UNES LAW REVIEW
+62 813 6511 8590
+62 813 6511 8590
https://review-unes.com/
uneslawreview@gmail.com

DOI: https://doi.org/10.31933/unesrev.v5i4
Diterima: 21/05/2023, Diperbaiki: 12/06/2023, Diterbitkan: 13/07/2023

TINJAUAN YURIDIS TERHADAP EFEKTIVITAS PENANGANAN KEJAHATAN SIBER TERKAIT PENCURIAN DATA PRIBADI MENURUT UNDANG-UNDANG NO. 27 TAHUN 2022 OLEH KOMINFO

Muhammad Yudistira[1], Ramadani[2]

[1]Fakultas Syariah dan Hukum, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: yudisyudis032@gmail.com

[2]Fakultas Syariah dan Hukum, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: ramadani@uinsu.ac.id

***Corresponding Author*: Muhammad Yudistira**

ABSTRACT

Law Number 27 of 2022 concerning Personal Data Protection was passed by the President of the Republic of Indonesia on October 17, 2022 with the main aim of protecting people's personal data managed by electronic system operators (PSE), such as the Ministry of Communication and Information Technology (Kominfo), as well as preventing crimes committed by irresponsible individuals. The need to address the problem of data leakage is the main focus that must be addressed immediately with a definite and secure solution. With the enactment of this personal data protection law, it is expected to be an effective solution in dealing with the problem of personal data leakage that often occurs in Indonesia. This Personal Data Protection Act was created with the aim of protecting the privacy rights of individuals. The Academic Paper of the Personal Data Protection Law explains that "the right to privacy through the protection of personal data is a key element for individual freedom and dignity". Therefore, this personal data protection regulation is enacted to safeguard the interests of the public to avoid misuse of their personal data. The author applies a normative juridical approach method that involves analyzing each writing, rules, and its application, Kominfo collaborates with the Siberkreasi movement to provide digital education to the public. The goal is for people to be smarter in sorting information, not easily influenced by hoaxes, and less dependent on information that cannot be ascertained. Kominfo continues to collaborate with the police in law enforcement related to the spread of hoaxes. Cyber security has a very important role in protecting data security. This is because of the importance of maintaining the information stored and ensuring the data transmitted remains safe.

***Keywords**: Law; Personal Data, Protection, Cyber*

ABSTRAK

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi disahkan oleh Presiden Republik Indonesia pada 17 Oktober 2022 dengan tujuan utama melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik (PSE), seperti Kementerian Komunikasi dan Informatika (Kominfo), serta mencegah kejahatan yang dilakukan oleh individu yang tidak bertanggung jawab. Kebutuhan untuk mengatasi masalah kebocoran data menjadi fokus utama yang harus segera diatasi dengan solusi yang pasti dan aman. Dengan berlakunya undang-undang perlindungan data pribadi ini, diharapkan dapat menjadi solusi efektif dalam menangani masalah kebocoran data pribadi yang sering terjadi di Indonesia. Undang-Undang Perlindungan Data Pribadi ini dibuat dengan tujuan melindungi hak privasi individu. Naskah Akademik Undang-Undang Perlindungan Data Pribadi menjelaskan bahwa "hak atas privasi melalui perlindungan data pribadi merupakan elemen kunci bagi kebebasan dan martabat individu". Oleh karena itu, regulasi perlindungan data pribadi ini diberlakukan untuk menjaga kepentingan masyarakat agar terhindar dari penyalahgunaan data pribadi mereka. penulis menerapkan metode pendekatan yuridis normatif yang melibatkan analisis terhadap setiap tulisan, aturan, dan penerapannya, Kominfo bekerja sama dengan gerakan Siberkreasi untuk memberikan pendidikan digital kepada masyarakat. Tujuannya adalah agar masyarakat menjadi lebih cerdas dalam memilah informasi, tidak mudah terpengaruh oleh hoaks, dan tidak terlalu bergantung pada informasi yang belum dapat dipastikan kebenarannya. Kominfo terus berkolaborasi dengan kepolisian dalam penegakan hukum terkait penyebaran hoaks. Keamanan siber memiliki peran yang sangat penting dalam melindungi keamanan data. Hal ini dikarenakan pentingnya menjaga informasi yang disimpan dan memastikan data yang dikirimkan tetap aman.

Kata Kunci: Hukum; Data Pribadi, Perlindungan, Siber

PENDAHULUAN

Di Indonesia, perkembangan kejahatan di dunia maya telah mencapai tingkat yang mengkhawatirkan, sehingga negara ini sering disebut sebagai negara dengan tingkat kejahatan internet yang tinggi. Pada tahun 2002, Kepolisian Indonesia berhasil mengungkap 109 kasus tindak pidana Teknologi Informasi (TI), yang melibatkan 124 tersangka yang merupakan warga negara Indonesia dan melakukan aksi mereka di berbagai kota di Indonesia. Secara umum, kejahatan terkait dengan teknologi informasi dapat diklasifikasikan ke dalam dua kategori. Pertama, kejahatan yang bertujuan merusak atau menyerang sistem atau jaringan komputer. Kedua, kejahatan yang menggunakan komputer atau internet sebagai alat untuk melakukan tindakan kejahatan. Ada banyak literatur dan situs yang membahas berbagai jenis kejahatan siber yang terjadi. Beberapa contoh kejahatan umum yang memanfaatkan teknologi antara lain penipuan kartu kredit, penipuan di pasar saham, penipuan di sektor perbankan, penyebaran pornografi anak, perdagangan narkoba, dan terorisme. Sementara itu, kejahatan yang melibatkan penggunaan teknologi informasi meliputi defacing, cracking, dan phreaking.[1]

[1] ANA MARIA F.PASARIBU, "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* 53, no. 9 (2017): 1689–99.

Di zaman digital yang sekarang, terdapat banyak tindak kejahatan yang menggunakan data pribadi sebagai alat atau sasaran, sehingga perlindungannya perlu ditingkatkan. Sayangnya, banyak orang tidak menyadari bahwa informasi pribadi mereka rentan disalahgunakan oleh pihak yang tidak bertanggung jawab. Di Indonesia, kurangnya upaya perlindungan data telah mengakibatkan serangkaian insiden peretasan dan kebocoran data yang meluas. Kejadian-kejadian semacam ini merupakan bentuk kejahatan di dunia digital, seperti peretasan akun media sosial dan pencurian identitas, yang memiliki potensi untuk mengakibatkan pelanggaran data pribadi, pemerasan, dan penipuan online. Kesadaran akan pentingnya regulasi yang mengatur perlindungan data pribadi secara bertahap mulai diperhatikan oleh pemerintah, yang tercermin dalam upaya mereka untuk menyusun dan mengesahkan Undang-Undang Nomor 27 tahun 2022.[2]

Kesulitan dalam menangani tindak kejahatan cyber dengan mengandalkan hukum positif konvensional sangatlah besar. Ini disebabkan karena kejahatan tersebut melibatkan lima faktor yang saling terkait, yaitu pelaku kejahatan, korban kejahatan, reaksi sosial terhadap kejahatan, dan hukum. Meskipun hukum memiliki peran penting dalam mencegah dan mengatasi kejahatan, menciptakan peraturan hukum yang sesuai dengan perkembangan teknologi informasi yang cepat bukanlah hal yang mudah. Oleh karena itu, seringkali peraturan hukum menjadi usang dengan cepat saat mengatur bidang yang terus berubah, seperti teknologi informasi, sehingga terjadi kekosongan hukum. Hal ini tampaknya juga terjadi dalam menghadapi kejahatan di internet atau *cyber crime*.[3]

Indonesia perlu memiliki persiapan yang memadai dalam menghadapi kejahatan siber *(cyber crime)*. Salah satu persiapan yang penting adalah sumber daya manusia yang kompeten dan memiliki pengetahuan serta keterampilan dalam bidang keamanan siber. Sumber daya manusia yang berkualitas dapat menciptakan cara berpikir yang positif terhadap perubahan lingkungan global, meningkatkan kesadaran terhadap perkembangan teknologi dan informasi, serta memahami berbagai dampak yang timbul dalam kehidupan masyarakat terkait dengan ancaman siber. Selain itu, Indonesia juga perlu memiliki fasilitas produksi pengamanan negara yang memadai. Fasilitas ini mencakup infrastruktur dan teknologi yang diperlukan untuk mendeteksi, mencegah, dan menanggulangi serangan siber. Investasi dalam pengembangan fasilitas produksi pengamanan negara yang mutakhir dan efektif menjadi penting guna menghadapi ancaman kejahatan siber yang semakin kompleks dan terus berkembang.Dengan memperkuat sumber daya manusia dan fasilitas produksi pengamanan negara, Indonesia dapat meningkatkan kemampuannya dalam menghadapi kejahatan siber. Ini melibatkan pendidikan dan pelatihan yang memadai untuk tenaga ahli keamanan siber, serta pengembangan dan

[2] Albert Lodewyk Sentosa Siahaan, "Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi," Majalah Hukum Nasional 52, no. 2 (2022): 210–22, https://doi.org/10.33331.

[3] ana Maria F.Pasaribu, "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* 53, no. 9 (2017): 1689-1699.

peningkatan infrastruktur teknologi yang dapat mengidentifikasi, melindungi, dan merespons serangan siber dengan cepat dan efektif.[4]

Perlindungan hukum terhadap data pribadi merupakan kebutuhan yang penting bagi setiap individu, dan tanggung jawab untuk melindungi hak-hak dasar tersebut harus diemban oleh negara sebagai lembaga yang membuat kebijakan. Sebagaimana yang telah ada di undang-undang no. 27 tahun 2022 yang menimbang :

1. Bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
2. Bahwa pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi
3. Bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi diperlukan pengaturan mengenai pelindungan data pribadi dalam suatu undang-undang

Berdasarkan beberapa permasalahan yang telah disampaikan di atas, maka rumusan masalah yang dapat diangkat dalam penulisan artikel ini adalah;

1. Bagaimana peran Kementerian Komunikasi dan Informatika dalam mengatasi masalah kejahatan siber terkait pencurian data pribadi?
2. Bagaiana Kementerian Komunikasi dan Informatik memberikan perlindungan yang memadai bagi korban kejahatan siber terkait pencurian data pribadi?
3. Apakah UU No. 27 Tahun 2022 sudah memadai dalam memenuhi tuntutan masyarakat dan perkembangan teknologi informasi terkait penanganan kejahatan siber terkait pencurian data pribadi?

METODE PENELITIAN

Dalam penelitian ini, penulis menerapkan metode pendekatan yuridis normatif yang melibatkan analisis terhadap setiap tulisan, aturan, dan penerapannya. Selain itu, penelitian juga mencakup studi kepustakaan atau literatur yang melibatkan analisis terhadap buku, jurnal, paper, dan media. Metode pendekatan yuridis normatif adalah suatu pendekatan yang merujuk pada hukum dan peraturan perundang-undangan yang berlaku. Dalam penelitian ini, penulis menggunakan bahan hukum yang relevan yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

HASIL DAN PEMBAHASAN

Peran Kementerian Komunikasi Dan Informatika Dalam Mengatasi Kajahatan Siber Terakait Pencurian Data Pribadi

[4] Ineu Rahmawati, "The Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense," Jurnal Pertahanan & Bela Negara 7, no. 2 (October 3, 2017): 51–66,.

Menurut Didik M. Arief Mansur dan Elisatris Gultom, kemajuan teknologi informasi dapat diamati dari peningkatan penggunaan internet. Meskipun penggunaan internet yang meningkat dapat memberikan dampak positif, namun dampak negatif yang disebabkan oleh kemajuan teknologi juga sangat banyak, bahkan seringkali berkaitan dengan tindakan pidana. Mereka berpendapat bahwa kelahiran kejahatan dunia maya (*cyber crime*) disebabkan oleh kurangnya kemampuan atau pengetahuan dari aparat penegak hukum dalam menangani kasus-kasus siber.[5] Kemajuan yang pesat dalam Teknologi Informasi memungkinkan manusia untuk tidak hanya melakukan aktivitas di dunia nyata, tetapi juga melakukan aktivitas melalui internet yang beroperasi secara virtual. Hal ini memungkinkan manusia untuk melakukan aktivitas di dunia maya atau siber[6]

Perkembangan teknologi informasi telah mengubah hampir semua aspek kehidupan. Di satu sisi, teknologi komputer memberikan keuntungan seperti kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan demokrasi, serta keuntungan lainnya. Namun, di sisi lain, teknologi ini dapat merusak kehidupan nyata yang telah kita jalani selama ini dengan segala masalah yang harus dihadapi sebelum kita melangkah lebih jauh ke dalam dunia maya yang kompleks. Bagi mereka yang memanfaatkan teknologi informasi untuk bisnis, pelayanan publik, dan hiburan media dengan membangun situs yang dapat diakses oleh masyarakat, perlu berhati-hati. Tidak semua orang yang mengunjungi dunia maya menikmati realitas virtual yang ditawarkan oleh situs-situs tersebut. Seperti kehidupan nyata, di dunia maya juga terdapat kejahatan yang dapat berdampak pada kehidupan nyata

Kejahatan siber menjadi ancaman serius dalam kehidupan manusia, yang menghadirkan tantangan bagi organisasi pemerintah dalam mengatasi kejahatan yang terjadi dalam lingkungan teknologi komputer. Dampak buruk dari kejahatan siber ini dirasakan oleh masyarakat secara luas. Hal ini disebabkan oleh kurangnya pemahaman tentang jenis kejahatan yang terjadi di ruang internet dan kekurangan perlindungan serta keamanan data pribadi yang tidak lagi efektif. Selama ini, perangkat dan sumber daya tambahan yang diperlukan untuk mengatasi masalah kejahatan siber tidak selalu tersedia. Oleh karena itu, diperlukan upaya yang lebih kuat untuk mengatasi masalah kejahatan siber *(cybercrime).*

Menteri Komunikasi dan Informatika telah mengumumkan bahwa Undang-Undang Perlindungan Data Pribadi ini mengatur hak-hak subjek data pribadi, yaitu individu yang memiliki data pribadi, serta subjek-subjek yang terkait dengan pemrosesan data pribadi seperti operator dan pengolah data pribadi. Undang-Undang ini juga mencakup pembentukan lembaga perlindungan data pribadi dan penerapan pembatasan terhadap pemrosesan data. Dalam rangka penegakan hukum, Undang-Undang ini memberlakukan dua jenis sanksi, yaitu sanksi administratif dan sanksi pidana, bagi pelanggar. Dengan adanya Undang-Undang Perlindungan Data Pribadi ini, diharapkan terbentuk kerangka hukum yang jelas dan kuat dalam menangani

[5] Sahat Maruli T. Situmeang, Cyber Law,(Bandung : penerbit Cakra, 2020), h. 28.
[6] danrivanto budhijanto, Cyberlaw Dan Revolusi Industri 4.0 – Literasi Digital, (Bandung : Logoz Publishing 2019),h 26.

kasus kebocoran data pribadi, serta memberikan sanksi yang tegas bagi pelanggar. Tujuan utamanya adalah meningkatkan keamanan dan perlindungan terhadap data pribadi di Indonesia.[7]

Keamanan siber memiliki peran yang sangat penting dalam melindungi keamanan data. Hal ini dikarenakan pentingnya menjaga informasi yang disimpan dan memastikan data yang dikirimkan tetap aman. Keamanan siber bertujuan untuk melindungi infrastruktur digital dari ancaman siber. Ini melibatkan perlindungan ganda terhadap catatan dan struktur data dari akses yang tidak sah melalui prinsip-prinsip kerahasiaan, integritas, otentikasi, non-penolakan, dan ketersediaan. Dengan adanya keamanan siber yang baik, kita dapat terhindar dari serangan siber yang berpotensi merugikan. Pendekatan yang dilakukan mencakup kombinasi kemampuan keamanan, deteksi, dan respons untuk menyediakan sistem yang terlindungi dan mampu merespons kejadian-kejadian yang mungkin terjadi.

Tantangan lain dalam penyempurnaan kebijakan keamanan siber adalah sifat ancaman siber yang multidimensi. Hal ini mengakibatkan penanggulangannya tidak hanya menjadi tanggung jawab TNI atau Polri, tetapi melibatkan berbagai kementerian seperti Kementerian Pertahanan dan Kementerian Komunikasi dan Informatika. Menurut Sjafrie Sjamsoeddin, ancaman siber termasuk dalam kategori ancaman asimetris yang membutuhkan pendekatan yang komprehensif. Karena sifat multidimensinya, keamanan siber melibatkan tidak hanya satu departemen, tetapi juga berbagai departemen lainnya. Oleh karena itu, diperlukan kebijakan keamanan siber atau pertahanan siber, yang dalam pelaksanaannya memerlukan kerangka koordinasi yang baik.[8]

Tingginya jumlah kasus kebocoran data pribadi di Indonesia menunjukkan adanya kekosongan hukum dalam penanganan kasus-kasus semacam itu. Sebelumnya, perlindungan data tersebar di berbagai peraturan perundang-undangan tanpa adanya regulasi khusus yang mengaturnya. Kondisi ini mendorong pemerintah untuk segera mengesahkan Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. Setelah menunggu sejak tahun 2019, RUU Perlindungan Data Pribadi akhirnya disetujui dan dijalankan sebagai Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-Undang ini bertujuan untuk mendukung hak individu dalam melindungi data pribadi, meningkatkan kesadaran akan perlindungan data pribadi, serta menjamin dukungan dan penghormatan terhadap perlindungan data pribadi.

Sanksi merupakan konsekuensi yang diberikan sebagai akibat dari pelanggaran peraturan atau norma yang berlaku. Sanksi tersebut digunakan sebagai alat kekuasaan untuk mendorong kepatuhan terhadap peraturan dan mengurangi kerugian akibat pelanggaran. Konsep sanksi administratif tidak secara jelas didefinisikan dalam undang-undang, sehingga terdapat berbagai pengertian yang berbeda-beda. Namun, secara umum, sanksi administratif dianggap sebagai akibat negatif dari pelanggaran tugas administratif dan bertujuan untuk menegakkan kepatuhan terhadap hukum.Penerapan sanksi administratif tidak terlepas dari prosedur umum untuk mengembalikan ketertiban, menjamin kepastian hukum, dan melindungi setiap individu.

[7] regina Ukurta, "Sanksi Administratif Dan Pidana Pasca Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," Jurnal Kertha Desa 11, no. 4 (2022).
[8] Febyola Indah, Arista Sidabutar, and Nurul Annisa, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus : Hacker Bjorka)," *Jurnal Bidang Penelitian Informatika* 1, no. 1 (2022).

Terdapat beberapa tujuan dari penerapan sanksi administratif dalam undang-undang. Pertama, sebagai upaya penegakan hukum untuk menindak pelanggaran norma peraturan perundang-undangan. Kedua, sanksi administratif digunakan untuk menghukum pelanggar dan memberikan efek jera agar tidak mengulangi pelanggaran di masa mendatang. Ketiga, sanksi administratif juga berfungsi sebagai langkah preventif untuk mencegah orang lain melakukan pelanggaran hukum. Sanksi administratif dalam konteks hukum administrasi diatur dalam Bab VIII pasal 57, yang mengatur pelaksanaan otoritas pemerintah dan wewenang. Pasal tersebut memberikan dasar hukum untuk memberlakukan sanksi administratif sebagai bentuk penegakan hukum dalam ranah administrasi.

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi telah disahkan oleh Presiden Republik Indonesia pada 17 Oktober 2022 dengan tujuan melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik (PSE) yaitu kominfo dan mencegah penyalahgunaan oleh individu yang tidak bertanggung jawab. Pentingnya menangani masalah kebocoran data harus menjadi fokus utama dan segera ditemukan solusi yang pasti dan aman. Hal ini dikarenakan kemajuan teknologi dan internet yang terus berkembang dan selalu menyertai adanya kejahatan di dalamnya. Perlindungan data menjadi kebutuhan masyarakat untuk menciptakan keamanan dalam berinteraksi dengan teknologi dan internet. Kejahatan siber memiliki dampak yang signifikan terhadap individu, kelompok, dan negara. Kerugian tersebut dapat mencakup bidang ekonomi, perbankan, politik, bahkan keamanan nasional.

Dengan berlakunya undang-undang perlindungan data pribadi ini, diharapkan dapat menjadi solusi yang efektif dalam menangani permasalahan kebocoran data pribadi yang sering terjadi di Indonesia. Undang-Undang Perlindungan Data Pribadi dibuat dengan maksud untuk melindungi hak privasi individu. Dalam Naskah Akademik Undang-Undang Perlindungan Data Pribadi, dijelaskan bahwa "hak atas privasi melalui perlindungan data pribadi merupakan elemen kunci bagi kebebasan dan martabat individu". Oleh karena itu, tujuan dari pengesahan Regulasi perlindungan data pribadi ini untuk menjaga kepentingan masyarakat agar terhindar dari penyalahgunaan data pribadi mereka..[9]

Menurut laporan dari perusahaan keamanan siber Surfshark, sekitar 1,04 juta akun pengguna di Indonesia mengalami kebocoran data selama kuartal II 2022. Angka ini mengalami peningkatan signifikan sebesar 143% dibandingkan dengan kuartal I 2022, yang hanya mencapai 430,1 ribu akun. Surfshark juga mencatat bahwa setiap menitnya, terdapat tiga akun yang mengalami kebocoran data di Indonesia pada periode Januari–Maret 2022. Jumlah ini meningkat menjadi delapan akun per menit pada periode April–Juni 2022. Jika melihat tren yang ada, jumlah akun yang mengalami kebocoran data di Indonesia sejak kuartal I 2020 cenderung fluktuatif. Puncaknya terjadi pada kuartal II 2020, dengan 39,6 juta akun yang berhasil diretas oleh para hacker. Kemudian, jumlah akun yang mengalami kebocoran data mengalami penurunan menjadi 669,4 ribu pada kuartal II 2021, namun kembali meningkat pada kuartal III

[9] Riyadi and Toto Tohir Suriaatmadja, "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, no.1 (2023) 227-231

2021. Pada akhir tahun 2021 hingga tiga bulan pertama tahun 2022, terjadi penurunan kasus kebocoran data di Indonesia. Namun, pada kuartal II 2022, jumlah kasus kembali meningkat, seperti yang terlihat pada grafik. Secara global, sejak awal tahun 2020, sekitar 2,3 miliar akun telah mengalami kebocoran data. Bahkan, jumlahnya mencapai 5,1 miliar akun yang telah dilanggar sejak tahun 2004.[10]

Perlindungan bagi korban pencurian data pribadi

Kominfo bekerja sama dengan gerakan Siberkreasi untuk memberikan pendidikan digital kepada masyarakat. Tujuannya adalah agar masyarakat menjadi lebih cerdas dalam memilah informasi, tidak mudah percaya pada hoaks, dan tidak terlalu bergantung pada informasi yang belum dapat dipastikan kebenarannya. Kominfo terus berkolaborasi dengan kepolisian dalam penegakan hukum terkait hoaks. Namun, Indonesia masih kurang sadar dan peduli terhadap keamanan dan perlindungan data pribadi, Seperti yang telah diterapkan oleh negara-negara seperti Australia dan Singapura, kehadiran regulasi yang kuat sangat penting sebagai kerangka hukum untuk mengatur perlindungan data pribadi dan aktivitas perusahaan yang berbasis internet.[11]

Salah satu tindakan yang diambil pemerintah dalam menanggulangi dan mencegah kebocoran data pribadi masyarakat adalah melalui penerapan Konsep *Indonesian Data Protection System* (IDPS). IDPS merupakan sebuah sistem yang bertujuan untuk meminimalisasi kejahatan siber terutama dalam penyalahgunaan data dan informasi pribadi. IDPS digunakan untuk mengamankan data pribadi seseorang pada pusat data atau pusat pengumpulan data. Selain itu, IDPS juga bertujuan memastikan pengelolaan data dan informasi pribadi yang tepat melalui koordinasi yang ada dalam sistem ini. IDPS secara administratif terhubung dengan Kementerian komunikasi dan Informatika (Kominfo). IDPS memiliki dua elemen penting, yaitu pusat data atau otoritas data dan petugas data. Fungsi pusat data atau otoritas data adalah mengumpulkan dan melindungi semua data dan informasi pribadi yang dimasukkan oleh petugas data. Hal ini bertujuan untuk memudahkan koordinasi terkait data dan informasi pribadi yang dimiliki oleh seseorang.[12]

Di Indonesia, terjadi kasus baru-baru ini terkait kebocoran data pribadi pada perusahaan plat merah seperti PT PLN dan Indihome (Telkom). Diduga PT PLN telah mengalami kebocoran data pribadi sebanyak 17 juta konsumennya yang kemudian diungkapkan oleh seorang peretas melalui media sosial miliknya. Pelaku juga menawarkan berbagai jenis data pelanggan, seperti ID lapangan, ID pelanggan, nama konsumen, alamat, tipe energi, nomor meter, dan besaran KWh. Selanjutnya, sebanyak 26 juta data pribadi konsumen Indihome juga telah bocor dan dijual di forum peretas.. Akibat kebocoran data pribadi konsumen di PT PLN, muncul pertanyaan

[10] "Kasus Kebocoran Data Di Indonesia Melonjak 143% Pada Kuartal II 2022," accessed June 9, 2023, https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022.

[11] Adnan Madjid Wildan Akbar Hashemi Rafsanjani, Syaiful Anwar, "Strategy Ministry Of Communication And Information For Help In," Jurnal Damai Dan Resolusi Konflik 6, no. 2 (2020): 233–50.

[12] Aryo Fadlian Akbari Amarul Zaman, Jumadi Anwar, "Pertanggung Jawaban Pidana Kebocoran Data Bpjs Dalam Perspektif Uu Ite," De Juncto Delictio 1, no. 2 (2008): 146–57.

tentang keamanan data pribadi konsumen yang telah terkumpul. Apakah data pribadi konsumen tersebut benar-benar aman atau justru berada dalam posisi rentan untuk diretas.[13]

Ancaman penyalahgunaan data pribadi di Indonesia semakin meningkat, terutama sejak diluncurkannya program KTP elektronik (e-KTP) oleh pemerintah. Program ini pertama kali diperkenalkan pada awal tahun 2011 sebagai bagian dari implementasi Nomor Induk Kependudukan (NIK). Tujuan dari program ini adalah menciptakan identitas tunggal bagi setiap penduduk, yang berlaku seumur hidup, dengan satu kartu untuk setiap individu yang mencantumkan NIK. Dalam pelaksanaan program e-KTP, pemerintah melakukan perekaman data pribadi penduduk, termasuk identitas dan ciri-ciri fisik mereka. Perekaman ciri-ciri fisik dilakukan melalui pemindaian sidik jari dan retina mata, yang nantinya akan digunakan untuk validasi biometrik pemegang KTP. Menurut informasi dari Kementerian Dalam Negeri, data yang terekam kemudian dienkripsi menggunakan algoritma kriptografi tertentu sebelum disimpan dalam chip di dalam e-KTP. Namun, kekhawatiran muncul terkait potensi penyalahgunaan data pribadi yang tercatat dalam e-KTP jika keamanannya tidak memadai. Data pribadi yang tersimpan dalam e-KTP bisa disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab jika mekanisme keamanannya tidak kuat atau rentan terhadap serangan atau pencurian data. Penting bagi pemerintah dan pihak terkait untuk memastikan keamanan yang ketat dalam pengelolaan dan pengamanan data pribadi yang terekam dalam e-KTP untuk melindungi privasi dan mencegah penyalahgunaan data oleh pihak yang tidak berwenang.[14]

Pada bulan Januari 2022, beberapa insiden kebocoran data menjadi perhatian publik. Salah satunya adalah insiden kebocoran data di Bank Indonesia yang telah dikonfirmasi oleh Badan Siber dan Sandi Negara (BSSN). Kejadian ini melibatkan 16 komputer di Kantor Cabang Bank Indonesia di Bengkulu yang mengalami kebocoran data. Pada bulan yang sama, terjadi juga kebocoran data terhadap calon pelamar kerja di PT *Pertamina Training and Consulting* (PTC). yang merupakan anak perusahaan dari Pertamina. Data yang terungkap meliputi informasi pribadi dari pelamar, seperti nama lengkap, nomor telepon, alamat rumah, tanggal dan tempat lahir, ijazah, kartu BPJS, transkrip akademik, dan *curriculum vitae.* Selanjutnya, ada juga kasus kebocoran data pribadi yang dilakukan oleh seorang peretas yang dikenal sebagai Hacker Bjorka. Bjorka melakukan serangan terhadap data dan situs resmi yang dimiliki oleh Pemerintah, serta melakukan tindakan doxing terhadap beberapa pejabat negara, termasuk Menteri Komunikasi dan Informatika Jhonny G Plate, Ketua DPR RI Puan Maharani, dan Menteri BUMN Erick Thohir. Tindakan ini mengungkapkan informasi pribadi pejabat negara tersebut secara tidak sah dan melanggar privasi mereka.[15]

[13] Gillang Achmad Riyadi and Toto Tohir Suriaatmadja, "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, no. 1 (2023): 227–231,

[14] Mexsasai Indra Emilda Firdausa, "Tanggung Jawab Negara Terhadap Perlindungan Data Pribadi Di Indonesia Dalam Perspektif Hak Asasi Manusia" IX, no. 2 (2016): 1–23.

[15] Elfian Fauzi and Alif Radika, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," Lex Renaissanee 7, no. 3 (2022): 445–461.

Urgensi Undang-Undang No 27 Tahun 2022 Dalam Memenuhi Tuntutan Masyarakat Dalam Perkembangan Teknnologi Dan Pencurian Data Pribadi

Menurut Kementerian Komunikasi dan Informatika, Undang-Undang Perlindungan Data Pribadi (UU PDP) akan membuka era baru dalam pengelolaan data pribadi di era digital Indonesia. UU ini secara substansial terdiri dari 18 bab dan 78 pasal yang mengatur berbagai aspek, termasuk transfer data pribadi, sanksi administratif, lembaga penegak hukum, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa, hukum acara, larangan penggunaan data pribadi, ketentuan pidana, serta ketentuan peralihan dan penutup.

Perlindungan data pribadi tidak dapat dipisahkan dari perlindungan hak asasi manusia yang mendasar. Dalam konteks perkembangan teknologi informasi dan ekonomi digital yang pesat di Indonesia, terdapat berbagai dampak negatif, termasuk ancaman terhadap hak privasi dan data pribadi individu. Beberapa negara telah mengakui perlindungan data sebagai hak konstitusional atau melalui konsep habeas data, yang memberikan seseorang hak untuk melindungi dan membenarkan data pribadinya ketika terjadi kesalahan. Hak atas perlindungan data pribadi bukan hanya penting, tetapi juga merupakan elemen kunci dalam menjaga harga diri dan kebebasan individu. Dengan perlindungan data yang efektif, hal ini dapat menjadi pendorong kuat bagi terwujudnya kebebasan politik, spiritual, dan keagamaan.

Berdasarkan peristiwa kegagalan perlindungan data pribadi yang telah terjadi, seringkali pengendali data pribadi baru mengetahui tentang adanya tindakan yang tidak sah atau melawan hukum terhadap data pribadi setelah tindakan tersebut terjadi atau setelah berita tentang peristiwa tersebut menjadi terkenal. Hal ini menyebabkan kurangnya tindakan yang optimal dilakukan oleh pengendali data pribadi.Tidak jarang pula terjadi bahwa pengendali data pribadi menyangkal adanya tindakan yang tidak sah atau melawan hukum terhadap data yang mereka kendalikan, meskipun ada bukti publik yang menunjukkan bahwa data pribadi telah diambil secara tidak sah atau melawan hukum oleh pihak peretas. Kondisi seperti ini membuat pengendali data pribadi tidak memiliki banyak pilihan untuk bertindak guna menyelamatkan data pribadi atau menjaga reputasi keamanan sistem perlindungan data yang mereka miliki.[16]

Berdasarkan hasil wawancara yang dilakukan dengan beberapa konsultan teknologi strategi siber dan privasi data, dapat disimpulkan bahwa perlindungan data pribadi dianggap penting dan merupakan bagian dari Hak Asasi Manusia. Oleh karena itu, diperlukan perlindungan dan kepastian hukum yang jelas terkait hal ini. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang disahkan pada Oktober 2022, merupakan langkah awal yang diambil oleh Pemerintah Indonesia untuk memberikan perlindungan dan kepastian hukum terkait data pribadi. Undang-Undang tersebut secara tidak langsung juga melindungi warga negara Indonesia dari penggunaan data pribadi yang tidak sah, yang dapat menyebabkan kerugian finansial dan merusak reputasi. Sebelum disahkan Undang-Undang Perlindungan Data Pribadi, Indonesia telah memiliki sejumlah peraturan sektoral yang mengatur perlindungan data pribadi. Misalnya, dalam sektor perbankan dan telekomunikasi, terdapat Undang-Undang

[16] M Rafifnafia Hertianto, "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia," Kertha Patrika 43, no. 1 (2021): 93,

Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik..[17]

implementasi pengamanan data dan keamanan siber, narasumber menjelaskan bahwa setiap sektor memiliki kebutuhan dan tujuan yang berbeda, serta perhatian yang berbeda terhadap area tersebut. Sebagai konsultan, narasumber menyarankan agar organisasi yang menjadi pengendali atau prosesor data pribadi melakukan penilaian kesenjangan *(gap assessment)* guna memahami kondisi dan posisi keamanan yang dimiliki oleh organisasi tersebut. Setelah itu, organisasi dapat merancang sebuah roadmap implementasi perlindungan data pribadi.Roadmap tersebut dapat mencakup langkah-langkah seperti penerapan consent management (pengelolaan persetujuan), praktik *records of processing activities (ROPA)* untuk mencatat aktivitas pemrosesan data pribadi, praktik *data protection impact assessment (DPIA*) untuk menilai dampak privasi, pembuatan *privacy notice atau privacy policy*, serta penunjukan *data protection officer (DPO)* atau pejabat perlindungan data pribadi. Roadmap ini biasanya dirancang untuk periode 2 hingga 5 tahun, disesuaikan dengan kebutuhan dan kemampuan organisasi. Selain itu, narasumber juga menjelaskan bahwa penting bagi organisasi untuk terus memantau perkembangan regulasi dan standar keamanan data pribadi, serta melibatkan semua pihak terkait, termasuk pimpinan organisasi, departemen teknologi informasi, keuangan, dan hukum. Melalui kerja sama dan kolaborasi antar departemen, organisasi dapat menciptakan lingkungan yang aman dan mematuhi aturan yang berlaku dalam perlindungan data pribadi. Narasumber juga menekankan pentingnya pendidikan dan pelatihan kepada karyawan mengenai kesadaran privasi dan keamanan siber. Hal ini dapat membantu meningkatkan pemahaman mereka tentang praktik yang benar dalam pengelolaan dan perlindungan data pribadi. Kesimpulannya, implementasi pengamanan data dan keamanan siber perlu disesuaikan dengan kebutuhan dan tujuan setiap sektor. Roadmap implementasi yang jelas dan melibatkan semua pihak terkait, serta pendidikan dan pelatihan kepada karyawan, merupakan langkah penting dalam menjaga keamanan dan perlindungan data pribadi.

Perlindungan data pribadi sebagai bagian dari perlindungan diri pribadi Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di dalamnya termasuk hak atas kepastian dan pengendalian atas data pribadi yang dimilikinya. undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan undang-undang yang secara khusus mengatur perlindungan data pribadi di Indonesia. Undang-undang ini memberikan perlindungan dan mengatur hak subjek data pribadi, termasuk hak untuk mendapatkan informasi tentang identitas yang jelas, dasar hukum kepentingan, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data pribadi. Selain itu, undang-undang ini juga memberikan hak kepada subjek data pribadi untuk

[17] Joko Widarto Cindy Vania, Markoni, Horadin Saragih, "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber," Jurnal Multidisiplin Indonesia 2, no. 3 (2023): 654–666.

mengakhiri pemrosesan, menghapus, atau memusnahkan data pribadi tentang dirinya. Subjek data pribadi juga memiliki hak untuk mengajukan gugatan dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi yang dilakukan terhadapnya.Undang-undang ini juga mendorong pencegahan kejahatan dengan melihat akar masalah kejahatan tersebut. Metode yang digunakan dalam upaya pencegahan kejahatan tersebut bersifat nonpenal, yang berarti tidak melibatkan sanksi pidana. Tujuan utamanya adalah mencegah terjadinya pelanggaran pemrosesan data pribadi dan melindungi hak-hak subjek data pribadi. Dengan adanya Undang-Undang Perlindungan Data Pribadi, pemerintah Indonesia berusaha memberikan perlindungan dan kepastian hukum bagi subjek data pribadi, serta mencegah terjadinya kejahatan dalam pengelolaan data pribadi dengan mengatasi akar masalah kejahatan tersebut.

Untuk memastikan perlindungan data pribadi yang efektif, sangat penting untuk menetapkan hak-hak dan kewajiban yang jelas bagi badan hukum yang mengelola data tersebut melalui undang-undang Perlindungan Data Pribadi. Pemrosesan data pribadi harus dilakukan secara terbatas dan spesifik, berdasarkan dasar hukum yang sah, dan transparan sesuai dengan tujuan yang ditetapkan. Hal ini harus memastikan bahwa hak-hak subjek data pribadi dihormati secara akurat, dengan menggunakan program mutakhir yang dapat dipertanggungjawabkan, dengan tujuan melindungi keamanan data pribadi. Setelah masa retensi atau masa pemrosesan data berakhir, data pribadi harus dihapus atau dimusnahkan, baik dalam bentuk elektronik maupun non-elektronik. Namun, terdapat pengecualian berdasarkan peraturan khusus yang diatur oleh instansi pengawas dan pengatur sektor terkait, yang mungkin mempengaruhi penghapusan data pribadi sesuai dengan permintaan subjek data pribadi. Salah satu upaya untuk memaksimalkan perlindungan data pribadi adalah melalui penggunaan alat pemrosesan data dalam fasilitas publik, seperti keamanan, pencegahan bencana, pengelolaan lalu lintas, dan analisis lalu lintas. Informasi tentang lokasi pemasangan alat pemroses atau pengolah data harus disediakan kepada publik. Manajer data pribadi, melalui asosiasi mereka, dapat menetapkan kode etik dalam pengelolaan data pribadi, baik secara inisiatif asosiasi maupun atas permintaan lembaga terkait. Dengan mengatur hak-hak dan kewajiban yang jelas, memastikan pemrosesan data yang sesuai, dan mengambil langkah-langkah perlindungan yang diperlukan, diharapkan bahwa perlindungan data pribadi dapat terjamin dengan baik..[18]

KESIMPULAN

Keamanan siber memiliki peran yang sangat penting dalam melindungi keamanan data. Hal ini dikarenakan pentingnya menjaga informasi yang disimpan dan memastikan data yang dikirimkan tetap aman. Keamanan siber bertujuan untuk melindungi infrastruktur digital dari ancaman siber. Ini melibatkan perlindungan ganda terhadap catatan dan struktur data dari akses yang tidak sah melalui prinsip-prinsip kerahasiaan, integritas, otentikasi, non-penolakan, dan ketersediaan. Dengan adanya keamanan siber yang baik, Anda dapat terhindar dari serangan siber yang berpotensi merugikan

[18] Wiwin Yulianingsih Yuly Sari kartika, "KAJIAN YURIDIS TINDAK PIDANA PEMALSUAN IDENTITAS DATA DIRI DALAM SITUS BANTUAN KARTU PRAKERJA Oleh:," *Jurnal Rectum* 5, no. 2 (2023): 1–15.

Menteri Komunikasi dan Informasi telah mengumumkan bahwa Undang-Undang ini mengatur hak subyek data pribadi, yaitu individu yang memiliki data pribadi, serta subjek yang terkait dengan pemrosesan data pribadi, operator dan pengolah data pribadi, pembentukan lembaga perlindungan data pribadi, dan penerapan pembatasan. Undang-Undang ini juga memberlakukan dua jenis sanksi bagi pelanggar, yaitu sanksi administratif dan sanksi pidana. Dengan adanya Undang-Undang Perlindungan Data Pribadi ini, diharapkan akan tercipta kerangka hukum yang jelas dan kuat dalam menangani kasus kebocoran data pribadi, serta memberikan sanksi yang tegas bagi pelanggar. Hal ini diharapkan dapat meningkatkan keamanan dan perlindungan terhadap data pribadi di Indonesia

Kominfo bekerja sama dengan gerakan Siberkreasi untuk memberikan pendidikan digital kepada masyarakat. Tujuannya adalah agar masyarakat menjadi lebih cerdas dalam memilah informasi, tidak mudah percaya pada hoaks, dan tidak terlalu bergantung pada informasi yang belum dapat dipastikan kebenarannya. Ketiga, Kominfo terus berkolaborasi dengan kepolisian dalam penegakan hukum terkait hoaks. Namun, Indonesia masih kurang sadar dan peduli terhadap keamanan dan perlindungan data pribadi, seperti yang telah dilakukan oleh negara-negara seperti Australia dan Singapura

Menurut Kementerian Komunikasi dan Informatika, Undang-Undang Perlindungan Data Pribadi (UU PDP) akan membuka era baru dalam pengelolaan data pribadi di era digital Indonesia. UU ini secara substansial terdiri dari 18 bab dan 78 pasal yang mengatur berbagai aspek, termasuk transfer data pribadi, sanksi administratif, lembaga penegak hukum, kerjasama internasional, partisipasi masyarakat, penyelesaian sengketa, hukum acara, larangan penggunaan data pribadi, ketentuan pidana, serta ketentuan peralihan dan penutup.

DAFTAR PUSTAKA

Akbari Amarul Zaman, Jumadi Anwar, Aryo Fadlian. “PERTANGGUNG JAWABAN PIDANA KEBOCORAN DATA BPJS DALAM PERSPEKTIF UU ITE.” *De Juncto Delictio* 1, no. 2 (2008): 146–57.

Albert Lodewyk Sentosa Siahaan. “URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI.” *Majalah Hukum Nasional* 52, no. 2 (2022): 210–22. https://doi.org/10.33331.

ANA MARIA F.PASARIBU. “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* 53, no. 9 (2017): 1689–99.

Cindy Vania, Markoni, Horadin Saragih, Joko Widarto. “TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DARI ASPEK PENGAMANAN DATA DAN KEAMANAN SIBER.” *Jurnal Multidisiplin Indonesia* 2, no. 3 (2023): 654–66. https://doi.org/10.58344/jmi.v2i3.157.

danrivanto budhijanto. *Cyberlaw Dan Revolusi Industri 4.0*, 2019. http://literasidigital.id/books/cyberlaw-dan-revolusi-industri-4-0/.

Emilda Firdausa, Mexsasai Indra. “TANGGUNG JAWAB NEGARA TERHADAP PERLINDUNGAN DATA PRIBADI DI INDONESIA DALAM PERSPEKTIF HAK

ASASI MANUSIA" IX, no. 2 (2016): 1–23.

Fauzi, Elfian, and Alif Radika. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissanee* 7, no. 3 (2022): 445–61.

Hertianto, M Rafifnafia. "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia." *Kertha Patrika* 43, no. 1 (2021): 93. https://doi.org/10.24843/kp.2021.v43.i01.p07.

Indah, Febyola, Arista Sidabutar, and Nurul Annisa. "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus : Hacker Bjorka)." *Jurnal Bidang Penelitian Informatika* 1, no. 1 (2022).

"Kasus Kebocoran Data Di Indonesia Melonjak 143% Pada Kuartal II 2022." Accessed June 9, 2023. https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022.

Rahmawati, Ineu. "THE ANALYSIS OFCYBER CRIME THREAT RISK MANAGEMENT TO INCREASE CYBER DEFENSE." *Jurnal Pertahanan & Bela Negara* 7, no. 2 (October 3, 2017): 51–66. https://doi.org/10.33172/jpbh.v7i2.193.

Riyadi, Gillang Achmad, and Toto Tohir Suriaatmadja. "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, no. 1 (2023): 227–31. https://doi.org/10.29313/bcsls.v3i1.4945.

Sahat Maruli T. Situmeang. *Cyber Law*. *Cv. Cakra*, 2020. https://doi.org/10.1016/j.clsr.2006.10.006.

Ukurta, Regina. "SANKSI ADMINISTRATIF DAN PIDANA PASCA DISAHKANNYA UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI." *Jurnal Kertha Desa* 11, no. 4 (2022).

Wildan Akbar Hashemi Rafsanjani, Syaiful Anwar, Adnan Madjid. "STRATEGY MINISTRY OF COMMUNICATION AND INFORMATION FOR HELP IN." *Jurnal Damai Dan Resolusi Konflik* 6, no. 2 (2020): 233–50.

Yuly Sari kartika, Wiwin Yulianingsih. "KAJIAN YURIDIS TINDAK PIDANA PEMALSUAN IDENTITAS DATA DIRI DALAM SITUS BANTUAN KARTU PRAKERJA Oleh:" *Jurnal Rectum* 5, no. 2 (2023): 1–15.