PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA SIBER TENTANG AKSES ILEGAL DI INDONESIA

Arifuddin Aljundani[1], Niru Anita Sinaga[2]
Faculty Of Law, Air Marshal Suryadarma University
Email : aljundan@gmail.com[1], nirusinaga@unsurya.ac.id[2]

Cititation: Arifuddin Aljundani., Niru Anita Sinaga. Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Akses Ilegal Di Indonesia. *LEX LAGUENS: Jurnal Kajian Hukum dan Keadilan* 3.2.2025. 176-193
Submitted: 01-06-2025 **Revised:** 01-07-2025 **Accepted:** 01-08-2025

Abstrak

Kejahatan siber, khususnya akses ilegal *(illegal access)*, telah menjadi problematika serius seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi (TIK). Fenomena ini menimbulkan kerugian material dan imaterial yang signifikan bagi individu, korporasi, dan negara, sebagaimana dibuktikan dengan berbagai kasus akses ilegal di Indonesia seperti kebocoran data ASN dan peretasan situs lembaga negara. Penelitian ini bertujuan untuk menganalisis secara mendalam penegakan hukum terhadap pelaku tindak pidana akses ilegal di Indonesia, mengkaji kendala yang dihadapi. Penelitian ini menggunakan metode penelitian hukum normatif dengan menelaah peraturan perundang-undangan terkait. Hasil penelitian menunjukkan bahwa penegakan hukum akses ilegal di Indonesia didasarkan pada Pasal 30 UU ITE yang secara tegas melarang akses tanpa izin terhadap sistem elektronik, memperoleh informasi elektronik secara ilegal, dan menjebol sistem pengamanan. Sanksi pidana penjara dan denda diatur dalam Pasal 46 UU ITE. Dengan berlakunya KUHP baru (UU No. 1 Tahun 2023), ketentuan akses ilegal kini juga diatur dalam Pasal 322 ayat (3), menunjukkan harmonisasi hukum pidana siber.
Kata Kunci : Penegakan Hukum, Tindak Pidana, Siber, Akses Ilegal

Abstract

Cybercrime, especially illegal access, has become a serious problem along with the rapid development of information and communication technology (ICT). This phenomenon causes significant material and immaterial losses for individuals, corporations, and the state, as evidenced by various cases of illegal access in Indonesia such as ASN data leaks and hacking of state institution sites. This study aims to analyze in depth the enforcement of the law against perpetrators of illegal access crimes in Indonesia, examining the obstacles faced. This study uses a normative legal research method by examining related laws and regulations. The results of the study show that the enforcement of the law on illegal access in Indonesia is based on Article 30 of the ITE Law which expressly prohibits unauthorized access to electronic systems, obtaining electronic information illegally, and breaking into security systems. Criminal sanctions for imprisonment and fines are regulated in Article 46 of the ITE Law. With the enactment of the new Criminal Code (Law No. 1 of 2023), the provisions on illegal access are now also regulated in Article 322 paragraph (3), indicating the harmonization of cyber criminal law.
Keyword : Law Enforcement, Crime, Cyber, Illegal Access

A. PENDAHULUAN

Kejahatan merupakan problematik yang membayangi umat manusia. Tidak dapat dipungkiri bahwa kejahatan pasti terjadi dimana terdapat manusia-manusia yang mempunyai kepentingan berbeda-beda. Kejahatan memang dapat terjadi tanpa mengenal ruang dan waktu, serta dapat dilakukan oleh siapa saja. Kejahatan bukan merupakan peristiwa hereditas (bawaan sejak lahir, warisan), juga bukan merupakan warisan biologis. Tindak kejahatan bisa dilakukan secara sadar yaitu difikirkan, direncanakan dan diarahkan pada maksud tertentu secara sadar

benar. Kejahatan merupakan suatu konsepsi yang bersifat abstrak, dimana kejahatan tidak dapat diraba dan dilihat kecuali akibatnya saja.[1]

Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa perubahan fundamental dalam berbagai aspek kehidupan manusia, mulai dari interaksi sosial, ekonomi, hingga tata kelola pemerintahan. Internet, sebagai tulang punggung utama revolusi digital, telah membuka gerbang menuju era konektivitas tanpa batas, memungkinkan pertukaran informasi secara instan, transaksi global, dan aksesibilitas data yang belum pernah terbayangkan sebelumnya. Namun, di balik kemudahan dan efisiensi yang ditawarkan, TIK juga menyajikan tantangan serius, salah satunya adalah munculnya bentuk-bentuk kejahatan baru yang memanfaatkan celah dan kerentanan dalam sistem digital. Inilah yang kemudian dikenal sebagai tindak pidana siber *(cybercrime).*

Di antara berbagai jenis tindak pidana siber, akses ilegal *(illegal access)* menjadi salah satu bentuk yang paling mendasar dan sering terjadi. Akses ilegal merujuk pada tindakan masuk atau menyusup ke dalam sistem komputer atau jaringan secara tidak sah, tanpa izin atau otorisasi dari pemilik atau administrator yang berwenang. Motivasi di balik akses ilegal sangat beragam, mulai dari sekadar iseng *(defacing),* pencarian celah keamanan (*penetration testing* tanpa izin), hingga tujuan yang lebih merugikan seperti pencurian data *(data theft),* sabotase sistem, penipuan, atau bahkan *spionase.* Kasus-kasus pembobolan akun pribadi, peretasan situs web pemerintah atau swasta, hingga penyusupan ke dalam basis data sensitif lembaga keuangan, telah menjadi berita umum di Indonesia dan menimbulkan kerugian material maupun imaterial yang tidak sedikit.

Indonesia, sebagai negara dengan jumlah pengguna internet terbesar keempat di dunia, tidak luput dari ancaman akses ilegal. Data menunjukkan peningkatan signifikan dalam insiden keamanan siber, termasuk kasus akses ilegal yang menargetkan individu, korporasi, hingga infrastruktur vital negara. Kebocoran data pribadi jutaan penduduk, peretasan sistem perbankan, hingga sabotase situs web lembaga penting, telah menjadi bukti nyata kerentanan siber yang masih dihadapi. Fenomena ini tidak hanya mengancam privasi dan keamanan data individu, tetapi juga stabilitas ekonomi, kepercayaan publik terhadap lembaga digital, bahkan kedaulatan negara.

Berikut adalah beberapa contoh kasus yang pernah terjadi di Indonesia:

[1] Wahyu Widodo, 2015, *Kriminologi Dan Hukum Pidana*, Semarang: Universitas PGRI Semarang Press, p. 19.

1) Kebocoran Data Satu Data ASN (2024): Data sensitif milik 4,7 juta Pegawai Negeri Sipil (PNS) bocor ke dark web oleh kelompok peretas TopiAx.
2) Pencurian Database Polri (2021): Pelaku berhasil mencuri sekitar 28.000 informasi login dan data pribadi dari database Kepolisian Republik Indonesia.
3) Pembobolan Data Kementerian Komunikasi dan Informatika (Kominfo) (2022): Pelaku dengan nama samaran "Bjorka" mencuri data registrasi kartu SIM Kominfo.
4) Peretasan Website Kejagung RI (2021): Website Kejaksaan Agung Republik Indonesia diretas oleh seorang remaja yang mengaku iseng.
5) Website DPR-RI Berganti Nama (2020): Website DPR-RI mengalami serangan DDoS dan namanya berubah.
6) Akses Ilegal pada Sistem Transportasi Online (Order Fiktif): Tujuh pengemudi Grab ditangkap karena memanipulasi aplikasi Grab dengan GPS agar seolah-olah mengantar penumpang, padahal tidak, untuk mendapatkan keuntungan finansial.

Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan landasan hukum utama dalam penanganan *cyber crime* di Indonesia. Undang-undang ini mengatur berbagai jenis perbuatan yang dikategorikan sebagai tindak pidana siber beserta sanksi pidana yang dapat dikenakan terhadap pelakunya.

Meskipun telah ada regulasi yang mengatur, penegakan hukum terhadap pelaku *cyber crime* di Indonesia masih menghadapi berbagai tantangan. Kompleksitas teknis kejahatan siber, kurangnya pemahaman aparat penegak hukum mengenai teknologi informasi, kesulitan dalam mengidentifikasi dan melacak pelaku yang seringkali beroperasi lintas negara, serta minimnya kerjasama internasional menjadi beberapa kendala yang dihadapi.

Selain itu, dinamika perkembangan *cyber crime* yang sangat cepat menuntut adanya adaptasi dan inovasi dalam metode penegakan hukum. Aparat penegak hukum perlu terus meningkatkan kapasitas dan keahlian dalam bidang *forensik digital*, analisis data, serta pemahaman terhadap modus operandi pelaku *cyber crime* yang semakin canggih.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara mendalam mengenai penegakan hukum terhadap pelaku tindak pidana *cyber crime* di Indonesia. Penelitian ini akan mengkaji efektivitas peraturan perundang-undangan yang ada, tantangan-tantangan yang dihadapi oleh aparat penegak hukum, serta upaya-upaya yang dapat dilakukan untuk meningkatkan efektivitas penegakan hukum dalam memberantas *cyber crime.*

Berdasarkan latar belakang yang telah di uraikan, menjadi penting untuk beberapa rumusan masalah, yaitu: bagaimana penegakan hukum terhadap pelaku tindak pidana kejahatan siber tentang akses ilegal di Indonesia? dan kendala apa yang dihadapi dalam penegakan hukum terhadap pelaku tindak pidana siber tentang akses ilegal di Indonesia?

B. METODE PENELITIAN

Jenis penelitian yang digunakan oleh penulis adalah penelitian normatif. Penelitian hukum normatif yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur yang berkaitan pendekatan perundang-undangan *(Statute Approach)* dan pendekatan kasus *(Case Approach).* Sesuai dengan jenis penelitiannya, maka dalam penelitian ini menggunakan jenis data sekunder.[2] Teknik pengumpulan data dalam penelitian hukum normatif dilakukan dengan studi pustaka terhadap bahan-bahan hukum, baik bahan hukum primer, bahan hukum sekunder, maupun bahan hukum tersier dan atau bahan non-hukum. Pengolahan bahan dilakukan dengan cara, melakukan seleksi data sekunder atau bahan hukum, kemudian melakukan klasifikasi menurut penggolongan bahan hukum dan menyusun data hasil penelitian tersebut secara sistematis.[3]

C. HASIL PENELITIAN DAN PEMBAHASAN

1. Penegakan Hukum Terhadap Pelaku Tindak Pidana Kejahatan Siber Tentang Akses Ilegal Di Indonesia

Kejahatan siber, khususnya akses ilegal *(unauthorized access),* telah menjadi ancaman serius dalam lanskap hukum di Indonesia seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Akses ilegal, yang seringkali menjadi pintu gerbang bagi kejahatan siber lain seperti pencurian data, hacking, atau penipuan daring, menimbulkan kerugian material dan immaterial yang signifikan, baik bagi individu, korporasi, maupun negara. Pembahasan ini akan menganalisis secara komprehensif aspek-aspek penegakan hukum

[2] Soerjono Soekanto, 2008, *Pengantar Penelitian Hukum*, Jakarta: Universitas Indonesia, p. 11.
[3] Niru Anita Sinaga, "Pelaksanaan Pembinaan Kemandirian Bagi Narapidana Di Lapas Perempuan Kelas IIa Jakarta (Periode 1 Mei S

terhadap pelaku tindak pidana akses ilegal di Indonesia, meliputi dasar hukum, tantangan, serta prospek ke depan dalam upaya menciptakan ruang siber yang aman dan tertib.[4]

3) Kerangka Hukum Penegakan Tindak Pidana Akses Ilegal

Penegakan hukum terhadap tindak pidana akses ilegal di Indonesia didasarkan pada seperangkat peraturan perundang-undangan, dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024 (UU ITE Perubahan Kedua) sebagai payung hukum utamanya.

a) Ketentuan Pidana dalam UU ITE

Pasal 30 UU ITE[5]

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperolehInformasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan

Pasal 30 UU ITE. Pasal ini secara tegas melarang:

3) Akses Ilegal Terhadap Komputer dan/atau Sistem Elektronik Orang Lain.

Pasal 30 Ayat 1 Ayat ini melarang tindakan akses tanpa izin terhadap komputer dan/atau sistem elektronik milik orang lain, dengan cara apa pun. Frasa "dengan cara apa pun" menunjukkan cakupan yang luas, meliputi segala upaya untuk masuk atau terhubung ke sistem tanpa adanya hak atau izin yang sah. Bahkan, upaya masuk yang tidak mengakibatkan perubahan data atau kerugian sekalipun sudah termasuk dalam larangan ini. Contohnya termasuk mencoba menebak password, menggunakan software untuk memindai port yang terbuka, atau

[4] Oky Syalendro et al., "Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan dan Penanganan Kasus Tindak Pidana Cyber Crime", *Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia*, Vol. 4 No. 1, January 2025.

[5] Indonesia, Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

mencoba masuk ke jaringan nirkabel tanpa izin. Intinya, niat untuk mengakses secara tidak sah, terlepas dari hasilnya, sudah dapat dipidana.[6]

3) Akses Ilegal untuk Memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Pasal 30 Ayat 2 secara khusus menargetkan tindakan akses ilegal yang disertai dengan niat untuk memperoleh informasi elektronik dan/atau dokumen elektronik secara tidak sah. Fokusnya adalah pada tujuan atau motif pelaku, yaitu mencuri, melihat, menyalin, atau mengambil data tanpa izin. Sebagai contoh, seorang individu yang berhasil masuk ke akun email orang lain dan membaca isinya, atau mengunduh dokumen rahasia perusahaan tanpa hak, dapat dijerat dengan ayat ini. Meskipun aksesnya mungkin tidak merusak sistem, niat untuk mengambil atau melihat data secara ilegal menjadi elemen penting dalam pasal ini.[7]

3) Akses Ilegal dengan Melanggar Sistem Pengaman

Pasal 30 Ayat 3 adalah yang paling spesifik, menargetkan tindakan akses ilegal yang dilakukan dengan cara melanggar, menerobos, melampaui, atau menjebol sistem pengaman. Ini secara langsung mengacu pada metode-metode peretasan atau *hacking* yang canggih, seperti menggunakan malware, eksploitasi celah keamanan *(vulnerability),* atau teknik-teknik cracking lainnya untuk menembus proteksi yang telah dipasang. Pasal ini menekankan bahwa tindakan peretasan terhadap sistem keamanan, meskipun mungkin tidak secara langsung mengambil data atau merusak sistem, sudah merupakan tindak pidana karena telah melanggar integritas keamanan siber.[8]

Ketentuan pidana terkait Pasal 30 UU ITE diatur lebih lanjut dalam Pasal 46 UU ITE yang mengatur sanksi bagi setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30. Sanksinya meliputi:

2) Ancaman Pidana Penjara: Bervariasi tergantung pada ayat yang dilanggar, mulai dari pidana penjara paling lama 6 (enam) tahun hingga 8 (delapan) tahun.

---

[6] Renata Christha Auli, June 28th, 2025, *"Bunyi Pasal 30 ayat (1) UU ITE tentang Peretasan"*, https://www.hukumonline.com/klinik/a/bunyi-pasal-30-ayat-1-uu-ite-tentang-peretasan-lt659e7c363776f/, Accessed on June 28th, 2025.

[7] Inggou David Purba, "Delik Pidana Akses Ilegal (Hacking) terhadap Komputer atau Sistem Elektronik", *Bulletin of Community Engagement*, Vol. 4 No. 2, August 2024.

[8] Choiriyah Indriyati Putri, June 28th, 2025, *"Pasal Berlapis untuk Pelaku Phishing, Pidana Penjara hingga Belasan Tahun!"*, https://www.inilah.com/pasal-berlapis-bagi-pelaku-phishing, Accessed on June 28th, 2025.

2) Denda: Sanksi denda juga diberlakukan, dengan nominal yang bervariasi dari paling banyak Rp600.000.000,00 (enam ratus juta rupiah) hingga Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 30 UU ITE memiliki peran vital dalam penegakan hukum siber di Indonesia karena:[9]

a) Melindungi Privasi dan Data Pribadi: Dengan melarang akses ilegal, pasal ini secara tidak langsung melindungi privasi individu dan kerahasiaan data pribadi yang tersimpan dalam sistem elektronik.
b) Menjaga Keamanan Sistem Elektronik: Pasal ini menegaskan bahwa setiap upaya untuk merusak atau menembus sistem keamanan adalah perbuatan melawan hukum, sehingga mendorong pengelola sistem untuk meningkatkan keamanan dan para pengguna untuk tidak melakukan tindakan yang merugikan.
c) Memberikan Kepastian Hukum: Adanya pasal ini memberikan landasan hukum yang jelas bagi penegak hukum untuk menindak pelaku kejahatan siber, sekaligus memberikan edukasi kepada masyarakat tentang batasan-batasan dalam berinteraksi di dunia digital.
d) Mendorong Etika Berinternet: Secara tidak langsung, pasal ini juga mendorong pengguna internet untuk memiliki etika yang

2) Peran Kitab Undang-Undang Hukum Pidana (KUHP)

Meskipun UU ITE secara spesifik mengatur tindak pidana akses ilegal, seringkali perbuatan tersebut tidak berhenti pada akses semata. Data yang berhasil diakses secara ilegal bisa jadi digunakan untuk melakukan tindak pidana lain yang diatur dalam KUHP. Inilah titik temu penting antara UU ITE dan KUHP:[10]

a) Pencurian Data yang Berujung pada Penipuan (Pasal 378 KUHP): Seorang peretas yang berhasil mengakses data pribadi seseorang, lalu menggunakan data tersebut untuk melakukan penipuan finansial, seperti mengajukan pinjaman online atas nama korban atau membeli barang secara ilegal. Dalam kasus ini, peretas dapat dijerat dengan Pasal 30 UU ITE untuk akses ilegalnya, dan sekaligus dengan Pasal 378 KUHP karena telah melakukan penipuan.

[9] Asaad Ahmad, June 28th, 2025, *"Illegal Access, Apakah Itu?"*, https://htlegalconsult.com/illegal-access-apakah-itu/, Accessed on June 28th, 2025.
[10] Muhammad Raihan Nugraha, June 29th, 2025, *"Cara Menentukan Pasal untuk Menjerat Pelaku Penipuan Online"*, https://www.hukumonline.com/klinik/a/cara-menentukan-pasal-untuk-menjerat-pelaku-penipuan-ionline-i-lt5d1ad428d8fa3/, Accessed on June 29th, 2025.

b) Akses Ilegal untuk Pemerasan (Pasal 368 KUHP): Ketika seseorang secara ilegal mendapatkan informasi atau foto sensitif dari sistem elektronik orang lain, kemudian menggunakan informasi tersebut untuk mengancam dan memeras korban agar menyerahkan uang atau keuntungan lain, maka pelaku tidak hanya melanggar Pasal 30 UU ITE tetapi juga Pasal 368 KUHP tentang pemerasan.
c) Penggelapan (Pasal 372 KUHP): Akses ilegal dilakukan untuk menguasai aset digital atau informasi yang bernilai ekonomis dan kemudian digunakan untuk kepentingan pribadi tanpa hak, bisa jadi terjadi persinggungan dengan tindak pidana penggelapan

Terlepas dari spesifikasi tindak pidana dalam UU ITE, proses hukum dan penanganan kasus tindak pidana akses ilegal tidak bisa lepas dari konsep-konsep dasar hukum pidana yang termaktub dalam KUHP. Konsep-konsep ini menjadi pondasi bagi aparat penegak hukum dalam menganalisis dan membuktikan suatu tindak pidana:

a) Percobaan *(Poging)*: KUHP mengatur konsep percobaan tindak pidana. Jika seseorang mencoba melakukan akses ilegal tetapi gagal, ia tetap dapat dijerat dengan Pasal 30 UU ITE juncto Pasal 53 KUHP tentang percobaan. Hal ini penting untuk menindak upaya-upaya kejahatan siber sejak dini, sebelum dampak buruknya terjadi.
b) Penyertaan *(Deelneming)*: Dalam kasus kejahatan siber yang melibatkan lebih dari satu pelaku (misalnya, satu orang melakukan hacking, yang lain menyediakan tools, dan yang lainnya lagi mendanai), konsep penyertaan dalam KUHP (Pasal 55 dan 56 KUHP) menjadi sangat relevan. KUHP memungkinkan penegak hukum untuk menjerat semua pihak yang terlibat, baik sebagai pelaku utama, penganjur, maupun pembantu.
c) Perbarengan Tindak Pidana *(Concursus)*: Ketika satu perbuatan melanggar lebih dari satu ketentuan pidana atau beberapa perbuatan membentuk satu rangkaian kejahatan, KUHP menyediakan mekanisme perbarengan tindak pidana (Pasal 63-66 KUHP). Konsep ini memastikan bahwa pelaku dipertanggungjawabkan atas semua tindak pidana yang dilakukannya, tidak hanya yang paling berat

3) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Berlakunya Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP baru), peran KUHP dalam konteks tindak pidana akses ilegal akan semakin krusial. KUHP baru membawa semangat harmonisasi dan sinkronisasi ketentuan pidana umum dengan perkembangan kejahatan modern, termasuk kejahatan siber.

Ketentuan mengenai akses ilegal dari UU ITE direformulasi dan dimuat dalam Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Secara spesifik, Pasal 322 ayat (3) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana mengatur tindak pidana akses ilegal: "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda."[11]

2. Penegakan Hukum Tindak Pidana Akses Ilegal

Tindak pidana akses ilegal *(unauthorized access)* merupakan salah satu bentuk kejahatan siber yang semakin meresahkan di era digital ini. Kejahatan ini melibatkan upaya seseorang untuk mendapatkan akses ke sistem komputer, jaringan, atau data tanpa izin yang sah. Penegakan hukum terhadap tindak pidana ini menjadi penting untuk menjaga keamanan siber, melindungi privasi data, dan memastikan integritas sistem informasi.

Penegakan hukum terhadap tindak pidana akses ilegal di Indonesia merupakan sebuah proses berlapis yang melibatkan berbagai tahapan dan institusi. Ini adalah upaya kolaboratif untuk memastikan bahwa pelaku kejahatan siber dapat diidentifikasi, diproses secara hukum, dan diberikan sanksi sesuai dengan undang-undang yang berlaku.[12]

Penegakan hukum tindak pidana akses ilegal melibatkan beberapa tahapan dan institusi:

1) Penyelidikan dan Penyidikan:
    a) Kepolisian Republik Indonesia (POLRI): POLRI, khususnya Unit-unit Siber seperti Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri, memegang peran sentral dan utama. Mereka adalah garda terdepan dalam menyelidiki dan menyidik kasus-kasus akses ilegal. Unit-unit ini dilengkapi dengan keahlian forensik digital yang mendalam dan peralatan canggih untuk mengumpulkan bukti elektronik yang rentan. Tim siber Polri terlatih untuk melacak jejak digital, mengidentifikasi alamat IP, menganalisis log server, dan melakukan data recovery dari perangkat yang terkompromi. Mereka juga berkoordinasi dengan lembaga internasional jika kejahatan tersebut bersifat lintas batas.

[11] Indonesia, Pasal 322 ayat (3) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.
[12] Adinda Lola Sariani, "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia", *Al-Dalil: Jurnal Ilmu Sosial, Politik, dan Hukum*, Vol. 2 No. 2, July 2024.

b) Jaksa Penuntut Umum (Kejaksaan RI): Setelah proses penyidikan oleh Polri selesai dan berkas perkara dianggap lengkap (sering disebut sebagai P-21), peran beralih ke Jaksa Penuntut Umum dari Kejaksaan RI. Jaksa akan meneliti berkas perkara, memastikan semua unsur pidana terpenuhi, dan menyusun surat dakwaan. Mereka kemudian akan melimpahkan perkara tersebut ke pengadilan untuk disidangkan. Jaksa juga bertanggung jawab dalam mengajukan tuntutan pidana selama persidangan.

c) PPNS (Penyidik Pegawai Negeri Sipil) di Kementerian Komunikasi dan Digital (Komdigi): Kementerian Komunikasi dan Digital (Komdigi) juga memiliki Penyidik Pegawai Negeri Sipil (PPNS) yang diberikan kewenangan untuk melakukan penyidikan terhadap pelanggaran Undang-Undang ITE. Meskipun dalam praktiknya sebagian besar kasus pidana yang kompleks dan besar, khususnya terkait akses ilegal, akan ditangani oleh Polri karena cakupan kewenangan dan kapasitas investigasi yang lebih luas, PPNS Komdigi dapat berperan dalam kasus-kasus yang lebih spesifik terkait pelanggaran administratif atau teknis dalam penyelenggaraan sistem elektronik yang diatur oleh Komdigi. Mereka sering kali berfokus pada pelanggaran yang berkaitan dengan peraturan turunan UU ITE.

2) Pembuktian:

Tahap pembuktian adalah inti dari proses peradilan, di mana fakta-fakta kejahatan diungkapkan dan disahkan di mata hukum.

a) Alat Bukti Elektronik: Dalam kasus akses ilegal, bukti elektronik memegang peranan yang sangat penting, bahkan krusial. Ini adalah tulang punggung dari setiap kasus siber. Bukti ini dapat beragam bentuknya, termasuk:
   a. Log sistem: Catatan otomatis dari aktivitas yang terjadi di server, komputer, atau jaringan, seperti upaya login yang gagal, akses file, atau koneksi jaringan.
   b. Catatan aktivitas jaringan: Informasi mengenai lalu lintas data, alamat IP, dan port yang digunakan.
   c. Salinan data: Duplikasi data yang diakses atau dimanipulasi oleh pelaku.
   d. Jejak digital di perangkat: Cache, cookies, riwayat Browse, atau file sisa di komputer pelaku atau korban yang menunjukkan aktivitas.

e. Metadata: Informasi tentang data itu sendiri, seperti tanggal pembuatan, modifikasi terakhir, atau pengguna yang mengaksesnya. Integritas dan keaslian bukti-bukti ini harus dijaga dengan ketat melalui proses chain of custody yang valid.

b) Ahli Forensik Digital: Karena sifat teknis dari bukti elektronik, keterangan ahli forensik digital menjadi sangat penting. Para ahli ini memiliki spesialisasi dalam menganalisis bukti elektronik, merekonstruksi kejadian siber (misalnya, bagaimana pelaku bisa menembus sistem), dan menjelaskan temuan teknis yang kompleks kepada penyidik, jaksa, dan hakim dengan bahasa yang mudah dipahami. Mereka memastikan bahwa bukti-bukti tersebut valid secara ilmiah dan dapat diterima di pengadilan.

Digital forensik adalah bidang ilmu yang berfokus pada identifikasi, pengumpulan, analisis, dan presentasi bukti digital yang ditemukan dalam perangkat elektronik seperti handphone, laptop, atau komputer. Digital forensik bertujuan untuk melacak kejahatan siber yang melibatkan penggunaan teknologi digital.

c) Saksi: Selain bukti teknis, saksi juga berperan dalam memperkuat kasus. Saksi dapat berupa:

a. Pemilik sistem yang diakses secara ilegal: Mereka dapat memberikan keterangan tentang bagaimana mereka mengetahui adanya akses ilegal atau dampak yang ditimbulkan.
b. Administrator jaringan: Mereka dapat memberikan informasi teknis tentang konfigurasi sistem, upaya keamanan yang telah dilakukan, atau log yang mereka amati.
c. Individu lain yang memiliki pengetahuan relevan: Misalnya, seseorang yang menemukan kerentanan, atau pihak yang berinteraksi dengan pelaku.

3) Persidangan:

Tahap akhir adalah persidangan, di mana kebenaran materiil diuji dan putusan hukum dijatuhkan.

a) Pengadilan: Perkara akan diadili di pengadilan negeri yang berwenang. Selama persidangan, hakim akan memimpin jalannya pemeriksaan, memastikan proses berjalan adil dan sesuai hukum acara. Hakim akan memeriksa semua bukti-bukti yang diajukan oleh penuntut umum dan pihak pembela, mendengarkan secara

cermat keterangan dari saksi-saksi dan ahli, serta mempertimbangkan semua fakta-fakta hukum yang relevan dengan kasus tersebut. Pihak pembela juga memiliki kesempatan untuk membantah bukti atau argumen yang diajukan oleh penuntut umum.

b) Putusan Hakim: Berdasarkan seluruh fakta yang terungkap selama persidangan, keyakinan hakim, dan alat bukti yang sah, hakim akan menjatuhkan putusan. Putusan ini bisa menyatakan apakah terdakwa terbukti bersalah atas tindak pidana akses ilegal sesuai dakwaan, atau tidak terbukti bersalah sehingga harus dibebaskan. Jika terdakwa dinyatakan bersalah, hakim akan menentukan jenis dan beratnya sanksi pidana yang akan dijatuhkan, yang harus sesuai dengan ancaman pidana yang diatur dalam Undang-Undang ITE atau KUHP baru.

Melalui kolaborasi antarlembaga ini dan proses yang terstruktur, diharapkan penegakan hukum terhadap tindak pidana akses ilegal dapat berjalan efektif, memberikan keadilan bagi korban, dan memberikan efek jera bagi pelaku kejahatan siber.

Berdasarkan kasus tujuh pengemudi Grab yang melakukan order fiktif, berikut analisis singkatnya sesuai aturan yang berlaku. Kasus ini dapat dijerat dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya:

1) Pasal 30 ayat (3) tentang Akses Ilegal: Pelaku sengaja dan tanpa hak mengakses sistem elektronik milik orang lain (Grab) dengan cara apa pun, yaitu memanipulasi GPS.
2) Pasal 32 ayat (1) tentang Perubahan Informasi Elektronik: Pelaku memodifikasi atau mengubah informasi pada sistem Grab, yaitu data lokasi perjalanan fiktif, untuk mendapatkan keuntungan ilegal.

Selain itu, pelaku juga bisa dikenai pasal pidana lain: Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) tentang Penipuan: Para pengemudi ini melakukan serangkaian perbuatan curang (memanipulasi sistem) untuk menggerakkan Grab (korban) agar menyerahkan uang (insentif atau biaya perjalanan) yang seharusnya tidak mereka terima.

Sanksi pidana yang dapat dijatuhkan kepada para pelaku cukup berat:

1) Akses Ilegal (Pasal 30 ayat 3 UU ITE): Ancaman hukuman pidana penjara maksimal 8 tahun dan/atau denda maksimal Rp800 juta.
2) Perubahan Informasi Elektronik (Pasal 32 ayat 1 UU ITE): Ancaman hukuman penjara maksimal 8 tahun dan/atau denda maksimal Rp2 miliar.
3) Penipuan (Pasal 378 KUHP): Ancaman hukuman penjara maksimal 4 tahun.

Selain konsekuensi hukum, para pengemudi ini juga akan menghadapi konsekuensi dari pihak Grab, seperti pemutusan mitra secara permanen dan tuntutan ganti rugi.

Dari pembahasan di atas penulis berpendapat bahwa kerangka hukum dan kelembagaan yang ada menunjukkan komitmen kuat Indonesia dalam menjaga keamanan siber. Namun, dinamika kejahatan siber menuntut adaptasi berkelanjutan dalam regulasi dan peningkatan kapasitas penegak hukum untuk memastikan efektivitas dan keadilan.

3. Kendala Yang Dihadapi Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Siber Tentang Aakses Ilegal Di Indonesia

Penegakan hukum terhadap tindak pidana siber, khususnya akses ilegal, di Indonesia menghadapi berbagai tantangan kompleks. Sifat kejahatan siber yang dinamis dan perkembangan teknologi yang pesat seringkali menjadi rintangan bagi aparat penegak hukum. Berikut adalah beberapa kendala utama yang dihadapi:

1) Karakteristik Tindak Pidana Siber yang Unik[13]
   a) Sifat Lintas Batas (*Transnasional*): Pelaku akses ilegal dapat berada di mana saja di dunia, meretas sistem yang berlokasi di Indonesia atau sebaliknya. Hal ini menimbulkan kesulitan dalam masalah yurisdiksi dan kerjasama internasional. Proses ekstradisi atau pertukaran informasi antarnegara seringkali memakan waktu lama dan melibatkan birokrasi yang rumit, atau bahkan terhambat oleh perbedaan hukum antarnegara.
   b) Anonimitas Pelaku: Pelaku kejahatan siber seringkali menggunakan berbagai teknik untuk menyembunyikan identitas dan lokasi mereka, seperti *Virtual Private Network* (VPN), jaringan Tor, *proxy server*, atau bahkan memanfaatkan *botnet* yang tersebar di berbagai belahan dunia. Hal ini membuat pelacakan identitas pelaku menjadi sangat sulit dan membutuhkan keahlian teknis yang tinggi serta sumber daya yang memadai.
   c) Perkembangan Modus Operandi yang Cepat: Dunia siber terus berkembang dengan munculnya teknologi baru setiap saat, begitu pula dengan metode kejahatan siber. Para peretas selalu mencari celah keamanan terbaru atau mengembangkan teknik baru untuk melakukan akses ilegal. Aparat penegak

[13] Muchlisin Riadi, June 28th, 2025, *"Pengertian, Bentuk dan Tindak Pidana Cyber Crime"*, https://www.kajianpustaka.com/2018/03/pengertian-bentuk-dan-tindak-pidana-cyber-crime.html, Accessed on June 28th, 2025.

hukum harus terus-menerus memperbarui pengetahuan dan keterampilan mereka agar tidak tertinggal.

2) Tantangan dalam Pembuktian Elektronik[14]
   a) Volatilitas Bukti Digital: Bukti elektronik sangat *volatile* (mudah berubah atau hilang). Data dapat dihapus, dienkripsi, atau dimodifikasi dalam hitungan detik. Jika penanganan tidak cepat dan tepat, integritas bukti bisa rusak atau bahkan hilang sama sekali, membuat sulit untuk digunakan di pengadilan.
   b) Kecukupan dan Keaslian Bukti: Memastikan bahwa bukti elektronik yang ditemukan itu asli dan tidak dimanipulasi adalah tantangan besar. Diperlukan prosedur forensik digital yang ketat dan standar operasional yang jelas untuk pengumpulan, analisis, dan penyajian bukti.
   c) Kurangnya Pemahaman Hukum tentang Bukti Elektronik: Meskipun UU ITE mengakui bukti elektronik, masih ada keterbatasan pemahaman di kalangan penegak hukum, jaksa, dan hakim mengenai seluk-beluk teknis bukti digital. Ini dapat menghambat proses persidangan dan memengaruhi keyakinan hakim dalam menilai bobot bukti tersebut.
3) Keterbatasan Sumber Daya dan Kapasitas Aparat Penegak Hukum[15]
   a) Kekurangan Sumber Daya Manusia Ahli: Indonesia masih kekurangan penyidik, analis forensik digital, dan jaksa yang memiliki spesialisasi mendalam dalam tindak pidana siber. Pelatihan yang memadai dan berkelanjutan sangat dibutuhkan untuk meningkatkan kapasitas ini.
   b) Keterbatasan Anggaran dan Peralatan: Investigasi kejahatan siber membutuhkan peralatan dan perangkat lunak forensik digital yang canggih, serta infrastruktur teknologi yang memadai. Keterbatasan anggaran seringkali menjadi kendala dalam pengadaan dan pembaruan fasilitas ini.
   c) Koordinasi Antar Lembaga: Penanganan kasus siber seringkali melibatkan berbagai instansi (Polri, Kejaksaan, Komdigi, Badan Siber dan Sandi Negara/BSSN, perbankan, penyedia layanan internet). Koordinasi dan

[14] Fauziah Lubis dan Sofia Ramadhani Purba, "Analisis Kritik Pembuktian Elektronik Dalam Hukum Acara Perdata: Tantangan Dan Prospek Di Era Digital", *Judge: Jurnal Hukum*, Vol. 05 No. 02, 2024.
[15] Muhammad Singgih Imam Wibowo et al., "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia", *Rewang Rencang: Jurnal Hukum Lex Generalis*, Vol. 5 No. 7, 2024.

sinkronisasi antarlembaga ini kadang masih menjadi tantangan, yang dapat memperlambat proses penegakan hukum

4) Permasalahan Regulasi dan Kebijakan

Dalam hal ini penulis berpandangan beberapa hal terkait permasalah regulasi dan kebijikan, diantaranya:

a) Perkembangan Hukum yang Tertinggal: Meskipun UU ITE telah ada, kecepatan perkembangan teknologi seringkali membuat regulasi menjadi usang atau kurang relevan dalam menangani modus kejahatan baru. Diperlukan revisi atau penambahan regulasi yang lebih responsif terhadap perubahan teknologi.
b) Penafsiran Hukum: Beberapa ketentuan dalam UU ITE masih dapat ditafsirkan secara multitafsir, yang bisa menimbulkan inkonsistensi dalam penegakan hukum. Klarifikasi melalui peraturan pelaksana atau yurisprudensi pengadilan sangat dibutuhkan.
c) Perlindungan Data Pribadi: Meskipun ada aturan tentang perlindungan data, implementasi dan penegakannya masih memerlukan penguatan, terutama dalam konteks penanganan data korban yang terkait dengan akses ilegal.

5) Tantangan Non-Teknis Lainnya

Beberapa tantangan dalam penegakan hukum kejahatan siber, yang penulis kemukan yaitu:

a) Kurangnya Pelaporan: Korban akses ilegal, terutama perusahaan, terkadang enggan melaporkan insiden karena khawatir akan reputasi buruk atau kerugian bisnis. Hal ini menyebabkan banyak kasus tidak terungkap dan pelaku tidak terjamah hukum.
b) Kesadaran Masyarakat yang Rendah: Tingkat kesadaran masyarakat tentang keamanan siber dan pentingnya melaporkan tindak pidana siber masih relatif rendah. Ini mempengaruhi partisipasi masyarakat dalam upaya pemberantasan kejahatan siber.

Dari kendala-kendala di atas penulis berpendapat bahwa dalam mengatasi kendala tersebut memerlukan pendekatan multi-pihak yang melibatkan pemerintah, lembaga penegak hukum, sektor swasta, akademisi, dan masyarakat. Peningkatan investasi dalam pelatihan dan teknologi, penguatan kerjasama internasional, serta penyempurnaan kerangka hukum akan

menjadi kunci untuk penegakan hukum yang lebih efektif terhadap pelaku tindak pidana akses ilegal di Indonesia.

D. KESIMPULAN

Penegakan hukum terhadap pelaku tindak pidana kejahatan siber tentang akses ilegal di Indonesia merupakan upaya multidimensional yang melibatkan kerangka hukum yang kuat, kapasitas aparat penegak hukum yang memadai, serta kerjasama lintas sektor. Meskipun tantangan yang dihadapi tidak sedikit, komitmen pemerintah dan adaptasi terhadap perkembangan teknologi menjadi kunci untuk menciptakan ruang siber yang aman. Dengan terus meningkatkan kapasitas, mempererat kolaborasi, dan berinovasi dalam pendekatan penegakan hukum, Indonesia dapat memperkuat pertahanannya melawan kejahatan siber dan menjamin keadilan bagi korban

Kendala yang dihadapi dalam penegakan hukum terhadap pelaku tindak pidana siber tentang aakses ilegal di Indonesia adalah perlunya pendekatan multi-pihak yang melibatkan pemerintah, lembaga penegak hukum, sektor swasta, akademisi, dan masyarakat. Peningkatan investasi dalam pelatihan dan teknologi, penguatan kerjasama internasional, serta penyempurnaan kerangka hukum akan menjadi kunci untuk penegakan hukum yang lebih efektif terhadap pelaku tindak pidana akses ilegal di Indonesia.

E. SARAN

Diperlukan pengembangan lebih lanjut terhadap hukum acara pidana siber yang secara spesifik mengakomodasi karakteristik unik bukti elektronik dan tantangan yurisdiksi. Ini bisa berupa pedoman teknis yang lebih detail atau bahkan amandemen hukum acara pidana.

Perlunya perhatian pemerintah terutama dalam peningkatkan kapasitas aparat, membuat peraturan pelaksana yang lebih jelas untuk menghindari multitafsir, meningkatkan koordinasi antar lembaga penegak hukum di dalam negeri (Polri, Kejaksaan, Kominfo, BSSN) serta pererat kerja sama internasional untuk mengatasi kejahatan siber lintas batas, standarisasi prosedur forensik digital dan manfaatkan teknologi terkini, dan gencarkan kampanye literasi digital untuk meningkatkan kesadaran masyarakat tentang risiko siber dan mendorong pelaporan insiden tanpa rasa takut.

DAFTAR PUSTAKA

Auli, Renata Christha. June 28th, 2025. *"Bunyi Pasal 30 ayat (1) UU ITE tentang Peretasan"*. https://www.hukumonline.com/klinik/a/bunyi-pasal-30-ayat-1-uu-ite-tentang-peretasan-lt659e7c363776f/. Accessed on June 28th, 2025.

Ahmad, Asaad. June 28th, 2025. *"Illegal Access, Apakah Itu?"*. https://htlegalconsult.com/illegal-access-apakah-itu/. Accessed on June 28th, 2025.

Indriyati Putri, Choiriyah. June 28th, 2025. *"Pasal Berlapis untuk Pelaku Phishing, Pidana Penjara hingga Belasan Tahun!"*. https://www.inilah.com/pasal-berlapis-bagi-pelaku-phishing. Accessed on June 28th, 2025.

Lubis, Fauziah, dan Sofia Ramadhani Purba. "Analisis Kritik Pembuktian Elektronik Dalam Hukum Acara Perdata: Tantangan Dan Prospek Di Era Digital". *Judge: Jurnal Hukum*. Vol. 05 No. 02. 2024.

Nugraha, Muhammad Raihan. June 29th, 2025. *"Cara Menentukan Pasal untuk Menjerat Pelaku Penipuan Online"*. https://www.hukumonline.com/klinik/a/cara-menentukan-pasal-untuk-menjerat-pelaku-penipuan-ionline-i-lt5d1ad428d8fa3/. Accessed on June 29th, 2025.

Purba, Inggou David. "Delik Pidana Akses Ilegal (Hacking) terhadap Komputer atau Sistem Elektronik". *Bulletin of Community Engagement*. Vol. 4 No. 2. August 2024.

Riadi, Muchlisin. June 28th, 2025. *"Pengertian, Bentuk dan Tindak Pidana Cyber Crime"*. https://www.kajianpustaka.com/2018/03/pengertian-bentuk-dan-tindak-pidana-cyber-crime.html. Accessed on June 28th, 2025.

Sariani, Adinda Lola. "Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia". *Al-Dalil: Jurnal Ilmu Sosial, Politik, dan Hukum*. Vol. 2 No. 2. July 2024.

Sinaga, Niru Anita. "Pelaksanaan Pembinaan Kemandirian Bagi Narapidana Di Lapas Perempuan Kelas IIa Jakarta (Periode 1 Mei Sampai 31 Juli 2024)". *Lex Laguens: Jurnal Kajian Hukum dan Keadilan*. 2025.

Soekanto, Soerjono. 2008. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia.

Syalendro, Oky et al. "Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan dan Penanganan Kasus Tindak Pidana Cyber Crime". *Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia*. Vol. 4 No. 1. January 2025.

Widodo, Wahyu. 2015. *Kriminologi Dan Hukum Pidana*. Semarang: Universitas PGRI Semarang Press.

Wibowo, Muhammad Singgih Imam et al. "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia". *Rewang Rencang: Jurnal Hukum Lex Generalis*. Vol. 5 No. 7. 2024.

Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.