# Kebijakan Kriminal dalam Penanggulangan Tindak Pidana Peretasan (Hacking) di Indonesia

Rifai Setya Kurniawan[1], Muhamad Aminulloh[2]

Universitas Djuanda, [1]rifaisetya44@gmail.com
Universitas Djuanda, [2]muhamad.aminulloh@unida.ac.id

**ABSTRAK**

Peretasan (hacking) telah menjadi salah satu bentuk kejahatan siber yang semakin sering terjadi di era digital, khususnya di Indonesia. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah mengatur tindak pidana ini, efektivitas kebijakan kriminal dalam penanggulangannya masih dipertanyakan, terutama terkait penegakan hukum yang lemah dan terbatasnya sanksi. Penelitian ini bertujuan untuk menganalisis kebijakan kriminal dalam penanggulangan peretasan di Indonesia, dengan fokus pada efektivitas, kelemahan, dan tantangan yang ada. Metode yang digunakan adalah yuridis normatif melalui analisis terhadap dokumen hukum, khususnya UU ITE, serta studi literatur terkait kejahatan siber. Hasil penelitian menunjukkan bahwa meskipun UU ITE memberikan landasan hukum, masih terdapat kelemahan dalam implementasi, seperti kurangnya keterampilan teknis aparat penegak hukum dan ketidakcukupan regulasi. Ditemukan juga bahwa kerja sama internasional diperlukan untuk menghadapi peretasan lintas negara. Penelitian ini terbatas pada analisis hukum dan tidak melibatkan data empiris dari kasus peretasan di Indonesia, yang dapat menjadi area untuk penelitian di masa mendatang. Kesimpulannya, revisi UU ITE dan peningkatan kapasitas penegak hukum sangat diperlukan untuk menanggulangi tindak pidana peretasan secara efektif.

**Kata Kunci:** kebijakan kriminal, peretasan, UU ITE, kejahatan siber

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mencatat kemajuan yang sangat pesat dalam dekade-dekade terakhir. Awal perkembangan ini dapat direkonstruksi dengan jelas mulai dari era awal ARPANET pada tahun 1983, ketika protokol TCP/IP diganti dari NCP, markah awal dari apa yang kita kenal sekarang sebagai Internet. Era 1990-an melihat internet berkembang pesat, menyambungkan banyak pengguna jaringan komputer global13. Pada tahun 1992, *World Wide Web* (WWW) diperkenalkan oleh CERN, yang kemudian menjadi platform sentral bagi

interaksi online. InterNIC dibentuk pada tahun 1993 untuk menyediakan layanan direktori, penyimpanan data, dan database, serta registrasi domain nama.

Perkembangan teknologi informasi dan komunikasi tidak hanya terbatas pada infrastruktur internet ia juga mempengaruhi berbagai aspek kehidupan manusia. Teknologi informasi dan komunikasi telah mempermudah semua aspek kehidupan manusia, termasuk komunikasi, transaksi ekonomi, dan akses informasi. Komputer dan telekomunikasi telah mengubah paradigma industri dengan cepat. Implementasi teknologi seperti LAN, WAN, GlobalNet, Intranet, Internet, Ekstranet, telah melewati batasan fisik antar negara, meninggalkan garis-garis batas tradisional dalam aliran informasi (Shadily et al., 2024).

Di era modern, teknologi informasi dan komunikasi telah menjadi bagian integral dari kehidupan sehari-hari. Penggunaan smartphone dan internet telah meningkatkan cara manusia berkomunikasi dan berinteraksi. Media sosial seperti TikTok telah menjadi platform populer bagi ekspresi diri dan interaksi online, walaupun juga memiliki dampak positif dan negatif bagi remaja. Tidak heran bahwa perkembangan teknologi informasi dan komunikasi berpengaruh signifikan terhadap pertumbuhan ekonomi.

Teknologi infor masi dan kumunikasi cenderung lebih efisien untuk mendukung produksi dan distribusi barang dan jasa, terutama di negara kepualauan seperti Indonesia. Indek Pembangunan Tekno-logi Informasi dan Komunikasi (IP-TIK) menunjukkan potensi pembangunan teknologi informasi dan komunikasi di wilayah-wilayah Asia, termasuk Indonesia, yang masih terus meningkat dari tahun 2017 hingga 2019 (Singgi et al., 2020).

Meningkatnya kasus peretasan di Indonesia merupakan fenomena yang kompleks dan terkait erat dengan faktor-faktor teknologis, sosial, dan administratif. Beberapa kasus yang tercatat menunjukkan betapa parahnya ancaman cybercrime terhadap institusi-institusi pemerintah dan swasta. Salah satu contoh yang menonjol adalah peretasan Situs Sekretariat Kabinet Indonesia pada tahun 2021. Peretasan ini

dilakukan dengan metode deface, dimana halaman situs utama berubah menjadi hitam dengan foto demonstran membawa bendera merah putih. Ini menunjukkan bahwa peretasan bukan hanya soal pencurian data, tapi juga soal manipulasi visual untuk memberikan pesan tertentu (Widayanti, 2022).

Aplikasi *Electronic Health Alert* (e-Hac) milik Kementerian Kesehatan juga pernah menjadi korban peretasan. Bocornya data 1,3 juta pengguna aplikasi ini terjadi karena kekurangan keamanan dalam sistem elastic search yang digunakan. Hasil pengecekan COVID-19, data rumah sakit, dan data staf e-Hac semuanya bocor, menunjukkan betapa sensitivitas data yang hilang. Selain itu, Polri juga pernah mengalami peretasan database yang cukup serius. Data personal seperti nama lengkap, data kelahiran, nomor registrasi pokok, alamat rumah, pangkat, golongan darah, dan informasi penting lainnya bocor. Peretas ini juga mengklaim telah melakukan peretasan pada situs milik Badan Siber dan Sandi Negara (BSSN) (Nuristiningsih, 2023).

Kasus peretasan website Kejaksaan Agung Republik Indonesia (Kejagung) juga menarik perhatian. Seorang remaja asal Lahat, Sumatera Selatan, meregang-alami situs Kejagung menggunakan metode deface dan berhasil mencuri 3,1 juta data pribadi. Dia menjual data tersebut ke forum online dengan harga Rp 400.000. Pertemuan antara hacker Indonesia dan Australia pada tahun 2013 juga menambah daftar kasus peretasan yang heboh. Serangan balasan antara kedua negara tersebut menunjukkan betapa intensifnya konflik cyber di level internasional.

Tindak pidana peretasan memiliki dampak yang signifikan dalam berbagai aspek, termasuk sosial, ekonomi, dan keamanan. Dari sisi sosial, peretasan dapat menimbulkan ketidakpastian dan kecemasan di kalangan masyarakat. Ketika data pribadi bocor, individu berisiko mengalami pencurian identitas dan penipuan, yang dapat merusak reputasi dan kepercayaan diri mereka. Selain itu, insiden peretasan sering kali menciptakan stigma negatif terhadap lembaga atau perusahaan yang

menjadi target, mengurangi kepercayaan publik terhadap kemampuan mereka dalam melindungi data (Utin Indah Permata Sari, 2022).

Dari perspektif ekonomi, dampak peretasan sangat besar. Misalnya, peretasan terhadap Pusat Data Nasional (PDN) Indonesia diperkirakan menyebabkan kerugian mencapai Rp6,3 triliun. Kerugian ini tidak hanya mencakup hilangnya pendapatan langsung tetapi juga dampak jangka panjang seperti penurunan investasi dan pertumbuhan ekonomi. Gangguan pada layanan publik dan swasta akibat peretasan dapat memperlambat aktivitas bisnis, menghambat transaksi keuangan, dan merusak rantai pasokan. Hal ini berpotensi menurunkan daya beli masyarakat dan mengurangi surplus usaha (Arisandy, 2021).

Dalam hal keamanan, peretasan menimbulkan ancaman serius terhadap infrastruktur digital negara. Kebocoran data sensitif dapat dimanfaatkan oleh pihak-pihak tertentu untuk tujuan yang merugikan, termasuk pengendalian ekonomi atau serangan lebih lanjut terhadap sistem kritis. Kejadian ini menyoroti kerentanan sistem keamanan siber yang ada dan pentingnya investasi dalam teknologi keamanan untuk melindungi data dan infrastruktur dari ancaman siber.

Urgensi penanggulangan tindak pidana peretasan di Indonesia semakin mendesak seiring dengan meningkatnya frekuensi serangan siber yang berdampak luas pada berbagai sektor. Kasus peretasan, seperti yang terjadi pada Pusat Data Nasional (PDN), menunjukkan bahwa infrastruktur digital Indonesia rentan terhadap ancaman yang dapat mengakibatkan kebocoran data sensitif dan gangguan layanan publik. Insiden ini tidak hanya menimbulkan kerugian finansial yang signifikan, tetapi juga menciptakan ketidakpastian di kalangan masyarakat dan investor, yang dapat menghambat pertumbuhan ekonomi (Wijaya, 2022).

Dari sisi ekonomi, kerugian akibat peretasan diperkirakan mencapai triliunan rupiah, mengingat dampaknya pada aktivitas bisnis dan kepercayaan publik. Gangguan pada layanan penting seperti perbankan dan perdagangan dapat memperlambat arus transaksi keuangan dan merusak rantai pasokan. Selain itu,

reputasi negara sebagai tujuan investasi juga terancam, karena investor cenderung ragu untuk menanamkan modal di negara dengan keamanan siber yang lemah.

Aspek sosial juga terpengaruh, di mana masyarakat menjadi semakin khawatir tentang keamanan data pribadi mereka. Kebocoran informasi dapat menyebabkan pencurian identitas dan penipuan, yang merugikan individu dan menurunkan kepercayaan publik terhadap pemerintah. Kejadian-kejadian ini menciptakan siklus ketidakpercayaan yang sulit untuk dipulihkan (Trisnawati & Hanifah, 2024).

## METODE PENELITIAN

Metode penelitian ini mengadopsi pendekatan yuridis normatif, yang berfokus pada kajian hukum dan peraturan terkait kejahatan siber, khususnya peretasan. Penelitian ini menggunakan studi literatur sebagai dasar untuk menganalisis Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya. Sumber data utama adalah data sekunder yang mencakup peraturan perundang-undangan, literatur akademik, dan penelitian sebelumnya yang relevan.

Teknik pengumpulan data dilakukan melalui studi dokumentasi, yang melibatkan analisis dokumen hukum dan literatur mengenai tindak pidana peretasan. Fokus utama analisis adalah pada UU ITE dan regulasi terkait lainnya, untuk memahami bagaimana hukum mengatur kejahatan siber serta dampaknya terhadap masyarakat. Dalam hal teknik analisis data, pendekatan kualitatif diterapkan untuk menginterpretasikan aturan hukum yang ada. Penelitian ini juga membandingkan kebijakan penanggulangan kejahatan siber di Indonesia dengan praktik di negara lain. Melalui analisis ini, diharapkan dapat diidentifikasi kekuatan dan kelemahan dalam regulasi yang ada, serta memberikan rekomendasi untuk perbaikan sistem hukum yang lebih efektif dalam menangani kejahatan siber (Saleh, 2021).

## HASIL DAN PEMBAHASAN

**Kebijakan Kriminal dalam Penanggulangan Tindak Pidana Peretasan di Indonesia**

Analisis terhadap Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menunjukkan bahwa undang-undang ini memiliki peran penting dalam penanggulangan kejahatan siber, termasuk peretasan. Pasal-pasal yang mengatur tentang hacking secara spesifik mencakup Pasal 30 hingga Pasal 35. Pasal 30 mengatur tentang akses ilegal ke komputer dan sistem elektronik orang lain tanpa hak, yang merupakan tindakan utama dalam peretasan. Sanksi untuk pelanggaran ini diatur dalam Pasal 46, yang memberikan hukuman penjara maksimal enam tahun dan denda hingga Rp600 juta untuk pelanggaran yang lebih ringan, serta hingga delapan tahun penjara dan denda Rp800 juta untuk pelanggaran yang lebih serius (Putri et al., 2022).

Pasal 31 melarang penyadapan informasi secara ilegal, sementara Pasal 32 mengatur tentang pengubahan dan transmisi informasi elektronik tanpa hak. Selain itu, Pasal 33 menyebutkan larangan mengganggu sistem elektronik sehingga tidak berfungsi dengan baik. Tindakan manipulasi data juga diatur dalam Pasal 35, yang mencakup pengubahan informasi agar terlihat otentik. UU ITE juga memperluas jangkauan hukum dengan mencakup tindakan yang dilakukan di luar wilayah Indonesia jika berdampak pada kepentingan Indonesia, sebagaimana diatur dalam Pasal 2 dan Pasal 37. Hal ini menunjukkan keseriusan pemerintah dalam menangani ancaman siber yang bersifat lintas negara.

Namun, meskipun UU ITE memberikan kerangka hukum untuk menangani kejahatan siber, masih terdapat tantangan dalam implementasinya. Beberapa pasal dianggap ambigu dan dapat disalahgunakan, seperti Pasal 28 yang berkaitan dengan ujaran kebencian, yang pernah digugat ke Mahkamah Konstitusi karena dianggap membatasi kebebasan berekspresi. Perlunya evaluasi dan memperbarui regulasi ini agar lebih efektif dalam menghadapi dinamika perkembangan teknologi informasi dan ancaman siber (Faridi, 2019).

Peran Kepolisian siber dan Badan Siber dan Sandi Negara (BSSN) dalam penegakan hukum di Indonesia sangat krusial mengingat meningkatnya ancaman kejahatan siber. BSSN, yang dibentuk berdasarkan Peraturan Presiden No. 53 Tahun 2017, bertugas untuk menjaga keamanan siber nasional melalui penyusunan kebijakan teknis dan evaluasi terhadap potensi kerawanan di dunia maya. Meskipun BSSN tidak memiliki kewenangan penindakan seperti aparat penegak hukum, lembaga ini berperan sebagai pengawas yang mengkoordinasikan

upaya pencegahan dan mitigasi terhadap ancaman siber, termasuk ransomware dan phishing.

Sementara itu, Kepolisian Republik Indonesia (Polri), khususnya Bareskrim, memiliki tanggung jawab langsung dalam penegakan hukum terhadap pelaku kejahatan siber. Polri melakukan penyelidikan dan penindakan berdasarkan laporan masyarakat atau deteksi internal terhadap aktivitas mencurigakan. Kerja sama antara BSSN dan Polri sangat penting, terutama dalam hal berbagi informasi dan analisis forensik digital untuk mengidentifikasi serta menangkap pelaku kejahatan siber. Kolaborasi ini juga melibatkan lembaga lain seperti Kementerian Komunikasi dan Informatika serta Kejaksaan, yang bersama-sama membentuk suatu ekosistem keamanan siber yang lebih kuat. Upaya penegakan hukum tidak hanya berfokus pada penangkapan pelaku tetapi juga pada peningkatan literasi digital masyarakat untuk mencegah serangan siber (Kelrey & Muzaki, 2019).

Langkah-langkah preventif, represif, dan rehabilitatif dalam penanggulangan tindak pidana peretasan adalah elemen penting dalam strategi keamanan siber. Pihak kepolisian melakukan upaya pre-emtif dengan menanamkan nilai-nilai baik dan norma-norma yang baik dalam masyarakat. Tujuannya adalah untuk menginternalisasikan perilaku etis dan legal dalam setiap individu, sehingga mereka tidak akan melakukan kejahatan meski ada kesempatan. Teori NKK (Niat + Kesempatan) digunakan untuk mendorong perilaku positif. Mengadakan program pendidikan dan sosialisasi tentang bahaya kejahatan siber. Contohnya, kegiatan sosialisasi yang menjelaskan cara-cara pencegahan kejahatan teknologi informasi, seperti mengganti username dan password secara teratur, tidak mudah mengklik link atau file yang tidak dikenal, dan meningkatkan fitur anti-phishing.

Memastikan bahwa sistem keamanan media elektronik yang terhubung dengan internet sudah dioptimalkan. Ini termasuk meningkatkan sistem firewall, antivirus, dan VPN untuk menghalangi akses ilegal ke data pribadi atau organisasi. Apabila terjadi tindak pidana peretasan, pihak kepolisian melakukan penyelidikan dan penindakan terhadap pelaku. Proses ini melibatkan pengumpulan bukti-bukti forensik digital dan investigasi lapangan untuk menemukan dan menangkap pelaku. Setelah pelaku ditangkap, mereka diproses di kepolisian dan kemudian dilemparkan ke kejaksaan untuk proses peradilan. Di sana, pelaku akan dijatuhi hukuman sesuai dengan sanksi yang telah ditentukan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Setelah dijatuhi

hukuman, beberapa kasus memungkinkan pelaku untuk menjalani program rehabilitasi. Program ini bertujuan untuk mengubah perilaku pelaku dan mengarahkannya menuju jalur yang lebih positif. Namun, detail rehabilitasi biasanya tidak disebutkan secara eksplisit dalam diskursus umum tentang penanggulangan kejahatan siber (Rahmasari et al., 2021).

**Permasalahan dalam Penegakan Hukum Terhadap Peretasan**

Kendala teknis dalam investigasi dan pembuktian digital adalah tantangan yang signifikan dalam penanggulangan kejahatan siber. Salah satu kendalan utama adalah ledakan jumlah data yang semakin besar dan kompleks, sehingga para ahli digital forensik harus menghadapi kasus-kasus di mana data yang harus dianalisis mencapai ratusan terabyte atau bahkan lebih. Kemampuan untuk mengelola data sebesar ini menjadi kunci, dan penerapan teknologi terbaru dalam analisis dan pemrosesan data akan menjadi suatu keharusan (Benny Cahyadi et al., 2024).

Selain itu, analisis forensik digital masih memiliki banyak kekurangan dan kerentanan, terutama pada tahap validasi. Dr. Ahmad Luthfi menyampaikan bahwa integrasi data yang dikumpulkan harus pasti untuk disajikan sebagai bukti yang sah dalam pengadilan. Dia mengusulkan sebuah model validasi dengan pendekatan yang sistematis dan teruji. Model ini melibatkan penggunaan empirical datasets yang sudah teruji, pengembangan matriks untuk mengukur presisi dan akurasi metode dan alat forensik, serta integrasi teknik pembelajaran mesin dan kecerdasan buatan untuk beralih dari analisis semi otomatis menjadi otomasi keseluruhan (Kurniawan & Maujuhan Syah, 2022).

Tantangan lainnya termasuk menjaga privasi dan keamanan data selama proses digital forensik. Pengumpulan dan penggunaan data digital memiliki potensi untuk melanggar privasi pengguna dan menimbulkan risiko keamanan. Selanjutnya, identifikasi dan penangkapan pelaku kejahatan siber sering kali sulit karena mereka dapat beroperasi dari lokasi yang berbeda-beda dan menggunakan teknik yang canggih, menyulitkan pelacakan.

Teknologi keamanan siber yang ada sering kali tidak mampu mengimbangi metode serangan siber yang semakin canggih, menciptakan celah yang dapat dieksploitasi oleh pelaku kejahatan. Kurangnya sumber daya manusia yang terlatih dalam bidang keamanan siber dan teknologi informasi juga menjadi hambatan dalam penanganan kejahatan siber. Proses hukum yang lambat dan birokrasi yang berbelit-belit dapat menghambat penanganan kasus kejahatan siber, mengurangi efektivitas penegakan hukum.

Kendala teknis dalam investigasi digital sangat kompleks dan memerlukan investasi yang tepat dalam pengembangan teknologi serta peningkatan kapasitas sumber daya manusia di bidang digital forensik. Melindungi data dan informasi penting dari serangan kejahatan komputer dan keamanan siber merupakan tugas yang krusial, dan upaya terus-menerus dalam meningkatkan keterampilan dan teknologi menjadi kunci untuk menjaga keamanan digital di era yang semakin maju. Kesesjangan hukum dan kurangnya koordinasi antar lembaga penegak hukum merupakan dua masalah yang saling terkait dalam struktur penegakan hukum di Indonesia. Fenomena ini tercermin dalam berbagai kasus yang menunjukkan ketidakadilan dan ketimpangan dalam penegakan hukum (Ridwan et al., 2023).

Kesenjangan hukum terjadi karena adanya diskriminasi dalam penegakan hukum. Diskriminasi ini dapat berbasis pada ras, suku, status sosial, atau golongan politik. Misalnya, dalam kasus Putri Candrawathi, tersangka pembunuhan berencana Brigadir J, penyidik kepolisian tidak menahan perempuan yang memiliki anak balita, padahal hal ini lazim dilakukan terhadap perempuan lainnya. Hal ini menunjukkan standard ganda dalam penahanan perempuan, yang dapat berakibat pada ketidakadilan dalam proses hukum (Benny Cahyadi et al., 2024).

Kurangnya koordinasi antar lembaga penegak hukum juga menjadi faktor penyebab kesesjangan hukum. Lebih-lebih lagi, kurangnya profesionalitas dan integritas aparat penegak hukum dapat menyebabkan pelanggaran hukum seperti suap, korupsi, dan intimidasi. Misalnya, dalam kasus Nenek Asyani yang dituduh

mencuri batang kayu jati, ia divonis 1 tahun penjara dan denda Rp500 juta, sementara banyak kasus lain yang tidak ditarik secara jelas dan malah terkesan "dilindungi". Hal ini menunjukkan bahwa hukum tidak berlaku secara adil bagi semua orang, terutama bagi masyarakat kelas bawah.

Mahkamah Agung (MA) telah mengeluarkan Surat Edaran (SE) terkait konsep peradilan restorative justice, namun penerapannya masih minim. Konsep ini seharusnya menjadi pegangan penegak hukum untuk melihat tindak pidana yang tidak menyebabkan banyak kerugian negara. Sayangnya, penerapan ini tidak terlihat saat kepemimpinan Presiden Jokowi saat ini, dan kebiijakan Menkum HAM Yasonna Laoly yang akan membuka lebar pintu kepada koruptor untuk mendapatkan remisi membuat situasi semakin buruk. Kesesjangan hukum dan kurangnya koordinasi antar lembaga penegak hukum merupakan dua masalah yang saling terkait dalam penegakan hukum di Indonesia. Solusi yang efektif membutuhkan komitmen dan kerja keras dari semua pihak untuk meningkatkan profesionalitas dan integritas aparat penegak hukum serta memaksimalkan koordinasi antar Lembaga (Kelrey & Muzaki, 2019).

Ketidakcukupan sanksi dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah menjadi topik hangat dalam debat hukum dan keamanan siber di Indonesia. Meskipun UU ITE telah menetapkan sanksi pidana yang beragam, seperti penjara dan denda, beberapa kritikus percaya bahwa sanksi ini masih terlalu rendah dan tidak efektif dalam mencegah kejahatan siber.

Contohnya, Pasal 30 UU ITE mengatur tentang akses ilegal ke komputer dan sistem elektronik orang lain, dengan sanksi penjara maksimal enam tahun dan denda Rp600 juta. Namun, beberapa kasus peretasan yang terjadi menunjukkan bahwa sanksi ini masih terlalu ringan untuk menghentikan tindakan pelaku. Misalnya, peretasan terhadap Pusat Data Nasional (PDN) yang berujung pada kehilangan data sensitif dan kerugian materiil yang signifikan, menunjukkan bahwa sanksi yang ditetapkan tidak proporsional dengan dampak yang dialami (Putri et al., 2022).

Hal ini makin terasa ketika dibandingkan dengan kasus-kasus kejahatan non-siber yang memiliki sanksi yang lebih berat. Misalnya, Pasal 44 UU Tipikom mengatur tentang pencucian uang dengan sanksi penjara maksimal lima belas tahun dan denda Rp15 miliar. Perbandingan ini menunjukkan bahwa sanksi untuk kejahatan siber masih relatif rendah.

Perlunya revisi hukum terkait kejahatan siber tidak hanya karena ketidakcukupan sanksi, tetapi juga karena perluasan definisi dan pengetatan tindakan yang dianggap pelanggaran. Misalnya, Pasal 27 UU ITE mengatur tentang pencemaran nama baik, sedangkan Pasal 28 mengatur tentang ujaran kebencian. Namun, beberapa kasus menunjukkan bahwa ambiguitas dalam definisi ini dapat digunakan untuk menghindari tanggung jawab hukum (Trisnawati & Hanifah, 2024).

Selain itu, revisi hukum juga harus memperhatikan aspek teknologi yang terus berkembang. Regulasi yang ada saat ini seperti UU ITE dan Perpres 47/2023, meskipun telah mencoba menangkap tren teknologi, masih butuh penyesuaian untuk mengantisipasi ancaman siber yang semakin canggih. Contohnya, penggunaan blockchain dan AI dalam kejahatan siber memerlukan respons hukum yang lebih spesifik. Ketidakcukupan sanksi dalam UU ITE dan perlunya revisi hukum terkait kejahatan siber menjadi isu yang tak terpisahkan dalam upaya meningkatkan keamanan siber di Indonesia. Revisi ini harus dilakukan dengan hati-hati untuk memastikan bahwa sanksi yang ditetapkan proporsional dengan dampak yang dialami, serta memperhatikan evolusi teknologi yang terus berkembang.

**Perbandingan dengan Kebijakan Kriminal di Negara Lain**

Studi perbandingan kebijakan penanggulangan hacking di negara-negara seperti Amerika Serikat, Uni Eropa, dan Singapura menunjukkan pendekatan yang berbeda namun saling melengkapi dalam menghadapi ancaman kejahatan siber. Di Amerika Serikat, kebijakan keamanan siber telah berkembang pesat, terutama setelah serangkaian serangan besar yang mengancam infrastruktur kritis.

Pemerintah AS mengadopsi berbagai strategi, termasuk pembentukan US Cyber Command (USCYBERCOM) pada tahun 2010, yang bertugas melindungi jaringan militer dan melakukan operasi siber. Selain itu, dokumen kebijakan seperti "*The National Strategy to Secure Cyberspace*" dan "*Cyberspace Policy Review*" menekankan pentingnya kolaborasi antara sektor publik dan swasta dalam mengamankan data dan sistem informasi. AS juga aktif dalam diplomasi siber untuk membangun kerjasama internasional dalam menghadapi ancaman global (Arisandy, 2021).

Di Uni Eropa, pendekatan penanggulangan hacking lebih terfokus pada regulasi dan perlindungan data pribadi. Dengan diberlakukannya *General Data Protection Regulation* (GDPR) pada tahun 2018, negara-negara anggota UE diharuskan untuk meningkatkan keamanan data dan memberikan hak lebih kepada individu terkait pengelolaan data pribadi mereka. Selain itu, Europol memiliki unit khusus yang menangani kejahatan siber, bekerja sama dengan negara anggota untuk berbagi informasi dan melakukan operasi bersama. Pendekatan ini mencerminkan komitmen UE terhadap perlindungan privasi sambil tetap berusaha untuk mengatasi kejahatan siber secara efektif.

Singapura juga menunjukkan langkah proaktif dalam penanggulangan hacking melalui kebijakan yang komprehensif. Negara ini telah meluncurkan *Cyber Security Strategy* yang mencakup penguatan infrastruktur kritis, peningkatan kemampuan respon insiden, dan pendidikan masyarakat tentang keamanan siber. Singapura juga mendirikan *Cyber Security Agency* (CSA) untuk mengkoordinasikan upaya nasional dalam menghadapi ancaman siber. Selain itu, Singapura aktif dalam kerjasama internasional, termasuk dengan AS dan UE, untuk berbagi informasi dan praktik terbaik dalam keamanan siber (Nuristiningsih, 2023).

Meskipun ketiga negara ini memiliki pendekatan yang berbeda, ada beberapa kesamaan yang dapat diidentifikasi. Semua negara menyadari pentingnya kolaborasi antara sektor publik dan swasta serta perlunya investasi dalam teknologi dan pendidikan untuk meningkatkan kesadaran masyarakat tentang keamanan siber.

Selain itu, mereka semua berupaya untuk memperkuat kerjasama internasional sebagai langkah strategis untuk menghadapi ancaman global yang semakin kompleks.

Studi perbandingan ini menunjukkan bahwa penanggulangan hacking memerlukan pendekatan multi-dimensi yang melibatkan regulasi yang ketat, kolaborasi antar lembaga, serta pendidikan masyarakat. Setiap negara memiliki konteks sosial dan politik yang berbeda, namun semua sepakat bahwa keamanan siber adalah isu yang harus ditangani secara serius untuk melindungi infrastruktur kritis dan data pribadi warganya (Singgi et al., 2020).

Untuk penguatan kebijakan penanggulangan kejahatan siber di Indonesia, beberapa pelajaran penting bisa diambil dari studi kasus internasional dan analisis domestik. Pelajaran pertama yang bisa diambil adalah perlunya adanya undang-undang spesifik mengenai keamanan siber. Seperti yang dijelaskan dalam artikel GovInsider, Indonesia belum memiliki RUU Keamanan Siber yang komprehensif meskipun negara tetangga Singapura dan Malaysia sudah mengesahkannya. Adanya hukum yang jelas dan spesifik akan meningkatkan postur keamanan nasional dan memberikan landasan hukum yang kukuh bagi lembaga-lembaga penegak hukum seperti Badan Siber dan Sandi Negara (BSSN).

Implementasi strategis dalam kebijakan penanggulangan kejahatan siber sangat penting. Misalnya, pemerintah harus memastikan bahwa rencana-rencana peningkatan pertahanan siber di masa depan disertai dengan penjelasan yang jelas dan transparansi publik. Insiden serangan ransomware terhadap Pusat Data Nasional (PDN) menunjukkan bahwa upaya pemulihan tanpa rencana-strategis yang jelas dapat membuat proses restorasi lambat dan tidak efektif (Shadily et al., 2024).

Koordinasi antar lembaga penegak hukum sangat esensial dalam penanggulangan kejahatan siber. Lebih lanjut lagi, koordinasi lintas sektor swasta juga diperlukan guna meningkatkan efektivitas respons terhadap ancaman global. Studi kasus pencurian data pribadi oleh komplotan peretas tahun 2022 menunjukkan

bahwa implementasi kebijakan penanganan kejahatan siber melibatkan koordinasi antara Polri, BSSN, dan kejaksaan, serta kolaborasi dengan sektor swasta untuk mendapatkan teknologi dan talenta siber yang diperlukan.

Literasi digital tingkat tinggi di kalangan masyarakat merupakan faktor penting dalam mencegah kejahatan siber. Eduksi dan literasi digital yang rendah dapat memicu risiko keamanan yang semakin tinggi. Program pendidikan yang fokus pada kesadaran dan literasi digital harus dikembangkan secara intensif untuk menjaga privasi individu dan melindungi diri dari ancaman online (Widayanti, 2022).

Evaluasi sistem keamanan secara periodik sangat penting untuk menghindari celah-celah keamanan yang potensial. Pasca insiden PDN, evaluasi ulang terhadap manajemen persiapan krisis siber harus dilakukan untuk meningkatkan kesiapsiagaan pemerintah dalam menjaga infrastruktur vital seperti server-server penting. Selain itu, standar sistem keamanan yang teruji harus diimplementasikan dan ditingkatkan secara berkala untuk mengantisipasi perkembangan teknologi yang cepat.

Kemampuan sumber daya manusia yang siap menghadapi serangan siber juga merupakan hal yang kritikal. Pelatihan dan pendidikan berkala kepada ahli teknisi harus dilakukan untuk meningkatkan kemampuan respon terhadap ancaman cybercrime. Uji coba praktik secara berkala dan pemahaman pola pikir para peretas juga diperlukan untuk siap menghadapi situasi-situasi ekstrem di masa depan.

Pelajaran-pelajaran ini dapat membantu penguatan kebijakan penanggulangan kejahatan siber di Indonesia dengan lebih efektif dan proaktif. Langkah-langkah ini mencakup regulasi yang spesifik, implementasi strategis, koordinasi lintas sektor, literasi digital tingkat tinggi, evaluasi ulang sistem keamanan, serta kemampuan sumber daya manusia yang siap menghadapi ancaman cybercrime (Utin Indah Permata Sari, 2022).

## KESIMPULAN

Peretasan (hacking) merupakan salah satu bentuk kejahatan siber yang semakin sering terjadi seiring perkembangan teknologi digital, khususnya di Indonesia. Meski telah ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tindak pidana peretasan, implementasinya masih menghadapi berbagai kendala. Penelitian ini bertujuan untuk menganalisis kebijakan kriminal dalam penanggulangan tindak pidana peretasan, serta mengidentifikasi kekuatan, kelemahan, dan tantangan dalam penegakan hukum di Indonesia. Metode yang digunakan dalam penelitian ini adalah pendekatan yuridis normatif, yaitu melalui studi literatur dan analisis dokumen hukum, terutama UU ITE dan peraturan terkait lainnya.

Hasil penelitian menunjukkan bahwa meskipun UU ITE sudah memberikan dasar hukum yang jelas untuk menangani peretasan, terdapat kelemahan signifikan dalam implementasinya. Salah satu tantangan terbesar adalah kurangnya kapasitas teknis dari aparat penegak hukum untuk menangani bukti digital dan mengatasi peretasan secara efektif. Selain itu, regulasi yang ada dianggap belum sepenuhnya memadai untuk menangani kompleksitas kejahatan siber yang berkembang, termasuk peretasan lintas negara.

Untuk mengatasi hal ini, diperlukan revisi UU ITE yang lebih komprehensif serta peningkatan keterampilan teknis penegak hukum melalui pelatihan yang lebih intensif. Kerja sama internasional juga sangat penting dalam menghadapi tantangan peretasan yang bersifat global. Penelitian ini terbatas pada analisis hukum, sehingga penelitian lebih lanjut dengan pendekatan empiris terhadap kasus peretasan di Indonesia diperlukan. Kesimpulannya, peningkatan kapasitas penegak hukum dan revisi regulasi menjadi kunci utama dalam menanggulangi tindak pidana peretasan secara efektif di Indonesia.

## REFERENSI

Arisandy, Y. O. (2021). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *1*(3), 162–169. https://doi.org/10.18196/ijclc.v1i3.11264

Benny Cahyadi, Erdy Gian Gara, Putra Pratama, Ginanjar Fitriadi, Arwansa, & Dwi Satya Arian. (2024). Hacker Anak Dalam Perspektif

Teori Differential Association: Studi Kasus Peretasan Situs Pengadilan Negeri Kabupaten Konawe. *IKRA-ITH HUMANIORA : Jurnal Sosial Dan Humaniora*, *8*(1), 1–12. https://doi.org/10.37817/ikraith-humaniora.v8i1.3588

Faridi, M. K. (2019). Kejahatan Siber Dalam Bidang Perbankan. *Cyber Security Dan Forensik Digital*, *1*(2), 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Kurniawan, D., & Maujuhan Syah, A. (2022). The Impact of Bjorka Hacker on the Psychology of the Indonesian Society and Government in a Psychological Perspective. *CONSEILS: Jurnal Bimbingan Dan Konseling Islam*, *2*(2), 53–60. https://doi.org/10.55352/bki.v2i2.627

Nuristiningsih, D. (2023). Upaya Penal Dan Non Penal Dalam Menanggulangi Tindak Pidana Teknologi Informasi. *Majalah Keadilan*, *23*, 62–90. https://journals.unihaz.ac.id/index.php/keadilan/article/view/4153%0Ahttps://journals.unihaz.ac.id/index.php/keadilan/article/download/4153/1702

Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Rahmasari, N. M. V. V., Budiartha, I. N. P., & Senastri, M. (2021). Pertanggungjawaban Para Pihak dalam Hal Terjadinya Peretasan Telepon Seluler. *Jurnal Preferensi Hukum*, *2*(2), 343–348. https://doi.org/10.22225/jph.2.2.3332.343-348

Ridwan, Nur, M., & Sulaiman. (2023). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan ( Hacker ) Dalam Undang-Undang Nomor Elektronik. *Jurnal Ilmiah Mahasiswa*, *VI*(1), 113–123.

Saleh, A. R. (2021). Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana. *HUKMY : Jurnal Hukum*, *1*(1), 91–108. https://doi.org/10.35316/hukmy.2021.v1i1.91-108

Shadily, F., Lisanawati, G., & Setiawan, P. J. (2024). Pemberatan Sanksi Pidana pada Tindakan Peretasan Situs Milik Dewan Kehormatan Penyelanggara Pemilu Indonesia. *Dialogia Iuridica Journal*, *15*(2).

Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334–339. https://doi.org/10.22225/jkh.2.1.2553.334-339

Trisnawati, T., & Hanifah, S. (2024). Perkembangan Alat Bukti Elektronik Hasil Peretasan (Hacker) Sebagai Alat Bukti Dalam Tindak Pidana. *Multidisciplinary Indonesian Center Journal (MICJO)*, *1*(3), 1344–1349. https://doi.org/10.62567/micjo.v1i3.162

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77.

https://doi.org/10.61084/jsl.v2i01.7

Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *2*(2), 1–21. https://doi.org/10.21274/legacy.2022.2.2.1-21

Wijaya, T. H. D. (2022). Penerapan Sanksi Sosial Sebagai Alternatif Pemidanaan Terhadap Pelaku Tindak Pidana Kejahatan Siber (Cyber Crime). *Al-Qisth Law Review*, *5*(2), 371. https://doi.org/10.24853/al-qisth.5.2.371-404