

Pertanggungjawaban Pidana, Pidana *Illegal Access* Data Kependudukan Dan Implikasi Hukumnya (Analisis Putusan PN. Cikarang No. 515/PID.SUS/2021/PN.CKR)

Timbo Mangaranap Sirait¹, Wibowo Laksono Widodo²

^{1,2}Ilmu Hukum Universitas 17 Agustus 1945 Jakarta, Indonesia

E-mail: mangaranaptimotius@gmail.com¹, wibowolks215@gmail.com²

Article History:

Received: 03 Februari 2026

Revised: 23 Maret 2026

Accepted: 06 April 2026

Keywords: Akses Ilegal,
Kejahatan Siber, Tanggung
Jawab Pidana, Perlindungan
Data.

Abstract: Perkembangan pesat ilmu pengetahuan dan teknologi informasi menciptakan berbagai kebutuhan publik seperti layanan administrasi kependudukan yang cepat sebagai manifestasi Negara Kesejahteraan dalam Pasal 1 ayat (3) Konstitusi yang mewajibkan negara untuk menyediakan layanan publik, namun ternyata layanan tersebut diakses secara ilegal oleh pelaku tindak pidana. Penelitian ini dilakukan dengan menggunakan Metode Yuridis Normatif, melalui studi literatur dan menyimpulkan, Pertama, penegakan hukum terhadap tindak pidana akses ilegal oleh Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN.Ckr telah dilakukan berdasarkan Undang-Undang ITE 2024 dan hukum acara pidana khusus yang sesuai, dengan menjadikan "bukti elektronik" sebagai bukti yang diperlukan, sehingga prosesnya objektif. Kedua, bahwa tanggung jawab pidana terdakwa diberikan hukuman yang lebih ringan yaitu penjara satu tahun dan denda sebesar Rp 200 juta, dan bahwa putusan tersebut tidak adil bagi pemilik data yang menjadi korban. Ketiga, bahwa kejahatan akses ilegal telah menimbulkan berbagai implikasi hukum, tidak hanya terkait dengan stabilitas administrasi negara, kepercayaan publik terhadap pemerintah, dan hak privasi warga negara, tetapi juga implikasi hukum mengenai aspek pembuktian.

PENDAHULUAN

Perkembangan pesat dalam ilmu pengetahuan dan teknologi informasi, serta dinamika berbagai aktivitas sosial di tingkat nasional maupun internasional, telah memunculkan sejumlah peristiwa hukum yang baru dan kompleks (Sirait, 2021). Berbagai kebutuhan publik yang berlayanan cepat sebagai wujud negara Welfare State dalam Pasal 1 ayat (3) UUDNRI 1945 yang derivasinya menuntut negara melakukan layanan publik (public service), seperti layanan administrasi kependudukan, kini dijalankan melalui sistem elektronik dalam menyimpan, mengolah, dan mendistribusikan data pribadi dalam jumlah besar. Kebergantungan pada teknologi digital ini menyebabkan setiap celah keamanan dalam sistem elektronik berpotensi mengakibatkan konsekuensi serius berupa kebocoran data, penyalahgunaan identitas, hingga kejahatan lintas negara (cyber-enabled crime) (Tobing et al., 2024).

Data kependudukan yang dikelola pemerintah, terutama Nomor Induk Kependudukan (NIK) dan informasi dalam Kartu Keluarga, merupakan kategori data pribadi yang bersifat spesifik sebagaimana dijelaskan dalam Pasal 1 angka (1) dan Pasal 4 ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ("UU PDP"). Kedudukan data ini sangat sensitif karena dapat digunakan pelaku kejahatan untuk mengakses layanan keuangan, mendaftar layanan digital, atau melakukan verifikasi identitas. Risiko meningkat ketika sistem pengelolaan data tidak dilengkapi kontrol keamanan yang memadai, sebagaimana banyak penelitian menyoroti bahwa rendahnya pemahaman pengguna, lemahnya pengawasan, serta kurangnya kapasitas teknis institusi pengelola memperparah potensi penyalahgunaan data kependudukan digital (Jagratarata et al., 2025).

Kewenangan negara dalam menjamin perlindungan data yang belum optimal dirasakan masyarakat dapat juga disebabkan oleh koordinasi yang kurang baik antar lembaga pelaksana teknis sehingga mandat perlindungan yang telah diterima tidak dapat terimplementasi secara menyeluruh (Azza Fitrahul Faizah, 2023). Karena itu kebocoran data tersebut dalam konteks administrasi kependudukan tidak hanya menimbulkan kerugian perorangan, tetapi juga mengancam kepercayaan publik terhadap pemerintah. Ambiguitas regulasi yang pernah terjadi sebelum lahirnya UU PDP menunjukkan bahwa penegakan hukum di bidang ini membutuhkan landasan hukum yang kuat sekaligus konsisten. (Bitus Tanjung. Marjan Miharja, 2023), dan menjadi bentuk kejahatan modern yang sulit dideteksi karena pelaku sering menyamarkan identitasnya, menggunakan perangkat anonim, dan memanfaatkan celah teknis sistem elektronik (Wantania, 2025).

Dalam kasus-kasus besar kebocoran data, pelaku memanfaatkan kerentanan sistem elektronik mulai dari kesalahan desain aplikasi, kelalaian operator, hingga lemahnya enkripsi untuk menembus lapisan keamanan, sebagaimana dalam kasus Terdakwa Chandra Kirana Saputra ("Chandra"), yang mencoba melakukan tindak pidana mengakses data kependudukan secara ilegal, kemudian mengakses sistem elektronik milik resmi Disdukcapil Kabupaten Bekasi, yakni sitedak.bekasikab.go.id, yang melayani sistem layanan administrasi kependudukan seperti KTP, KK, Akta Kelahiran, dan Kartu Identitas Anak, dan berhasil memperoleh akses ke database internal dan menemukan kredensial masuk ke panel PHPMyAdmin, yakni username SIAK_OFF. Chandra tanpa hak atau persetujuan dari Disdukcapil, secara sistematis mengunduh seluruh data penduduk Kabupaten Bekasi sebanyak 2.339.060 data kemudian menjual data tersebut untuk dimanfaatkan calon pembeli dalam aktivitas ilegal, seperti pendaftaran SIM-card palsu atau permohonan pinjaman online menggunakan identitas orang lain. Namun, aktivitas ilegal tersebut kemudian terungkap oleh Pihak Disdukcapil, kemudian setelah berkoordinasi dengan Kementerian Dalam Negeri dan pihak kepolisian, akhirnya diproses secara hukum, dan ke Pengadilan Negeri Cikarang, dengan dakwaan Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE sebagaimana Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr.

Berdasarkan uraian-uraian tersebut, maka permasalahan yang diangkat dalam penelitian ini adalah untuk mengetahui: (1) Bagaimana Objektifitas Penegakan Hukum Kasus Illegal Akses dalam Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr ?; (2) Bagaimana Pertanggungjawaban Pidana Pelaku Illegal Access dalam Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr ?, dan (3) Bagaimana Implikasi Hukum Tindak Pidana Illegal Access terhadap berbagai Aspek Hukum dalam perkara tersebut ?

METODE PENELITIAN

Penelitian ini menggunakan metode Yuridis Normatif melalui studi kepustakaan dengan berbagai pendekatan, seperti pendekatan perundang-undangan (statute approach) yang dilakukan

dengan mengkaji bahan hukum primer antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, KUHP-1946 dan Undang-undang lain yang relevan. Kemudian pendekatan konseptual dengan mengkaji buku-buku, kamus, dan literatur yang relevan untuk memahami konstruksi hukum mengenai akses tanpa hak, perlindungan data pribadi, keamanan sistem elektronik, dan tanggung jawab hukum pengendali data, serta pendekatan kasus (*case approach*) atas putusan No. 515/Pid.Sus/2021/PN.Ckr, kemudian dianalisis secara kualitatif, kemudian disimpulkan.

HASIL DAN PEMBAHASAN

Penegakan hukum Tindak Pidana Akses Ilegal Dalam Perkara Pengadilan Negeri Cikarang No. 515/Pid.Sus/2021/PN.Ckr

Teknologi informasi (*Information Technology*) memegang peran yang penting, baik dimasa kini maupun dimasa yang akan datang. Kasus kebocoran data kependudukan di Kabupaten Bekasi tersebut, menjadi contoh paling nyata mengenai dampak serius akses tanpa hak terhadap keamanan identitas nasional. Putusan Pengadilan Negeri Cikarang No. 515/Pid.Sus/2021/PN.Ckr perbuatan Terdakwa Chandra Kirana Saputra ("Chandra") mengakses secara tidak sah ke website Disdukcapil Kabupaten Bekasi. Pelaku Chandra melalui unggahan file berformat PHP ke menu unggah dokumen, sehingga file tersebut bekerja sebagai skrip berbahaya yang membuka jalur akses menuju file manager dan basis data "PHPMyAdmin" milik Disdukcapil tersebut. Keberhasilan pelaku masuk ke server menunjukkan bahwa mekanisme verifikasi, validasi file, serta standar keamanan tidak dilakukan secara ketat. Putusan ini mencatat pelaku kemudian mengunduh 2.339.060 data NIK dan Kartu Keluarga dalam format CSV dalam satu sesi akses ilegal. Pelanggaran data di Indonesia menyoroti kelemahan signifikan dalam sistem keamanan data nasional dan menimbulkan kekhawatiran tentang perlindungan hukum terhadap data pribadi (Muhammad Asthi Seta Ari Yuwana, 2025).

Dalam perspektif peraturan perundang-undangan, implikasi hukum akses ilegal terhadap data kependudukan tidak hanya berkaitan dengan pelanggaran terhadap UU ITE, melainkan juga menyentuh aspek perlindungan data pribadi sebagaimana tertuang dalam UU PDP. NIK, alamat, dan data keluarga merupakan komponen data pribadi spesifik yang menurut Pasal 4 ayat (2) UU PDP wajib dilindungi oleh penyelenggara sistem elektronik melalui mekanisme keamanan berlapis seperti enkripsi, kontrol akses, audit berkala, dan mitigasi risiko pemrosesan data. (Tobing *et al.*, 2024).

Hakim dalam putusan 515/Pid.Sus/2021/PN.Ckr menilai bahwa tindakan pelaku bukan hanya memenuhi unsur *access unlawful*, tetapi juga menimbulkan kerugian besar bagi negara, karena data yang diambil merupakan data publik yang bersifat strategis untuk berbagai layanan administratif dan kebijakan publik. dan kasus tersebut juga memperlihatkan bagaimana bukti elektronik memiliki peran strategis dalam membuktikan tindak pidana akses ilegal. Kajian tentang pembuktian tindak pidana *illegal access* menegaskan bahwa bukti elektronik, termasuk *log activity* dan tangkapan layar, merupakan alat bukti yang sah sesuai Pasal 5 UU ITE, yang menyetarakan posisi informasi elektronik dengan alat bukti lain dalam sistem pembuktian hukum pidana Indonesia.

Implementasi hukum acara atas "bukti elektronik" yang diperlukan untuk Pembuktian, dalam penegakan hukum ITE menjadi penting dalam perkara tersebut, keberhasilan penegak hukum menemukan pelaku tidak terlepas dari *scientific based investigation*, termasuk pemeriksaan perangkat, analisis sidik jari pada perangkat fisik, dan pemulihan data digital. Pembuktian

mengandung arti bahwa benar suatu peristiwa pidana telah terjadi dan terdakwa yang bersalah melakukannya, sehingga harus mempertanggungjawabkannya (Darwan Prinst, 1988).

Dalam situasi ini, akses ilegal seperti pada kasus Cikarang tidak hanya mengganggu sistem kependudukan, tetapi berpotensi berdampak pada layanan lainnya (Firdaus, 2022), dan Pemerintah sebagai pengendali data memiliki kewajiban hukum yang diatur dalam Pasal 39 UU PDP untuk memastikan data yang diproses terlindungi dari akses ilegal, pengungkapan tanpa dasar, serta pemrosesan yang tidak sesuai tujuan. Kegagalan menjalankan kewajiban ini berpotensi mengakibatkan pelanggaran hak konstitusional warga sebagaimana dijamin Pasal 28G ayat (1) UUDNRI1945 mengenai perlindungan diri pribadi dan keamanan data pribadi.

Pertanggungjawaban Pidana dan Pemidanaan Pelaku *Illegal Access* dalam Putusan PN Cikarang No. 515/Pid.Sus/2021/ PN.Ckr

Perkembangan pada era digital telah mengubah posisi data pribadi, tidak hanya sebagai elemen administratif yang esensial tetapi juga sebagai sebuah aset strategis yang menentukan dalam berbagai sektor kehidupan (Nethan, 2025). Karena menjadi aset strategis, sering terjadi di akses secara tidak sah (*illegal access*) dan hal tersebut merupakan suatu bentuk perbuatan yang dilarang yang berkaitan dengan kegiatan memasuki sistem elektronik tanpa hak, di mana tindakan tersebut dilakukan secara sadar untuk mengakses, menguasai, atau memperoleh informasi yang dilindungi oleh pemilik sistem. Kajian mengenai kejahatan dunia maya dalam salah satu file yang diunggah menggambarkan bahwa *illegal access* termasuk dalam kategori *cyber dependent crime*, yaitu kejahatan yang hanya dapat terjadi menggunakan perangkat komputer dan jaringan sebagai sarana utama sehingga proses terjadinya selalu melibatkan teknik pembobolan, penyusupan, atau eksploitasi kerentanan sistem elektronik. (Wati *et al.*, 2024). Perbuatan akses tanpa hak seringkali dilakukan melalui manipulasi teknis yang memungkinkan pelaku memperoleh pintu masuk yang tidak tersedia bagi pengguna biasa, dan itulah sebabnya kejahatan ini dipandang sebagai ancaman serius terhadap integritas sistem elektronik (Andhitya & Umam, 2025).

Di Indonesia, konsep pertanggungjawaban pidana akses ilegal dirumuskan secara jelas dalam UU-ITE 2024, yang menyatakan, “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dalam cara apa pun (Pasal 30 ayat 1) .” Rumusan tersebut menunjukkan bahwa larangan berlaku mutlak terhadap setiap bentuk pengaksesan tanpa otorisasi, baik melalui teknik sederhana maupun menggunakan metode peretasan yang kompleks. Unsur “dengan sengaja” menjadi penentu pertanggungjawaban pidana karena menunjukkan bahwa pelaku harus memiliki kemauan dan pengetahuan bahwa tindakannya merupakan kegiatan yang dilarang.

Pemidanaan perbuatan *illegal access* atau akses tanpa hak telah diatur melalui Pasal 30 UU-ITE 2024”, yang memuat larangan bagi setiap orang untuk mengakses komputer atau sistem elektronik milik pihak lain secara sengaja dan tanpa hak. Ketentuan ini menegaskan bahwa akses tersebut menjadi tindak pidana apabila dilakukan dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik (Pasal 30 UU-ITE 2024). Unsur dalam Pasal tersebut sangat relevan dalam kasus-kasus ilegal akses data kependudukan karena pelaku umumnya tidak hanya memasuki sistem, tetapi juga mengambil basis data yang berisi identitas jutaan penduduk, lalu mempolanya untuk kepentingan ekonomi ilegal seperti penipuan, registrasi kartu SIM palsu, maupun pinjaman online, sebagaimana terurai dalam berbagai penelitian mengenai kejahatan akses ilegal terhadap sistem publik (Rahmawati *et al.*, 2025).

Di dalam Pasal 30 ayat (2) menambahkan unsur lebih spesifik, yaitu “dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik.” Ketentuan ini menegaskan bahwa

seseorang yang memasuki sistem elektronik untuk mengambil data, dokumen, atau informasi apapun akan menghadapi sanksi yang lebih berat. Hal tersebut kemudian diperkuat oleh Pasal 46 ayat (2) UU ITE yang mengatur ancaman pidana penjara maksimal tujuh tahun serta denda hingga Rp800 Juta bagi setiap orang yang memenuhi unsur Pasal 30 ayat (2), memperlihatkan bahwa negara memberikan perhatian serius terhadap perlindungan data digital, terutama data yang berkaitan dengan identitas penduduk atau informasi sensitif lainnya yang disimpan dalam sistem pemerintah.

Pengaturan mengenai *illegal access* selaras dengan prinsip-prinsip perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 4 UU PDP menyebut bahwa data pribadi spesifik, termasuk identitas kependudukan seperti NIK dan informasi keluarga, harus dikelola dalam sistem elektronik yang aman serta dilindungi dari penyalahgunaan. Kewajiban ini menunjukkan bahwa setiap pelanggaran berupa pengambilan data tanpa izin bukan hanya pelanggaran terhadap UU ITE, tetapi menyentuh aspek perlindungan hak konstitusional warga sebagaimana diatur dalam Pasal 28G ayat (1) Konstitusi. Dengan demikian, konstruksi normatif mengenai *illegal access* telah memiliki dasar hukum yang kuat dan terintegrasi dalam kerangka perlindungan data nasional (Anggraeni & Amin, 2025).

Dalam konteks Putusan PN Cikarang No. 515/Pid.Sus/2021/ PN.Ckr, mengenai tindak pidana akses ilegal, perbuatan terdakwa terbukti memenuhi unsur “mengakses secara tanpa hak” sebagaimana dimaksud dalam Pasal 30 ayat (2), dalam hal ini Terdakwa bukan pegawai Disdukcapil dan tidak memiliki otorisasi apapun, namun memasuki sistem menggunakan jalur yang tidak diperbolehkan. Putusan PN Cikarang mencatat bahwa terdakwa melakukannya dengan sengaja. Hal ini menjadi tolak ukur terpenuhinya unsur kesengajaan sebagai elemen penting pertanggungjawaban pidana. Unsur “tujuan memperoleh informasi elektronik” dalam juga terbukti dari tindakan terdakwa mengunduh data penduduk sebanyak 2.339.060 berupa NIK dan informasi keluarga dalam format file CSV, yang kemudian disimpan pelaku ke dalam Google Drive miliknya.

Pertanggungjawaban pidana terdakwa pada Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr semakin jelas ketika melihat alat bukti yang diajukan dalam persidangan. Penerapan metode ini tampak jelas dalam perkara Cikarang, di mana penyidik berhasil memulihkan bukti digital dari perangkat terdakwa secara komprehensif.

Majelis hakim pada PN Cikarang dalam pertimbangannya menegaskan bahwa seluruh unsur tindak pidana telah terbukti secara sah dan meyakinkan. Hakim menilai bahwa rangkaian perbuatan terdakwa bukan hanya sekadar pelanggaran teknis, tetapi termasuk tindakan yang berpotensi menimbulkan akibat luas bagi kepercayaan publik terhadap lembaga pemerintah.

Dalam putusan Putusan PN Cikarang No. 515/Pid.Sus/2021/ PN.Ckr, hakim menjatuhkan pidana penjara selama empat tahun dan denda sebesar Rp200 juta dengan ketentuan subsidiar enam bulan kurungan. Hukuman ini berada dalam batas yang diizinkan Pasal 46 ayat (2) UU ITE, sehingga mencerminkan proporsionalitas antara perbuatan dan konsekuensi hukumnya. Pertimbangan hakim menyebutkan bahwa jumlah data yang diambil sangat besar, metode yang digunakan terdakwa bersifat terencana, dan data yang dicuri merupakan data strategis negara yang seharusnya tidak boleh diakses oleh individu tidak berwenang. Hal ini mempertegas konsep bahwa pertanggungjawaban pidana harus mempertimbangkan dampak sosial dan tingkat ancaman terhadap objek yang dilindungi.

Dalam doktrin hukum pidana, pengakuan terdakwa Chandra tidak menghapus kesengajaan, karena perbuatan terdakwa tersebut telah dilakukan berdasarkan pilihan dengan kehendak bebas dan pemahaman penuh mengenai larangan UU-ITE 2024. Hal dimaksud sejalan dengan teori pertanggungjawaban yang menegaskan bahwa seseorang tetap bertanggung jawab atas

perbuatannya ketika ia sadar mengenai konsekuensi yang mungkin timbul dari tindakan tersebut, dengan demikian putusan tersebut masih terlalu ringan dibandingkan pertanggungjawaban yang harus dipikulnya dalam UU-ITE 2024. Hubungan erat antara kesengajaan, motif, dan tindakan teknis yang dilakukan pelaku. Kesengajaan dibuktikan melalui langkah terencana, motif tampak dari keinginan menjual data, dan tindakan teknis terbukti dari tahapan peretasan sistem. Ketiganya membentuk satu rangkaian pertanggungjawaban hukum yang tidak dapat dipisahkan, dan atas perbuatan tersebut, Hakim dalam putusan PNCikarang No. 515/Pid.Sus/2021/PN.Ckr, dalam amarnya memutuskan: 1) Menyatakan Terdakwa Chandra telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dengan cara apapun dengan tujuan untuk memperoleh dokumen elektronik” sebagaimana dalam dakwaan alternatif kesatu; 2) Menjatuhkan pidana kepada Terdakwa oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan denda sebesar Rp 200 juta.

Implikasi Hukum Tindak Pidana *Illegal Access* terhadap Keamanan dan Perlindungan Data Kependudukan

Tindak pidana *illegal access* yang menargetkan data kependudukan menimbulkan berbagai implikasi hukum yang sangat luas, karena ada sangkut-pautnya dengan stabilitas administrasi negara, yaitu kepercayaan masyarakat terhadap pemerintah, dan pemenuhan hak konstitusional warga atas perlindungan data pribadi. Keamanan data kependudukan memiliki posisi strategis dalam penyelenggaraan pemerintahan modern, sebab seluruh proses identifikasi penduduk, pelayanan publik, hingga urusan verifikasi administratif bertumpu pada integritas data tersebut (Annas & Fatiha, 2025). Ketika terjadi akses tanpa hak seperti yang terungkap dalam Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr, struktur keamanan data terguncang dan membuka peluang bagi terjadinya penyalahgunaan data secara berantai, termasuk pencurian identitas, manipulasi informasi, dan penyebaran data sensitif ke pasar ilegal yang beroperasi secara global. Studi mengenai *cybercrime* dalam file yang diunggah menggambarkan bahwa kejahatan berbasis akses ilegal memiliki dampak jauh melampaui tindakan awalnya, karena data yang dicuri dapat diproses kembali oleh pihak ketiga dalam berbagai tindak pidana digital lainnya.

Implikasi hukum dari *illegal access* terhadap keamanan data kependudukan berkaitan erat dengan konsep perlindungan data pribadi sebagaimana dirumuskan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, di mana pada Pasal 4 ayat (2) UU PDP menegaskan bahwa data pribadi spesifik seperti identitas kependudukan wajib dilindungi melalui sistem keamanan yang andal. Setiap tindakan yang menyebabkan hilangnya kendali terhadap data tersebut dapat dipandang sebagai pelanggaran terhadap kewajiban pengendali data (Mugiono & Wiraguna, 2025). Ketika seorang pelaku dalam Putusan PN Cikarang tersebut mengakses sistem Disdukcapil Bekasi dan mengambil 2.339.060 data penduduk secara ilegal, maka pelanggaran yang tercipta tidak hanya berupa tindak pidana akses tanpa hak, tetapi berpotensi menggoyahkan fondasi perlindungan data yang seharusnya dijalankan oleh lembaga pemerintah yang mengelola informasi penduduk tersebut.

Implikasi lain yang penting adalah ancaman terhadap hak privasi warga negara. Hak ini merupakan bagian dari hak asasi manusia yang dijamin Pasal 28G ayat (1) UUD 1945. Ketika data kependudukan diretas dan diperjualbelikan di forum internasional seperti *Raidforums*, hal itu menciptakan kondisi di mana warga negara kehilangan kendali atas identitasnya. Data yang beredar di luar pengawasan negara berpotensi digunakan dalam pendaftaran layanan digital, penipuan keuangan, hingga tindakan kriminal berbasis identitas (Firdaus & Pratama, 2025). Ketika data yang

bocor dipalsukan atau disalahgunakan, potensi kesalahan identifikasi meningkat dan dapat mengakibatkan kerusakan serius terhadap akurasi basis data nasional (Mahpudin & Ahmad Tazzul Aripin, 2025).

Implikasi hukum yang tampak dalam perkara Putusan PN Cikarang No. 515/Pid.Sus/2021/PN.Ckr juga terkait erat dengan tanggung jawab negara dalam menjamin keamanan sistem elektronik yang digunakan dalam penyelenggaraan pelayanan publik. Dalam konteks UU PDP, Pasal 39 mewajibkan pengendali data untuk menyediakan mekanisme keamanan berlapis yang mampu mengurangi risiko akses ilegal. Ketika kerentanan dapat dieksploitasi oleh individu luar, konsekuensi hukumnya menuntut adanya perbaikan, evaluasi, serta pertanggungjawaban atas kelalaian yang berpotensi mengancam hak subjek data.

Demikian juga implikasi hukum pada aspek pembuktian dalam tindak pidana siber. Putusan PN Cikarang tersebut memperlihatkan pentingnya bukti elektronik sebagai alat bukti sah sesuai Pasal 5 UU ITE. Penyidik mengumpulkan berbagai bukti digital berupa *log server*, file unggahan berbahaya, tangkapan layar akun *Raidforums*, serta perangkat elektronik pelaku. Kajian dalam file penelitian yang diunggah menyatakan bahwa jejak digital pelaku menjadi unsur penting dalam memastikan identitas dan substansi perbuatan dalam kasus akses ilegal, karena metode peretasan biasanya tidak meninggalkan bukti fisik tradisional seperti tindak pidana konvensional. Implikasi ini memperkuat posisi bukti elektronik dalam perkara pidana modern.

Sedangkan dalam konteks perlindungan hukum, tindakan *illegal access* memengaruhi bagaimana negara membangun kepercayaan publik terhadap penyelenggaraan administrasi kependudukan digital. Putusan PN Cikarang dalam perkara tersebut menunjukkan bahwa kebocoran data terjadi bukan karena kelalaian pengguna, seharusnya tidak boleh terjadi, sehingga kebocoran data tersebut akan berdampak pada legitimasi negara di mata warganya.

Adapun implikasi terhadap tata kelola pemerintahan terlihat dalam cara lembaga negara harus meninjau ulang standar keamanan sistem elektroniknya setelah terjadi tindak pidana akses ilegal.. Fakta dalam perkara tersebut memperlihatkan bahwa pengamanan sistem membutuhkan pendekatan yang lebih serius, karena data kependudukan termasuk kategori data strategis yang dapat memengaruhi proses administrasi pemerintahan jika jatuh ke tangan yang salah. Sedangkan implikasi terhadap sistem hukum nasional tampak melalui semakin pentingnya sinkronisasi antara UU ITE dan UU PDP dalam menangani kejahatan digital yang menasar data penduduk. Dua undang-undang tersebut memiliki ruang lingkup berbeda namun saling berkaitan, di mana UU ITE mengatur tindakan pidana yang berkaitan dengan sistem elektronik, sedangkan UU PDP mengatur perlindungan terhadap data pribadi yang menjadi objek kejahatan. Perkara Cikarang menegaskan bahwa kejahatan akses ilegal tidak dapat dipahami semata-mata sebagai pelanggaran sistem elektronik, tetapi juga sebagai pelanggaran terhadap hak informasi warga negara yang dilindungi oleh undang-undang (Wati *et al.*, 2024).

KESIMPULAN

Berdasarkan uraian-uraian di atas tersebut, maka dapat penelitian ini disimpulkan: Pertama, penegakan hukum tindak pidana akses ilegal dalam perkara pada Pengadilan Negeri Cikarang No. 515/Pid.Sus/2021/ PN.Ckr dengan terdakwa “Chandra” yang melakukan perbuatan mengakses secara tidak sah website Disdukcapil kabupaten Bekasi, mulai dari penyidikan hingga pemeriksaan dipengadilan telah dilakukan berdasarkan UU-ITE 2024 dan hukum acara pidana khusus yang tepat, karena dijadikannya “bukti elektronik” yang diperlukan untuk pembuktian, sehingga proses penegakan hukum dalam putusan PN Cikarang tersebut sudah objektif.

Kedua, bahwa pertanggungjawaban Pidana Pelaku Illegal Access dalam Putusan PN

Cikarang No. 515/Pid.Sus/2021/PN.Ckr., di mana menurut Majelis semua untur telah terpenuhi maka pertanggungjawaban pidana atas akses tanpa hak (illegal access) yang diatur Pasal 30 ayat (2) UU-ITE 2024” dengan ancaman pidana penjara maksimal tujuh tahun serta denda hingga Rp800 Juta, namun terdakwa dihukum lebih ringan dengan penjara selama 1 (satu) tahun dan denda sebesar Rp 200 juta, dan putusan tersebut tidak berkeadilan bagi para pemilik data yang menjadi korban.

Ketiga, bahwa Tindak Pidana Illegal Access menimbulkan berbagai implikasi hukum yang sangat luas, di mana selain karena ada sangkut-pautnya dengan stabilitas administrasi negara, serta kepercayaan masyarakat terhadap pemerintah, dan pemenuhan hak konstitusional warga atas perlindungan data pribadi. juga terkait hak privacy warga negara bagian dari hak asasi manusia yang dijamin Pasal 28G ayat (1) UUDNRI 1945, serta tanggungjawab negara yang mewajibkan pengendali data untuk menyediakan mekanisme keamanan berlapis yang mampu mengurangi risiko akses ilegal. Demikian juga implikasi hukum pada aspek pembuktian dalam tindak pidana siber memperlihatkan pentingnya bukti elektronik sebagai alat bukti sah.

DAFTAR REFERENSI

- Andhitya, R., & Umam, J. (2025). Analisis Kritis Penegakan Hukum Kejahatan Siber Data Breach Dalam Perspektif Hukum Pidana Indonesia. *Rewang Rencang : Jurnal Hukum Lex Generalis*, 6(8), 1–16.
- Anggraeni, A., & Amin, R. (2025). Penyidikan Berbasis Ilmiah Dalam Penegakan Hukum Tindak Pidana Akses Ilegal. *Jurnal Kajian Ilmu Kepolisian dan Anti Korupsi*, 2(1), 71–86.
- Annas, G. K., & Fatiha, N. (2025). Perlindungan Hukum Terhadap Korban Tindak Pidana Cyber: Tantangan Dan Solusi. *Jurnal Kliendi Law*, 2, 98–114. <https://jurnalkliendi-law.com/index.php/JKL/article/view/13%0Ahttps://jurnalkliendi-law.com/index.php/JKL/article/download/13/13>
- Azza Fitrahul Faizah, Sinta Dewi Rosadi & Garry Gumelar Pratama, “Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong dan Singapura,” Hakim: Jurnal Ilmu Hukum dan Sosial 1, no. 3 (2023): 1-27.
- Bayu Abdi, R. Juli Moertiono, “ Analisis Hukum Terhadap Akses Ilegal Website Pemerintah Untuk Digunakan Sebagai Website Perjudian (Studi Putusan Nomor 1308/Pid.Sus/2021/PN Jkt Utr) “Jurnal Pencerah Bangsa Volume 2, Nomor 2, (2023): 99-103 .
- Bitus Tanjung. Marjan Miharja, “Penerapan Sanksi Pidana Bagi Pelaku Tindak Pidana Peretasan (Studi Kasus Putusan Pengadilan Negeri Cikarang Nomor 515/PID.SUS/2021/PN.CKR),“ *Iblam Law Review*, Volume 4, Nomor 4, (2024):99-110. <https://doi.org/10.52249/ilr.v4i4.471>
- Darwan Prinst. (1998). *Hukum Acara Pidana Dalam Praktik*, Jakarta: Djambatan
- Febrianti, R. R., & Otto Yudianto. (2023). Upaya Perlindungan Hukum Bagi Korban Tindak Pidana Pencurian Secara Digital. *Sosialita*, 2(1), 75–84.
- Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia*, 4(2), 23–31. <https://doi.org/10.52005/rechten.v4i2.98>
- Firdaus, & Pratama, B. P. (2025). Judge’s Consideration of Evidence in the Crime of Illegal Access. *Ekasakti Journal of law and Justice*, 4(1), 64–71.
- Mahpudin, M., & Ahmad Tazzul Aripin. (2025). Akuntabilitas Komisi Pemilihan Umum Kota Serang Dalam Mengatasi Pencatutan Data Masyarakat Secara Ilegal Melalui Sistem Informasi Partai Politik (SIPOL) Pada Pilkada Tahun 2024. *Jurnal Silatene Sosial Humaniora*, 3(1), 1–9. <https://doi.org/10.53611/d8065b02>

- Mugiono, M., & Wiraguna, S. A. (2025). Antara Kemudahan dan Kerentanan: Analisis Yuridis Perlindungan Data Identitas Kependudukan dalam Aplikasi Digital. *COSMOS: Jurnal Ilmu Pendidikan, Ekonomi dan Teknologi*, 2(3), 684–691. <https://cosmos.iaisambas.ac.id/index.php/cms/article/view/287%0Ahttps://cosmos.iaisambas.ac.id/index.php/cms/article/download/287/144>.
- Muhammad Asthi Seta Ari Yuwana, Andhika Pratama Adhi, Abdul Hakim Al Baihaki, M. Asif Nur Fauzi, "Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 Dalam Perspektif HAM," *Jurnal Hukum dan HAM Wicarana*, Volume 4, Nomor 1, Maret 2025.
- Nethan, "Implementasi Fungsi Perlindungan Kementerian Komunikasi Dan Digital Dalam Melindungi Data Pribadi Warga Negara Indonesia," *Jurnal Kertha Semaya*, Vol. 13 No. 10 (2025): 2339-2349.
- Rahmawati, D. S., Rosadi, S. D., & Amelia Cahyadi. (2025). Implementasi Pelindungan Data Pribadi Berupa Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) pada Sistem Pemerintahan Berbasis Elektronik Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*, 3(2), 739–749. <https://ojs.daarulhuda.or.id/index.php/MHI/article/view/2038%0Ahttps://ojs.daarulhuda.or.id/index.php/MHI/article/download/2038/2189>
- Sirait, T. M. (2021). *Hukum Pidana Khusus dalam Teori dan Penegakannya*. CV Budi Utama.
- Tobing, C. I., Tiofanny Marilyn Surya, Selvias, L. R., Stepania Rehulina Girsang, Putri Berliana Azzahra, Lustri Yolanda Purba, Mahezha Agnia Putera, & Nurrahman Rusmana. (2024). Globalisasi Digital Dan Cybercrime: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. *Jurnal Hukum Sasana*, 10(2), 105–123. <https://doi.org/10.31599/sasana.v10i2.3170>
- Wantania, Z. J. (2025). Analysis of The Development of Legal Protection For Personal Data Security In The Digital Era. *Jurnal RechtsVinding*, 14(87), 179–194.
- Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *Jurnal Bevinding*, 2(1), 44–55.