VOLUME 11 NO. 1 JUNI 2026 ISSN CETAK 2597-968X
ISSN ONLINE 2548-8244

PERTANGGUNGJAWABAN PIDANA DALAM KEJAHATAN SIBER TERHADAP INFRASTRUKTUR DIGITAL NEGARA MENURUT UNDANG-UNDANG NOMOR 1 TAHUN 2024 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (STUDI KASUS PERETASAN PUSAT DATA NASIONAL SEMENTARA 2 INDONESIA)

Oleh :
Muhammad Faeyza[1], Aan Asphianto[2], Reine Rofiana[3]

Muhammad Faeyza Rabbani Harahap[1]
Fakultas Hukum Universitas Sultan Ageng Tirtayasa
Jl. Raya Jkt No. 3, Sindangsari, Serang
Email: 1111210102@untirta.ac.id

Aan Asphianto[2]
Fakultas Hukum Universitas Sultan Ageng Tirtayasa
Jl. Raya Jkt No. 3, Sindangsari, Serang
Email: 1111210102@untirta.ac.id

Reine Rofiana[3]
Fakultas Hukum Universitas Sultan Ageng Tirtayasa
Jl. Raya Jkt No. 3, Sindangsari, Serang
Email: Reine@untirta.ac.id

ABSTRACT

The development of information and communication technology has had a positive impact in various areas of life, including government systems. However, on the other hand, this development has also given rise to new forms of digital crime, one of which is cybercrime that targets a country's digital infrastructure. One case that emerged in Indonesia was the hacking of the Temporary National Data Center 2 (PDNS 2) in June 2024, which resulted in disruptions to 239 government agencies and large-scale data leaks. This study aims to analyze the forms of cybercrime against the country's digital infrastructure based on the theory of cybercrime in Indonesian criminal law and to examine the criminal liability of the perpetrators of the PDNS 2 hack. The research method used is normative juridical with a legislative and case study approach. The data used was sourced from primary and secondary legal materials, including official reports from BSSN and several news media publications. The results of the study show that the hacking of PDNS 2 is a form of cybercrime that falls under the category of unauthorized access to computer systems and services and cyber sabotage, which can be charged under the provisions of Articles 30, 32, 52, and 46 of the ITE Law and Article 482 of the Criminal Code. Although there has been no legal action against the perpetrators to date, normatively, the elements of criminal liability have been fulfilled, including the existence of unlawful acts, fault, the ability to be held responsible, and the absence of justifiable or exculpatory reasons.
***Keywords**: Cyber Crime, State Digital Infrastructure, Hacking, Criminal Liability, ITE Law*

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah membawa dampak positif dalam berbagai bidang kehidupan, termasuk dalam sistem pemerintahan. Namun di sisi lain, perkembangan tersebut juga melahirkan bentuk-bentuk kejahatan baru yang bersifat digital, salah satunya adalah kejahatan siber (cybercrime) yang menargetkan infrastruktur digital negara. Salah satu kasus yang muncul di Indonesia adalah peretasan terhadap Pusat Data Nasional Sementara 2 (PDNS 2) pada bulan Juni 2024,

yang mengakibatkan gangguan pada 239 instansi pemerintahan dan kebocoran data berskala besar. Penelitian ini bertujuan untuk menganalisis bentuk kejahatan siber terhadap infrastruktur digital negara berdasarkan teori kejahatan siber dalam hukum pidana Indonesia serta mengkaji pertanggungjawaban pidana terhadap pelaku peretasan PDNS 2. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan studi kasus. Data yang digunakan bersumber dari bahan hukum primer dan sekunder, termasuk laporan resmi dari BSSN dan beberapa publikasi media berita. Hasil penelitian menunjukkan bahwa peretasan terhadap PDNS 2 merupakan bentuk kejahatan siber yang termasuk dalam bentuk unauthorized access to computer system and service dan cyber sabotage yang dapat dijerat berdasarkan ketentuan Pasal 30, 32, 52, dan 46 UU ITE serta Pasal 482 KUHP. Meskipun hingga saat ini belum terdapat proses penegakan hukum terhadap pelaku, secara normatif unsur-unsur pertanggungjawaban pidana telah terpenuhi, meliputi adanya perbuatan melawan hukum, kesalahan, kemampuan bertanggung jawab, serta tidak adanya alasan pembenar maupun pemaaf.
Kata kunci: Kejahatan Siber, Infrastruktur Digital Negara, Peretasan, Pertanggungjawaban Pidana, UU ITE

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di abad ke-21 telah menyebabkan perubahan yang penting dalam berbagai aspek kehidupan manusia, termasuk dalam sistem pemerintahan yang modern. Digitalisasi dalam penyelenggaraan pemerintahan dengan memanfaatkan sistem elektronik dan pusat data yang terpusat merupakan bagian dari transformasi digital nasional guna meningkatkan efektivitas, efisiensi, dan mutu layanan publik. Namun, kemajuan ini juga menghadirkan tantangan berat berupa bertambahnya kejahatan siber yang menargetkan infrastruktur digital penting negara.

Di Indonesia, salah satu kejadian terbesar terjadi pada bulan Juni 2024 ketika kelompok *Brain Cipher Ransomware* melakukan peretasan terhadap Pusat Data Nasional Sementara 2 (PDNS 2). Serangan tersebut menyebabkan gangguan pada 239 lembaga pemerintahan, mengganggu layanan publik, kehilangan ratusan data penting dari kementerian dan lembaga, serta menimbulkan dampak ekonomi, administratif, dan sosial yang cukup luas. Pelaku bahkan meminta tebusan sebesar *USD* 8 juta, sementara kemampuan pemulihan data oleh pemerintah dinilai masih kurang efektif.[1] Kejadian ini tidak hanya menggambarkan kelemahan dalam sistem keamanan digital negara, tetapi juga menguji kemampuan hukum pidana Indonesia untuk menanggapi kejahatan siber yang menargetkan infrastruktur penting negara.

Secara normatif, tindakan peretasan dan akses tidak sah ke sistem elektronik telah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang terakhir diubah dengan Undang-Undang Nomor 1 Tahun 2024. Ketentuan dalam Pasal 30, Pasal 32, Pasal 46, dan Pasal 52 ayat (2) memberikan landasan hukum untuk menindak pelaku kejahatan, terutama apabila objek kejahatan adalah sistem elektronik yang dimiliki oleh pemerintah atau layanan publik. Namun, sampai saat penelitian ini dilaksanakan, penegakan hukum terhadap kasus PDNS 2 belum menunjukkan kemajuan yang signifikan, sehingga menimbulkan pertanyaan tentang efektivitas regulasi dan pelaksanaan pertanggungjawaban pidana dalam kasus kejahatan siber di Indonesia.

Isu tersebut diperkuat oleh sejumlah temuan sebelumnya yang mengindikasikan rendahnya kesiapan lembaga pemerintah dalam menangani insiden kebocoran data, minimnya respons terhadap pemberitahuan

[1] Tim CNN Indonesia (2024), Pakar Ungkap Risiko Jika Tebusan Rp131 Miliar untuk PDNS Tak Dibayar, https://www.cnnindonesia.com/teknologi/20240627063013-192-1114686/pakar-ungkap risiko-jika-tebusan-rp131-miliar-untuk-pdns-tak-dibayar, diakses pada 28 Agustus 2024, Pukul 11.06 WIB.

ISSN CETAK 2597-968X
ISSN ONLINE 2548-8244

keamanan dari BSSN, serta ketidakadaan prosedur penanganan insiden yang terstandarisasi secara nasional. Tingkat kesiapan keamanan siber yang rendah dan penerapan sistem pertanggungjawaban pidana yang lemah dapat mengakibatkan ancaman serius terhadap kedaulatan data negara, keamanan nasional, serta perlindungan masyarakat.[2]

Berdasarkan latar belakang tersebut, penelitian ini sangat diperlukan untuk menjawab dua pertanyaan utama, yaitu: pertama, bagaimana bentuk kejahatan siber terhadap infrastruktur digital negara menurut sudut pandang teori kejahatan siber dalam hukum pidana di Indonesia; dan kedua, bagaimana pertanggungjawaban pidana bagi pelaku peretasan PDNS 2 berdasarkan ketentuan dalam Undang-Undang Nomor 1 Tahun 2024 mengenai Informasi dan Transaksi Elektronik.

Penelitian ini dilaksanakan dengan metode hukum normatif menggunakan pendekatan peraturan perundang-undangan dan analisis kasus. Studi ini menganalisis peraturan hukum, teori hukum, kajian ilmiah, serta data sekunder yang berhubungan dengan insiden PDNS 2 untuk memeriksa konsep kejahatan siber dan penerapan tanggung jawab pidana terhadap pelakunya. Penelitian ini berfokus pada konteks Indonesia, dengan lokasi permasalahan di peretasan Pusat Data Nasional Sementara 2 yang merupakan salah satu infrastruktur digital penting bagi negara.

Studi ini sangat penting karena berkaitan dengan keamanan data negara, keberlangsungan sistem pemerintahan yang menggunakan teknologi, perlindungan hak-hak masyarakat, serta wibawa negara dalam menjalankan hukum. Secara teoritis, studi ini diharapkan dapat memperkaya kemajuan ilmu hukum pidana dan hukum siber. Secara praktis, studi ini diharapkan dapat memberikan sumbangan kepada pemerintah, lembaga penegak hukum, dan pihak-pihak terkait dalam memperkuat kebijakan keamanan siber serta sistem pertanggungjawaban pidana bagi pelaku kejahatan siber.

Oleh karena itu, penelitian ini memiliki tujuan untuk: (1) menganalisis bentuk kejahatan siber yang menargetkan infrastruktur digital negara sesuai dengan teori kejahatan siber dalam hukum pidana di Indonesia; dan (2) meneliti bagaimanakah pertanggungjawaban pidana bagi pelaku peretasan PDNS 2 Indonesia berdasarkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Hasil penelitian diharapkan bisa menjadi acuan baik di bidang akademis maupun praktik untuk memperkuat sistem hukum siber Indonesia di masa depan.

2. METODE PENELITIAN

Penelitian ini memakai metode yuridis normatif yang berfokus pada analisis terhadap peraturan perundang-undangan, doktrin hukum, dan data sekunder yang terkait. Sumber data dalam penelitian ini mencakup bahan hukum utama yang terdiri atas Undang-Undang Nomor 1 Tahun 2024 mengenai Perubahan Kedua pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta peraturan yang relevan lainnya; bahan hukum sekunder yang meliputi literatur, jurnal ilmiah, buku teks dalam bidang hukum pidana dan hukum siber, serta pandangan para ahli; dan bahan hukum tersier yang berupa kamus hukum dan ensiklopedia hukum. Data penelitian diperoleh melalui kajian pustaka dan pencarian dokumen resmi, termasuk laporan dari Badan Siber dan Sandi Negara (BSSN), publikasi dari pemerintah, serta informasi terpercaya yang berkaitan dengan peretasan Pusat Data Nasional Sementara tahun 2024.

[2] Fikri Irfan, Erika Ramadhani (2024), "Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede", Selekta Manajemen: *Jurnal Mahasiswa Bisnis & Manajemen*, Vol. 2 No. 6, 2024, hlm. 196

Pengumpulan data dilakukan setelah peristiwa peretasan PDNS 2 untuk mendapatkan data yang telah berkembang.

Dalam penelitian normatif ini, data dianalisis dengan menggunakan pendekatan perundang-undangan dan pendekatan kasus untuk menilai kesesuaian norma hukum terhadap fakta yuridis yang terjadi. Analisis dilakukan dengan pendekatan kualitatif yang fokus pada tafsiran hukum, penyusunan argumen hukum, dan penilaian norma terkait pertanggungjawaban pidana pelaku peretasan. Metode ini diharapkan dapat menghasilkan analisis yang mendalam, menyeluruh, dan sesuai dalam menjawab permasalahan penelitian.

3. HASIL DAN PEMBAHASAN

Penelitian ini menemukan bahwa peretasan terhadap Pusat Data Nasional Sementara 2 (PDNS 2) pada Juni 2024 merupakan salah satu insiden kejahatan siber terbesar di Indonesia yang ditujukan terhadap infrastruktur digital strategis negara. Serangan yang dilakukan menggunakan *Brain Cipher Ransomware* tersebut menyebabkan gangguan pada 239 instansi pemerintahan, mengakibatkan lumpuhnya sejumlah layanan publik, hilangnya akses data, serta ancaman kebocoran data berskala luas. Pelaku bahkan menuntut tebusan senilai USD 8 juta agar data dapat dipulihkan sepenuhnya. Dari sisi dampak, insiden ini menimbulkan gangguan administratif, ketidakpastian pelayanan publik, risiko penyalahgunaan data, serta menurunnya kepercayaan publik terhadap keamanan sistem elektronik pemerintah.[3]

Dari segi bentuk tindak pidana, hasil penelitian menunjukkan bahwa peretasan PDNS 2 merupakan bentuk kejahatan siber *unauthorized access to computer system and services* serta *cyber sabotage and extortion*, karena mengandung unsur akses tanpa hak (illegal), pengambilalihan sistem elektronik, penguncian data, serta penghancuran dan pengubahan data elektronik.[4] Secara normatif, hasil telaah menunjukkan bahwa tindakan tersebut memenuhi ketentuan dalam Pasal 30, Pasal 32, Pasal 46, dan Pasal 52 Undang-Undang Nomor 1 Tahun 2024 tentang ITE,[5] khususnya karena objek yang diserang merupakan sistem elektronik milik negara yang memiliki fungsi layanan publik. Selain itu, unsur pemerasan melalui permintaan tebusan menunjukkan adanya tindakan melawan hukum yang memperkuat posisi perbuatan sebagai tindak pidana yang memiliki konsekuensi hukum sesuai tercantum di pasal 482 KUHP.[6] Pertanggungjawaban pidana terhadap pelaku peretasan PDNS 2 secara normatif telah memenuhi unsur-unsur hukum pidana. Pertanggungjawaban pidana menurut Moeljatno merujuk pada konsekuensi hukum yang timbul akibat perbuatan pidana yang dilakukan oleh individu. Konsekuensi ini dapat dikenakan kepada seseorang yang memiliki kemampuan untuk bertanggungjawab (*toerekeningsvatbaar*).[7] Meskipun hingga kini pelaku secara individual belum ditangkap dan belum diproses secara hukum, secara normatif unsur-unsur pertanggungjawaban pidana terhadap pelaku peretasan PDNS 2 telah terpenuhi. Pertama, terdapat perbuatan melawan hukum berupa akses ilegal dan perusakan sistem elektronik milik negara. Kedua, pelaku memiliki kemampuan untuk bertanggung jawab secara hukum, terbukti dari perencanaan matang dan kemampuan teknis yang tinggi. Ketiga, terdapat unsur kesengajaan (*dolus*), yakni kehendak sadar untuk mencuri, mengunci data dengan metode *ransomware* dan memeras pemerintah. Keempat, tidak terdapat alasan pembenar maupun pemaaf yang dapat

[3] Tim CNN Indonesia, *Loc. Cit*
[4] Maskun, *Kejahatan Siber (Cybe Crime): Suatu Pengantar* (2022), Kencana, Jakarta, hlm. 51
[5] Undang.Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
[6] Kitab Undang-Undang Hukum Pidana
[7] Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, (2008), hlm. 64.

menghapus kesalahan pelaku. Dengan demikian, berdasarkan ketentuan dalam Pasal 30, 32, 52, dan 46 UU ITE serta Pasal 482 KUHP, pelaku dapat dikenai sanksi pidana atas dasar pertanggungjawaban pidana.

Namun demikian, hasil penelitian juga menunjukkan bahwa hingga penelitian ini dilakukan, proses penegakan hukum terhadap pelaku belum terlaksana secara efektif. Belum adanya pelaku yang diproses secara pidana menimbulkan kesenjangan antara norma hukum yang telah tersedia dengan realitas penegakan hukum. Di sisi lain, sejumlah laporan resmi pemerintah menunjukkan bahwa terdapat kelemahan pada aspek keamanan siber pemerintah, termasuk rendahnya tingkat respons terhadap peringatan keamanan, belum optimalnya tata kelola keamanan data, serta belum adanya prosedur baku penanganan insiden siber secara nasional. Temuan ini memperlihatkan bahwa kesiapan sistem hukum dan kelembagaan pemerintah dalam menghadapi kejahatan siber terhadap infrastruktur digital negara masih belum maksimal. Secara normatif, keberadaan Undang-Undang ITE sebagai *lex specialis* telah memberikan instrumen hukum yang jelas untuk menjerat pelaku. Namun, kesenjangan antara norma dan pelaksanaan menunjukkan bahwa tantangan terbesar bukan hanya pada aspek regulasi, tetapi juga pada aspek implementasi, kapasitas kelembagaan, kesiapan infrastruktur keamanan digital, dan koordinasi antarinstansi. Sejumlah penelitian terdahulu juga menegaskan hal yang sama, bahwa persoalan keamanan siber di Indonesia tidak hanya terletak pada lemahnya teknologi keamanan, tetapi juga pada lemahnya tata kelola keamanan siber dan penegakan hukum yang belum optimal.

Pembahasan ini menunjukkan bahwa kejahatan siber terhadap infrastruktur digital negara bukan sekadar persoalan kriminalitas, tetapi juga menyangkut aspek keamanan nasional, kedaulatan data, perlindungan masyarakat, serta kewibawaan negara dalam penegakan hukum. Dengan demikian, penguatan sistem pertanggungjawaban pidana terhadap pelaku kejahatan siber merupakan kebutuhan yang mendesak sekaligus strategis. Selain itu, dibutuhkan penguatan kebijakan keamanan siber, peningkatan kapasitas aparat penegak hukum, dan penyusunan standar prosedur penanganan insiden siber secara nasional agar penegakan hukum dapat berjalan efektif.

Berdasarkan analisis tersebut, dapat ditegaskan bahwa hasil penelitian ini tidak hanya menjawab rumusan masalah mengenai bentuk kejahatan siber dalam kasus PDNS 2 dan pertanggungjawaban pidana terhadap pelakunya, tetapi juga memberikan kontribusi teoretis dan praktis bagi pengembangan hukum siber dan hukum pidana di Indonesia. Secara teoretis, penelitian ini menegaskan relevansi hukum pidana dalam menghadapi perkembangan kejahatan digital. Secara praktis, penelitian ini memberikan dasar argumentatif bagi penguatan regulasi, kebijakan, serta strategi penegakan hukum dalam menangani kejahatan siber terhadap infrastruktur digital negara.

4. PENUTUP

Kejahatan siber yang menargetkan infrastruktur digital negara tergolong sebagai tindak pidana dengan karakteristik khusus, karena menargetkan sistem elektronik vital yang menopang fungsi pemerintahan dan pelayanan publik. Kasus peretasan Pusat Data Nasional Sementara 2 (PDNS 2) merupakan contoh konkret bentuk kejahatan ini. Serangan yang dilakukan oleh kelompok Brain Cipher Ransomware menggunakan metode ransomware, yang secara teknis mengunci dan menyandera data, serta menuntut tebusan kepada pemerintah. Tindakan ini termasuk dalam bentuk *unauthorized access to computer system and service* serta *cyber sabotage and extortion*. Tindakan ini merupakan bentuk serangan yang secara langsung menjadikan sistem digital negara

sebagai target, dan memiliki dampak serius terhadap ketahanan layanan publik dan kedaulatan data nasional. Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, tindakan ini merupakan tanpa hak atau melawan hukum dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Berdasarkan Kitab Undang-Undang Hukum Pidana pasal 482 ayat (1), 108 tindakan ini merupakan pemerasan, karena meminta tebusan kepada pemerintah apabila data yang dicuri ingin dikembalikan.

Pertanggungjawaban pidana terhadap pelaku peretasan PDNS 2 secara normatif telah memenuhi unsur-unsur hukum pidana. Meskipun hingga kini pelaku secara individual belum ditangkap dan belum diproses secara hukum, secara normatif unsur-unsur pertanggungjawaban pidana terhadap pelaku peretasan PDNS 2 telah terpenuhi. Pertama, terdapat perbuatan melawan hukum berupa akses ilegal dan perusakan sistem elektronik milik negara. Kedua, pelaku memiliki kemampuan untuk bertanggung jawab secara hukum, terbukti dari perencanaan matang dan kemampuan teknis yang tinggi. Ketiga, terdapat unsur kesengajaan (*dolus*), yakni kehendak sadar untuk mengunci data dan memeras pemerintah. Keempat, tidak terdapat alasan pembenar maupun pemaaf yang dapat menghapus kesalahan pelaku. Dengan demikian, berdasarkan ketentuan dalam Pasal 30, 32, 52, dan 46 UU ITE serta Pasal 482 KUHP, pelaku dapat dikenai sanksi pidana atas dasar pertanggungjawaban pidana.

Pemerintah melalui aparat penegak hukum dan lembaga terkait seperti BSSN dan Kementerian Komunikasi dan Digital Republik Indonesia perlu mengambil langkah aktif untuk menindaklanjuti kasus peretasan PDNS 2. Penegakan hukum terhadap pelaku kejahatan siber perlu dilakukan secara tegas, meskipun pelaku berada di luar negeri atau tergabung dalam jaringan siber transnasional. Kerja sama internasional dalam bentuk *mutual legal assistance* (MLA) dan penelusuran digital lintas batas harus diperkuat untuk memastikan bahwa kejahatan siber tidak menjadi kejahatan impunitas (tidak tersentuh hukum). Insiden PDNS 2 mengungkap lemahnya kesiapan sistem keamanan digital nasional, termasuk lemahnya backup data dan proteksi terhadap sistem strategis. Oleh karena itu, perlu adanya penguatan infrastruktur hukum melalui peraturan turunan dari UU ITE yang lebih detail terkait keamanan siber. Selain itu, pemerintah perlu memastikan pelaksanaan Standar Operasional Prosedur (SOP) penanganan insiden siber di setiap instansi, meningkatkan literasi siber, membangun security operation center nasional yang aktif 24 jam, dan melakukan audit berkala terhadap sistem data vital negara. Merujuk pada terpenuhinya unsur pertanggungjawaban pidana secara normatif, proses identifikasi pelaku, penangkapan, dan penuntutan seharusnya menjadi fokus utama agar tidak ada kekosongan dalam penegakan hukum. Hal ini penting untuk memberikan kepastian hukum, menciptakan efek jera, dan menjamin perlindungan terhadap infrastruktur digital negara di masa mendatang.

DAFTAR PUSTAKA

Buku

Moeljatno (2008), *Asas-Asas Hukum Pidana*, Jakarta, Rineka Cipta.

Maskun (2022), *Kejahatan Siber (Cybe Crime): Suatu Pengantar*, Jakarta, Kencana

Artikel dari Jurnal

Fikri Irfan, Erika Ramadhani, “Analisis Dampak Kebocoran Data Pusat Data

ISSN CETAK 2597-968X
ISSN ONLINE 2548-8244

Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede", Selekta Manajemen: *Jurnal Mahasiswa Bisnis & Manajemen*, Vol. 2 No. 6, 196 (2024)

Peraturan

Undang.Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Kitab Undang-Undang Hukum Pidana.

Web Page

Tim CNN Indonesia (2024), Pakar Ungkap Risiko Jika Tebusan Rp131 Miliar untuk PDNS Tak Dibayar, https://www.cnnindonesia.com/teknologi/20240627063013-192-1114686/pakar-ungkap risiko-jika-tebusan-rp131-miliar-untuk-pdns-tak-dibayar, diakses pada 28 Agustus 2024, Pukul 11.06 WIB.

ISSN CETAK 2597-968X
ISSN ONLINE 2548-8244