PERLINDUNGAN HUKUM ATAS DATA PRIBADI DALAM KASUS KEBOCORAN DATA PUSAT DATA NASIONAL SEMENTARA (PDNS) DALAM PERSPEKTIF HUKUM PIDANA

Alza Gabriel
Fakultas Hukum Universitas 17 Agustus 1945 Surabaya, alsagbrl@gmail.com

Abstract
The data breach at the Temporary National Data Centre (PDNS) in Indonesia highlights significant weaknesses in the national data security system and raises concerns about the legal protection of personal data. Millions of personal records, including sensitive information, were leaked, underscoring the need to review and enhance Indonesia's legal framework for data protection. Although Law No. 27 of 2022 on Personal Data Protection (UU PDP) outlines data management and protection, its implementation is challenged by gaps in the current regulations, insufficient technological infrastructure, and inadequate public and institutional awareness about data protection. The PDNS breach demonstrates that personal data protection in Indonesia is still not fully guaranteed. The law's effectiveness is hindered by a lack of socialization and understanding among law enforcement and the general public. Insufficient investment in advanced technology and the lack of expertise in digital forensics and cybersecurity among law enforcement officers exacerbate the problem. Moreover, stronger collaboration among national and international institutions is essential to address complex and cross-border cyber threats. Enhanced cooperation between the government, private sector, and international organizations is crucial to improve the enforcement of criminal law and effectively protect personal data.
Keywords: *data protection, data breach, personal data, cybersecurity, law enforcement, personal data protection law.*

Abstrak
Pelanggaran data di Pusat Data Nasional Sementara (PDNS) di Indonesia menyoroti kelemahan signifikan dalam sistem keamanan data nasional dan menimbulkan kekhawatiran tentang perlindungan hukum terhadap data pribadi. Jutaan catatan pribadi, termasuk informasi sensitif, bocor, menekankan perlunya meninjau dan meningkatkan kerangka hukum Indonesia untuk perlindungan data. Meskipun Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur pengelolaan dan perlindungan data, implementasinya menghadapi tantangan berupa celah dalam regulasi saat ini, infrastruktur teknologi yang tidak memadai, dan kurangnya kesadaran publik serta institusi tentang perlindungan data. Pelanggaran PDNS menunjukkan bahwa perlindungan data pribadi di Indonesia masih belum sepenuhnya terjamin. Efektivitas undang-undang ini terhambat oleh kurangnya sosialisasi dan pemahaman di kalangan penegak hukum dan masyarakat umum. Investasi yang tidak mencukupi dalam teknologi canggih dan kurangnya keahlian dalam forensik digital dan keamanan siber di antara petugas penegak hukum memperburuk masalah ini. Selain itu, kolaborasi yang lebih kuat antara lembaga nasional dan internasional sangat penting untuk menangani ancaman siber yang kompleks dan lintas batas. Kerjasama yang ditingkatkan antara pemerintah, sektor swasta, dan organisasi internasional sangat penting untuk memperbaiki penegakan hukum pidana dan melindungi data pribadi secara efektif.
Kata Kunci: perlindungan data, kebocoran data, data pribadi, keamanan siber, Undang-Undang Perlindungan Data Pribadi.

Pendahuluan

Di era digital, data pribadi adalah aset berharga yang rentan terhadap ancaman. Teknologi informasi yang berkembang mengubah cara data dikumpulkan, disimpan, dan diproses, termasuk informasi sensitif seperti nama, alamat, dan data keuangan[1]. Perlindungan data pribadi penting karena mencerminkan identitas seseorang yang perlu dijaga kerahasiaannya, dan diakui sebagai

hak fundamental oleh hukum internasional dan nasional. Kebocoran data di Pusat Data Nasional Sementara (PDNS) mengungkap kelemahan keamanan data nasional dan menimbulkan keprihatinan tentang perlindungan hukum di Indonesia. Kebocoran ini melibatkan jutaan data pribadi yang dapat digunakan untuk tujuan kriminal, menunjukkan perlunya peningkatan sistem hukum perlindungan data. Hukum pidana Indonesia, termasuk UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, mengatur pengelolaan dan perlindungan data, tetapi pelaksanaannya masih menghadapi tantangan.

Pada Juli 2024, kebocoran data besar-besaran yang melibatkan informasi pribadi milik Kominfo. Data tersebut diposting dan dijual di situs "Breach Forums" oleh akun bernama "aptikakominfo"[2]. Informasi yang bocor mencakup Nama, Nomor Induk Kependudukan (NIK), Rekening Bank, NPWP, dan Nomor Rekening, serta data pribadi lainnya. Data ini dijual dengan harga USD 121,000, menimbulkan kekhawatiran serius terkait privasi dan keamanan bagi para individu yang informasinya terungkap. Insiden ini menyoroti kebutuhan mendesak akan peningkatan keamanan siber dan perlindungan data di Indonesia.

Kesadaran masyarakat dan lembaga tentang pentingnya perlindungan data masih rendah, dengan dampak kebocoran yang merugikan, seperti kerugian finansial dan pencurian identitas. Penelitian ini bertujuan mengkaji kerangka hukum di Indonesia terkait perlindungan data pribadi dalam perspektif hukum pidana, termasuk analisis kasus kebocoran data PDNS dan efektivitas hukum dalam melindungi data pribadi. Regulasi internasional seperti GDPR di Uni Eropa memberikan perlindungan komprehensif, dan Indonesia dapat belajar dari pengalaman negara lain[3]. Diharapkan rekomendasi dari penelitian ini dapat memperkuat perlindungan data pribadi di Indonesia melalui peraturan yang lebih ketat, penegakan hukum yang efektif, dan peningkatan kesadaran masyarakat.

Metode Penelitian

Dalam penelitian ini, jenis dan format penelitian diklasifikasikan bergantung pada pedoman klasifikasi yang dijadikan acuan. Metode penelitian yang dilakukan adalah penelitian hukum preskriptif atau biasa dikenal dengan penelitian hukum kepustakaan yang bertujuan untuk menyelidiki bahan pustaka yang ada dengan fokus pada norma hukum yang berlaku. Penelitian ini menggunakan metode yang meliputi metode kasus, metode undang-undang, dan metode konsepsual dengan mempertimbangkan ketentuan hukum terkait. Penulis juga menggunakan penelitian dan hasil empiris dari bidang hukum dan bidang keilmuan lainnya sebagai bahan analisis dalam konteks ilmu normatif. Peneliti menggunakan informasi yang berasal dari artikel, jurnal ilmiah, penelitian terdahulu, dan sumber-sumber yang diperoleh dari internet untuk melengkapi penulisan penelitian ini.

Hasil dan Pembahasan

1. Pusat Data Nasional (PDN), Pusat Data Nasional Sementara (PDNS), Telkom Sigma dan Kasus Kebocoran Data

Pusat Data Nasional (PDN) adalah inisiatif yang dilakukan oleh Kementerian Komunikasi dan Informatika (Kominfo) Indonesia untuk mengintegrasikan dan mengelola data dari berbagai instansi pemerintah secara terpusat. Tujuan utama dari pembangunan PDN adalah untuk meningkatkan efisiensi, keamanan, dan interoperabilitas data pemerintah, serta mendukung implementasi kebijakan berbasis data. Langkah ini sejalan dengan transformasi digital yang sedang digalakkan oleh pemerintah Indonesia untuk memajukan pelayanan publik dan pengambilan keputusan berbasis data[4].

Sebelum adanya PDN, data pemerintah tersebar di berbagai instansi dengan sistem yang berbeda-beda, yang menyebabkan kesulitan dalam integrasi dan analisis data. Fragmentasi data ini menghambat efisiensi operasional dan pengambilan keputusan yang cepat dan akurat. Dengan latar belakang tersebut, Kementerian Kominfo berinisiatif membangun PDN untuk menyatukan dan mengelola data pemerintah secara lebih efektif.

PDN terdiri dari beberapa komponen utama, termasuk pusat data fisik, platform pengelolaan data, dan sistem keamanan siber yang canggih. Pusat data fisik dibangun dengan standar internasional untuk memastikan keandalan dan keamanan data. Platform pengelolaan data memungkinkan integrasi dan analisis data dari berbagai sumber, sedangkan sistem keamanan siber dirancang untuk melindungi data dari ancaman eksternal dan internal.

Keamanan data adalah salah satu fokus utama dalam pembangunan PDN. Menurut Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, pemerintah harus memastikan bahwa data pribadi yang disimpan dalam PDN dilindungi dengan prosedur keamanan yang ketat. Termasuk dengan penggunaan enkripsi, autentikasi multi-faktor, dan pemantauan aktivitas jaringan secara terus-menerus untuk mendeteksi dan mencegah ancaman siber.

PDN memberikan berbagai manfaat bagi pemerintah Indonesia, termasuk peningkatan efisiensi operasional, pengurangan biaya, dan peningkatan akurasi data. Dengan adanya PDN, data dari berbagai instansi pemerintah dapat diintegrasikan dan dianalisis dengan lebih cepat, yang mendukung pengambilan keputusan yang lebih cepat dan lebih baik. Selain itu, PDN juga membantu dalam mengurangi redundansi data dan mengoptimalkan penggunaan sumber daya.

Sekalipun mempunyai banyak manfaat, pembangunan PDN juga mempunyai berbagai tantangannya sendiri. Salah satu tantangan utama adalah memastikan interoperabilitas antara sistem yang berbeda dari berbagai instansi pemerintah. Selain itu, memastikan keamanan data dari ancaman siber yang semakin canggih juga menjadi tantangan yang signifikan. Pemerintah harus terus berinvestasi dalam teknologi keamanan terbaru dan melatih personel untuk mengelola dan melindungi data[5].

Sebagai studi kasus, Estonia telah berhasil membangun sistem data nasional yang terintegrasi melalui e-Estonia. Sistem ini memungkinkan berbagai instansi pemerintah untuk berbagi data secara efisien dan aman. Indonesia dapat belajar dari pengalaman Estonia dalam hal standar keamanan, interoperabilitas, dan penggunaan teknologi digital untuk meningkatkan pelayanan publik.

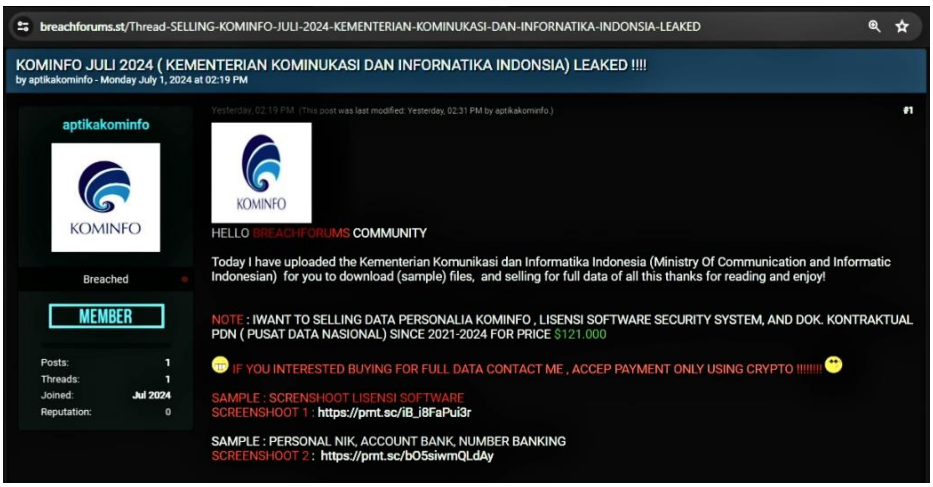
PDN memiliki potensi besar untuk mendukung kebijakan publik yang lebih efektif dan berbasis data. Dengan data yang terintegrasi dan akurat, pemerintah dapat merumuskan kebijakan yang lebih sesuai dan tepat sasaran terhadap kebutuhan masyarakat. Selain itu, PDN juga dapat meningkatkan transparansi dan akuntabilitas dalam pengelolaan data pemerintah, yang pada gilirannya dapat meningkatkan kepercayaan publik.

Empat pusat data Tier-4 global akan dibangun oleh Kementerian Komunikasi dan Informatika RI di seluruh Indonesia. Kawasan Industri Deltamas di Cikarang Pusat, Kabupaten Bekasi, Jawa Barat, akan menjadi lokasi pembangunan PDN pertama. Kawasan ini dipilih karena di sana pusat pemerintahan saat ini berada. Nongsa Digital Park yang berlokasi di Kota Batam, Kepulauan Riau dipilih untuk pembangunan PDN yang kedua dikarenakan wilayah tempat tersebut terdapat infrastruktur berbentuk jaringan serat optik yang dapat menyambungkan bagian Batam dengan daerah barat Indonesia. Untuk mendukung pusat pemerintahan baru IKN di Balikpapan, Kalimantan Timur, akan dibangun PDN ketiga. Selain itu, PDN yang keempat direncanakan akan dibangun di Labuan Bajo, Kabupaten Manggarai Barat, Provinsi Nusa Tenggara Timur, yang akan menyambungkan wilayah timur dan barat Indonesia.

Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Infornatika pada tanggal 12 Juni tahun 2023 menargetkan PDN yang terdapat di Bekasi dipastikan akan selesai dan dapat diresmikan pada bulan oktober tahun 2024, sedangkan PDN yang berada di Batam diharapkan akan selesai pada tahun 2025. Lebih lanjut, PDN yang berada di Manggarai Barat dan di Balikpapan sedang dalam tahap perencanaan, sedangkan PDN Batam dalam proses tender. Sementara ini Pembangunan Pusat Data Nasional belum selesai pembangunannya dan data nasional masih tersimpan pada program Pusat Data Nasional Sementara (PDNS).

Pusat Data Nasional Sementara (PDNS) dikelola oleh PT Sigma Cipta Caraka (Telkom Sigma) perusahaan ini adalah anak usaha dari Telkom Indonesia yang berkantor di Jakarta, Sentul,

Serpong, Bali, dan Surabaya dan bergerak di bidang teknologi informasi. Sejak tanggal 20 Juni 2024 Pusat Data Nasional (PDN) yang dioperasikan oleh Kementerian Komunikasi menghadapi gangguan. Gangguan itu menyebabkan beberapa layanan digital pemerintahan lumpuh diantaranya layanan Penerimaan Peserta Didik Baru (PPDB) milik Kementrian Pendidikan di beberapa daerah mengalami gangguan, sehingga pemerintah daerah memperpanjang waktu pendaftaran lalu Direktorat Jenderal Imigrasi Kementerian Hukum dan Hak Asasi Manusia. Hal ini merupakan dampak penyerangan siber yang terjadi di Pusat Data Nasional Sementara (PDNS) Surabaya yang dikelola oleh PT Sigma Cipta Caraka.



Gambar 1: Kebocoran data PDN milik Kominfo yang di jual di situs "Breach Forums"

Pelaku peretas Pusat Data Nasional (PDN) menggunakan virus yang sama pada peretasan yang terjadi di Bank Syariah Indonesia pada bulan mei 2023 dengan menggunakan jenis varian yang sama yang disebut ransomware LockBit 3.0. Pelaku menuntut uang sebesar 8 juta USD kepada pemerintahan indonesia apabila ingin 210 data yang diretas untuk dikembalikan.

2. Penerapan Hukum Pidana di Indonesia Dalam Memberikan Perlindungan Terhadap Data Pribadi Dalam Kasus Kebocoran Data dari Pusat Data Nasional Sementara (PDNS)

Pada tanggal 20 Juni 2024, terdapat kasus kebocoran data yang signifikan akibat serangan ransomware LockBit 3.0 yang dihadapi oleh Pusat Data Nasional Sementara (PDNS), pelaku meminta tebusan sebesar 8 juta USD untuk memulihkan akses data yang dienkripsi. Kasus ini menyoroti pentingnya penerapan hukum pidana dalam melindungi data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan landasan aturan utama yang mengurus perlindungan data pribadi di Indonesia. Undang-undang ini menentukan prinsip-prinsip dasar seperti kerahasiaan dalam pengelolaan data pribadi, transparansi, integritas, dan akuntabilitas. UU PDP juga mengatur kewajiban pengelola data untuk menjaga data pribadi dari jalan akses yang tidak legal dan kebocoran. UU PDP menetapkan sanksi pidana bagi pelanggaran perlindungan data pribadi, termasuk denda dan penjara. Penegakan hukum yang efektif merupakan hal penting untuk memberikan efek jera kepada pelaku kejahatan siber. Sanksi yang tegas juga menunjukkan komitmen pemerintah dalam melindungi data pribadi warganya[6].

Kasus kebocoran data di PDNS akibat serangan ransomware LockBit 3.0 menegaskan urgensi penerapan hukum pidana yang ketat dalam memberikan perlindungan terhadap data pribadi. Serangan ini tidak hanya menimbulkan kerugian finansial yang besar, tetapi juga membahayakan privasi individu yang datanya dikelola oleh PDNS. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) berfungsi sebagai alat hukum utama untuk menangani kasus pelanggaran semacam ini. UU PDP mengatur bahwa pengelola data harus memastikan data pribadi terlindungi dari akses yang tidak sah, termasuk melalui penerapan

langkah-langkah keamanan yang memadai. Dalam kasus PDNS, kegagalan dalam menjaga keamanan data ini merupakan pelanggaran langsung terhadap ketentuan UU PDP, yang dapat dikenakan sanksi pidana yang berat.

Dalam kasus PDNS, penerapan sanksi pidana yang ketat terhadap pelaku serangan ransomware tidak hanya penting untuk menegakkan hukum, tetapi juga untuk menunjukkan bahwa pemerintah tidak akan mentolerir pelanggaran terhadap keamanan data[7]. UU PDP juga mencakup kewajiban pengelola data untuk melaporkan setiap insiden kebocoran data kepada otoritas yang berwenang dan individu yang terdampak. Dalam kasus PDNS, pelaporan yang cepat dan transparan tentang kebocoran data ini akan memungkinkan individu yang terkena dampak untuk mengambil tindakan pencegahan, seperti memantau akun mereka untuk aktivitas yang mencurigakan dan mengambil langkah-langkah untuk melindungi identitas mereka. Selain itu, UU PDP juga mengharuskan pengelola data untuk menyediakan layanan pemulihan identitas bagi korban kebocoran data. Layanan ini dapat mencakup pemantauan kredit, asuransi pencurian identitas, dan bantuan dalam pemulihan identitas yang dicuri. Penyediaan layanan semacam ini penting untuk membantu korban mengatasi dampak dari kebocoran data dan meminimalkan kerugian yang mereka alami. Menurut Solove dan Schwartz, langkah-langkah pemulihan ini tidak hanya membantu korban dalam jangka pendek tetapi juga membangun kepercayaan publik terhadap kemampuan pemerintah dalam menangani insiden kebocoran data[8].

Secara keseluruhan, penerapan hukum pidana yang ketat dan efektif berdasarkan UU PDP merupakan langkah penting untuk melindungi data pribadi di indonesia. Kasus kebocoran data di PDNS menyoroti perlunya penegakan hukum yang kuat, transparansi dalam pelaporan insiden, dan upaya berkelanjutan untuk meningkatkan keamanan siber. Menurut Acquisti, Friedman, dan Telang, penerapan hukum yang tegas terhadap pelaku kejahatan siber dapat memberikan efek jera dan mencegah insiden serupa di masa depan.

Akses ilegal yang masuk ke dalam sistem elektronik diatur dalam Pasal 30 UU ITE, menurut pasal ini setiap orang yang secara sadar dan sengaja melanggar hukum mengakses sistem elektronik dan/atau komputer milik orang lain dengan cara apa pun dapat dijatuhi sanksi pidana. Akses ilegal ini mencakup tindakan yang bertujuan untuk mendapatkan informasi, data, atau keuntungan lainnya secara tidak sah. Pelaku ransomware yang mengakses sistem elektronik tanpa izin, termasuk untuk mengunci atau mengenkripsi data, jelas melanggar ketentuan ini.

Lebih lanjut, Pasal 32 UU ITE mengatur tentang pengubahan, penghilangan, atau pemindahan informasi elektronik tanpa izin. Pasal ini menetapkan bahwa setiap orang yang dengan sadar dan sengaja dan tanpa hak atau melakukan perbuatan pelanggaran hukum seperti pengubahan, penghilangan, atau pemindahan informasi elektronik milik orang lain, baik seluruhnya maupun sebagian, dapat dikenakan sanksi pidana. Pelaku ransomware yang mengenkripsi data tanpa izin, sehingga mengubah status aksesibilitas data tersebut, dapat dijerat dengan ketentuan ini.

Dalam kasus kebocoran data di Pusat Data Nasional Sementara (PDNS) di mana pelaku menggunakan ransomware, UU ITE dapat digunakan untuk menuntut pelaku dengan tuduhan akses ilegal dan pengubahan informasi elektronik tanpa izin. Tindakan pelaku yang mengakses sistem PDNS dan mengenkripsi data pribadi warga negara merupakan pelanggaran yang jelas terhadap ketentuan UU ITE.

Penegakan hukum yang efektif berdasarkan UU ITE melibatkan berbagai tahap, mulai dari investigasi forensik digital untuk mengidentifikasi dan mengumpulkan bukti kejahatan, hingga penuntutan dan pengadilan pelaku. Investigasi forensik digital sangat penting dalam mengumpulkan bukti elektronik yang sah dan dapat diterima di pengadilan. Bukti ini mencakup *log* akses, jejak *digital*, dan data enkripsi yang digunakan oleh pelaku. Penegak hukum harus bekerja sama dengan pakar forensik digital untuk memastikan bahwa bukti yang dikumpulkan dapat mengidentifikasi pelaku dan mendukung penuntutan yang efektif.

Setelah bukti terkumpul, penuntutan dilakukan berdasarkan pasal-pasal UU ITE yang relevan. Sanksi yang ditetapkan oleh UU ITE meliputi hukuman penjara dan, yang bermaksud bertujuan untuk memberikan efek jera pada pelaku kejahatan siber dan mencegah terjadinya insiden serupa di masa depan.

Secara internasional, perlindungan data pribadi diakui sebagai komponen dari hak asasi manusia. Maka dari itu sebagai salah satu aspek hukum yang penting di seluruh dunia maka perlindungan data pribadi harus dijunjung tinggi. Berdasarkan Deklarasi Universal Hak Asasi Manusia, setiap individu memiliki hak atas privasinya sendiri dan perlindungan terhadap intervensi tangan yang tidak sah. Pasal 12 Deklarasi UN General Assembly Tahun 1948 ini menyatakan, "Tidak seorang pun boleh diganggu kehidupan pribadinya baik dalam urusan keluarga, rumah tangga maupun korespondensi, ataupun dihina nama baiknya dan kehormatannya. Setiap individu mempunyai hak untuk dilindungi secara hukum terhadap gangguan atau penghinaan seperti itu". Pengakuan ini menunjukkan pentingnya privasi sebagai dasar untuk melindungi kebebasan individu dari intervensi yang tidak sah.

Berbagai kebijakan nasional dan internasional mengakui perlindungan data pribadi sebagai komponen dari hak asasi manusia. Di Uni Eropa misalnya, General Data Protection Regulation (GDPR) atau yang disebut Peraturan Perlindungan Data Umum secara ketat mengontrol perlindungan data pribadi dan menekankan bahwa privasi data adalah hak dasar yang harus dihormati oleh negara dan bisnis. GDPR berisi konsep-konsep seperti transparansi, legalitas, dan akuntabilitas dalam penanganan data pribadi, serta hak-hak yang luas bagi individu untuk mengontrol data mereka.[9].

Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mencerminkan komitmen untuk melindungi hak asasi manusia dalam konteks digital. UU PDP menegaskan bahwa perlindungan data pribadi juga merupakan komponen dari hak asasi manusia dan menetapkan kewajiban bagi pengelola data untuk menjaga keamanan dan kerahasiaan data pribadi. UU tersebut juga memberikan hak-hak kepada individu, seperti hak untuk mengakses, memperbaiki, menghapus, dan membatasi pemrosesan data pribadi mereka.

Keamanan siber adalah salah satu faktor penting yang menentukan keamanan data pribadi. Hal ini mencakup langkah-langkah teknis dan organisasi untuk melindungi sistem informasi dan data dari ancaman. Menurut Solove dan Schwartz, keamanan siber yang efektif melibatkan penggunaan enkripsi, firewall, dan sistem deteksi intrusi untuk mencegah akses yang tidak sah dan kebocoran data[10]. Mereka menekankan bahwa teknologi keamanan canggih harus digunakan untuk menjaga integritas dan kerahasiaan data. Dalam konteks ini, UU PDP mengharuskan pengelola data untuk mengikuti tahapan-tahapan keamanan yang sesuai untuk melindungi informasi data pribadi.

Keamanan siber bukan hanya tentang teknologi, tetapi juga tentang proses dan kebijakan yang mendukung penggunaan teknologi tersebut. Menurut sebuah studi oleh Cate, keamanan siber yang komprehensif memerlukan pendekatan holistik yang mencakup teknologi, proses, dan manusia untuk mengurangi risiko kebocoran data dan serangan siber[11].

Pengelola data memiliki tanggung jawab untuk melindungi data pribadi yang mereka kelola. Ini termasuk memastikan bahwa sistem keamanan yang digunakan cukup kuat untuk mencegah kebocoran data dan merespons insiden dengan cepat dan efektif[12]. UU PDP menetapkan bahwa pengelola data harus melaporkan kebocoran data kepada otoritas yang berwenang dan individu yang terdampak. Pelaporan ini penting untuk memberikan transparansi dan memungkinkan individu untuk mengambil langkah-langkah perlindungan diri.

Tanggung jawab pengelola data juga mencakup penerapan kebijakan perlindungan data yang ketat dan pelatihan karyawan secara berkala untuk memastikan bahwa semua pihak memahami pentingnya menjaga keamanan data pribadi.

Hukuman pidana dapat menjadi salah satu alat untuk mengurangi dan mencegah terjadinya kebocoran data di masa depan. Menurut Acquisti, Friedman, dan Telang, penerapan hukuman yang

tegas terhadap pelaku kejahatan siber, termasuk ransomware, dapat memberikan efek jera dan mengurangi insiden serupa[13]. Mereka berpendapat bahwa sanksi yang berat tidak hanya menghukum pelaku tetapi juga mengirimkan pesan yang jelas bahwa pelanggaran terhadap keamanan data tidak akan ditoleransi.

UU PDP memberikan sanksi pidana yang signifikan untuk pelanggaran perlindungan data pribadi, ini termasuk denda yang besar dan hukuman penjara bagi individu atau entitas yang terbukti bersalah atas kebocoran data pribadi. Sanksi ini dirancang untuk memastikan bahwa pengelola data serius dalam melindungi data pribadi yang mereka kelola.

Pendekatan konseptual terhadap perlindungan data pribadi mencakup pengakuan hak atas privasi sebagai hak asasi manusia, penerapan langkah-langkah keamanan siber yang komprehensif, tanggung jawab pengelola data untuk melindungi data pribadi, dan penggunaan hukuman pidana sebagai alat pencegahan[14]. UU PDP Indonesia mengadopsi prinsip-prinsip ini untuk memastikan bahwa data pribadi dilindungi dengan baik dan bahwa pelanggaran terhadap privasi tidak dibiarkan begitu saja. Penerapan konsep-konsep ini dalam praktik sehari-hari membutuhkan komitmen dari semua pihak yang terlibat, termasuk pemerintah, perusahaan, dan individu. Dengan kerangka kerja hukum yang kuat dan penegakan hukum yang efektif, Indonesia dapat membangun sistem perlindungan data pribadi yang tangguh dan dapat dipercaya.

Penyebab utama kebocoran data di PDNS adalah kegagalan dalam menerapkan langkah-langkah keamanan yang memadai. LockBit 3.0 adalah jenis ransomware yang dikenal karena kemampuannya untuk mengenkripsi data dengan cepat dan efektif, serta sulit untuk dipecahkan tanpa kunci dekripsi yang tepat. Sistem keamanan PDNS ternyata tidak mampu mendeteksi dan mencegah serangan ini pada waktunya. Ini menunjukkan bahwa infrastruktur keamanan siber yang ada di PDNS belum memadai untuk menghadapi ancaman siber yang semakin kompleks. Kelemahan dalam sistem keamanan ini bisa jadi disebabkan oleh kurangnya investasi dalam teknologi keamanan terbaru, kurangnya pelatihan bagi staf keamanan, atau kegagalan dalam menerapkan prosedur keamanan yang ketat.

Setelah kebocoran data terdeteksi, pemerintah Indonesia telah segera mengambil langkah-langkah untuk mengatasi situasi tersebut. Langkah-langkah ini termasuk meningkatkan infrastruktur keamanan siber, melakukan audit keamanan menyeluruh, dan bekerja sama dengan pakar keamanan siber untuk mengembalikan akses data tanpa membayar tebusan[15].

Selain langkah-langkah teknis, pemerintah juga wajib memberikan menyediakan layanan pemulihan identitas bagi individu yang terdampak. Layanan ini meliputi pemantauan kredit, asuransi pencurian identitas, dan bantuan dalam pemulihan identitas yang dicuri. Penyediaan layanan semacam ini penting untuk membantu korban mengatasi dampak dari kebocoran data dan meminimalkan kerugian yang mereka alami.

Selain menyediakan layanan pemulihan identitas, pemerintah juga wajib bertanggung jawab untuk memberikan kompensasi dan dukungan kepada korban kebocoran data. Kompensasi ini dapat berupa layanan gratis yang membantu korban memantau dan melindungi informasi pribadi mereka. Pemerintah juga harus memastikan bahwa individu yang datanya terkena dampak diberitahukan tentang insiden tersebut dan tindakan apa yang diambil untuk melindungi data mereka di masa depan.

Penegakan hukum yang efektif juga merupakan komponen penting dalam menangani kebocoran data seperti yang dialami PDNS. UU PDP menetapkan berbagai sanksi pidana bagi pelanggaran perlindungan data pribadi, termasuk denda yang signifikan dan hukuman penjara. Dalam kasus PDNS, penerapan sanksi pidana yang ketat terhadap pelaku serangan ransomware tidak hanya penting untuk menegakkan hukum, tetapi juga untuk menunjukkan bahwa pemerintah tidak akan mentolerir pelanggaran terhadap keamanan data.

Secara keseluruhan, insiden kebocoran data di PDNS menunjukkan perlunya peningkatan infrastruktur keamanan siber, edukasi dan pelatihan bagi pegawai pemerintah, serta penegakan hukum yang tegas. Penegakan hukum yang efektif diperlukan untuk memastikan bahwa pelanggar

regulasi perlindungan data menerima sanksi yang sesuai. Regulasi seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan berbagai sanksi pidana bagi pelanggaran, termasuk denda dan hukuman penjara, yang dirancang untuk memberikan efek jera dan memastikan kepatuhan terhadap standar keamanan data. Pemerintah harus memastikan bahwa otoritas perlindungan data mempunyai sumber daya yang memadahi untuk mengoperasikan tugasnya secara efektif, termasuk tenaga kerja yang terlatih dan teknologi yang memadai[16].

Selain itu, mekanisme penegakan yang kuat sangat penting termasuk kemampuan untuk melakukan investigasi yang mendalam dan cepat terhadap insiden kebocoran data serta penuntutan yang efektif terhadap pelaku. Pemerintah juga harus bertanggung jawab atas segala hal yang menyebabkan kebocoran data terjadi.[17] Ini mencakup kewajiban untuk melaporkan insiden kebocoran data kepada publik dengan segera dan transparan, serta menginformasikan tindakan-tindakan apa yang diambil untuk mengatasi masalah tersebut dan mencegah apabila terjadi insiden yang sama di masa depan. Transparansi dalam pelaporan insiden kebocoran data memungkinkan individu yang terdampak untuk mengambil tindakan perlindungan yang diperlukan, seperti memantau akun mereka untuk aktivitas yang mencurigakan dan memperkuat keamanan informasi pribadi mereka[18].

Kebocoran data pribadi merupakan masalah serius yang memerlukan atensi khusus dari pemerintah dan organisasi[11]. UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan kerangka hukum yang kuat untuk melindungi data pribadi di Indonesia. Namun, implementasi efektif dari perlindungan data pribadi memerlukan upaya bersama dari pemerintah, perusahaan, dan masyarakat. Edukasi, kebijakan privasi yang transparan, dan penegakan hukum yang tegas adalah kunci untuk menghadapi tantangan perlindungan data pribadi di masa depan[19]. Kasus kebocoran data PDNS pada 20 Juni 2024 menunjukkan perlunya peningkatan keamanan siber, edukasi, dan kerjasama internasional untuk melindungi data pribadi dengan lebih baik.

Kesimpulan

Penerapan hukum pidana di Indonesia dalam memberikan perlindungan terhadap data pribadi dalam kasus kebocoran data dari Pusat Data Nasional Sementara (PDNS) masih memerlukan banyak perbaikan. Undang-Undang Perlindungan Data Pribadi (UU PDP) yang telah disahkan merupakan langkah penting dalam upaya melindungi data pribadi warga negara. Namun, efektivitas penerapannya masih terbatas oleh kurangnya sosialisasi dan pemahaman di kalangan penegak hukum dan masyarakat luas. Tanpa pemahaman yang menyeluruh, UU PDP tidak dapat diimplementasikan dengan optimal.

Kendala utama yang dihadapi dalam penegakan hukum pidana terkait kebocoran data pribadi di PDNS mencakup kurangnya infrastruktur teknologi dan sumber daya manusia yang memadai. Sistem keamanan yang ketinggalan zaman dan minimnya investasi dalam teknologi canggih membuat PDNS rentan terhadap serangan siber. Selain itu, banyak penegak hukum yang belum memiliki keahlian khusus dalam bidang forensik digital dan keamanan siber, sehingga sulit untuk menangani kasus kebocoran data secara efektif.

Selain masalah teknologi dan sumber daya manusia, kolaborasi antar lembaga, dalam tingkat nasional maupun internasional, masih perlu ditingkatkan. Kerjasama yang kuat antara pemerintah, sektor swasta, dan lembaga internasional sangat penting untuk mengatasi ancaman siber yang semakin kompleks dan lintas batas. Tanpa koordinasi yang baik, upaya penegakan hukum pidana akan tetap menghadapi berbagai hambatan.

Ucapan Terima Kasih

Dengan penuh rasa syukur dan hormat, penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas 17 Agustus 1945 Surabaya atas segala ilmu, dukungan dan fasilitas yang diberikan selama penelitian ini berlangsung. Kami juga menghaturkan penghargaan setinggi-tingginya kepada para peneliti terdahulu yang telah memberikan landasan yang kokoh bagi studi

penulis. Terima kasih yang tulus penulis sampaikan kepada seluruh pemberi data dan informan atas kerjasama dan kontribusinya yang sangat berharga, yang tanpa bantuan mereka, penelitian ini tidak akan dapat terselesaikan dengan baik.

Daftar Pustaka

[1] O. Tene and J. Polonetsky, "Privacy in the age of big data: A time for big decisions," *Stanford Law Rev. Online*, vol. 64, pp. 63–69, 2012.
[2] Breach Forums, "KOMINFO JULI 2024 (KEMENTRIAN KOMUNIKASI DAN INFORMATIKA INDONESIA) LEAKED!," 2024. https://breachforums.st/Thread-KOMINFO-JULI-2024-KEMENTERIAN-KOMINUKASI-DAN-INFORNATIKA-INDONSIA-LEAKED (accessed Jul. 01, 2024).
[3] B. Santoso, "Perlindungan Data Pribadi di Indonesia: Pembelajaran dari GDPR," 2023.
[4] Kominfo, "Pusat Data Nasional: Inisiatif untuk Integrasi Data Pemerintah," *Siaran Pers Kominfo*.
[5] L. Floridi, "Open data, data protection, and group privacy," *Philos. Technol.*, vol. 27, no. 1, pp. 1–3, 2014.
[6] R. La Porta, "Investor Protection and Cororate Governance," *J. financ. econ.*, no. 58, p. 9, 1999.
[7] N. Purtova, "The law of everything. Broad concept of personal data and future of EU data protection law.," *Law, Innov. Technol.*, vol. 10, no. 1, pp. 40–81, 2018.
[8] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *New York Univ. Law Rev.*, vol. 86, pp. 1814–1894, 2011.
[9] General Data Protection Regulation, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," *Off. J. Eur. Union*, 2016.
[10] D. J. Solove and P. M. Schwartz, "Information Privacy Law," *Wolters Kluwer*, 2020.
[11] F. H. Cate, "The failure of fair information practice principles," *Consum. Prot. Age Inf. Econ.*, pp. 341–378, 2006.
[12] S. Zuboff, "Big other: Surveillance capitalism and the prospects of an information civilization," *J. Inf. Technol.*, vol. 30, no. 1, pp. 75–89, 2015.
[13] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? An event study," *Am. Law Rev.*, 2016.
[14] A. F. Westin, "Privacy and Freedom," *Atheneum*, 1967.
[15] Kominfo, "Insiden Kebocoran Data di PDNS," *Siaran Pers Kominfo*.
[16] A. Rouvroy and Y. Poullet, "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy," *Reinventing Data Prot.*, vol. 45, pp. 194–212, 2009.
[17] L. Lessig, "Code and Other Laws of Cyberspace," *Basic Books*, 1999.
[18] D. Hardianto. and Q. Nurul., "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta*, vol. 13, no. 1, 2018.
[19] S. Ahmed, "Cybersecurity and Data Protection Law Review: Challenges in Developing Countries," 2021.