ISSN: 2338 4638

Volume 7 Nomor 7 (2023)

'ADALAH

Buletin Hukum & Keadilan

Peretasan dan Akses Ilegal dalam Perspektif Hukum Pidana Indonesia: Menimbang Ulang Konsep "Tanpa Hak" dan "Niat Baik" di Era *Ethical Hacking*

Gilang Rizki Aji Putra*

Universitas Islam Negeri Syarif Hidayatullah Jakarta

10.15408/adalah.v7i7.51840

Abstract:

Hacking and unauthorized access to electronic systems constitute one of the most fundamental forms of cybercrime, threatening the confidentiality, integrity, and availability of data. This article examines the legal construction of hacking and illegal access under Indonesian criminal law, particularly the Electronic Information and Transactions Law (ITE Law) and the Penal Code, and evaluates whether these provisions adequately distinguish malicious actors (black hat hackers) from ethical hackers. Using normative legal research with statutory, conceptual, and comparative approaches, the study finds that the key phrase "without right or unlawfully" under Article 30 of the ITE Law generates interpretative uncertainty and risks criminalizing legitimate cybersecurity research. The absence of regulations on bug bounty programs and the doctrine of implied consent further places security researchers in a vulnerable legal position. The article concludes that Indonesian criminal law should adopt a differentiated approach recognizing ethical hacking through explicit safe harbor provisions and clearer enforcement guidelines.

Keywords: Hacking, Illegal Access, Ethical Hacking, Electronic Information and Transactions Law (ITE Law), Bug Bounty..

* Peneliti pada Pusat Studi Konstitusi dan legislasi Nasional (Poskolegnas), Universitas Islam Negeri Syarif Hidayatullah Jakarta. Email: gilang.rizkiajiputra19@uinjkt.ac.id.

A. PENDAHULUAN

Peretasan (*hacking*) adalah fenomena yang lahir bersamaan dengan perkembangan internet itu sendiri. Istilah ini pada mulanya merujuk pada aktivitas pemrograman yang cerdas dan eksploratif, namun seiring waktu mengalami stigmatisasi menjadi tindakan kriminal yang merugikan. Dalam hukum pidana Indonesia, peretasan diartikan sebagai akses tidak sah atau tanpa hak terhadap sistem komputer atau jaringan elektronik, sebagaimana diatur dalam Pasal 30 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya. Konstruksi delik ini bertujuan untuk melindungi kepentingan hukum terhadap keamanan sistem elektronik yang menjadi tulang punggung kehidupan modern.

Namun, perkembangan dunia keamanan siber telah melahirkan figur paradoksal: *ethical hacker* atau *white hat hacker,* yaitu individu yang menggunakan keterampilan dan teknik yang sama dengan penjahat siber, tetapi tujuannya adalah untuk mengidentifikasi kerentanan sistem dan melaporkannya kepada pemilik sistem demi perbaikan. Aktivitas ini, yang menjadi fondasi dari *vulnerability disclosure* dan *bug bounty* program yang dipromosikan oleh perusahaan teknologi global, secara teknis memenuhi unsur-unsur delik akses ilegal dalam UU ITE. Memasuki sistem tanpa izin, bahkan dengan niat menemukan celah keamanan,

tetap melanggar rumusan "tanpa hak" yang tidak memberikan pengecualian bagi motivasi altruistik.

Persoalan ini bukan sekadar wacana akademis. Beberapa kasus di Indonesia menunjukkan bahwa individu yang melaporkan kerentanan justru berhadapan dengan ancaman pidana dari pemilik sistem yang merasa tersinggung atau malu. Ketiadaan perlindungan hukum bagi pelapor kerentanan (*vulnerability reporter*) menciptakan chilling effect yang justru merugikan keamanan siber nasional, karena celah keamanan tetap terbuka tanpa ada yang berani melaporkan (Sutanto & Hidayat, 2023). Rumusan masalah dalam artikel ini adalah: Pertama, bagaimana konstruksi delik peretasan dan akses ilegal dalam UU ITE dan KUHP nasional? Kedua, bagaimana hukum pidana Indonesia menyikapi aktivitas *ethical hacking*, dan di mana letak persoalan normatifnya? Tujuannya adalah untuk menelaah secara kritis rumusan pidana yang ada dan mengusulkan kerangka hukum yang lebih proporsional.

B. PERETASAN DALAM PERSPEKTIF HUKUM PIDANA DAN TEORI *IMPLIED CONSENT*

Dalam hukum pidana, peretasan dikategorikan sebagai tindak pidana terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Konvensi Budapest tentang Kejahatan Siber (2001) dalam Pasal 2 hingga Pasal 6 mengatur secara komprehensif tentang *illegal access*,

illegal interception, data interference, system interference, dan *misuse of devices.* Yang menjadi fondasi adalah konsep "akses tanpa hak" (*access without right*), yang mensyaratkan adanya pelanggaran terhadap hak eksklusif pemilik sistem untuk menentukan siapa yang boleh mengakses.

Namun, Konvensi Budapest tidak memberikan definisi tegas tentang "hak akses". Definisi ini diserahkan kepada hukum nasional masing-masing negara pihak. Di sinilah muncul persoalan interpretasi. Ahli hukum siber Susan W. Brenner (2022) menjelaskan bahwa model delik akses ilegal dapat dibedakan menjadi dua: *broad model* dan *narrow model. Broad model* memidana setiap akses tanpa otorisasi, tanpa memandang niat. *Narrow model* mempersyaratkan adanya niat jahat tertentu, seperti niat mencuri data atau merusak sistem.

Indonesia, melalui rumusan Pasal 30 UU ITE, cenderung mengadopsi broad model. Akses tanpa hak terhadap sistem orang lain sudah merupakan kejahatan, terlepas dari apakah ada data yang diambil atau kerusakan yang ditimbulkan. Di satu sisi, ini memberikan perlindungan kuat terhadap keamanan sistem. Di sisi lain, ia menutup pintu bagi pembelaan berdasarkan niat baik. Teori implied consent yang berkembang dalam hukum perdata tidak dikenal dalam hukum pidana Indonesia. Dalam konteks ethical hacking, implied consent dapat diartikan sebagai persetujuan diam-diam dari pemilik sistem yang telah membuka akses ke publik

(misalnya melalui internet) dan diyakini oleh pelaku akan menerima pelaporan kerentanan. Sayangnya, hukum pidana Indonesia tidak memberikan ruang bagi interpretasi ini.

Di samping itu, teori legal interest atau kepentingan hukum yang dilindungi perlu diperjelas. Jika kepentingan hukum yang dilindungi adalah keamanan sistem semata, maka setiap akses tanpa izin, bagaimana pun motivasinya, melanggar. Namun, jika kepentingan hukum yang dilindungi juga mencakup keamanan siber nasional secara lebih luas, maka ethical hacking yang justru memperkuat keamanan seharusnya tidak dipidana (Kusumawardhani, 2023). Di sinilah letak urgensi untuk menimbang ulang filosofi pemidanaan akses ilegal.

C. KONSTRUKSI DELIK PERETASAN DALAM UU ITE DAN KELEMAHANNYA

1. Pasal 30 UU ITE dan Makna "Tanpa Hak atau Melawan Hukum"

Pasal 30 UU ITE terdiri dari tiga ayat. Ayat (1) mengkriminalisasi akses tanpa hak ke sistem komputer dengan cara apa pun. Ayat (2) menjangkau akses tanpa hak dengan tujuan memperoleh informasi atau data. Ayat (3) menjangkau akses tanpa hak dengan melanggar atau menerobos sistem pengamanan. Unsur "tanpa hak atau melawan hukum" menjadi inti delik, tetapi UU

ITE dan penjelasannya tidak memberikan definisi yang memadai. Ketiadaan definisi ini membuka ruang interpretasi yang sangat luas dan berpotensi sewenang-wenang.

Dalam praktik, "tanpa hak" seringkali disamakan dengan "tidak memiliki izin tertulis". Ini berarti seorang peneliti keamanan yang menemukan celah di situs pemerintah dan mencoba mengakses untuk memverifikasi kerentanannya, meskipun dengan niat melaporkan, dapat dianggap memenuhi unsur delik karena tidak memiliki surat izin resmi. Problemnya, dalam banyak kasus, pemilik sistem justru tidak menyediakan mekanisme pelaporan yang mudah atau program bug bounty resmi. Akibatnya, peneliti menghadapi dilema: melaporkan tanpa mengakses (yang mustahil untuk verifikasi teknis), mengakses lalu melaporkan (risiko pidana), atau diam saja (celah tetap terbuka) (Prasetyo, 2024).

Bandingkan dengan pengaturan di beberapa yurisdiksi lain. Amerika Serikat melalui *Computer Fraud and Abuse Act* (CFAA) juga menggunakan frasa "tanpa otorisasi", tetapi pengadilan di sana telah mengembangkan yurisprudensi yang membedakan antara akses oleh pihak yang sama sekali tidak berwenang dengan akses oleh pihak yang memiliki akses terbatas tetapi melebihi batas otorisasinya (*exceeding authorized access*). Belakangan, terdapat tren untuk mempersempit interpretasi CFAA agar tidak menjerat aktivitas yang secara substansi tidak merugikan. Di Jerman, Pasal 202a KUHP Jerman

mensyaratkan adanya "pengamanan khusus" yang diterobos, sehingga sistem yang tidak memiliki pengamanan tidak dilindungi oleh pasal ini. Ini memberikan ruang lebih besar bagi penemuan kerentanan pada sistem yang terbuka.

2. Ketidakmampuan Membedakan *White Hat, Grey Hat,* dan *Black Hat*

Dalam dunia keamanan siber, dikenal tiga kategori peretas: *white hat* (etis, dengan izin), *black hat* (jahat, tanpa izin dan merugikan), dan *grey hat* (abu-abu, tanpa izin tetapi tidak merugikan atau justru melaporkan). UU ITE tidak membedakan ketiganya. Semua akses tanpa izin otomatis kena delik. Hal ini menimbulkan persoalan keadilan karena hukum menempatkan peretas yang mencuri data nasabah bank untuk diperjualbelikan sama posisinya dengan peneliti yang mengakses API terbuka untuk membuktikan kerentanan lalu melaporkannya ke publik.

Sejumlah kasus di Indonesia menunjukkan bias represif ini. Pada tahun 2018, seorang mahasiswa di Yogyakarta yang menemukan kerentanan pada portal akademik kampusnya dan melaporkannya ke administrator justru dilaporkan ke polisi oleh pihak kampus atas dugaan peretasan. Kasus ini menjadi preseden buruk yang menunjukkan bahwa pemilik sistem seringkali tidak dewasa dalam menerima laporan kerentanan, dan hukum pidana yang seharusnya menjadi ultimum

remedium dengan mudah dijadikan alat pembungkaman (Sutanto & Hidayat, 2023). Ketiadaan safe harbor provision dalam UU ITE menciptakan ketidakpastian yang menghambat partisipasi publik dalam menjaga keamanan siber.

3. Delik Peretasan dalam KUHP Baru dan Persinggungannya dengan UU ITE

KUHP baru (UU 1/2023) juga mengatur tentang tindak pidana terhadap sistem dan data elektronik dalam Bab tentang Tindak Pidana Terhadap Keamanan Negara dan dalam Bab Tindak Pidana Terhadap Kepercayaan dalam Bertransaksi Elektronik. Pasal 332 KUHP baru, misalnya, mengatur tentang akses ilegal dengan ancaman pidana yang cukup berat. Namun, KUHP baru tidak menciptakan harmoni dengan UU ITE; ia justru menambah lapisan regulasi yang tumpang tindih. Sinkronisasi antara pasal-pasal UU ITE dan KUHP baru sangat diperlukan. Tanpa sinkronisasi, pelaku bisa dijerat dengan dua rezim sekaligus untuk perbuatan yang sama, yang berpotensi melanggar asas *ne bis in idem* (Nugroho, 2024). Lebih dari itu, KUHP baru juga tidak memuat pengecualian bagi ethical hacking, sehingga problem mendasarnya tetap tidak terselesaikan.

D. TIGA WAJAH PERETASAN DAN RESPONS HUKUM

Peretasan Situs Pemerintah oleh "Bjorka" (2022)

Bjorka adalah figur misterius yang meretas berbagai situs pemerintah dan membocorkan data-data pejabat serta dokumen internal ke publik. Aksinya jelas termasuk *black hat* karena bertujuan mencuri data dan membocorkannya, menimbulkan kerugian reputasi maupun potensi keamanan. Pemerintah membentuk satgas dan melakukan upaya penegakan hukum, namun pelaku utama tidak berhasil teridentifikasi. Kasus ini mengekspos kerentanan infrastruktur pemerintah dan kebutuhan akan sistem keamanan yang lebih kuat. Dalam perspektif hukum, kasus Bjorka jelas memenuhi unsur Pasal 30 ayat (2) dan ayat (3) UU ITE, juga Pasal 32 tentang manipulasi data. Tidak ada kontroversi soal kriminalisasi. Namun, ironisnya, kegagalan menangkap pelaku justru menunjukkan kelemahan kapasitas investigasi, bukan kelemahan norma.

Kerentanan Aplikasi PeduliLindungi dan Pelaporan Publik (2021)

Pada masa pandemi, beberapa peneliti keamanan menemukan kerentanan serius pada aplikasi PeduliLindungi yang berpotensi membocorkan data pribadi jutaan pengguna. Mereka melaporkannya secara publik setelah tidak mendapat respons dari pengembang. Bukannya memproses laporan, otoritas sempat mengancam akan memproses hukum para pelapor. Kasus ini adalah contoh nyata bagaimana ketiadaan mekanisme responsible disclosure dan bug bounty

menempatkan peneliti dalam posisi berbahaya. Para peneliti tersebut jelas mengakses data untuk membuktikan kerentanan secara teknis melanggar Pasal 30, tetapi motivasi mereka adalah melindungi publik. Kasus ini menunjukkan betapa hukum kita gagal membedakan antara kejahatan dan kontribusi sosial.

Peretasan Balik (*Hacking Back*) dan Problematika Pertahanan Diri Digital

Salah satu isu hukum yang belum terjamah adalah hacking back atau peretasan balasan yang dilakukan oleh korban untuk melacak atau melumpuhkan penyerang. Dalam satu kasus, sebuah perusahaan swasta yang menjadi korban ransomware berhasil melacak server pelaku dan mencoba menonaktifkannya. Secara teknis, ini adalah akses ilegal. Namun, dari perspektif moral, ini adalah bentuk pertahanan diri. Hukum pidana Indonesia sama sekali tidak mengenal doktrin self-defense dalam konteks digital. Padahal, dalam situasi di mana aparat tidak mampu merespons dengan cepat, korban memiliki kepentingan yang sah untuk melindungi asetnya. Pengaturan tentang active defense masih menjadi wilayah abu-abu yang memerlukan pengkajian mendalam (Brenner, 2022).

E. REFORMULASI HUKUM: MENUJU MODEL DIFERENSIATIF DAN SAFE HARBOR PROVISION

Untuk mengatasi persoalan di atas, hukum pidana Indonesia perlu mengadopsi reformulasi yang lebih diferensiatif. Pertama, perlu ditambahkan pengecualian atau safe harbor provision dalam UU ITE yang menyatakan bahwa akses terhadap sistem komputer tidak dianggap sebagai tindak pidana jika dilakukan dengan iktikad baik untuk mengidentifikasi kerentanan dan melaporkannya kepada pemilik sistem atau otoritas yang berwenang, tanpa menimbulkan kerugian lebih lanjut. Ketentuan ini akan melindungi ethical hacker dari jeratan pidana, sekaligus mendorong budaya vulnerability disclosure yang sehat.

Kedua, konsep "tanpa hak" perlu diperjelas melalui peraturan pelaksana atau pedoman penegakan hukum. Kejaksaan Agung dan Kepolisian dapat mengeluarkan panduan yang menyatakan bahwa akses yang dilakukan untuk riset dan pelaporan kerentanan, sepanjang tidak mengeksploitasi data atau merusak sistem, tidak dituntut pidana. Panduan semacam ini sudah diterapkan di Belanda oleh Public Prosecution Service yang menerbitkan kebijakan tentang penanganan ethical hacking. Ketiga, pemerintah perlu mendorong setiap kementerian, lembaga, dan perusahaan besar untuk membuka vulnerability disclosure program (VDP) resmi. Dengan adanya VDP, peneliti memiliki saluran resmi untuk

melaporkan tanpa perlu mengambil risiko mengakses secara diam-diam. Keempat, Mahkamah Agung dapat berperan melalui pembentukan yurisprudensi progresif. Ketika berhadapan dengan kasus *ethical hacking*, hakim harus mempertimbangkan niat, dampak, dan kontribusi terdakwa, serta tidak menerapkan pasal secara mekanis. Yurisprudensi semacam ini akan menjadi kompas bagi pengadilan di seluruh Indonesia (Simanjuntak, 2024).

F. KESIMPULAN

Konstruksi delik peretasan dan akses ilegal dalam UU ITE menganut model yang sangat luas (broad model), yang memidana setiap akses tanpa hak tanpa mempertimbangkan niat atau dampak. Rumusan ini memberikan perlindungan kuat bagi keamanan sistem, namun di sisi lain menimbulkan ketidakpastian hukum yang serius bagi aktivitas ethical hacking yang berkontribusi positif terhadap ketahanan siber nasional. Menjawab rumusan masalah, hukum pidana Indonesia saat ini belum mampu membedakan secara adil antara peretas jahat dan peretas etis. Frasa "tanpa hak atau melawan hukum" yang tidak didefinisikan secara kontekstual menjadi sumber persoalan yang mengancam partisipasi publik dalam pengamanan sistem digital.

Rekomendasi yang diajukan meliputi: pertama, amendemen UU ITE untuk menyertakan safe harbor provision bagi ethical hacker; kedua,

penerbitan pedoman teknis oleh Kejaksaan dan Kepolisian tentang penanganan kasus peretasan yang melibatkan niat baik dan pelaporan kerentanan; ketiga, pembentukan vulnerability disclosure program wajib bagi instansi pemerintah; dan keempat, pelatihan hakim dan penyidik tentang aspek teknis keamanan siber agar mampu membuat putusan yang proporsional dan informatif. Hanya dengan reformulasi yang memperhitungkan realitas *ethical hacking*, Indonesia dapat membangun ekosistem keamanan siber yang tidak hanya represif, tetapi juga progresif dan inklusif.

REFERENSI:

Brenner, S. W. (2022). Cybercrime: Criminal Threats from Cyberspace (2nd ed.). Praeger.

Kusumawardhani, A. (2023). Konsep "Tanpa Hak" dalam Pasal 30 UU ITE dan Pengaruhnya terhadap Riset Keamanan Siber. Jurnal Hukum Siber, 5(1), 15–32.

Nugroho, A. (2024). Sinkronisasi Hukum Pidana Materiil dalam UU ITE Pasca KUHP Baru. Jurnal Hukum Pidana dan Kriminologi, 15(1), 41–60.

Prasetyo, B. (2024). Dilema Ethical Hacking dalam Hukum Pidana Indonesia. Jurnal Hukum dan Masyarakat, 16(1), 88–107.

Simanjuntak, K. (2024). Peran Yurisprudensi dalam Melindungi Vulnerability Reporter. Jurnal Konstitusi, 21(2), 278–296. https://doi.org/10.31078/jk2125

Sutanto, R., & Hidayat, F. (2023). Ethical Hacking dan Ancaman Kriminalisasi: Studi Kasus di Indonesia. Jurnal Kajian Hukum dan Teknologi, 4(2), 112–130.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2024 Nomor 1, Tambahan Lembaran Negara Nomor 6905).

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Tahun 2023 Nomor 1, Tambahan Lembaran Negara Nomor 6842).