

ANALISIS PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA PENCURIAN DATA PRIBADI DI INDONESIA

Sultan Fathan Azhari¹⁾, Listyowati Sumanto²⁾

Magister Ilmu Hukum, Universitas Trisakti^{1,2}

11001241002325@std.trisakti.ac.id¹, p.listyowati@trisakti.ac.id²

Abstract: The development of information technology in the digital era has brought significant impacts on people's lives, one of which is the increasing risk of personal data theft. This research aims to analyze the effectiveness of law enforcement against perpetrators of personal data theft in Indonesia using the Lawrence M. Friedman legal system theory approach, specifically focusing on the element of legal substance. This study uses a normative juridical research type and is descriptive in nature. Secondary data is analyzed qualitatively. Conclusions are drawn using deductive logic. The research results indicate that despite the availability of relatively complete legal instruments, there are still various obstacles in their implementation, including unclear legal norms, weak criminal sanctions, the unavailability of supporting technical regulations, and a lack of comprehensive integration among regulations governing personal data protection. Through an analysis of several actual cases, it was found that there is disparity in the imposition of sanctions and the legal system has not been optimal in providing a deterrent effect for perpetrators. Therefore, reformulation of legal substance and harmonization of regulations are necessary to address the challenges of personal data protection in the digital era comprehensively and effectively.

Keywords: Law Enforcement, Personal Data Protection, Legal System.

Abstrak: Perkembangan teknologi informasi di era digital telah membawa dampak signifikan terhadap kehidupan masyarakat, salah satunya adalah meningkatnya risiko pencurian data milik pribadi. Penelitian ini bertujuan untuk menganalisis efektivitas penegakan hukum terhadap pelaku tindak pidana pencurian data pribadi di Indonesia dengan menggunakan pendekatan teori sistem hukum Lawrence M. Friedman, khususnya pada elemen substansi hukum. Penelitian ini menggunakan tipe penelitian yuridis normatif dan bersifat deskriptif. Data sekunder dianalisis secara kualitatif. Penarikan kesimpulan menggunakan logika deduktif. Hasil penelitian menunjukkan bahwa meskipun telah tersedia instrumen hukum yang relatif lengkap, masih terdapat berbagai kendala dalam implementasinya, termasuk ketidakjelasan norma hukum, lemahnya sanksi pidana, belum tersedianya aturan teknis pendukung, dan belum adanya integrasi menyeluruh antar peraturan yang mengatur perlindungan data pribadi. Melalui analisis terhadap sejumlah kasus aktual, ditemukan adanya disparitas dalam penjatuhan sanksi dan belum optimalnya sistem hukum dalam memberikan efek jera bagi pelaku. Oleh karena itu, reformulasi substansi hukum dan harmonisasi regulasi diperlukan guna menjawab tantangan perlindungan data pribadi di era digital secara komprehensif dan efektif.

Kata Kunci: Penegakan Hukum; Perlindungan Data Pribadi, Sisteme Hukum

A. Pendahuluan

Pada zaman Modern yang ditandai dengan akselerasi perkembangan ilmu pengetahuan dan teknologi telah mentransformasikan interaksi sosial dan ekonomi pada masyarakat global. Fenomena ini secara garis besar dipengaruhi oleh berkembangnya teknologi internet yang sangat masif. Evolusi teknologi internet telah merubah gaya hidup, cara bersosialisasi, dan mengubah kebiasaan cara bertansaksi pada kehidupan sehari-hari. Manifestasi kemajuan teknologi internet dapat dilihat dengan munculnya berbagai macam platform dan media

digital dalam mempermudah kegiatan kehidupan sehari-hari, beberapa platform tersebut antara lain hadirnya media sosial, pasar elektronik (*E-Commerce*), platform dompet digital (*E-Wallet*), dan internet atau mobile banking. Secara khusus, kehadiran media sosial telah membuat kehidupan menjadi lebih mudah dan praktis.

Walaupun kehadiran teknologi informasi membawa perubahan yang sangat signifikan dalam kehidupan sehari-hari, perkembangan teknologi pun berjalan seiring dengan berkembangnya jenis dan tipologi tindak pidana yang menargetkan data pribadi milik user atau pengguna sebagai objek tindak pidananya. Data pribadi yang kini menjadi aset berharga, semakin sering menjadi target tindak pidana, contohnya adalah pencurian data pribadi. Insiden pencurian data pribadi dapat menimbulkan kerugian signifikan bagi korban, mulai dari kerugian finansial, pencemaran nama baik, hingga potensi penyalahgunaan penyalahgunaan untuk melakukan tindak pidana yang lebih serius. Hal ini pun menandakan bahwasannya kehadiran sistem informasi/teknologi informasi memiliki dampak positif dan negatif.

Indonesia saat ini masih menjadi target serangan kejahatan siber berupa pencurian data pribadi. Berdasarkan data yang dihimpun oleh APJII, pada tahun 2022, jumlah pengguna internet di Indonesia mencapai angka mengejutkan, sebanyak 210 juta individu. Dalam upaya mengakses internet, masyarakat mengandalkan berbagai perangkat elektronik, seperti Smartphone, laptop, tablet, dan jam pintar. Menariknya, sebanyak 93,5% dari populasi tersebut aktif berpartisipasi dalam berbagai platform media sosial.

Sebagai contoh, dikutip dari Kompas.com, seperti yang terjadi pada tahun 2023 di Kabupaten Garut, sejumlah 407 warga terdiri dari enam Rukun Warga Desa Sukabakti, Kecamatan Tarogong Kidul, Kabupaten Garut, Jawa Barat telah menjadi korban dari pinjaman atau kredit fiktif yang tidak pernah mereka ajukan kepada PT. Pemodal Nasional Madani (PNM). Oleh karena itu, muncul indikasi bahwasannya terjadi pencurian data pribadi yang dialami oleh warga Desa Sukabakti pada saat proses verifikasi dan pendaftaran data kepada PT. Pemodal Nasional Madani (PNM). Menyikapi semakin masif dan maraknya kasus pencurian data milik pribadi di Indonesia, Pemerintah Indonesia telah membuat Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain Undang-Undang Perlindungan Data Pribadi, Pemerintah juga masih memiliki beberapa Undang-undang yang mengatur tentang data pribadi, yaitu Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan Peraturan Pemerintah Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Data Transaksi Elektronik. Dalam ketiga peraturan ini, belum mengatur secara spesifik dan rinci tentang perlindungan data pribadi masyarakat luas.

Berdasarkan beberapa contoh kasus data pribadi diatas. Walaupun Indonesia sudah memiliki instrumen hukum tentang perlindungan Data Pribadi, kasus pencurian data pribadi di Indonesia masih sangat masif terjadi. Hal ini mengindikasikan bahwasannya masih lemahnya penegakan hukum terhadap para pelaku Pencurian data pribadi, serta masih lemahnya implementasi penegakan hukum mengenai perlindungan data pribadi di Indonesia. Berdasarkan permasalahan diatas, penulis merumuskan permasalahan yang ingin dikaji yaitu: Bagaimana Efektivitas Penegakan Hukum terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. Dalam kajian ini, penulis melakukan kajian yang tidak sama dengan kajian-kajian sebelumnya. Adapun beberapa kajian yang menjadi acuan penulis dalam menulis dan melakukan penelitian ini antara lain: 1) Lili Ekayani dkk, Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (*Phising*) Di Lingkungan Perbankan, Jurnal Off Philosophy (JOP), Vol 4, No 1, 2023. dengan kesimpulan bahwa beberapa faktor yang menyebabkan efektivitas perlindungan hukum

nasabah terhadap kejahatan tindakan phising di lingkungan perbankan yaitu Faktor pengetahuan nasabah tentang apa itu phising masih sangat rendah, Faktor sarana & prasarana berupa teknologi, faktor psikologis masyarakat, faktor budaya privasi & faktor pendidikan dan pengetahuan nasabah yang rendah sehingga masih sangat diperlukan edukasi tentang bahaya kejahatan siber, dan 2) Adindaa Lolaa Sarianii, Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia, Jurnal Ilmu Sosial, Politik, dan Hukum Al-Dalil, Vol 2, No 2, 2024. Dengan kesimpulan bahwa Penegakan hukum terhadap tindak pidana siber di Indonesia dalam era informasi digital menghadapi tantangan yang banyak. Meskipun kemajuan teknologi memberikan banyak kebaikan namun juga memfasilitasi terjadinya kejahatan siber yang meresahkan masyarakat, seperti pencurian data, penipuan online, dan perdagangan ilegal. Ancaman tersebut mengancam sektor ekonomi dan keamanan nasional, serta membawa resiko bagi pertumbuhan ekonomi. Kerja sama antara pemerintah, swasta & masyarakat dalam melindungi keamanan dan kedaulatan negara dari ancaman siber semakin diperkuat, termasuk dengan mengadopsi kebijakan dan regulasi serta pendirian Badan Siber dan Sandi Negara (BSSN).

B. Metodologi Penelitian

Dalam Artikel ini, Penulis menggunakan tipe penelitian yuridis normatif. dengan spesifikasi penelitian deskriptif. Selanjutnya mengenai menggunakan Sumber Data yaitu Data Sekunder. Teknik pengumpulan data menggunakan Metode Pengumpulan Data dengan cara Studi Kepustakaan atau (library research) Analisis data dilakukan dengan cara kualitatif. Penarikan kesimpulan memakai logika deduktif adalah metode berpikir yang dimulai dari premis atau pernyataan umum untuk mencapai kesimpulan yang bersifat khusus.

C. Hasil dan Pembahasan dan Analisa

Kasus-kasus Pencurian data pribadi di Indonesia sangat marak dan masif, namun diantara beberapa kasus yang disebutkan di bawah ini, ada beberapa kasus yang sudah berkekuatan hukum tetap berupa vonis pengadilan, Dan dalam beberapa kasus di bawah ini, para pelaku pencurian data pribadi sudah dijerat dan divonis menggunakan instrument hukum Uddang-Udang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Beberapa contoh konkret kasus-kasus, tersebut antara lain:

Kasus Pencurian Data Pribadi Warga Desa Sukabakti Kabupaten Garut, Sebanyak 407 warga di Kabupaten Garut yang terdiri dari enam Rukun Warga desa Sukabakti, Kecamatan Tarogong Kidul, Kabupaten Garut, Jawa Barat menjadi korban dari pinjaman atau kredit palsu dari PT. Pemodal Nasional Madani (PNM) yang belum tidak ajukan. Para warga masyarakat yang masih dalam satu desa kaget saat mengetahui bahwasannya nama-nama mereka terdata sebagai peminjam, dengan nilai yang beragam mulai dari Rp850.000 (delapan ratus ribu rupiah) rupiah sampai Rp2.000.000 (dua juta rupiah). Berdasarkan kasus tersebut, muncul indikasi bahwasannya terjadi pencurian data pribadi yang dialami oleh warga Desa Sukabakti tersebut pada saat proses verifikasi dan pendaftaran data kepada PT. Pemodal Nasional Madani (PNM). Sebagai respons, banyak warga membuat surat pernyataan resmi kepada desa bahwa mereka tidak pernah berutang kepada PNM. Sebanyak 407 warga telah melaporkan kasus ini ke pihak desa.

Menurut Sinta, seorang warga yang menjadi korban, keanehan ini pertama kali dialami oleh Bu Ayu yang diberitahu oleh saudaranya bahwa namanya tercatat memiliki utang di sebuah lembaga penyalur dana ("bank emok"). Padahal, Bu Ayu memastikan tidak pernah melakukan pinjaman, namun tercatat memiliki tunggakan sekitar Rp850 ribu. Sinta menambahkan bahwa tagihan yang diterima warga bervariasi antara Rp800 ribu hingga Rp2 juta. Ia merasa bingung kenapa muncul hutang yang belum pernah ia ajukan dan menngira ada penyalahgunaan data oleh pihak yang tidak berhak, dengan dugaan 560 Kartu Keluarga (KK)

yang terdampak.

Data dari Desa Sukabakti mencatat 407 warga yang dilaporkan memiliki pinjaman namun tidak merasa pernah berutang. Pihak desa dan PNM kini bekerja sama untuk menyelidiki masalah ini. Kepala Desa Sukabakti, Wawan Gunawan, mengungkapkan hasil penelusurannya yang mengarah pada dugaan bahwa sudah terjadi pencurian data pribadi yang dialami ratusan warga desa yang pelakunya adalah Ketua Program PNM Mekaar. Kepolisian Resor Garut telah membuka posko pengaduan untuk masyarakat yang telah menjadi korban pinjaman atau hutang fiktif dari PNM.

Kepala Kepolisian Resor Garut (Kapolres) Rohman Yonky Dilatha, menyatakan bahwa penyelidikan terkait kasus ini terus dilakukan dan posko pengaduan telah dibuka di tingkat Polsek dan Polres. AKBP Rohman Yonky Dilatha menyampaikan bahwa polisi telah menerima informasi mengenai banyaknya warga Desa Sukabakti yang terjerat pinjaman fiktif dari PNM. Meskipun demikian, sampai dengan saat ini belum ada pelaporan resmi dari masyarakat yang merasa menjadi korban pencatutan identitas untuk pengajuan pinjaman ke PNM. Pihak kepolisian masih menunggu laporan resmi sebagai dasar untuk tindakan lebih lanjut.

Kasus Penipuan Menggunakan Data Pribadi Milik Orang Lain Yang Dilakukan Andi Irma Malasari, Dalam kasus ini, Andi Irma Malasari, selaku supervisor penjualan pada sebuah perusahaan telekomunikasi, terdiri dari pemberian insentif berupa bonus guna mengapai target penjualan kartu SIM dalam jumlah besar. Guna meningkatkan pendapatannya, yang bersangkutan berbuat tindakan penipuan. Bukannya mendistribusikan kartu SIM kepada konsumen yang sah, Andi berkolusi dengan seorang pihak eksternal bernama Raja Firdaus untuk meregistrasi kartu SIM yang belum terjual dengan menggunakan Nomor Induk Kependudukan (NIK) hasil pencurian. Raja Firdaus secara berkala, yakni setiap tiga hingga enam bulan, memberikan kepada Andi sejumlah NIK curian yang diperoleh melalui jaringan orang dalam di salah satu perusahaan telekomunikasi.

Kasus Kebocoran Data BPJS Ketenagakerjaan, Pada awal bulan Maret tahun 2023, jagat maya di Indonesia dihebohkan dengan munculnya laporan mengenai dugaan kebocoran data dalam skala masif yang sedang terjadi pada Badan Penyelenggara Jaminan Sosial (BPJS) Ketenagakerjaan. Seorang individu atau kelompok yang menggunakan nama samaran "Bjorka" menjadi pusat perhatian. Melalui berbagai forum daring dan kanal media sosial, Bjorka mengklaim telah berhasil mengakses dan mencuri sejumlah besar data pribadi milik para peserta BPJS Ketenagakerjaan.

Rincian Data yang Diklaim Bocor: Menurut klaim yang dilontarkan oleh Bjorka, jumlah data yang berhasil diperoleh mencapai sekitar 19,5 juta catatan pengguna. Informasi yang diduga kuat telah jatuh ke tangan pihak yang tidak berwenang ini mencakup detail-detail sensitif seperti: a) Nomor Induk Kependudukan (NIK); b) Nama lengkap peserta; c) Alamat surat elektronik (email); d) Nomor telepon seluler; e) Tanggal lahir; f) Nomor Kartu Peserta Jamsostek (KPJ); dan g) Status keaktifan kepesertaan.

Menanggapi isu kebocoran data yang mencuat dan menimbulkan keresahan di masyarakat, pihak BPJS Ketenagakerjaan segera mengeluarkan pernyataan resmi. Dalam pernyataan tersebut, mereka menegaskan akan melakukan investigasi internal secara menyeluruh dan intensif untuk memverifikasi kebenaran dari klaim kebocoran data yang beredar. Pada tahap awal, respons dari BPJS Ketenagakerjaan cenderung berhati-hati, tidak secara langsung mengakui skala kebocoran seperti yang diklaim oleh peretas, namun mereka tidak menampik adanya potensi insiden keamanan yang sedang diselidiki.

Serangan Ransomware Pusat Data Nasional Sementara, Pada bulan Juni tahun 2024, sebuah insiden keamanan siber yang sangat mengkhawatirkan terjadi pada Pusat Data Nasional Sementara (PDNS) yang berlokasi di Soerabaya. PDNS adalah infrastruktur teknologi informasi yang sangat penting karena berfungsi sebagai pusat penyimpanan data dan

aplikasi untuk berbagai layanan publik yang diselenggarakan oleh pemerintah. Kelompok peretas yang bertanggung jawab atas serangan ini berhasil diidentifikasi sebagai Brain Cipher, sebuah kelompok yang dikenal aktif dalam melakukan serangan ransomware. Adapun kronologi lengkap terkait kasus diatas sebagai berikut:

Ariandi Putra, perwakilan Badan Siber dan Sandi Negara (BSSN), menyatakan bahwa masalah tersebut bermula pada 17 Juni 2024 dan mencapai titik tertinggi ketika Hacker mengatasnamakan sebagai peretas menulis tebusan senilai 8 juta dolar AS. Lebih lanjut, Ariandi menjelaskan bahwa BSSN mendeteksi adanya usaha untuk mematikan fitur security Windows Defender sejak 17 Juni 2024 pukul 23.15 WIB, yang membuka celah bagi tindakan berbahaya. Pernyataan ini disampaikan pada Senin, 24 Juni 2024. Menurut Ariandi, modus operandi ransomware ini adalah dengan melumpuhkan sistem keamanan Windows Defender agar dapat menginstal file berbahaya. Setelah berhasil masuk pada 17 Juni, kegiatan yang mencurigakan sudah ditemukan pada 20 Juni 2024 pukul 00.54, termasuk mengizinkan penginstallan file yang sangat berbahaya, menghapus data sangat penting, dan menghentikan beberapa layanan. Akibatnya, beberapa file yang berhubungan dengan penyimpanan seperti VSSs, Hyper V Volume, VirtualDisk, dan Veeam vPower NFS menjadi nonaktif dan tidak berfungsi. Melalui postingan di akun Instagram resmi @ditjen_imigrasi pada Kamis sore, Direktorat Jenderal Imigrasi Kementerian Hukum dan HAM menginformasikan bahwa gangguan pada Pusat Data Nasional Kementerian Komunikasi dan Informatika mempengaruhi seluruh layanan keimigrasian.

Hingga kini, Ariandi menyatakan bahwa tim BSSN masih berusaha melakukan kegiatan penelusuran mendalam terhadap bukti-bukti forensik, walaupun menghadapi banyak kendala sedikitnya bukti. Salah satu hambatannya adalah bukti-bukti yang terenkripsi oleh ransomware. Kendati demikian, Ariandi mengungkapkan bahwa BSSN telah berhasil mengidentifikasi asal serangan ransomware, yaitu Brain Cipher Ransomware, yang merupakan evolusi dari ransomware Lockbit 3.0. Sampel ransomware ini akan segera dianalisis lebih lanjut dengan melibatkan lembaga keamanan siber lainnya. Senada dengan perwakilan BSSN, Menteri Komunikasi dan Informatika, Budia Arie Setiadi, menginformasikan bahwa pelaku peretasan PDN menulis tebusan senilai 8 juta dolar AS. Tetapi, ia dengan tegas menyatakan jika pemerintah tidak akan membayar atau memenuhi tuntutan yang diajukan oleh hacker. Penegasan ini disampaikan Budi Arie kepada wartawan setelah menghadiri Sidang Kabinet Paripurna tentang Perekonomian di Istana Kepresidenan Jakarta pada hari Senin. Budi menyampaikan jika gangguan pada pusat layanan publik saat ini sudah berhasil diatasi. Lebih lanjut, ia menyatakan bahwa serangan ransomware yang menargetkan PDNS 2 sedang dalam proses evaluasi.

Serangan ransomware terhadap PDNS ini memiliki dampak yang sangat luas dan signifikan terhadap berbagai layanan publik di Indonesia. Beberapa layanan penting yang mengalami gangguan akibat serangan ini termasuk sistem keimigrasian (menyebabkan kendala pada proses imigrasi di berbagai bandara), layanan kependudukan dan pencatatan sipil, serta berbagai layanan online lainnya yang mengandalkan data dan infrastruktur dari PDNS. Gangguan ini menyebabkan ketidaknyamanan dan bahkan kerugian bagi masyarakat. Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kominfo) dan Badan Siber dan Sandi Negara (BSSN) segera mengambil tindakan untuk merespons dan mengatasi serangan ransomware ini. Tim teknis dari berbagai instansi dikerahkan untuk melakukan upaya pemulihan sistem yang terenkripsi dan melakukan investigasi forensik untuk mengidentifikasi akar penyebab serangan serta potensi kerentanan dalam sistem PDNS. Pemerintah juga secara tegas menyatakan kebijakan untuk tidak membayar tebusan kepada kelompok penyerang.

Pada dasarnya, penegakan hukum pada intinya merupakan proses dalam mewujudkan konsep keadilan, kepastian hukum dan kebaikan sosial. Selain itu, setiap masyarakat Indonesia

memiliki hak terhadap perlindungan hukum dari negara. Hukum pidana berfungsi untuk menentukan jenis-jenis perbuatan yang dianggap melanggar norma sosial dan hukum, serta menetapkan larangan terhadap perbuatan-perbuatan tersebut, dilengkapi dengan ancaman pemberian sanksi pidana bagi pihak-pihak yang melanggarinya. Dalam hal ini, tujuan pemidanaan tidak hanya berfokus pada pemberian balasan terhadap pelanggaran yang telah terjadi, tetapi juga mencakup pertimbangan mengenai dampak jangka Panjang serta efektifitas pemidanaan terhadap pelaku dan masyarakat secara keseluruhan. Oleh karena itu, persoalan pemidanaan harus dipahami sebagai bagian dari upaya membentuk tatanan sosial yang lebih baik di masa depan. Secara umum, tujuan dari adanya hukum pidana adalah untuk menciptakan keamanan, ketertiban, serta melindungi kepentingan masyarakat dan individu. Selain itu, Tujuan hukum pidana adalah untuk melindungi kepentingan individu dari tindakan sewenang-wenang penguasa.

Berdasarkan temuan hasil penelitian diatas, dapat diketahui bahwasannya. Kebijakan baru pemerintah dalam hal pengaturan mengenai perlindungan data milik pribadi di Indonesia saat ini telah diatur dalam Undang-undang nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Tetapi sebelum Indonesia memiliki Undang-undang nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, peraturan mengenai perlindungan data pribadi tersebut di berbagai macam peraturan Perundang-undangan. Sebelum membahas permasalahan pokok, terlebih dahulu kita harus mengetahui pengertian atau makna dari perlindungan data pribadi itu sendiri. Perlindungan terhadap keamanan data pribadi merupakan salah satu perwujudan dari hak pribadi yang sudah diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, pengertian mengenai hak pribadi yaitu:

- 1) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari berbagai macam gangguan
- 2) Hak pribadi merupakan hak bisa berkomunikasi dengan orang lain tanpa tindakan dimata-mata
- 3) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi.

Berdasarkan hasil di atas diketahui bahwasannya Indonesia sudah memiliki beberapa instrument hukum tentang Perlindungan Data Pribadi beserta Sanksi hukum Pidana terhadap pencurian data pribadi. Namun pada kenyataannya, sebelum Indonesia memiliki Undang-undang Perlindungan Data Pribadi, pemberlakuan sanksi Pidana Terhadap Pelaku Pencurian data pribadi hanya diatur di Undang-Undang No. 19 Tahun 2016e yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, belum mengatur secara spesifik mengenai sanksi Pidana Terhadap pelaku pencurian data pribadi baik pelaku secara individu, maupun pelaku secara korporasi dalam hal ini penyelenggara sistem elektronik.

Hal ini menjadi kelemahan terhadap penegakan hukum mengenai pencurian data pribadi sebelum disahkannya Undang-undang Perlindungan Data Pribadi. Setelah Undang-Undang No. 19 Tahun 2016e yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang No. 19 Tahun 2016e yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik perlindungan data pribadi disahkan, kasus pencurian data pribadi di Indonesia masih belum menunjukkan trend penurunan, yang terjadi adalah, kasus pencurian data pribadi masih mengalami peningkatan pasca disahkannya Undang-undang perlindungan data pribadi. Hal tersebut dapat diketahui berdasarkan kasus-kasus yang sudah disebutkan diatas bahwasannya kasus pencurian data pribadi semakin marak terjadi, tetapi terjadi disparitas dalam penjatuhan sanksi pidana terhadap para pelaku berdasarkan uraian kasus diatas.

Dalam kerangka teori sistem hukum yang pernah dituliskan oleh Lawrence M. Friedman didalam bukunya yang berjudul *The Legal System: A Social Science Perspective*. pada bagian elemen Substansi hukum, ia mengungkapkan bahwa “*The substance is composed of substantive rules and also about how institutions should behave.*” Berdasarkan kerangka teori sistem hukum Lawrence M. Friedman pada elemen substansie hukum yang merujuk pada keseluruhan aturan hukum yang mengatur mengenai tindake pidanae pencurian data milik pribadi. Selain itu, Dalam Yang dimaksud dalam substansi hukum dalam teorinya Friedman ialah norma, pola prilaku dan norma dalam kehidupan manusia. Selain itu pula yang dimaksud substansi ialah aturan-aturan hukum seperti peraturan perundangg-undangann yang berlaku. Di Indonesia, Undange-Undange No. 19 Tahun 2016e yang merupakan perubahan atas Undange-Undange No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya menjadi fondasi utama dalam pengaturan tindak pidana di ranah siber, termasuk yang terkait dengan data pribadi Undange-Undange No. 19 Tahun 2016e yang merupakan perubahan atas Undange- Undange No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur mengenai tindak pidana *access illegale* (akses ilegal) dan penyalahgunaan data, yang secara tidak langsung memberikan perlindungan terhadap data pribadi.

Analisis Kasus BPJS berdasarkan perspektif teori Friedman. Struktur hukum mencakup institusi dan aktor yang menjalankan sistem hukum, seperti lembaga legislatif, eksekutif, yudikatif, serta badan administratif. Dalam konteks ini, Badan Penyelenggara Jaminan Sosial (BPJS) Ketenagakerjaan berperan sebagai Penyelenggara Sistem Elektronik (PSE) yang bertanggung jawab atas pengelolaan data peserta. Namun, insiden kebocoran data menandakan adanya indikasi kelemahan pada sistem keamanan informasi yang dikelola oleh BPJS Ketenagakerjaan. Hal ini mengindikasikan perlunya peningkatan kapasitas dan pengawasan terhadap lembaga-lembaga yang mengelola data pribadi masyarakat

Substansi hukum merujuk pada norma, aturan, dan kebijakan yang mengatur perilaku dalam masyarakat. Indonesia telah memiliki Undang- Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur kewajiban PSE dalam melindungi data pribadi. Namun, implementasi UU PDP masih menghadapi tantangan, terutama dalam penegakan hukum dan sanksi terhadap pelanggaran. Dalam kasus BPJS Ketenagakerjaan, belum ada kejelasan mengenai pertanggungjawaban hukum atas kebocoran data yang terjadi, yang mencerminkan adanya kesenjangan antara norma hukum dan pelaksanaannya

Budaya hukum mencerminkan sikap, nilai, dan pemahaman masyarakat terhadap hukum dan institusi hukum. Kasus kebocoran data BPJS Ketenagakerjaan mengindikasikan bahwa kesadaran masyarakat akan pentingnya perlindungan data pribadi masih minim. Masih banyaknya individu yang belum paham mengenai hak dan kewajiban mereka terkait data pribadi dan mekanisme pengaduan yang tersedia. Selain itu, budaya hukum di kalangan penyelenggara sistem elektronik juga perlu diperkuat, agar mereka lebih proaktif dalam memastikan keamanan data dan mematuhi regulasi yang berlaku. Dalam perspektif Friedman, ketiga komponen sistem hukum harus berjalan secara sinergis untuk menciptakan sistem hukum yang efektif. Insiden kebocoran data BPJS Ketenagakerjaan menunjukkan bahwa kelemahan dalam salah satu komponen dapat berdampak pada keseluruhan sistem. Oleh karena itu, diperlukan upaya terpadu untuk memperkuat struktur hukum melalui peningkatan kapasitas institusi, menyempurnakan substansi hukum dengan penegakan yang konsisten, dan membangun budaya hukum yang mendukung perlindungan data pribadi.

Analisis Kasus Serangan Ransomware Pusat Data Nasional Berdasarkan penjabaran pada bagian hasil penelitian, dapat diketahui bahwasannya Serangan Ransomware pada Pusat Data Nasional dalam perspektif teori Friedman dapat dianalisis sebagai berikut. Struktur Hukum Struktur hukum mencakup institusi dan aparat yang menjalankan sistem hukum. Dalam

kasus ini, Badan Siber dan Sandi Negara (BSSN) berperan sebagai lembaga utama dalam menangani insiden tersebut. Namun serangan ini mengungkap kelemahan koordinasi antarinstansi dan kurangnya kesiapsiagaan dalam menghadapi ancaman siber. Meskipun BSSN telah melakukan investigasi dan koordinasi dengan Kementerian Komunikasi dan Informatika serta pihak terkait lainnya, respons awal terhadap serangan menunjukkan perlunya peningkatan kapasitas dan sinergi dengan berbagai macam Lembaga.b. Substansi HukumSubstansi hukum mengacu pada norma, aturan, dan kebijakan yang mengatur perilaku dalam masyarakat. Indonesia telah memiliki Undangg- Undangg Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang mengatur kewajiban setiap Penyelenggaraesistem Elektronik (PSE) dalam melindungi data pribadi. Tetapi, implementasi UU PDP masih menghadapi tantangan, terutama dalam penegakan hukum dan sanksi terhadap pelanggaran. Dalam kasus PDNS, belum ada kejelasan mengenai pertanggungjawaban hukum atas kebocoran data yang terjadi, yang mencerminkan adanya kesenjangan antara norma hukum dan pelaksanaannya.c. Budaya HukumBudaya hukum mencerminkan sikap, nilai, dan pemahaman masyarakat terhadap hukum dan institusi hukum. Kasus serangan ransomware ini menunjukkan bahwa kepedulian akan pentingnya keamanan siber dan perlindungan data pribadi masih perlu ditingkatkan, baik di kalangan penyelenggara sistem elektronik maupun masyarakat umum. Selain itu, budaya hukum di kalangan penyelenggara sistem elektronik juga perlu diperkuat, agar mereka lebih proaktif dalam memastikan keamanan data dan mematuhi regulasi yang berlaku.

Analisis Kasus Pencurian Data Pribadi Warga Desa Sukabakti Kabupaten Garut Berdasarkan penjabaran pada bagian hasil penelitian, dapat diketahui bahwasannya Kasus Pencurian Data Pribadi Warga Desa Sukabakti Kabupaten Garut dalam perspektif teori Friedman dapat dianalisis sebagai berikut:a. Struktur HukumStruktur hukum mencakup institusi dan aparat yang menjalankan sistem hukum. Dalam kasus ini, PT PNM sebagai lembaga keuangan mempunyai tanggung jawab untuk menjaga kerahasiaan data pribadi nasabah. Namun, insiden pencurian data menandakan bahwa badanya kelemahan dalam sistem keamanan internal lembaga tersebut. Polisi juga telah membuka posko pengaduan untuk menindaklanjuti kasus ini, namun respons yang lambat dan kurangnya koordinasi antar lembaga menunjukkan adanya kelemahan dalam struktur hukum yang ada.b. Substansi HukumSubstansi hukum merujuk pada norma, aturan, dan kebijakan yang mengatur perilaku dalam masyarakat. Undangg- Undangg Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi dasar hukum dalam menangani pelanggaran terkait data pribadi. Namun, implementasi UU PDP masih dalam tahap transisi, dan belum ada sanksi yang tegas terhadap pelanggaran yang terjadi. Hal ini menghambat efektivitas perlindungan data pribadi di Indonesia.c. Budaya HukumBudaya hukum mencerminkan sikap, nilai, dan pemahaman masyarakat terhadap hukum dan institusi hukum. Kasus ini menunjukkan rendahnya kepedulian betapa pentingnya perlindungan data pribadi, baik di kalangan individu maupun pemerintahan baik swasta maupun pemerintah. Praktik penyalahgunaan data pribadi untuk keuntungan pribadi menunjukkan adanya kesenjangan dalam budaya kepatuhan terhadap hukum.

Analisis Kasus Andi Irma Malasari Berdasarkan penjabaran pada bagian hasil penelitian, dapat diketahui bahwasannya Kasus yang dilakukan oleh Andi Irma Malasari dalam perspektif teori Friedman dapat dianalisis sebagai berikut:a. Struktur HukumStruktur hukum mencakup institusi dan aparat yang menjalankan sistem hukum. Dalam kasus ini, aparat penegak hukum berhasil mengidentifikasi dan memproses pelanggaran terhadap Undang- Undang Perlindungan Data Pribadi, menunjukkan keberfungsiannya struktur hukum dalam menanggapi kejahatan siber. Substansi hukumSubstansi hukum merujuk pada norma, aturan, dan kebijakan yang mengatur perilaku dalam masyarakat. Undang- Undang Perlindungan Data Pribadi memberikan landasan hukum untuk melindungi data pribadi dan menetapkan

sanksi bagi pelanggarannya. Penerapan undang-undang ini dalam kasus Andi Irma menunjukkan bahwa substansi hukum telah mulai diimplementasikan untuk menanggulangi penyalahgunaan data pribadi. Budaya dan hukum mencerminkan sikap, nilai, dan persepsi masyarakat terhadap hukum dan institusi hukum. Kasus ini mengindikasikan bahwa kesadaran akan pentingnya perlindungan data pribadi masih perlu ditingkatkan, baik di kalangan individu maupun institusi. Praktik penyalahgunaan data pribadi untuk keuntungan pribadi menunjukkan adanya kesenjangan dalam budaya kepatuhan terhadap hukum.

Berdasarkan hasil analisis kasus di atas, Dalam penelitian ini Penulis menganalisis menggunakan elemen substansi hukum pada teori sistem hukum Friedman. Salah satu kelebihan dalam substansi hukum di Indonesia adalah adanya upaya untuk terus memperkuat kerangka regulasi. Pengesahan Rancangan Undang-Undang Perlindungan Data Pribadi (UU PDP) yang telah disahkan diharapkan bisa menjadi langkah maju yang signifikan. Undang-Undang Perlindungan Data Pribadi bertujuan untuk memberikan perlindungan yang lebih komprehensif terhadap data pribadi dengan mengatur secara lebih detail hak dan kewajiban pemilik data, pengelola data, serta cara penegakan hukum yang lebih efektif. Maka demikian, substansi hukum diharapkan menjadi lebih kuat dan relevan dengan perkembangan teknologi dan kebutuhan masyarakat. Namun pada implementasi di lapangan, Penegakan hukum kepada para pelaku tindak pidana pencurian data pribadi di Indonesia hingga kini masih menghadapi berbagai hambatan serius. Dalam pandangan teori sistem hukum Lawrence M. Friedman, ketidakefektifan tersebut dapat diidentifikasi secara lebih tajam melalui analisis pada elemen substansi hukum, yakni aturan, norma, dan perilaku resmi yang mengatur bagaimana aturan hukum seharusnya dijalankan. Beberapa penyebab tersebut antara lain:

Ketidakjelasan dan Ketidakkonsistensiannya Norma Hukum Elemen substansi hukum menurut Friedman meliputi produk hukum yang mengatur perilaku sosial. Dalam hal ini, substansi hukum Indonesia masih tidak jelas dalam mengatur pencurian data pribadi. Beberapa penyebabnya ialah:
a) Definisi Data Pribadi Yang masih sangat umum Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mendefinisikan apa itu data pribadi, definisi tersebut masih terlalu umum dan tidak mengantisipasi perkembangan jenis data baru seperti metadata, genetic data, dan behavioral data. Akibatnya, terjadi kesenjangan dalam perlindungan hukum terhadap berbagai bentuk data yang berkembang di era digital.
b) Ketidakjelasan Kualifikasi Tindak Pidana Undang-Undang Perlindungan Data Pribadi tidak secara spesifik mengkualifikasikan semua bentuk pencurian data pribadi sebagai tindak pidana. Sebagian besar delik baru berfokus pada pelanggaran administratif, dengan pengaturan tindak pidana terbatas pada pelanggaran tertentu, menyebabkan ruang abu-abu dalam pengkualifikasiannya tindakan kriminal.

Belum Idealnya Sanksi Hukum yang dimiliki Oleh Peraturan Perundang-Undangan Substansi hukum efektif harus menampilkan keseimbangan antara pelanggaran dan hukuman. Namun, dalam kasus pencurian data pribadi di Indonesia, Sanksi terhadap pelaku pencurian data pribadi menurut penulis belum memberikan Efek Jera. Hal ini dikarenakan ancaman pidana penjara dalam Undang-Undang Perlindungan Data Pribadi maksimal 6 tahun dan denda administratif maksimal 2% dari pendapatan tahunan. Hal ini dianggap masih terlalu ringan, terutama jika dibandingkan dengan besarnya kerugian yang ditimbulkan oleh kebocoran dan pencurian data. Ketidakproporsionalan ini mengurangi daya preventif dari hukum itu sendiri.

Tidak tersedianya Aturan teknis pendukung dan tambahan dalam Menjalankan Undang-undang Perlindungan Data Pribadi Dalam perspektif Friedman, substansi hukum tidak hanya berupa norma tertulis tetapi juga meliputi mekanisme operasional yang disediakan hukum. Di Indonesia, beberapa kekurangan tersebut antara lain:
a) Minimnya Aturan Pedoman Teknis Hingga saat ini, aturan pelaksana seperti peraturan pemerintah dan peraturan

mengenai pembentukan lembaga pelindung data pribadi belum tersedia untuk mendukung dan menjalankan Undang-Undang Perlindungan Data Pribadi. Hal ini menyebabkan proses penegakkan hukum dalam menjerat para pelaku tindak pidana pencurian data pribadi belum dapat dilakukan secara maksimal.b) Kurangnya Instrumen Pembuktian KhususBelum ada aturan substansial tentang bagaimana pembuktian dalam kasus pencurian data harus dilakukan, seperti keabsahan digital evidence, standar pembuktian dalam kejahatan siber, atau penggunaan ahli forensik digital dalam proses peradilan.

Substansi Hukum yang Belum Kontekstual dengan Perubahan Sosial Friedman menekankan bahwa substansi hukum harus menyesuaikan diri dengan dinamika sosial dan teknologi Tetapi dalam kenyataanya implementasi yang terjadi adalah:a.Regulasi Berbasis Paradigma KonvensionalBanyak ketentuan hukum masih berangkat dari paradigma perlindungan data ala sistem manual (arsip fisik), bukan berbasis realitas ekosistem digital seperti big data, artificial intelligence, dan cloud computing.b. Lambatnya Respons Lembaga Legislatif terhadap Perkembangan Ancaman BaruHukum di Indonesia belum responsif dalam mengantisipasi modus- modus baru pencurian data, seperti data scraping, social engineering, dan ransomware attacks.

Belum Terintegrasi Aturan Mengenai Perlindungan Data milik PribadiSelain di dalam Undang-Undang Perlindungan Data Pribadi, pengaturan perlindungan data pribadi juga masih tersebar dalam banyak peraturan perundang-undangan lainnya yaitu dalam Undang-Undang ITE, Undang- Undang Kesehatan, dan Undang-Undang Perbankan. Belum terintegrasi peraturan mengenai perlindungan data pribadi menyebabkan tumpang tindih dan kekosongan hukum dalam menjerat pelaku pencurian data lintas sektor.

Belum tersedianya infrastruktur siber yang kuatPelaksanaan di lapangan terkait UU PDP juga bergantung dariada infrastruktur siber di Indonesia yang kuat. Saat ini, baik lembaga pemerintahan dan pihak swasta masih kekurangan sumber daya manusia yang mumpuni dalam mengelola keamanan dan ketahanan siber terkait pengamanan data pribadi di Indonesia.

D. Penutup

Hukum pidana adalah bagian integral dari sistem hukum nasional yang berfungsi tidak hanya sebagai instrumen pembalasan atas pelanggaran hukum, tetapi juga sebagai sarana untuk membentuk tatanan sosial yang tertib dan adil. Dalam konteks perlindungan data milik pribadi di Indonesia, pengesahan oendang-oendang Perlindungan Data Pribadi (UU PDP) merupakan langkah signifikan menuju penguatan substansi hukum di ranah siber. Meskipun demikian, berdasarkan kerangka teori sistem hukum Lawrence M. Friedman, khususnya pada elemen substansi hukum, masih terdapat berbagai kelemahan yang menghambat efektivitas pelaksanaan hukum terhadap tindak pidana pencurian data pribadi. Kelemahan tersebut mencakup ketidakjelasan definisi data pribadi ketidaktegasan dalam mengkualifikasi bentuk-bentuk pencurian data sebagai tindak pidana, serta sanksi yang belum mencerminkan prinsip proporsionalitas dan efek jera. Selain itu, ketiadaan regulasi teknis pendukung, keterbatasan instrumen pembuktian digital, serta belum kontekstualnya regulasi dengan dinamika teknologi dan sosial modern semakin memperlemah daya operasional dari substansi hukum yang ada. Ditambah dengan belum terintegrasi berbagai ketentuan perlindungan data pribadi dalam sistem hukum nasional, menyebabkan terjadi tumpang tindih dan kekosongan hukum dalam praktiknya. Makae dari itu, dapat ditarik kesimpulan bahwa meskipun Indonesia sudah memiliki dasar hukum yang lebih kuat dalam bentuk UU PDP, efektivitasnya dalam melindungi data pribadi dan menindak pelaku pencurian data masih terganggu oleh kelemahan dalam elemen substansi hukum. Maka dari itu, diperlukan reformulasi dan harmonisasi regulasi yang lebih spesifik, adaptif, dan terintegrasi guna menjawab berbagai macam tantangan perlindungan data pribadi di era digital secara lebih komprehensif.

Daftar Pustaka

- Adinda, Lola Sariani. "Efektivitas Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *Jurnal Ilmu Sosial, Politik, dan Hukum Al-Dalil* 2, no. 2 (2024).
- Adi Arief, Wibawa. "Problematika Proses Penyelidikan TPPU Kejahatan dalam Perbankan." *Jurnal Globalisasi* 1, no. 2 (2024): 296.
- Anriyani, Dian. "Perbandingan Penyelesaian Sengketa Rahasia Dagang melalui Lembaga Arbitrase dan Pengadilan Negeri." *Jurnal Globalisasi Hukum* 2, no. 1 (2025): 48.
- Atmanegara, Eva Zahra, dan Elfrida Ratnawatie. "Upaya Penegakan Hukum Terkait Korban Penipuan Media Elektronik pada Masa Pandemi Covid-19." *Gorontalo Law Review* 6, no. 2 (2023): 234.
- Binsar Anggiat Simangunsong. "Ketidakselarasan Aturan Pemberian Wilayah Izin Usaha Pertambangan Khusus terhadap Badan Usaha Milik Organisasi Kemasyarakatan Keagamaan." *Jurnal Globalisasi Hukum* 2, no. 2 (2025): 330.
- CNN Indonesia. "Detik-Detik PDNS Diretas Lewat Windows Defender." 27 Juni 2024. <https://www.cnnindonesia.com/teknologi/20240626185721-192-1114570/detik-detik-pdns-diretas-lewat-windows-defende>. Diakses 28 April 2025 pukul 13.43.
- Disemadi, Hari Sutra, et al. "Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1, no. 2 (2023): 68. <https://doi.org/10.37253/sasenal.v1i2.8579>.
- Fandy, Herianto. "Analisis Putusan Pengadilan Tinggi DKI Jakarta No. 629/Pdt/2023/PT.DKI atas Kebocoran Data Pribadi di Facebook." *Jurnal Globalisasi Hukum* 2, no. 1 (2025): 6.
- Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.
- Galgani, Gemma Malino. "Urgensi PP Nomor 24 Tahun 2010 dalam Pencegahan Pembukaan Kawasan Lahan Perkebunan secara Ilegal di Kawasan Hutan Produksi." *Jurnal Globalisasi Hukum* 2, no. 2 (2025): 361.
- Jessica. "Perlindungan Hukum Kekayaan Intelektual atas Merek Terkenal terhadap Barang dalam Transaksi E-Commerce di Indonesia." *Jurnal Globalisasi Hukum* 2, no. 1 (2025): 37.
- K&K Advocates. "Kasus-Kasus Awal dari Implementasi Sanksi Pidana dalam UU PDP." *K&K Advocates News*, 9 Agustus 2024. <https://www.kk-advocates.com/news/read/kasus-awal-implementasi-sanksi-pidana-dalam-uu-pdp>. Diakses 29 April 2025 pukul 19.32.
- Liuhua, Wei. "Perlindungan Data Pribadi dalam Era Digital: Regulasi dan Praktik Hukum di Indonesia." *Jurnal Globalisasi Hukum* 2, no. 2 (2025): 326.
- Mulyana, Kurniawan Eka. "Pakar Keamanan Siber Sebut Ada Kemungkinan Pencurian Data Pribadi di Kasus Pinjaman Fiktif di Garut." *Kompas TV*. Diakses 29 April 2025. <https://www.kompas.tv/regional/427682/pakar-keamanan-siber-sebut-ada-kemungkinan-pencurian-data-pribadi-di-kasus-pinjaman-fiktif-di-garut>.
- Rangga, dan Elfrida Ratnawati. "Sanksi Rehabilitasi Tindak Pidana Penyalahgunaan Narkotika Berdasarkan UU No. 35 Tahun 2009 tentang Narkotika." *Unes Law Review* 5, no. 3 (2023): 1403.
- Rogate, Luvito. "Hak Royalti dalam Industri Musik: Analisis Perlindungan Hukum terhadap Pencipta Lagu terkait Cover Lagu." *Jurnal Globalisasi Hukum* 1, no. 2 (2024): 325.

- Sembiring, Sentosa. "Tanggung Jawab Dropshipper dengan Distributor pada Transaksi Bisnis Online." *Jurnal Globalisasi Hukum* 1, no. 2 (2024): 364.
- Siahaan, M. P. H. Sahala. "Tindak Pidana Pelecehan Seksual yang Terjadi di Transportasi Umum Berdasarkan UU No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual." *Jurnal Globalisasi Hukum* 2, no. 1 (2025): 129.
- Suong, Moh. Akli, Lilis Ekayani, dan Hardianto Djanggih. "Perlindungan Hukum Nasabah terhadap Kejahatan Pencurian Data Pribadi (Phishing) di Lingkungan Perbankan." *Journal of Philosophy* 4, no. 1 (2023): 22–40.
- Tempo.co. "Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah." 21 September 2024. <https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403>. Diakses 29 April 2025 pukul 22.37.
- Tempo.co. "Kronologi Serangan Siber yang Lumpuhkan PDN hingga Tuntutan 8 Juta Dolar." 2024. <https://www.tempo.co/ekonomi/kronologi-serangan-siber-yang-lumpuhkan-pdn-hingga-tuntutan-8-juta-dolar-46121>. Diakses 28 April 2025 pukul 13.32.
- Triadi, Muhammad. "Perlindungan terhadap Korban Pencurian Data Pribadi melalui Media Digital." *Jurnal Ilmu Hukum Reusam* 11, no. 1 (2023): 4. <https://doi.org/10.29103/reusam.vxii1.10178>.
- Vidya, Agatha Nariswari. "Kronologi Warga Sekampung di Garut Kaget Tiba-Tiba Punya Utang, Korban 407 Orang." Suara.com, 20 Juli 2023. <https://www.suara.com/news/2023/07/20/132146/kronologi-warga-sekampung-di-garut-kaget-tiba-tiba-punya-utang-korban-407-orang?page=all>. Diakses 28 April 2025 pukul 21.44.