as the General Data Protection Regulation (GDPR) in Europe, this article identifies various obstacles such as unclear regulations, law enforcement issues, data leaks, and lack of transparency in data use. As a solution, this article proposes increasing international regulatory harmonization, strengthening the capacity of supervisory institutions, implementing stricter privacy-based policies, and increasing public awareness of their rights related to personal data. With this approach, it is hoped that a safer system can be created that can protect individual personal data from potential misuse in the Big Data era.*
***Keywords:** Personal Data Protection, Big Data, Legal Challenges, Legal Solutions, GDPR.*

ABSTRAK; Perlindungan data pribadi menjadi isu yang semakin krusial di era Big Data, di mana volume, kecepatan, dan variasi data yang dikumpulkan oleh berbagai pihak meningkat secara signifikan. Artikel ini bertujuan untuk mengeksplorasi tantangan hukum yang dihadapi dalam melindungi data pribadi di tengah perkembangan pesat teknologi Big Data dan memberikan solusi hukum untuk mengatasi tantangan tersebut. Fokus utama artikel ini adalah dua rumusan masalah: pertama, apa saja tantangan hukum yang muncul dalam perlindungan data pribadi di era Big Data? Kedua, bagaimana solusi hukum yang dapat diterapkan untuk mengatasi tantangan-tantangan tersebut? Melalui analisis terhadap regulasi perlindungan data pribadi yang

ada, termasuk perbandingan dengan kebijakan yang diterapkan di berbagai negara seperti General Data Protection Regulation (GDPR) di Eropa, artikel ini mengidentifikasi berbagai kendala seperti ketidakjelasan regulasi, masalah penegakan hukum, kebocoran data, serta kurangnya transparansi dalam penggunaan data. Sebagai solusi, artikel ini mengusulkan peningkatan harmonisasi regulasi internasional, penguatan kapasitas lembaga pengawas, penerapan kebijakan berbasis privasi yang lebih ketat, serta peningkatan kesadaran masyarakat mengenai hak-hak mereka terkait data pribadi. Dengan pendekatan ini, diharapkan dapat tercipta sistem yang lebih aman dan dapat melindungi data pribadi individu dari potensi penyalahgunaan di era Big Data.
Kata Kunci: Perlindungan Data Pribadi, Big Data, Tantangan Hukum, Solusi Hukum, GDPR.

PENDAHULUAN

Di era digital saat ini, data pribadi telah menjadi aset yang sangat berharga, bahkan melebihi nilai kekayaan fisik. Data pribadi mencakup informasi yang dapat digunakan untuk mengidentifikasi seseorang secara langsung atau tidak langsung, seperti nama, alamat, nomor identitas, informasi keuangan, hingga data perilaku online. Dalam berbagai sektor, mulai dari perbankan, kesehatan, pendidikan, hingga media sosial, data pribadi menjadi bahan baku utama dalam proses pengambilan keputusan, pemasaran, inovasi produk, dan pelayanan publik. Pentingnya perlindungan data pribadi semakin meningkat seiring dengan perkembangan teknologi seperti big data, kecerdasan buatan (AI), dan Internet of Things (IoT), yang memungkinkan pengumpulan, penyimpanan, dan analisis data dalam skala besar dan cepat. Jika tidak dikelola dengan baik, data pribadi berisiko disalahgunakan untuk tujuan yang merugikan individu, seperti pencurian identitas, penipuan keuangan, penyebaran informasi palsu, hingga pelanggaran hak privasi. Selain itu, kepercayaan publik terhadap sistem digital bergantung pada sejauh mana data pribadi mereka dilindungi. Konsumen cenderung hanya berinteraksi dengan platform atau layanan yang dapat menjamin keamanan informasi mereka. Oleh karena itu, dalam konteks era digital, perlindungan data pribadi bukan hanya soal privasi, melainkan juga menyangkut keamanan nasional, stabilitas ekonomi, dan hak asasi manusia. Dengan demikian, regulasi yang kuat dan kesadaran kolektif tentang pentingnya menjaga data pribadi menjadi kebutuhan yang mendesak.

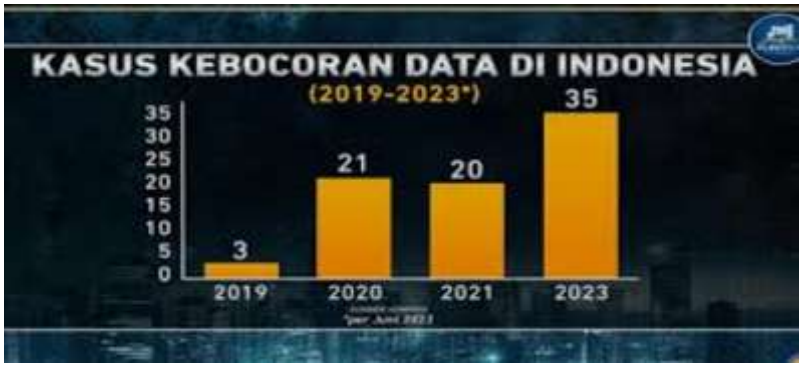
Perlindungan data pribadi menjadi isu krusial di era Big Data, di mana volume dan kompleksitas data yang dikumpulkan dan diproses sangat besar. Data pribadi tidak hanya mencakup informasi dasar seperti nama dan alamat, tetapi juga data perilaku, lokasi, dan biometrik yang semakin meluas penggunaannya. Di Indonesia, perlindungan terhadap data pribadi masih lemah dan rentan terhadap penyalahgunaan, sehingga menimbulkan kebutuhan mendesak untuk regulasi yang kuat dan efektif. Secara hukum, hak atas perlindungan data pribadi di Indonesia diakui sebagai bagian dari hak asasi manusia yang tercantum dalam Pasal 28G UUD 1945 dan diperkuat dengan hadirnya Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang – Undangan ini bertujuan memberikan payung hukum yang jelas dan mengatur tata kelola serta perlindungan data pribadi di sektor publik dan swasta, sebagai respons terhadap maraknya kebocoran dan penyalahgunaan data pribadi. Big Data menghasilkan jutaan gigabyte data setiap hari yang harus diproses dengan cepat, sehingga meningkatkan risiko kebocoran dan pelanggaran privasi. Banyak data dikumpulkan tanpa persetujuan eksplisit pengguna, misalnya melalui pelacakan lokasi dan cookie, yang menimbulkan masalah etika dan hukum terkait hak privasi individu. Pengguna sering tidak mengetahui bagaimana data mereka digunakan setelah dikumpulkan, membuka peluang penyalahgunaan data untuk tujuan yang tidak diinginkan. Data berasal dari berbagai format dan sumber yang tersebar, seperti perangkat IoT dan sistem terhubung, yang menyulitkan pengelolaan dan perlindungan data secara efektif. Sautunnida, L. (2018).

Penerapan UU PDP di Indonesia memberikan kerangka hukum yang jelas untuk melindungi data pribadi dari eksploitasi yang tidak sah dan meningkatkan kepastian hukum. Pendekatan yang mengintegrasikan prinsip privasi sejak tahap desain produk atau layanan untuk memastikan perlindungan data secara proaktif. Penggunaan enkripsi data, pengelolaan akses berbasis peran, audit dan pemantauan aktivitas data, serta konsolidasi data untuk mengurangi risiko kebocoran dan penyalahgunaan. Masyarakat dan pelaku bisnis perlu diedukasi tentang pentingnya perlindungan data pribadi dan cara-cara melindungi data secara mandiri, seperti penggunaan kata sandi kuat dan otentikasi multi-faktor. Pemerintah dan lembaga terkait harus aktif melakukan pengawasan dan penegakan hukum terhadap pelanggaran perlindungan data pribadi sesuai dengan ketentuan UU PDP.

Tujuan dari artikel berjudul "Perlindungan Data Pribadi: Tantangan dan Solusi di Era Big Data" adalah untuk Mengidentifikasi dan menjelaskan berbagai tantangan utama dalam perlindungan data pribadi yang muncul akibat perkembangan pesat teknologi Big Data, seperti volume data yang sangat besar, kecepatan pemrosesan data, pengumpulan data tanpa izin, ketidakjelasan penggunaan data, serta risiko kebocoran dan penyalahgunaan data pribadi. Menguraikan solusi-solusi efektif yang dapat diterapkan untuk mengatasi tantangan tersebut, termasuk penerapan enkripsi, kontrol akses, anonimisasi data, kebijakan privasi yang transparan, serta kepatuhan terhadap regulasi perlindungan data seperti GDPR dan CCPA. Menekankan pentingnya peran kebijakan privasi dan penegakan hukum dalam menjaga keamanan dan privasi data pribadi, serta membangun kepercayaan pengguna di era digital yang serba terkoneksi ini.

Memberikan wawasan bagi organisasi dan individu mengenai langkah- langkah strategis yang harus diambil untuk melindungi data pribadi secara efektif di Tengah Kompleksitas dan resiko yang ditimbulkan oleh era big data. Regulasi perlindungan data pribadi berfungsi untuk memberikan kerangka hukum yang jelas mengenai bagaimana data dikumpulkan, disimpan, digunakan, dan dibagikan. Regulasi ini mengatur kewajiban pihak-pihak yang mengelola data, seperti instansi pemerintah, perusahaan, dan penyedia layanan digital, untuk menjaga kerahasiaan, integritas, dan keamanan data pribadi. Selain itu, regulasi juga menjamin hak-hak individu, seperti hak untuk mengakses data mereka, hak untuk mengoreksi kesalahan data, dan hak untuk menghapus data.

Di tingkat internasional, regulasi seperti **General Data Protection Regulation (GDPR)** Uni Eropa telah menjadi standar acuan dalam menetapkan prinsip perlindungan data pribadi. Sementara di Indonesia, hadirnya **Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)** merupakan langkah penting dalam membangun sistem hukum yang responsif terhadap tantangan era digital. Perlindungan hukum yang kuat juga menciptakan iklim kepercayaan dalam ekosistem digital. Individu merasa lebih aman dalam bertransaksi dan berinteraksi secara online, sementara pelaku usaha digital lebih terdorong untuk mengadopsi praktik pengelolaan data yang bertanggung jawab. Oleh karena itu, keberadaan regulasi dan perlindungan hukum yang memadai merupakan fondasi utama dalam menjamin hak privasi, mendukung inovasi digital yang berkelanjutan, serta menjaga kedaulatan data di tengah arus globalisasi informasi.



Grafik tersebut menunjukkan perkembangan jumlah kasus kebocoran data di Indonesia dalam periode 2019 hingga 2023. Pada tahun 2019, tercatat hanya ada 3 kasus kebocoran data. Namun, pada tahun 2020 jumlah ini melonjak tajam menjadi 21 kasus. Pada tahun berikutnya, 2021, angka kebocoran data sedikit menurun menjadi 20 kasus. Menariknya, grafik tidak menampilkan data untuk tahun 2022, sehingga ada kekosongan informasi di tahun tersebut. Sementara itu, pada tahun 2023, hingga bulan Juni saja, kasus kebocoran data telah mencapai 35 kasus, angka tertinggi dibandingkan tahun-tahun sebelumnya. Data ini diambil dari sumber Kementerian Komunikasi dan Informatika (Kominfo) dan menunjukkan tren yang mengkhawatirkan terhadap meningkatnya insiden keamanan data di Indonesia. Peningkatan signifikan ini menjadi indikasi perlunya perhatian lebih serius terhadap perlindungan data pribadi dan keamanan siber di tanah air.

Dalam era digital yang ditandai dengan pertukaran data yang masif dan cepat, keberadaan regulasi dan perlindungan hukum terhadap data pribadi menjadi sangat penting. Data pribadi rentan terhadap berbagai ancaman, seperti pencurian identitas, penyalahgunaan informasi, dan pelanggaran privasi. Tanpa landasan hukum yang kuat, individu akan sulit mendapatkan perlindungan atas hak-hak pribadinya, sementara pelaku pelanggaran tidak memiliki batasan yang jelas atau konsekuensi hukum yang tegas. Rizal, M. S. (2019).

Rumusan Masalah

1. Apa saja tantangan hukum dalam melindungi data pribadi di era big data?
2. Bagaimana solusi hukum untuk mengatasi tantangan tersebut?

METODE PENELITIAN

Penelitian ini menggunakan metode normatif yuridis, yaitu suatu metode penelitian hukum yang dilakukan dengan menelaah bahan-bahan hukum primer dan sekunder untuk mengkaji perlindungan data pribadi di era big data. Metode ini bertujuan untuk menganalisis ketentuan hukum yang mengatur tentang perlindungan data pribadi, serta menilai sejauh mana regulasi yang ada mampu menghadapi tantangan yang ditimbulkan oleh perkembangan teknologi big data. Bahan hukum primer yang digunakan dalam penelitian ini meliputi peraturan perundang-undangan nasional, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), serta berbagai regulasi terkait lainnya. Selain itu, bahan hukum sekunder berupa jurnal ilmiah, literatur hukum, hasil seminar, dan panduan praktik dari lembaga-lembaga internasional seperti GDPR (General Data Protection Regulation) Uni Eropa juga dianalisis untuk memperkaya perspektif. Analisis dalam penelitian ini dilakukan secara normatif, yaitu dengan mengkaji norma-norma hukum yang berlaku, serta interpretasi terhadap ketentuan tersebut untuk mengidentifikasi kelemahan, tantangan, dan peluang perbaikan regulasi di masa depan. Pendekatan ini diharapkan mampu memberikan solusi hukum yang aplikatif dalam rangka memperkuat perlindungan data pribadi di tengah perkembangan pesat big data.

HASIL DAN PEMBAHASAN

Data pribadi adalah segala informasi yang berkaitan dengan individu yang dapat diidentifikasi secara langsung maupun tidak langsung. Identifikasi ini bisa melalui nama, nomor identitas, data lokasi, informasi fisik, fisiologis, genetis, ekonomi, budaya, atau faktor sosial seseorang. Dengan kata lain, data pribadi mencakup informasi yang, baik secara tunggal maupun dikombinasikan dengan informasi lain, dapat mengungkapkan identitas seseorang. Secara hukum, definisi data pribadi dapat ditemukan dalam berbagai regulasi. Misalnya, menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, data pribadi didefinisikan sebagai "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya secara langsung atau tidak langsung melalui sistem elektronik dan/atau non-elektronik."Sementara itu, dalam standar internasional seperti General Data Protection Regulation (GDPR) Uni Eropa, data

pribadi didefinisikan sebagai "segala informasi yang berkaitan dengan orang perseorangan yang diidentifikasi atau dapat diidentifikasi."Data pribadi umumnya dibedakan menjadi dua kategori, Data Pribadi Umum, seperti nama, alamat, tanggal lahir, atau nomor telepon. Data Pribadi Sensitif, seperti data kesehatan, data biometrik, data keuangan, orientasi seksual, atau kepercayaan agama. Perlindungan terhadap data pribadi sangat penting untuk mencegah penyalahgunaan informasi yang dapat berdampak pada kerugian moral, sosial, atau finansial bagi individu. Oleh karena itu, pemahaman yang jelas tentang definisi data pribadi menjadi dasar utama dalam menyusun kebijakan perlindungan privasi di era digital. Niffari, H. (2020).

Perlindungan data dalam perspektif hukum merujuk pada upaya untuk melindungi informasi pribadi dan data yang berkaitan dengan individu dari penyalahgunaan, pengungkapan yang tidak sah, atau pemrosesan yang melanggar hak privasi individu. Di banyak negara, hukum perlindungan data bertujuan untuk menjaga keseimbangan antara penggunaan data untuk kepentingan publik dan bisnis serta hak individu atas privasi mereka. Beberapa aspek utama perlindungan data dalam perspektif hukum. Prinsip – prinsip perlindungan data Data pribadi harus diproses dengan cara yang transparan bagi individu yang bersangkutan, Data pribadi hanya boleh diproses untuk tujuan yang sah, dan berdasarkan izin atau kontrak yang jelas, Pengumpulan dan pemrosesan data harus dibatasi pada yang diperlukan untuk tujuan yang sah, Individu memiliki hak untuk mengakses data pribadi mereka dan memperbaikinya jika ada kesalahan. Regulasi perlindungan data **GDPR (General Data Protection Regulation)**: Di Eropa, GDPR adalah salah satu regulasi yang paling komprehensif untuk perlindungan data pribadi. GDPR memberikan hak kepada individu untuk mengontrol data pribadi mereka dan menetapkan kewajiban bagi perusahaan untuk melindungi data tersebut. **UU Perlindungan Data Pribadi (di Indonesia)**: Pada tahun 2020, Indonesia mengesahkan undang-undang perlindungan data pribadi yang mengatur tentang pengumpulan, penggunaan, dan distribusi data pribadi oleh organisasi, baik pemerintah maupun swasta. Niffari, H. (2020).

Hak – hak individu meliputi Individu berhak mengetahui data apa yang dikumpulkan tentang mereka dan untuk apa data itu digunakan, Individu memiliki hak untuk menentang pemrosesan data pribadi mereka dalam beberapa situasi tertentu, alam beberapa keadaan, individu dapat meminta agar data pribadi mereka dihapus, yang sering

disebut sebagai "hak untuk dilupakan". Pengendali data bertanggung jawab untuk memastikan bahwa data pribadi yang dikumpulkan diproses dengan benar dan sesuai dengan hukum yang berlaku. Pemroses data adalah pihak yang melakukan pemrosesan data atas nama pengendali data, dan mereka juga harus mematuhi kewajiban hukum terkait perlindungan data. Pemroses data adalah pihak yang melakukan pemrosesan data atas nama pengendali data, dan mereka juga harus mematuhi kewajiban hukum terkait perlindungan data. Penegakan hukum juga melibatkan pengawasan oleh otoritas perlindungan data yang bertanggung jawab untuk memastikan kepatuhan terhadap undang-undang perlindungan data. Perlindungan dalam perspektif hukum merujuk pada upaya yang dilakukan untuk melindungi hak-hak individu atau entitas, baik yang bersifat material maupun non-material, dari tindakan yang merugikan atau tidak sah. Perlindungan hukum terkait hak asasi manusia bertujuan untuk memastikan bahwa individu dilindungi dari pelanggaran hak dasar mereka, seperti hak atas kehidupan, kebebasan, dan privasi. Negara memiliki kewajiban untuk melindungi, menghormati, dan memenuhi hak-hak ini sesuai dengan konstitusi dan hukum internasional. Perlindungan Hukum terhadap Individu, Mengacu pada perlindungan terhadap hak milik seseorang, baik itu harta benda, tanah, atau properti lainnya, agar tidak dirampas atau disalahgunakan tanpa izin. Perlindungan terhadap data pribadi dan informasi sensitif yang berkaitan dengan individu, yang seringkali diatur dalam undang-undang perlindungan data. Perlindungan terhadap individu atau kelompok yang dapat menjadi sasaran diskriminasi, seperti berdasarkan ras, agama, jenis kelamin, atau orientasi seksual. Perlindungan hukum juga mencakup kelompok-kelompok tertentu dalam masyarakat yang rentan terhadap eksploitasi atau perlakuan tidak adil. Misalnya, perlindungan terhadap hak-hak pekerja, perlindungan terhadap anak-anak, perempuan, atau minoritas. Perlindungan Hukum dalam Konteks Bisnis. Mengatur agar perusahaan tidak terlibat dalam praktik monopoli atau kartel yang merugikan pasar atau konsumen.

Big Data merujuk pada kumpulan data yang sangat besar, kompleks, dan berkembang dengan cepat, yang sulit atau bahkan tidak mungkin dikelola, diproses, dan dianalisis menggunakan alat atau metode tradisional. Big data mengacu pada volume, variasi, dan kecepatan data yang luar biasa tinggi yang berasal dari berbagai sumber. Konsep ini sering dijelaskan menggunakan tiga elemen utama yang dikenal dengan sebutan 3V. **Volume** merujuk pada jumlah data yang sangat besar. Data ini dapat berasal

dari berbagai sumber seperti media sosial, sensor, transaksi online, perangkat IoT (Internet of Things), dan banyak lagi. Seiring berkembangnya teknologi dan digitalisasi, volume data yang dihasilkan setiap hari semakin meningkat pesat. Misalnya, setiap menit ada ribuan terabyte data yang dihasilkan oleh jutaan pengguna internet di seluruh dunia. **Variety** merujuk pada berbagai jenis dan format data yang berbeda. Data tidak hanya berbentuk teks atau angka, tetapi juga dapat berupa gambar, video, suara, data sensor, log, atau data tidak terstruktur lainnya. Data dapat berformat terstruktur (seperti database relasional), semi-terstruktur (seperti XML atau JSON), atau tidak terstruktur (seperti teks bebas atau video). Keberagaman format ini memerlukan teknologi dan metode pemrosesan yang lebih canggih. **Velocity** Merujuk pada kecepatan data yang dihasilkan dan diproses. Big data seringkali datang dalam waktu nyata atau hampir nyata, dan harus diproses dengan cepat untuk menghasilkan wawasan yang berguna. Misalnya, data transaksi di e-commerce yang harus diproses dalam hitungan detik atau data sensor di mobil otonom yang perlu diproses secara langsung untuk pengambilan keputusan instan. Untuk memanfaatkan Big Data, diperlukan alat dan teknologi yang dapat menangani volume, variasi, dan kecepatan data yang luar biasa ini. Beberapa teknologi yang digunakan dalam pengolahan Big Data. Hadoop Platform open-source yang digunakan untuk menyimpan dan memproses data dalam jumlah besar secara terdistribusi, Spark Framework pemrosesan data yang lebih cepat dan lebih efisien dibandingkan Hadoop dalam beberapa kasus. Machine Learning & AI Teknologi yang digunakan untuk menganalisis pola dalam data besar dan membuat prediksi atau rekomendasi berdasarkan data tersebut. Contoh apilikasi big data Bisnis dan E-Commerce, Kesehatan, keungan, transportasi.

Hubungan antara Big Data dan risiko kebocoran data sangat erat, karena semakin besar dan kompleks data yang dikelola, semakin besar pula potensi risiko terhadap keamanan dan privasi data tersebut. Beberapa faktor yang memperburuk risiko kebocoran data terkait dengan penggunaan Big Data. Big Data mencakup jumlah data yang sangat besar, yang biasanya mengandung berbagai informasi sensitif dan pribadi. Ketika data tersebut disimpan dan dikelola dalam skala besar, risiko kebocoran atau akses yang tidak sah menjadi lebih tinggi, terutama jika data tersebut tidak dilindungi dengan baik. Data berasal dari berbagai sumber, seperti transaksi online, media sosial, sensor, dan perangkat IoT. Banyaknya sumber data ini bisa memperbesar kemungkinan kebocoran, karena data

sering kali tersebar di berbagai platform dan sistem yang berbeda, meningkatkan peluang untuk terjadi pelanggaran. Big Data sering kali mencakup data yang tidak terstruktur atau semi-terstruktur (seperti teks, gambar, atau video), yang sulit untuk dikelola dan diamankan dengan sistem tradisional. Data yang tidak terstruktur ini lebih sulit untuk diproses dan dilindungi secara efektif, yang dapat mempermudah kebocoran informasi jika tidak ditangani dengan benar. Untuk mendapatkan wawasan yang lebih baik, banyak organisasi mengintegrasikan data dari berbagai sumber. Proses integrasi data ini bisa mengakibatkan risiko kebocoran jika ada kebocoran pada satu titik integrasi atau jika data tidak terenkripsi dengan baik. Banyak aplikasi Big Data mengandalkan pemrosesan data secara real-time atau hampir real-time, yang meningkatkan risiko kebocoran jika tidak ada kontrol yang ketat terhadap aliran data dan sistem yang memprosesnya. Kecepatan yang tinggi dalam pemrosesan data dapat mengabaikan langkah-langkah keamanan yang lebih menyeluruh, sehingga meningkatkan potensi kebocoran.

Dalam Big Data, sering kali data yang dikumpulkan berisi informasi pribadi pengguna, seperti data kesehatan, informasi keuangan, riwayat transaksi, dan lainnya. Jika data ini jatuh ke tangan yang salah, atau jika data tersebut diakses tanpa izin, kebocoran data yang melibatkan informasi sensitif dapat terjadi, mengakibatkan kerugian bagi individu dan perusahaan. Dengan volume data yang sangat besar dan beragam, pengelolaan akses terhadap data menjadi lebih kompleks. Jika kontrol akses tidak ditangani dengan benar, orang yang tidak berwenang dapat mengakses atau mengubah data. Misalnya, jika ada kesalahan dalam pengaturan hak akses pengguna dalam sistem Big Data, kebocoran data bisa terjadi. Big Data sering menjadi target serangan siber karena nilainya yang tinggi bagi para penyerang. Jika sistem Big Data tidak dilindungi dengan baik, serangan seperti ransomware atau pencurian data bisa terjadi, yang menyebabkan kebocoran data. Priliasari, E. (2019).

Minimnya kesadaran hukum terhadap perlindungan data pribadi adalah isu yang semakin relevan di era digital ini, di mana informasi pribadi sering kali dikumpulkan, diproses, dan disebarkan tanpa sepengetahuan atau persetujuan individu. Kurangnya pemahaman tentang hak-hak terkait data pribadi dan perlindungannya dapat mengakibatkan pelanggaran yang merugikan individu dan masyarakat secara keseluruhan. Berikut adalah beberapa aspek yang terkait dengan minimnya kesadaran hukum mengenai perlindungan data pribadi dan dampaknya. Banyak individu yang

belum memahami apa itu data pribadi, apa yang termasuk dalam kategori data pribadi, dan mengapa data pribadi mereka harus dilindungi. Mereka mungkin tidak tahu bahwa informasi seperti nama, alamat, nomor telepon, alamat email, data biometrik, atau bahkan aktivitas online bisa dianggap sebagai data pribadi yang perlu dilindungi. Masyarakat sering kali tidak menyadari potensi risiko yang muncul jika data pribadi mereka jatuh ke tangan yang salah, seperti pencurian identitas, penipuan, atau penyalahgunaan data untuk tujuan yang merugikan. Banyak orang tidak tahu bahwa mereka memiliki hak tertentu terkait perlindungan data pribadi, seperti hak untuk mengetahui data apa yang dikumpulkan, hak untuk meminta akses, hak untuk mengoreksi data yang salah, hak untuk menghapus data (hak untuk dilupakan), atau hak untuk menentang pemrosesan data tertentu. Walaupun ada peraturan seperti **General Data Protection Regulation (GDPR)** di Eropa atau **UU Perlindungan Data Pribadi (PDP)** di Indonesia, tidak semua orang mengetahui atau memahami apa yang tercantum dalam regulasi ini, dan bagaimana hak-hak tersebut dapat mereka manfaatkan untuk melindungi data pribadi mereka. Banyak individu yang tidak menyadari pentingnya mengamankan data pribadi mereka, misalnya dengan menggunakan kata sandi yang kuat, enkripsi, atau menghindari berbagi informasi pribadi secara sembarangan di platform digital. Misalnya, pengguna media sosial yang secara tidak sadar membagikan data pribadi mereka melalui profil, postingan, atau aplikasi pihak ketiga yang mereka gunakan. Penyuluhan mengenai perlindungan data pribadi masih minim di banyak negara, khususnya di negara berkembang. Banyak orang tidak memiliki kesempatan untuk mempelajari tentang pentingnya menjaga privasi mereka, bagaimana melindungi data pribadi mereka, dan bagaimana cara melaporkan pelanggaran terhadap hak-hak mereka. Banyak aplikasi atau situs web yang tidak memiliki sistem keamanan yang memadai untuk melindungi data pribadi yang mereka kumpulkan, sehingga data bisa terekspos atau bocor. Ketika data pribadi yang dikumpulkan oleh layanan digital jatuh ke tangan yang salah, misalnya akibat serangan siber, individu menjadi korban pencurian data, yang sering kali disebabkan oleh kurangnya kesadaran mereka terhadap pentingnya melindungi data pribadi. Hisbulloh, M. H. (2021).

Harmonisasi dan perbaikan regulasi antara **UU PDP** dan **GDPR** dapat dilakukan dengan cara memperkenalkan ketentuan yang lebih spesifik, transparan, dan mudah diterapkan. Hal ini bertujuan untuk melindungi data pribadi dengan lebih efektif di era

digital, memastikan hak-hak individu dihormati, serta memberikan sanksi yang tegas bagi mereka yang melanggar aturan perlindungan data. Peningkatan kapasitas institusi pengawasan data sangat penting dalam konteks perlindungan data pribadi, mengingat pesatnya perkembangan teknologi dan volume data yang terus meningkat. Lembaga pengawas data harus memiliki kekuatan dan kapabilitas untuk melaksanakan tugas mereka dengan efektif, memastikan bahwa aturan perlindungan data pribadi dipatuhi dan hak-hak individu terlindungi. lembaga pengawasan data perlu mendapatkan pelatihan yang berkelanjutan untuk memahami hukum dan regulasi terkait data pribadi, serta teknologi terbaru yang berkaitan dengan pengolahan data. Mereka juga harus dibekali dengan pengetahuan tentang keamanan siber, privasi digital, serta hak-hak individu. Institusi pengawasan data perlu memiliki alat atau perangkat lunak yang canggih untuk memantau, menganalisis, dan mendeteksi pelanggaran terhadap peraturan perlindungan data pribadi. Teknologi seperti AI (kecerdasan buatan), machine learning, dan blockchain dapat digunakan untuk mendeteksi anomali atau pelanggaran dalam pemrosesan data secara otomatis. Institusi pengawasan data harus lebih proaktif dalam memantau kepatuhan terhadap regulasi perlindungan data pribadi. Ini termasuk melakukan audit rutin pada organisasi atau perusahaan yang mengelola data pribadi dan memastikan bahwa mereka mematuhi peraturan yang ada. Memberikan sanksi yang cukup besar untuk pelanggaran yang terjadi, baik berupa denda finansial, pemblokiran akses data, atau tindakan hukum lainnya. Penegakan yang tegas akan memberikan efek jera kepada pihak yang tidak mematuhi peraturan. Lembaga pengawas data perlu lebih aktif dalam menyelenggarakan program penyuluhan kepada masyarakat mengenai hak-hak mereka terkait data pribadi dan bagaimana cara melindunginya. Penyuluhan ini harus dilakukan melalui berbagai media (offline dan online) dengan bahasa yang mudah dipahami oleh masyarakat umum. Memasukkan edukasi mengenai privasi dan perlindungan data pribadi dalam kurikulum pendidikan dari tingkat dasar hingga perguruan tinggi. Hal ini akan membantu menciptakan kesadaran yang lebih besar tentang pentingnya perlindungan data pribadi di kalangan generasi muda. Fikri, M., & Rusdiana, S. (2023).

KESIMPULAN

Tantangan Hukum dalam Melindungi Data Pribadi di Era Big Data, kepatuhan terhadap regulasi yang terus berkembang seperti, Di banyak negara, peraturan

perlindungan data pribadi sering kali tidak mengikuti perkembangan teknologi atau cenderung lambat dalam merespons dinamika penggunaan Big Data. Banyak negara yang belum memiliki regulasi yang jelas dan komprehensif mengenai pengolahan data dalam skala besar. Terdapat keterbatasan pada penegakan hukum dan banyak terjadi kebocoran data di karenakan perlindungan data yang kurang memadai, dan juga banyak terjadi penggunakan data tanpa persetujuan yang jelas, penyalahgunaan teknologi untuk pengawasan dan untuk melakukan tindak deskriminasi. Untuk menghadapi tantangan hukum dalam perlindungan data pribadi di era Big Data, berikut adalah beberapa solusi hukum yang dapat dipertimbangkan. Regulasi perlindungan data pribadi, seperti **GDPR** di Uni Eropa, harus diadopsi atau disesuaikan di berbagai negara dengan fleksibilitas yang memungkinkan untuk beradaptasi dengan perkembangan teknologi yang sangat cepat. Negara-negara juga perlu membuat peraturan yang mencakup seluruh siklus hidup data pribadi, mulai dari pengumpulan, pemrosesan, penyimpanan, hingga penghapusan. Pemerintah perlu memastikan bahwa regulasi diperbarui secara berkala untuk mencakup perkembangan baru dalam teknologi, seperti AI, blockchain, dan Internet of Things (IoT), yang semakin mempengaruhi pengolahan data pribadi. Djafar, W. (2019).

Dapat dilakukan dengan peningkatan pengawasan dan penegakan hukum melalui penguatan institusi pengawasan data dan penerapan sanksi yang tegas. Transparansi dan harus mendapat persetujuan yang jelas seperti penerapan Privacy by Design (privasi sejak awal), peningkatan edukasi kepada Masyarakat pentingnya perlindungan data pribadi dan juga memperketat keamanan data pribadi. Menghadapi tantangan hukum dalam melindungi data pribadi di era Big Data memerlukan pendekatan Yuniarti, S. (2019). yang komprehensif dan adaptif. Peningkatan regulasi yang lebih baik, penegakan hukum yang lebih tegas, transparansi dalam persetujuan penggunaan data, serta penerapan standar keamanan yang tinggi adalah langkah-langkah yang krusial. Selain itu, pendidikan dan kesadaran publik mengenai hak-hak mereka atas data pribadi juga akan memainkan peran besar dalam menciptakan ekosistem digital yang aman dan terlindungi.

DAFTAR PUSTAKA

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Budianto, H. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024). *Jurnal Kolaboratif Sains*, *8*(1), 506-511.

Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In *Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM* (Vol. 26, pp. 1-14).

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis risiko teknologi informasi pada bank syariah: Identifikasi ancaman dan tantangan terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *5*(2), 87-100.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, *5*(1), 39-57.

Ginanjar, D., & Lubis, A. F. (2022). Urgensi perlindungan data pribadi dalam menjamin keamanan data. *Jurnal Hukum dan HAM Wara Sains*, *1*(01), 21-26.

Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum*, *37*(2), 119-133.

Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, *1*(1), 42-54.

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, *7*(1), 105-119.

Priliasari, E. (2019). Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Majalah Hukum Nasional*, *49*(2), 1-27.

Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, *10*(2), 218-227.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369-384.

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data. *Jurnal Kewarganegaraan*, *6*(1), 976-982.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132-142.

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, *52*(1), 97-106.

Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, *1*(1), 147-154