Jurnal Retentum
Volume: 07, Number: 01, 2025, Page : 48-64
https://jurnal.darmaagung.ac.id/index.php/retentum

p-ISSN 2686-5432
e-ISSN 2686-5440

Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital

Annisa Erikha[1], Zainal Arifin Hoesein[2]

[1,2]Universitas Borobudur
Email: formallyerikha@gmail.com[1*], zainal.arifin@umj.ac.id[2]

History:
Received : 05 Januari 2025
Revised : 10 Januari 2025
Accepted : 14 Januari 2025
Published: 15 Januari 2025

Publisher: Pascasarjana UDA

Abstrak

Perlindungan data pribadi di Indonesia menghadapi berbagai tantangan di era digital yang berkembang pesat. Kebocoran data pribadi menjadi masalah serius yang memerlukan perhatian dari semua pihak, termasuk pemerintah, sektor swasta, dan masyarakat. Upaya perlindungan data pribadi harus dilakukan melalui kolaborasi yang erat antara berbagai sektor, dengan memperkuat kebijakan dan regulasi yang ada, meningkatkan kesadaran masyarakat, serta memperkuat infrastruktur dan teknologi keamanan siber. Pemerintah Indonesia telah mengeluarkan Undang-Undang Perlindungan Data Pribadi sebagai langkah awal, namun implementasi yang konsisten dan koordinasi yang lebih baik masih menjadi tantangan. Selain itu, perlu adanya edukasi kepada masyarakat untuk meningkatkan literasi digital agar mereka lebih sadar akan pentingnya menjaga data pribadi mereka. Dalam penelitian ini, dibahas tantangan yang dihadapi dalam upaya perlindungan data pribadi di Indonesia dan strategi yang perlu diterapkan untuk meningkatkan keamanan data pribadi serta kesadaran masyarakat akan ancaman siber yang semakin canggih.

Kata Kunci: Perlindungan data pribadi, kebocoran data, keamanan siber

Abstract

Personal data protection in Indonesia faces various challenges in the rapidly developing digital era. Personal data leaks are a serious problem that requires attention from all parties, including the government, private sector, and the public. Efforts to protect personal data must be carried out through close collaboration between various sectors, by strengthening existing policies and regulations, increasing public awareness, and strengthening cybersecurity infrastructure and technology. The Indonesian government has issued the Personal Data Protection Law as an initial step, but consistent implementation and better coordination are still challenges. In addition, there needs to be education for the public to improve digital literacy so that they are more aware of the importance of protecting their personal data. This study discusses the challenges faced in efforts to protect personal data in Indonesia and the strategies that need to be implemented to improve personal data security and public awareness of increasingly sophisticated cyber threats.

Keywords: *Personal data protection, data leaks, cybersecurity*

PENDAHULUAN

Data pribadi merujuk pada informasi yang dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Jenis-jenis data pribadi meliputi data identitas

seperti nama, alamat, nomor identitas, dan tanggal lahir, serta informasi terkait kehidupan pribadi seperti status pernikahan, agama, dan riwayat pekerjaan. Selain itu, data pribadi juga mencakup informasi keuangan, data kesehatan, serta data yang diperoleh melalui aktivitas online seperti lokasi, riwayat pencarian, dan preferensi pengguna. Keberadaan data pribadi ini sangat penting, baik untuk keperluan administrasi, bisnis, maupun interaksi sosial di dunia digital, sehingga pengelolaannya memerlukan perlindungan yang serius untuk menjaga privasi individu. (Rosadi, 2015)

Kebocoran data pribadi dapat menimbulkan dampak yang sangat merugikan bagi individu, organisasi, dan negara. Bagi individu, kebocoran data pribadi dapat menyebabkan pencurian identitas, penipuan finansial, dan kerugian emosional yang signifikan. Bagi organisasi, kebocoran data dapat merusak reputasi, mengurangi kepercayaan pelanggan, serta berpotensi menghadirkan sanksi hukum dan kerugian finansial. Di tingkat negara, kebocoran data pribadi dapat mengancam keamanan nasional, karena informasi sensitif yang dimiliki oleh warga negara atau instansi pemerintahan bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat, bersama dengan semakin meningkatnya penggunaan platform digital, menjadikan data pribadi semakin rentan bocor. Meskipun teknologi memberikan kemudahan dalam berbagai aspek kehidupan, hal ini juga membuka celah bagi peretas untuk mengeksploitasi sistem yang ada dan mencuri data pribadi melalui serangan siber, seperti peretasan, phishing, atau malware.(Rianarizkiwati, 2020)

Di era digital saat ini, data pribadi sering kali menjadi sasaran tindak kejahatan siber, yang mengakibatkan perlindungan terhadap informasi ini menjadi sangat penting. Banyak individu yang belum sepenuhnya menyadari bahwa data pribadi mereka rentan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Di Indonesia, kurangnya upaya yang memadai dalam melindungi data pribadi telah menyebabkan sejumlah insiden peretasan dan kebocoran data yang meluas, di mana kasus-kasus peretasan akun media sosial dan pencurian identitas menjadi sangat umum. Kejadian-kejadian tersebut berisiko menimbulkan pelanggaran privasi, pemerasan, serta penipuan online. Melihat permasalahan ini, kesadaran akan perlunya regulasi yang lebih kuat untuk melindungi data pribadi mulai tumbuh, yang tercermin dalam langkah pemerintah yang menyusun dan mengesahkan Undang-Undang Nomor 27 Tahun 2022 sebagai landasan hukum untuk perlindungan data pribadi di Indonesia. (Aswandi et al., 2020)

Namun, menghadapi kejahatan siber melalui pendekatan hukum konvensional memiliki tantangan besar. Kejahatan siber melibatkan lima faktor yang saling berkaitan, yaitu pelaku, korban, reaksi sosial, dan hukum. Meskipun hukum memiliki peran yang vital dalam mencegah dan mengatasi kejahatan, menciptakan peraturan yang selaras dengan perkembangan teknologi informasi yang pesat bukanlah perkara mudah. Salah satu kendala utama adalah

kecepatan perkembangan teknologi yang seringkali membuat peraturan hukum menjadi ketinggalan zaman atau usang, yang pada gilirannya menciptakan kekosongan hukum. Hal ini sangat terasa dalam menangani kejahatan di dunia maya, seperti cybercrime, di mana ruang lingkup dan dinamisnya ancaman siber berkembang begitu cepat.(Pasaribu, 2017)

Untuk itu, Indonesia harus mempersiapkan diri dengan sumber daya manusia yang kompeten dan terampil dalam bidang keamanan siber. Kualitas sumber daya manusia yang baik akan berkontribusi pada kemampuan untuk berpikir kritis terhadap perubahan lingkungan global, memahami perkembangan teknologi dan informasi, serta menyadari dampak yang ditimbulkan oleh ancaman siber terhadap masyarakat. Selain itu, negara juga perlu memperkuat infrastruktur pengamanan siber yang mencakup teknologi yang dapat mendeteksi, mencegah, dan merespons ancaman dengan cepat. Dengan meningkatkan kapasitas sumber daya manusia dan fasilitas pengamanan siber, Indonesia dapat lebih siap dalam menghadapi tantangan kejahatan siber yang semakin kompleks. Hal ini tidak hanya melibatkan pelatihan tenaga ahli, tetapi juga pengembangan dan perbaikan infrastruktur yang memungkinkan deteksi dan respons terhadap serangan siber yang lebih efektif. Sebagai landasan hukum, Undang-Undang Nomor 27 Tahun 2022 juga menekankan perlunya perlindungan data pribadi sebagai hak asasi manusia yang dijamin oleh negara, guna menciptakan kesadaran masyarakat dan memastikan perlindungan yang lebih efektif terhadap data pribadi.(Siahaan, 2022)

Kebocoran data pribadi telah menjadi fenomena yang kerap terjadi baik di Indonesia maupun di tingkat internasional, dengan dampak yang sangat merugikan bagi individu dan organisasi. Beberapa kasus kebocoran data pribadi yang terkenal di Indonesia termasuk kebocoran data pengguna layanan digital, seperti Tokopedia, Bukalapak, dan Go-Jek, yang melibatkan jutaan data pribadi pelanggan, termasuk nama, alamat, nomor telepon, dan email. Kasus serupa juga terjadi di tingkat global, seperti kebocoran data Facebook yang melibatkan lebih dari 530 juta akun pengguna yang tersebar di berbagai negara, serta kebocoran data pengguna aplikasi Zoom yang mempengaruhi jutaan orang di seluruh dunia. Kasus-kasus ini menunjukkan betapa rentannya data pribadi, baik yang disebabkan oleh serangan siber dari peretas (hacker) maupun kelalaian dalam pengelolaan data oleh pihak yang bertanggung jawab, seperti kebocoran akibat kebijakan keamanan yang lemah atau kesalahan teknis dalam sistem penyimpanan data.(Rahmawati, 2017)

Penyebab utama kebocoran data pribadi umumnya berkaitan dengan serangan siber yang dilakukan oleh pihak yang tidak bertanggung jawab, seperti peretasan sistem atau serangan malware yang menargetkan organisasi atau individu. Namun, kelalaian atau kesalahan pengguna juga menjadi faktor signifikan dalam kebocoran data pribadi, seperti penggunaan kata sandi yang lemah, pengabaian langkah-langkah keamanan digital, atau ketidaktahuan tentang cara melindungi informasi pribadi secara online. Dampak dari kebocoran data pribadi terhadap

korban bisa sangat serius, mulai dari kerugian finansial yang disebabkan oleh pencurian identitas dan penipuan, hingga rusaknya reputasi yang dapat berpengaruh pada kehidupan pribadi atau profesional korban. Dalam banyak kasus, pencurian identitas dapat menyebabkan korban kesulitan dalam mengakses layanan finansial atau bahkan terjebak dalam masalah hukum. Selain itu, bagi organisasi, kebocoran data dapat merusak kepercayaan konsumen, menurunkan nilai perusahaan, dan menimbulkan sanksi hukum yang berat, yang semuanya berisiko merusak stabilitas ekonomi dan sosial.(Ukurta & Dahana, 2023)

Kementerian Komunikasi dan Informatika (Kominfo) memiliki peran penting dalam mengatur dan mengawasi pelaksanaan perlindungan data pribadi di Indonesia. Sebagai lembaga yang bertanggung jawab dalam pengelolaan dan pengawasan sektor komunikasi dan informatika, Kominfo memastikan bahwa perlindungan data pribadi dilaksanakan sesuai dengan peraturan yang berlaku. Salah satu kebijakan utama yang diterapkan adalah pengembangan regulasi yang mengatur pengumpulan, penyimpanan, dan pemrosesan data pribadi, guna melindungi hak-hak warga negara dari penyalahgunaan informasi. Kominfo juga berperan dalam penyusunan Undang-Undang Perlindungan Data Pribadi yang disahkan pada tahun 2022, yang menjadi dasar hukum bagi kebijakan perlindungan data pribadi di Indonesia. Selain itu, Kominfo juga melakukan pengawasan terhadap implementasi kebijakan ini untuk memastikan bahwa organisasi atau perusahaan yang mengelola data pribadi mematuhi ketentuan yang ada, serta mengambil tindakan yang tepat jika terjadi pelanggaran.(Indah et al., 2023)

Dalam mengedukasi masyarakat mengenai pentingnya perlindungan data pribadi, Kominfo menerapkan berbagai kebijakan dan strategi, termasuk melaksanakan program pelatihan dan seminar bagi publik. Program ini bertujuan untuk meningkatkan kesadaran masyarakat tentang pentingnya menjaga keamanan data pribadi di dunia digital, serta bagaimana cara melindunginya dari ancaman siber. Kominfo juga berupaya meningkatkan literasi digital melalui kampanye nasional mengenai keamanan siber, dengan tujuan memberikan pemahaman lebih mendalam kepada masyarakat tentang bahaya yang mengintai di ruang digital. Dalam hal pengaturan keamanan siber, Kominfo mengembangkan berbagai regulasi dan sistem yang mengatur bagaimana infrastruktur teknologi di Indonesia harus memenuhi standar keamanan tertentu, serta bagaimana institusi terkait harus menjaga data pribadi agar tidak jatuh ke tangan yang salah.

Gerakan Siberkreasi merupakan salah satu inisiatif penting dari pemerintah Indonesia yang bertujuan untuk mengedukasi masyarakat mengenai ancaman dunia digital dan perlindungan data pribadi. Program ini fokus pada peningkatan literasi digital melalui pelatihan, seminar, dan kampanye yang menyasar berbagai lapisan masyarakat. Siberkreasi juga berkolaborasi dengan berbagai pihak, seperti sekolah, universitas, dan sektor swasta, untuk mengedukasi generasi muda dan masyarakat umum tentang pentingnya menjaga privasi serta cara

menghindari potensi risiko yang ada di dunia maya. Selain itu, Gerakan Siberkreasi berperan dalam membangun budaya literasi digital di Indonesia, yang memungkinkan masyarakat memiliki kemampuan untuk memahami, memanfaatkan, dan melindungi diri dari potensi ancaman siber yang semakin kompleks. Dengan pendekatan yang terintegrasi dan inklusif, Gerakan Siberkreasi membantu menciptakan kesadaran kolektif mengenai pentingnya menjaga keamanan data pribadi dalam kehidupan sehari-hari.

Namun, meskipun terdapat berbagai upaya, tantangan dalam pencegahan kebocoran data pribadi masih banyak dihadapi, seperti rendahnya kesadaran masyarakat tentang pentingnya perlindungan data pribadi, keterbatasan teknologi, dan lemahnya pengawasan di lapangan. Banyak individu yang masih belum memahami risiko yang terkait dengan penggunaan data pribadi di platform digital, sehingga mereka cenderung tidak berhati-hati dalam berbagi informasi secara online. Selain itu, meskipun peraturan sudah ada, implementasinya di lapangan seringkali terkendala oleh kurangnya sumber daya, baik dalam hal pengawasan maupun kapasitas teknologi yang dimiliki oleh instansi terkait. Faktor-faktor seperti kesenjangan pengetahuan teknologi, tantangan dalam edukasi yang efektif, serta kurangnya konsistensi dalam penegakan hukum juga mempengaruhi tingkat keberhasilan kebijakan perlindungan data pribadi. Oleh karena itu, dibutuhkan strategi yang lebih efektif dalam melindungi data pribadi serta meningkatkan kolaborasi antara pemerintah, masyarakat, dan sektor swasta untuk menciptakan ekosistem digital yang lebih aman. Seiring dengan perkembangan teknologi yang terus berubah, penguatan regulasi dan pembaruan kebijakan yang cepat menjadi hal yang sangat penting untuk memastikan perlindungan data pribadi tetap terjaga dengan baik.

METODE PENELITIAN

Metode penelitian yuridis normatif digunakan dalam penelitian ini untuk menganalisis norma-norma hukum yang terdapat dalam peraturan perundang-undangan terkait perlindungan data pribadi. Pendekatan ini berfokus pada kajian terhadap peraturan-peraturan yang ada, seperti Undang-Undang Perlindungan Data Pribadi, serta kebijakan dan regulasi lain yang berkaitan dengan keamanan data dan privasi di Indonesia. Dengan menggunakan metode yuridis normatif, penelitian ini bertujuan untuk mengevaluasi sejauh mana peraturan tersebut dapat melindungi data pribadi dalam konteks hukum yang berlaku, serta bagaimana implementasi dan pengawasan terhadap regulasi tersebut dapat meningkatkan perlindungan data pribadi di Indonesia. Selain itu, pendekatan perundang-undangan dan analitis digunakan untuk mengkaji peraturan-peraturan yang relevan dengan perlindungan data pribadi dan pencegahan kebocoran data, serta untuk menganalisis dampak dari kebijakan-kebijakan tersebut terhadap efektivitas pencegahan kebocoran data. Pendekatan perundang-undangan mengutamakan analisis terhadap teks-teks hukum dan peraturan yang ada, sementara pendekatan analitis digunakan untuk mengevaluasi implementasi dan penerapan kebijakan tersebut dalam

praktik di lapangan. Penelitian ini akan mengidentifikasi tantangan, hambatan, dan potensi perbaikan dalam sistem hukum yang ada untuk menciptakan perlindungan yang lebih efektif terhadap data pribadi masyarakat Indonesia.

HASIL DAN PEMBAHASAN

Peran Kementerian Komunikasi dan Informatika (Kominfo) dalam Mengatur dan Mengawasi Perlindungan Data Pribadi di Indonesia

Perkembangan teknologi informasi telah memberikan dampak yang sangat besar dalam berbagai aspek kehidupan, mulai dari kemudahan akses informasi hingga efisiensi komunikasi. Dengan adanya internet, digitalisasi, dan berbagai perangkat cerdas, kita memasuki era di mana teknologi memainkan peran penting dalam kehidupan sehari-hari. Namun, seiring dengan perkembangan pesat teknologi ini, ada sisi negatif yang juga muncul, yaitu meningkatnya kerentanannya terhadap ancaman siber. Teknologi yang terus berkembang memungkinkan lebih banyak data pribadi dan informasi sensitif untuk disimpan, diproses, dan dibagikan melalui platform digital. Proses digitalisasi ini menciptakan ruang bagi pengumpulan data dalam jumlah besar yang, apabila tidak dikelola dengan baik, dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

Keberadaan kejahatan siber semakin menjadi ancaman serius dengan kemajuan teknologi informasi. Kejahatan siber, atau cybercrime, mengacu pada berbagai tindakan ilegal yang memanfaatkan teknologi digital, seperti peretasan, pencurian data, penipuan online, dan penyebaran malware. Ancaman ini meluas seiring dengan peningkatan ketergantungan manusia terhadap dunia maya dalam aktivitas sosial, ekonomi, dan pemerintahan. Para pelaku kejahatan siber menggunakan teknologi untuk meretas sistem informasi yang mengandung data pribadi, informasi keuangan, dan data sensitif lainnya. Kejahatan ini bersifat global, di mana serangan dapat dilakukan dari berbagai penjuru dunia dan mempengaruhi banyak korban dalam waktu yang sangat cepat, membuat penanganannya menjadi lebih kompleks dan menantang.(Riyadi & Suriaatmadja, 2023)

Munculnya kejahatan terhadap data pribadi menjadi salah satu dampak langsung dari fenomena kejahatan siber. Data pribadi, yang meliputi informasi seperti nama, alamat, nomor telepon, nomor identitas, hingga informasi finansial, kini menjadi sasaran empuk bagi para pelaku kejahatan siber. Pencurian data pribadi dapat terjadi melalui berbagai metode, seperti peretasan (hacking), phishing, malware, dan serangan sosial engineering. Kebocoran data pribadi ini dapat menyebabkan kerugian besar, baik bagi individu yang menjadi korban maupun bagi organisasi yang bertanggung jawab atas pengelolaan data tersebut. Selain kerugian finansial, kebocoran data pribadi dapat merusak reputasi korban dan organisasi, mengancam privasi, serta membuka jalan bagi tindak penipuan dan penyalahgunaan identitas. Dengan meningkatnya kejahatan terhadap data pribadi, penting bagi semua pihak untuk meningkatkan kewaspadaan, menerapkan sistem

keamanan yang lebih baik, serta meningkatkan pemahaman tentang pentingnya perlindungan data pribadi di era digital.(Ikhsano et al., 2023)

Tingginya jumlah kasus kebocoran data pribadi di Indonesia menunjukkan adanya kekosongan hukum yang signifikan dalam menangani permasalahan ini. Sebelumnya, perlindungan data pribadi diatur dalam berbagai peraturan perundang-undangan yang tersebar, tanpa adanya satu regulasi khusus yang mengaturnya secara komprehensif. Kekosongan hukum ini memicu kebutuhan mendesak untuk merumuskan dan mengesahkan sebuah undang-undang yang dapat menangani secara spesifik isu perlindungan data pribadi. Untuk itu, pemerintah Indonesia segera mengesahkan Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi yang telah dibahas sejak 2019 dan akhirnya disetujui menjadi Undang-Undang Nomor 27 Tahun 2022. Undang-Undang ini bertujuan untuk memberikan perlindungan hukum terhadap hak individu dalam melindungi data pribadi mereka, serta meningkatkan kesadaran masyarakat mengenai pentingnya menjaga keamanan data pribadi.(Oktaviani et al., 2021)

Undang-Undang Perlindungan Data Pribadi ini juga mencakup sanksi sebagai bentuk penegakan hukum bagi pelanggaran yang terjadi. Sanksi merupakan konsekuensi yang diberikan kepada pihak-pihak yang melanggar peraturan terkait perlindungan data pribadi. Sanksi administratif, yang menjadi salah satu jenis sanksi dalam undang-undang ini, bertujuan untuk memastikan kepatuhan terhadap peraturan yang ada serta mencegah kerugian yang disebabkan oleh pelanggaran tersebut. Meskipun pengertian sanksi administratif belum didefinisikan secara tegas dalam undang-undang, pada dasarnya, sanksi ini digunakan sebagai alat untuk mendorong pematuhan terhadap aturan dan memberikan efek jera bagi pelanggar, agar tidak mengulangi tindakan yang merugikan. Penerapan sanksi administratif ini bertujuan untuk menjaga ketertiban hukum dan melindungi hak-hak individu yang terganggu akibat kebocoran data pribadi.(Gunadi et al., 2023)

Dengan disahkannya Undang-Undang Perlindungan Data Pribadi ini, diharapkan Indonesia dapat memiliki solusi yang lebih efektif dalam menangani permasalahan kebocoran data pribadi, yang selama ini sering terjadi. Dengan semakin pesatnya perkembangan teknologi dan internet, kejahatan siber yang menyasar data pribadi semakin meningkat dan membawa dampak yang signifikan bagi individu, organisasi, bahkan negara. Kejahatan-kejahatan ini dapat menimbulkan kerugian dalam berbagai aspek, mulai dari ekonomi, perbankan, hingga politik dan keamanan nasional. Undang-Undang Perlindungan Data Pribadi, yang bertujuan untuk melindungi privasi individu dan mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab, diharapkan dapat menjadi landasan hukum yang kuat untuk mencegah penyalahgunaan data pribadi. Regulasi ini memberikan dasar hukum yang jelas dalam rangka menjaga hak privasi masyarakat, serta memastikan agar data pribadi tidak jatuh ke tangan yang salah,

sehingga membangun kepercayaan dan keamanan dalam ekosistem digital.(Cenyvesta & Gunadi, 2024)

Pada tahun 2023, Indonesia mengalami peningkatan signifikan dalam insiden kebocoran data pribadi. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), terdapat 103 dugaan insiden kebocoran data yang terdeteksi sepanjang tahun tersebut, dengan 69% di antaranya terjadi di sektor administrasi pemerintahan. Selain itu, sektor keuangan dan teknologi informasi juga mengalami kebocoran data yang signifikan, masing-masing dengan 165 ribu dan 161 ribu data yang tersebar secara tidak sah. Memasuki tahun 2024, kasus kebocoran data pribadi di Indonesia terus menjadi perhatian serius. Pada September 2024, terungkap bahwa data pribadi 34.900.867 Warga Negara Indonesia (WNI) yang terkait dengan paspor diduga telah bocor. Selain itu, Indonesia tercatat sebagai negara dengan kebocoran data terbesar ketiga di dunia, dengan estimasi 94,22 juta akun yang bocor antara Januari 2020 hingga Januari 2024. Angka-angka ini menunjukkan bahwa meskipun telah ada upaya untuk meningkatkan keamanan siber, tantangan dalam melindungi data pribadi di Indonesia masih sangat besar.

Kementerian Komunikasi dan Informatika (Kominfo) bekerja sama dengan Gerakan Siberkreasi untuk memberikan edukasi digital kepada masyarakat Indonesia. Tujuan dari kolaborasi ini adalah agar masyarakat lebih bijak dalam memilih informasi yang diterima, menghindari hoaks, dan tidak mudah terpengaruh oleh informasi yang belum dapat dipastikan kebenarannya. Kominfo juga terus berupaya meningkatkan penegakan hukum terkait penyebaran hoaks, bekerja sama dengan kepolisian dalam memerangi misinformasi di dunia maya. Namun, meskipun berbagai upaya telah dilakukan, kesadaran masyarakat mengenai pentingnya perlindungan data pribadi masih tergolong rendah. Berbagai negara maju seperti Australia dan Singapura sudah mengimplementasikan regulasi perlindungan data yang kuat, yang memberikan kerangka hukum untuk memastikan perlindungan data pribadi yang lebih efektif. Regulasi semacam itu penting untuk diadopsi oleh Indonesia agar lebih maksimal dalam menjaga data pribadi masyarakat.(Fauzi & Shandy, 2022)

Pemerintah Indonesia juga mengembangkan konsep Indonesian Data Protection System (IDPS) sebagai salah satu langkah untuk meminimalisasi kejahatan siber, terutama terkait penyalahgunaan data pribadi. IDPS bertujuan untuk mengamankan data pribadi yang tersimpan dalam pusat data atau pusat pengumpulan informasi. Sistem ini bekerja melalui koordinasi antara otoritas data dan petugas data yang bertanggung jawab untuk mengumpulkan dan melindungi data pribadi. Koordinasi ini penting agar data dapat dikelola dengan aman dan sesuai dengan aturan yang berlaku. IDPS dikelola oleh Kementerian Komunikasi dan Informatika (Kominfo), yang bertindak sebagai otoritas utama dalam pengelolaan dan pengawasan perlindungan data pribadi di Indonesia. Meskipun sistem ini telah diterapkan, tantangan besar tetap ada, mengingat maraknya kebocoran data pribadi yang

terjadi dalam beberapa tahun terakhir.(Hertianto, 2021)

Beberapa kasus kebocoran data yang baru-baru ini terjadi menunjukkan betapa rentannya sistem perlindungan data pribadi di Indonesia. Salah satu kasus yang mencuat adalah kebocoran data pribadi yang melibatkan perusahaan milik negara, PT PLN, yang diduga mengalami kebocoran data sebanyak 17 juta konsumen. Data yang bocor tersebut mencakup informasi sensitif seperti nama pelanggan, alamat, ID pelanggan, dan konsumsi energi. Selain itu, data dari 26 juta konsumen Indihome juga terungkap dan dijual di forum peretas. Kasus lainnya termasuk kebocoran data pada Bank Indonesia, PT Pertamina Training and Consulting, serta tindakan peretasan yang dilakukan oleh seorang hacker bernama Bjorka terhadap situs-situs resmi pemerintah, termasuk informasi pribadi pejabat negara. Kejadian-kejadian ini menyoroti pentingnya memperkuat pengamanan data pribadi agar tidak jatuh ke tangan yang salah, yang dapat menimbulkan kerugian besar baik bagi individu maupun negara.

Undang-Undang Perlindungan Data Pribadi (UU PDP), yang disahkan pada Oktober 2022, diharapkan dapat membawa perubahan signifikan dalam pengelolaan data pribadi di Indonesia, seiring dengan pesatnya perkembangan teknologi informasi dan ekonomi digital. UU ini mencakup 18 bab dan 78 pasal yang mengatur berbagai hal terkait perlindungan data pribadi, mulai dari pengaturan transfer data, sanksi administratif, hingga kerjasama internasional. UU PDP juga memperkenalkan mekanisme untuk melindungi hak atas data pribadi sebagai bagian dari hak asasi manusia, yang semakin penting dalam konteks ancaman terhadap privasi individu. Perlindungan data pribadi diakui sebagai elemen penting dalam menjaga harga diri, kebebasan individu, dan mencegah penyalahgunaan data yang dapat merugikan individu maupun negara. Selain itu, dalam rangka menjamin kepastian hukum dan perlindungan terhadap data pribadi, UU PDP menetapkan hak-hak subjek data pribadi, seperti hak untuk mengakses, menghapus, atau mengakhiri pemrosesan data mereka. Dengan perlindungan yang jelas, UU ini juga mendorong pencegahan kejahatan dengan pendekatan non-penal, yang lebih berfokus pada pencegahan pelanggaran dan menjaga hak-hak subjek data pribadi.

Implementasi UU PDP mengharuskan pengelola data pribadi, baik itu lembaga pemerintah maupun sektor swasta, untuk mematuhi kewajiban yang jelas dalam hal pengumpulan, pengolahan, dan penghapusan data. Semua pemrosesan data harus dilakukan secara transparan dan dengan dasar hukum yang sah, sesuai dengan tujuan yang ditetapkan di awal. Data pribadi harus diproses dengan cara yang aman, dan jika masa retensi data telah berakhir, data tersebut harus dihapus atau dimusnahkan, kecuali ada pengecualian berdasarkan peraturan khusus yang berlaku di sektor tertentu. Selain itu, untuk memastikan perlindungan yang maksimal, perlu adanya pengawasan yang ketat, termasuk penggunaan teknologi yang mutakhir dalam pengelolaan data pribadi, serta penerapan kode etik oleh asosiasi yang relevan. UU ini juga

mendorong badan hukum yang mengelola data untuk terus memantau perkembangan regulasi, serta melibatkan berbagai pihak dalam organisasi untuk menjaga dan memastikan keamanan data pribadi secara berkelanjutan.

Kementerian Komunikasi dan Informatika (Kominfo) memiliki peran yang sangat penting dalam pengaturan dan pengawasan perlindungan data pribadi di Indonesia. Sebagai lembaga yang bertanggung jawab, Kominfo tidak hanya berperan dalam menyusun kebijakan dan regulasi, tetapi juga mengawasi implementasi kebijakan tersebut di seluruh sektor. Tugas utama Kominfo mencakup pembuatan kebijakan yang menyeluruh terkait perlindungan data pribadi, pengawasan terhadap praktik pengumpulan, penyimpanan, dan pemrosesan data, serta penegakan hukum terhadap pelanggaran yang terjadi. Kominfo berperan sebagai penghubung antara pemerintah, sektor swasta, dan masyarakat dalam memastikan data pribadi dilindungi dengan baik. Selain itu, Kominfo juga memiliki tanggung jawab dalam menyediakan pedoman teknis dan prosedural bagi penyelenggara sistem elektronik yang mengelola data pribadi, agar mereka dapat mematuhi standar perlindungan yang berlaku.

Kominfo telah menerbitkan beberapa kebijakan dan regulasi untuk melindungi data pribadi, yang salah satunya adalah Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada 2022. UU ini menjadi landasan hukum yang kuat untuk mengatur pengumpulan, penyimpanan, dan pemrosesan data pribadi di Indonesia. Di samping itu, Kominfo juga mengeluarkan peraturan-peraturan turunan yang menjelaskan lebih rinci tentang implementasi dari UU PDP, seperti Peraturan Pemerintah, peraturan menteri, dan pedoman teknis untuk sektor-sektor tertentu, termasuk sektor telekomunikasi dan perbankan. Kebijakan ini memastikan bahwa data pribadi hanya dapat diproses untuk tujuan yang sah, dengan persetujuan yang jelas dari pemilik data, dan harus disimpan dengan cara yang aman. Kominfo juga memiliki wewenang untuk memberikan sanksi administratif terhadap pelanggaran yang terjadi terkait pengelolaan data pribadi, sehingga memberi kepastian hukum bagi masyarakat dan dunia usaha.

Upaya Kominfo dalam meningkatkan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi semakin intensif dengan berbagai program edukasi dan sosialisasi. Kominfo mengadakan berbagai kegiatan untuk memberikan pemahaman kepada masyarakat tentang pentingnya menjaga data pribadi mereka di era digital yang semakin berkembang. Program edukasi ini mencakup kampanye informasi melalui media sosial, seminar, dan lokakarya yang melibatkan berbagai kalangan, termasuk sektor pendidikan, pemerintahan, dan masyarakat umum. Tujuan dari program ini adalah untuk membantu masyarakat memahami langkah-langkah yang dapat mereka ambil dalam melindungi data pribadi mereka, seperti cara memilih kata sandi yang kuat, mengenali potensi risiko keamanan, serta memahami hak mereka terkait data pribadi. Melalui program ini, Kominfo berharap masyarakat semakin

sadar akan pentingnya menjaga privasi mereka dalam dunia digital yang penuh tantangan, dan dapat menghindari risiko penyalahgunaan data pribadi.

Hambatan yang Dihadapi dalam Pencegahan Kebocoran Data Pribadi di Indonesia

Upaya pencegahan kebocoran data pribadi di Indonesia menghadapi sejumlah hambatan yang cukup kompleks, yang berkaitan dengan faktor teknis, sosial, dan hukum. Meskipun pemerintah telah menerapkan kebijakan dan regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai langkah lainnya untuk memperkuat sistem perlindungan data, realitas di lapangan menunjukkan bahwa upaya tersebut masih terbentur oleh berbagai tantangan. Di antara hambatan utama yang dihadapi adalah keterbatasan infrastruktur keamanan siber yang memadai, rendahnya kesadaran masyarakat akan pentingnya perlindungan data pribadi, serta penerapan regulasi yang belum optimal. Selain itu, ancaman serangan siber yang semakin canggih dan keterbatasan sumber daya dalam pengawasan semakin memperburuk situasi. Oleh karena itu, diperlukan pemahaman yang mendalam mengenai hambatan-hambatan ini agar langkah-langkah yang lebih efektif dapat diambil untuk melindungi data pribadi masyarakat Indonesia.

Keterbatasan infrastruktur keamanan siber di Indonesia menjadi salah satu hambatan utama dalam upaya pencegahan kebocoran data pribadi. Baik sektor publik maupun swasta masih menghadapi kesulitan dalam menyediakan sistem keamanan yang memadai untuk melindungi data pribadi. Banyak organisasi yang masih menggunakan teknologi yang sudah ketinggalan zaman atau belum sepenuhnya aman, sehingga rentan terhadap serangan siber (Dermawan et al., 2023). Seringkali, pembaruan sistem dan perangkat keamanan tidak dilakukan secara berkala, sehingga kelemahan-kelemahan dalam sistem keamanan ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain itu, terdapat ketidakseragaman antara sektor-sektor dalam hal tingkat keamanan yang diterapkan, yang semakin memperburuk situasi perlindungan data pribadi di seluruh negara.

Kurangnya kesadaran masyarakat tentang perlindungan data pribadi juga menjadi faktor penghambat yang signifikan dalam mencegah kebocoran data. Meskipun berbagai program edukasi telah dilakukan, banyak individu yang masih tidak memahami pentingnya menjaga informasi pribadi mereka, terutama di dunia digital. Salah satu penyebab utama adalah rendahnya tingkat literasi digital yang ada di masyarakat. Tanpa pemahaman yang memadai tentang potensi risiko yang dapat timbul dari kebocoran data pribadi, banyak orang cenderung mengabaikan langkah-langkah perlindungan dasar, seperti penggunaan kata sandi yang kuat atau menjaga kerahasiaan informasi pribadi secara online. Hal ini membuat masyarakat rentan terhadap serangan phishing, malware, dan praktik-praktik kejahatan siber lainnya yang dapat mengakses data pribadi secara tidak sah.

Selain itu, penerapan regulasi yang belum optimal juga menjadi kendala

besar dalam upaya pencegahan kebocoran data pribadi di Indonesia. Meskipun Undang-Undang Perlindungan Data Pribadi (UU PDP) telah disahkan, implementasinya di tingkat lapangan masih menghadapi banyak tantangan. Salah satunya adalah kurangnya konsistensi dalam pelaksanaan regulasi oleh berbagai lembaga terkait, yang menyebabkan kesenjangan dalam perlindungan data pribadi antara sektor-sektor yang berbeda. Selain itu, regulasi yang ada juga sering kali tidak dapat mengakomodasi dinamika kebutuhan industri yang berkembang pesat, seperti sektor teknologi dan e-commerce. Proses penegakan hukum yang terkait dengan kebocoran data juga terhambat oleh berbagai kendala administratif dan teknis, yang membuatnya sulit untuk menindak tegas pihak-pihak yang melanggar aturan.

Kurangnya koordinasi antar lembaga menjadi hambatan serius dalam menangani kebocoran data pribadi di Indonesia. Berbagai lembaga pemerintah, sektor swasta, dan organisasi terkait seharusnya bekerja sama dalam mengatur dan mengawasi pengelolaan data pribadi, namun sering kali komunikasi dan koordinasi antara mereka tidak berjalan efektif. Hal ini menyebabkan kebijakan dan regulasi yang diterapkan menjadi kurang terintegrasi, bahkan terkadang tumpang tindih. Misalnya, beberapa kementerian atau lembaga memiliki kewenangan yang hampir serupa dalam hal pengawasan data pribadi, namun tidak ada sinergi dalam pelaksanaannya. Tumpang tindih kebijakan ini membuat implementasi tindakan preventif yang efektif menjadi lebih sulit, karena tidak ada kesepahaman yang jelas mengenai siapa yang bertanggung jawab atas keamanan data pribadi di sektor tertentu.

Keamanan data pada platform digital dan aplikasi juga menjadi tantangan besar dalam melindungi data pribadi. Banyak platform digital dan aplikasi yang digunakan masyarakat tidak sepenuhnya mematuhi standar perlindungan data pribadi yang cukup, atau bahkan tidak memiliki sistem keamanan yang memadai untuk melindungi informasi pribadi pengguna (Suari & Sarjana, 2023). Dalam banyak kasus, kebocoran data dapat terjadi akibat kelalaian atau kelonggaran standar keamanan dari aplikasi atau platform yang digunakan. Selain itu, masalah lain yang kerap terjadi adalah data pribadi yang jatuh ke tangan pihak ketiga yang memiliki akses terhadap data pengguna, misalnya dalam hal pengiklan atau mitra pihak ketiga yang bekerja sama dengan platform tersebut. Serangan siber yang semakin canggih juga menjadi ancaman besar terhadap perlindungan data pribadi. Serangan seperti phishing, malware, dan ransomware telah berkembang menjadi metode yang lebih sulit dideteksi dan dihentikan. Kejahatan siber ini tidak hanya mengancam integritas data pribadi tetapi juga dapat merusak sistem yang ada dan menyebabkan kerugian finansial yang besar. Serangan semacam ini sering kali melibatkan teknik yang lebih canggih, seperti penyamaran identitas atau pengendalian sistem tanpa terdeteksi, yang membuatnya semakin sulit untuk dilawan dengan sistem keamanan konvensional. Akibatnya, inovasi dalam teknologi perlindungan data sangat diperlukan untuk mengatasi

ancaman tersebut.

Keterbatasan sumber daya dan kapasitas pengawasan yang dimiliki lembaga terkait, seperti Kementerian Komunikasi dan Informatika (Kominfo) serta Badan Siber dan Sandi Negara (BSSN), menjadi tantangan utama dalam mengawasi dan memantau seluruh ekosistem digital Indonesia. Seiring dengan berkembangnya teknologi dan semakin meluasnya penggunaan platform digital, jumlah entitas yang harus dipantau semakin besar. Namun, keterbatasan jumlah personel, anggaran, serta alat dan teknologi yang memadai untuk mendeteksi dan mengatasi ancaman kebocoran data membuat pengawasan menjadi kurang optimal (Rosidah et al., 2023). Lembaga-lembaga tersebut sering kali kesulitan dalam menjalankan fungsi pengawasan yang efektif karena kurangnya kapasitas untuk memonitor dengan cermat seluruh aktivitas digital yang dapat berisiko terhadap perlindungan data pribadi. Dalam hal penegakan hukum, tantangan yang dihadapi cukup signifikan, terutama terkait dengan kesulitan dalam menegakkan hukum terhadap pelaku kebocoran data pribadi. Proses hukum yang lambat sering kali menjadi hambatan utama dalam menangani kasus kebocoran data, karena bukti yang diperlukan untuk mendakwa pelaku atau mengungkap penyalahgunaan data seringkali sulit ditemukan. Selain itu, hambatan teknis dalam pelacakan dan pemrosesan data yang bocor juga menghambat langkah-langkah penegakan hukum yang cepat dan efektif.

Strategi Yang Perlu Diterapkan Untuk Meningkatkan Perlindungan Data Pribadi Dan Mengedukasi Masyarakat Mengenai Keamanan Siber Melalui Kolaborasi Antara Pemerintah, Masyarakat, Dan Sektor Swasta

Dalam era digital yang semakin berkembang pesat, perlindungan data pribadi menjadi salah satu tantangan utama yang harus dihadapi oleh masyarakat, pemerintah, dan sektor swasta. Kebocoran data pribadi tidak hanya mengancam hak privasi individu, tetapi juga dapat menimbulkan dampak finansial, reputasi, dan keamanan yang signifikan (Priliasari, 2023). Untuk mengatasi ancaman ini, diperlukan strategi komprehensif yang melibatkan kolaborasi erat antara pemerintah, masyarakat, dan sektor swasta. Dengan menggabungkan upaya dari semua pihak, seperti penguatan regulasi, edukasi masyarakat, dan pengembangan teknologi keamanan siber, perlindungan data pribadi dapat ditingkatkan secara signifikan. Kerja sama yang solid di antara ketiga elemen ini menjadi kunci untuk menciptakan ekosistem digital yang aman dan terpercaya bagi seluruh lapisan masyarakat.

Kolaborasi antarlembaga dan antarsektor menjadi fondasi utama dalam upaya meningkatkan perlindungan data pribadi. Pemerintah memegang peranan penting dalam menciptakan regulasi yang komprehensif dan memberikan kerangka kerja yang mendukung sinergi dengan sektor swasta dan masyarakat. Mekanisme koordinasi yang terstruktur antara lembaga pemerintah, perusahaan swasta, dan organisasi non-pemerintah sangat diperlukan untuk memastikan respons terpadu terhadap ancaman keamanan data. Misalnya, penguatan kemitraan publik-swasta dapat

dilakukan dengan berbagi sumber daya, teknologi, dan informasi mengenai ancaman keamanan siber. Pendekatan ini tidak hanya akan meningkatkan efisiensi dalam menangani risiko kebocoran data, tetapi juga menciptakan lingkungan yang lebih aman bagi ekosistem digital di Indonesia.

Untuk menghadapi ancaman siber yang terus berkembang, diperlukan investasi besar-besaran dalam infrastruktur keamanan siber, termasuk adopsi teknologi modern dan pengembangan tenaga ahli yang kompeten. Lembaga pemerintah seperti BSSN dan sektor swasta harus meningkatkan kapasitas mereka untuk mendeteksi, mencegah, dan menangani serangan siber. Salah satu langkah penting adalah pembentukan pusat respons insiden siber (CSIRT) di setiap sektor strategis, yang mampu memberikan respons cepat terhadap insiden kebocoran data (Prabaswari et al., 2022). Dengan infrastruktur yang kuat dan sumber daya manusia yang terampil, kemampuan nasional dalam menjaga keamanan data pribadi dapat ditingkatkan secara signifikan.

Selain penguatan infrastruktur, edukasi masyarakat tentang pentingnya melindungi data pribadi menjadi langkah krusial. Pemerintah dapat menjalankan program edukasi dan kampanye kesadaran publik untuk memberikan pemahaman mengenai risiko dunia digital dan langkah-langkah preventif yang dapat diambil individu. Literasi digital harus ditanamkan sejak dini melalui kerja sama dengan institusi pendidikan untuk memasukkan keamanan siber ke dalam kurikulum formal. Selain itu, pelatihan keamanan digital untuk masyarakat umum juga penting agar mereka lebih siap menghadapi ancaman siber dan lebih berhati-hati dalam berbagi informasi pribadi secara online.

Regulasi yang adaptif terhadap perkembangan teknologi menjadi kunci untuk menjaga relevansi perlindungan data pribadi. Pemerintah perlu menyusun undang-undang yang tidak hanya mencakup kebutuhan saat ini tetapi juga mampu mengantisipasi perubahan di masa depan. Penegakan hukum juga harus diperkuat melalui peningkatan kapasitas aparat penegak hukum dalam melacak dan menangani pelanggaran perlindungan data pribadi. Selain itu, penerapan sanksi yang lebih tegas diperlukan untuk menciptakan efek jera, sehingga kepatuhan terhadap regulasi dapat ditingkatkan di seluruh sektor.

Kemajuan teknologi dapat menjadi senjata ampuh untuk meningkatkan perlindungan data pribadi. Pemerintah perlu mendorong inovasi dalam teknologi keamanan, seperti enkripsi canggih, sistem autentikasi biometrik, dan pengelolaan akses data yang terintegrasi. Insentif, seperti subsidi atau pengurangan pajak, dapat diberikan kepada perusahaan teknologi yang mengembangkan solusi inovatif di bidang ini. Selain itu, pengujian keamanan rutin terhadap platform digital yang digunakan oleh masyarakat perlu dilakukan untuk memastikan bahwa standar keamanan selalu dipatuhi dan data pribadi tetap terlindungi.

Transparansi dalam pengelolaan data pribadi menjadi aspek penting untuk membangun kepercayaan masyarakat. Perusahaan dan organisasi yang mengelola data harus secara

terbuka memberikan informasi kepada pengguna tentang bagaimana data mereka dikumpulkan, digunakan, dan dilindungi. Pelaporan insiden kebocoran data secara transparan dan langkah mitigasi yang dilakukan juga harus menjadi kewajiban. Untuk memperkuat akuntabilitas, audit keamanan data secara rutin dapat diterapkan, sehingga organisasi pengelola data pribadi dapat terus meningkatkan standar perlindungan yang mereka terapkan. Dengan pendekatan kolaboratif dan langkah-langkah strategis ini, keamanan data pribadi dapat ditingkatkan secara berkelanjutan.

SIMPULAN

Perlindungan data pribadi di era digital menjadi tantangan yang semakin kompleks seiring dengan berkembangnya teknologi dan meningkatnya penggunaan layanan digital oleh masyarakat. Ancaman seperti kebocoran data, serangan siber, dan penyalahgunaan informasi pribadi menuntut upaya kolaboratif dari berbagai pihak, termasuk pemerintah, sektor swasta, dan masyarakat. Kendala seperti keterbatasan infrastruktur keamanan, kurangnya literasi digital, dan penerapan regulasi yang belum optimal menjadi hambatan yang harus diatasi bersama. Melalui penguatan regulasi, peningkatan kapasitas keamanan siber, serta kolaborasi antarsektor, Indonesia dapat memperkuat perlindungan data pribadi dan menciptakan ekosistem digital yang lebih aman bagi seluruh penggunanya.

Untuk menghadapi tantangan ini, langkah konkret perlu dilakukan. Pemerintah sebaiknya mempercepat pengembangan regulasi yang adaptif dan tegas dalam menghadapi ancaman keamanan data, serta memberikan insentif bagi sektor swasta untuk menerapkan teknologi perlindungan data mutakhir. Di sisi lain, masyarakat harus didorong untuk meningkatkan literasi digital melalui program edukasi dan kampanye publik yang inklusif. Selain itu, kemitraan publik-swasta perlu dioptimalkan untuk berbagi pengetahuan, teknologi, dan sumber daya dalam menangani ancaman keamanan siber. Dengan strategi yang holistik dan partisipasi aktif dari seluruh elemen, Indonesia dapat mewujudkan perlindungan data pribadi yang lebih baik, sekaligus membangun kepercayaan masyarakat terhadap transformasi digital yang sedang berlangsung.

DAFTAR PUSTAKA

Aswandi, R., Muchin, P. R. N., & Sultan, M. (2020). PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS). Jurnal Legislatif, 3(2), 167–190. https://doi.org/10.20956/jl.v3i2.14321

Cenyvesta, M., & Gunadi, A. (2024). KONSEP TANGGUNG JAWAB NEGARA TERHADAP KEWAJIBAN MELINDUNGI DATA PRIBADI MASYARAKAT DI INDONESIA (STUDI KASUS KEBOCORAN DATA NPWP MASYARAKAT INDONESIA) THE CONCEPT OF STATE RESPONSIBILITY IN FULFILLING THE OBLIGATION TO PROTECT PERSONAL DATA OF CITIZENS IN INDONESIA (A CASE STUDY ON THE LEAKAGE OF INDONESIAN CITIZENS'

TAXPAYER IDENTIFICATION NUMBERS). Rewang Rencang : Jurnal Hukum Lex Generalis., 5(12).

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. Jurnal Informasi Dan Teknologi, 5(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Fauzi, E., & Shandy, N. A. R. (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

Gunadi, C. G., Subiran, D., Lee, E. P., Gunawan, L. A., & Baretta, N. (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. Proceeding of Conference on Law and Social Studies.

Hertianto, M. R. (2021). Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia. Kertha Patrika, 43(1), 93. https://doi.org/10.24843/KP.2021.v43.i01.p07

Ikhsano, A., Sutanto, D. F., & Stellarosa, Y. (2023). Communication Strategy of the Ministry of Communication and Information Technology in Preventing the Spread of Hoax on Social Media. Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia, 8(1), 208–216. https://doi.org/10.25008/jkiski.v8i1.750

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus : Hacker Bjorka). Jurnal Bidang Penelitian Informatika, 1(1), 57–64. https://ejournal.kreatifcemerlang.id/index.php/jbpi/article/view/78

Oktaviani, S., Dewata, Y. J., & Fadlian, A. (2021). PERTANGGUNG JAWABAN PIDANA KEBOCORAN DATA BPJS DALAM PERSPEKTIF UU ITE. De Juncto Delicti: Journal of Law, 1(2), 146–157. https://doi.org/10.35706/djd.v1i2.5732

Pasaribu, A. M. F. (2017). Kejahatan Siber Sebagai Dampak Negatif Dari Perkembangan Teknologi Dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Persfektif Hukum Pidana. Journal of Chemical Information and Modeling.

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. Matra Pembaruan, 6(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14

Priliasari, E. (2023). PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA . Jurnal RechtsVinding, 12(2), 261–279.

Rahmawati, I. (2017). The Analysis Ofcyber Crime Threat Risk

Management to Increase Cyber Defense. Jurnal Pertahanan Dan Bela Negara, 7(2), 37–52. https://doi.org/10.33172/jpbh.v7i2.193

Rianarizkiwati, N. (2020). Kebebasan Informasi versus Hak atas Privasi Tanggung Jawab Negara dalam Perlindungan Data Pribadi. Infermia Publishing.

Riyadi, G. A., & Suriaatmadja, T. T. (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

Rosadi, S. D. (2015). Aspek Data Privasi Menurut Hukum Internasional, Regional, Dan Nasional. Refika Aditama.

Rosidah, I., Gunardi, Priatna Kesumah, & Royke Bahagia Rizka. (2023). TRANSPARASI DAN AKUNTABILITAS DALAM PENCEGAHAN FRAUD DIINSTANSI PEMERINTAH (STUDI KASUS KANTOR KEC. CIWIDEY). Jurnal Ekonomi Manajemen Bisnis Dan Akuntansi : EMBA, 2(1), 137–156. https://doi.org/10.59820/emba.v2i1.110

Siahaan, A. L. S. (2022). URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI: Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances. Majalah Hukum Nasional, 52(2), 209–223. https://doi.org/10.33331/mhn.v52i2.169

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. https://doi.org/10.38043/jah.v6i1.4484

Ukurta, R., & Dahana, C. D. (2023). Sanksi Administratif Dan Pidana Pasca Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Kertha Desa, 11(4), 2180–2188.