Volume 11 Issue 3, 2025
P-ISSN: 2442-8019, E-ISSN: 2620-9837

PERTANGGUNGJAWABAN PIDANA TERHADAP KEJAHATAN *HACKING*

Kayla Cahya Ayunda[1], Sartika Dewi[2], Yuniar Rahmatiar[3]

[1] Fakultas Hukum, Universitas Buana Perjuangan Karawang, Indonesia. E-mail: hk21.kaylaayunda@mhs.ubpkarawang.ac.id
[2] Fakultas Hukum, Universitas Buana Perjuangan Karawang, Indonesia.
[3] Fakultas Hukum, Universitas Buana Perjuangan Karawang, Indonesia.

Abstract: *Rapid advancements in information technology have significantly contributed to the escalation of cybercrime incidents, particularly hacking, which poses serious risks to individual data security and national resilience. The hacking activities associated with Bjorka highlight the fragility of Indonesia's data protection framework. This research seeks to examine the scope of criminal responsibility imposed on hacking offenders under Indonesian criminal law while also assessing the government's effectiveness in mitigating such offenses. Employing a normative legal research method, the study adopts statutory, conceptual, and case-based approaches, drawing on primary, secondary, and tertiary data sources analyzed through qualitative techniques. The research indicate that individuals involved in hacking may be prosecuted under Articles 30 and 46 of Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE Law), facing potential imprisonment ranging from six to eight years and/or monetary penalties between IDR 600 and 800 million, in addition to possible supplementary sanctions. The Indonesian government has taken steps by establishing regulations such as the Electronic Information and Transactions Law, the Personal Data Protection Law, and the Telecommunications Law, as well as by increasing the capacity of law enforcement officials, providing digital forensics training, and engaging in international cooperation.*

Keywords: *Hacking; Criminal Liability; ITE Law.*

How to Site: Kayla Cahya Ayunda, Sartika Dewi, Yuniar Rahmatiar (2025). Pertanggung Jawaban Pidana Terhadap Kejahataan *Hacking*. Jurnal hukum *to-ra*, 11 (3), pp. 589-600. DOI. 10.55809/tora.v11i3.593

Introduction

Kemajuan teknologi yang berlangsung sangat cepat membawa konsekuensi luas, baik yang bersifat konstruktif maupun destruktif terhadap kehidupan manusia. Salah satu faktor pendorong utama percepatan tersebut adalah arus globalisasi yang menghilangkan batas-batas ruang dan waktu. Namun, derasnya perkembangan ini tidak selalu diimbangi dengan kemampuan masyarakat untuk mengelola pengetahuan yang dihasilkan secara tepat. Ketidakmampuan sebagian individu dalam memanfaatkan teknologi secara bijak justru memunculkan berbagai kerugian, termasuk meningkatnya

tindak kejahatan siber seperti peretasan (*Hacking*) yang merupakan salah satu dampak negatif dari kemajuan teknologi.[1]

Hacking merujuk pada aktivitas mengakses atau menembus sistem komputer milik pihak lain tanpa otorisasi, biasanya untuk memanfaatkan atau menelaah celah keamanan yang ada. Meskipun umumnya dikategorikan sebagai tindakan ilegal, praktik ini dalam konteks tertentu dapat dilakukan dengan tujuan positif, misalnya untuk menemukan dan memperbaiki kerentanan keamanan siber. Aktivitas semacam ini sering disebut sebagai *ethical hacking* atau peretasan etis. Tujuan dari *hacker* melakukan tindakan ini sangatlah beragam. Ada yang melakukannya sebagai tindak pencurian atau bahkan melakukan pengancaman kepada pemilik sistem atau jaringan komputer. Hal ini tentunya merugikan bagi pemilik sistem atau jaringan komputer dari segi finansial dan reputasi. *Hacker* memiliki berbagai metode yang digunakan untuk membobol hak akses terhadap sistem atau jaringan komputer. Berbagai metode tersebut adalah sebagai berikut; *Malware, Phising, DoS dan DdoS, Clickjacking,* Peretasan password, Memanfaatkan Wi-fi tidak aman, Perekaman Keyboard, dan *Ethical hacking.*[2]

Kasus maupun insiden yang berkaitan dengan kebocoran data pribadi bukanlah hal asing di Indonesia, sebab peristiwa serupa kerap berulang dan semakin marak terjadi sepanjang periode 2023 hingga 2024.[3] Berdasarkan pemberitaan yang dilansir oleh Liputan6, laporan "*National Cyber Security Index"* (NCSI) mencatat bahwa pada tahun 2022, indeks keamanan siber Indonesia mencapai skor 38,96 dari 100. Dalam lingkup negara-negara G20, Indonesia menempati posisi ketiga. Secara global, posisi Indonesia menempati peringkat ke-83 dari 160 negara yang tercantum dalam laporan tersebut (Gideon, 2023). Memasuki tahun 2024, tercatat sebanyak 40 kasus dugaan pelanggaran keamanan data pribadi di Indonesia. Salah satu yang cukup menonjol adalah kebocoran data PDNS yang berdampak pada terganggunya operasional sejumlah layanan publik, serta kasus peretasan data NPWP sebanyak 6,6 juta identitas yang kemudian diperdagangkan di platform ilegal di *dark web*.

Salah satu insiden peretasan yang sempat menghebohkan publik di Indonesia adalah kasus Bjorka, yang menjadi perbincangan luas di dunia maya akibat aksi pencurian data berskala besar. Bjorka berhasil membobol sistem dan memperoleh berbagai dokumen penting, termasuk dokumen pribadi Presiden Joko Widodo dan sejumlah surat dari

[1] Ridwan, Muhammad Nur, Sulaiman. 2023. "*Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik."* Jurnal Ilmiah Mahasiswa (JIM FH). Vol. VI. No. 1. Hal. 2-3

[2] Dr. Budiyanto, S.H., M.H., 2023. "*Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*." Sada Kurnia Pustaka. Banten. Hlm. 23-27.

[3] Liputan6.com, "keamanan siber indonesia peringkat 3 terbawah di G20, ego sektoral kronis jadi biang keladinya" https://www.liputan6.com/bisnis/read/5243523/keamanan-siber-indonesia-peringkat-3-terbawah-di-g20-ego-sektoral-kronis-jadi-biang-keladinya?page=2 di akses pada 7 Agustus 2025

Badan Intelijen Negara (BIN). Selain itu, ia juga mempublikasikan data pribadi beberapa Aparatur Sipil Negara (ASN), dimulai dengan penyebaran data pribadinya sendiri. Skandal ini melibatkan kebocoran 1,3 miliar data kartu SIM seluler, rekam jejak penelusuran internet 26 juta pengguna Indihome, serta 105 juta data kependudukan yang dikelola oleh Komisi Pemilihan Umum Republik Indonesia (KPU RI). Meskipun demikian, respons pemerintah terlihat lebih terpusat pada upaya pelacakan dan penangkapan Bjorka dibandingkan penanganan dampak kebocoran data tersebut.[4] Sebagaimana "Pasal 30 Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur larangan mengakses komputer dan/atau sistem elektronik dengan cara membobol atau melanggar sistem keamanannya," Bjorka terancam hukuman penjara hingga delapan tahun serta denda sebesar Rp800 juta. UU ITE memberikan sanksi hanya kepada pelaku peretasan, namun tidak mengatur secara tegas mengenai kelalaian lembaga atau instansi yang bertanggung jawab atas keamanan data. Selain itu, jika terbukti melakukan penghapusan, perusakan, atau manipulasi data, dapat dikenakan Pasal 32 UU ITE. Dalam KUHP, asas legalitas memastikan bahwa perbuatan Bjorka termasuk tindakan pidana karena sudah diatur secara tegas pada UU. Namun, penegakan hukum terhadap kasus ini menghadapi tantangan seperti Identitas pelaku sulit diungkap karena penggunaan anonimitas dan lokasi operasi lintas negara, Keterbatasan SDM forensik digital di Indonesia, Lemahnya kerja sama internasional dalam penanganan kejahatan siber.

Urgensi pengaturan dan penegakan hukum terhadap kejahatan hacking menjadi semakin penting, mengingat dampaknya yang dapat merugikan negara, masyarakat, dan stabilitas keamanan nasional. Meskipun Indonesia telah memiliki sejumlah regulasi seperti UU No 1 Tahun 2024 terkait UU ITE, masih terdapat tantangan dalam hal penerapan pertanggungjawaban pidana terhadap pelaku kejahatan siber, khususnya yang bersifat lintas yurisdiksi dan bersifat anonim. Permasalahan utama yang muncul adalah bagaimana konsep pertanggungjawaban pidana diterapkan terhadap pelaku kejahatan hacking dalam sistem hukum Indonesia, serta sejauh mana instrumen hukum yang ada mampu menjangkau dan memberikan efek jera terhadap pelaku. Setiap individu yang melakukan pelanggaran hukum wajib menanggung konsekuensi atas tindakan yang dilakukannya.

Pertanggungjawaban pidana berkaitan dengan penentuan apakah seseorang dapat dimintai tanggung jawab atas tindakan kriminal yang telah diperbuatnya melalui pendekatan konsep kesalahan pidana. Secara substansial, pertanggungjawaban pidana berfungsi menilai apakah individu tersebut layak dijatuhi pidana atau justru dibebaskan.

[4] Kompas.Com, "*Rekap Kasus Kebocoran Data hacker Bjorka Hingga Pelacakan Keberadaan dan Identitasnya".* https://www.kompas.com/tren/read/2022/09/15/093000865/rekap-kasus-kebocoran-data-hacker-bjorka-hingga-pelacakan-keberadaan-dan diakses pada tanggal 15 Juli 2025.

Dalam terminologi hukum, dikenal dua istilah utama terkait pertanggungjawaban, yaitu *liability* dan *responsibility*. *Liability* merupakan istilah hukum yang menggambarkan ruang lingkup tanggung jawab seseorang atas risiko tertentu, mencakup aspek hak dan kewajiban, baik yang bersifat aktual maupun potensial. Cakupannya bisa meliputi ancaman, tindak pidana, kerugian, modal, ataupun kondisi yang menuntut pemenuhan kewajiban hukum sesuai peraturan perundang-undangan. Sementara itu, *responsibility* mengacu pada kapasitas seseorang untuk mempertanggungjawabkan kewajiban yang diemban, melibatkan unsur keputusan, keterampilan, keahlian, dan kompetensi dalam menjalankan peraturan hukum yang berlaku. Secara ringkas, *liability* lebih menitikberatkan pada aspek tanggung gugat secara yuridis akibat kesalahan yang menimbulkan dampak pada subjek hukum, sedangkan *responsibility* lebih mengarah pada bentuk pertanggungjawaban politik yang berkaitan dengan posisi, kebijakan, atau kewenangan tertentu.[5]

Discussion

Bentuk Pertanggungjawaban Pidana Yang Dapat Dikenakan Terhadap Pelaku Hacking Menurut Hukum Pidana Indonesia

Kemajuan teknologi dan arus informasi di era digital yang semakin masif membuat data pribadi individu rentan terekspos dan dimanfaatkan oleh pihak-pihak yang tidak berwenang. Fenomena ini tidak hanya berkaitan dengan aktivitas *hacking* yang dilakukan oleh seorang *hacker*, tetapi juga mencakup tindakan *cracking* yang dilakukan oleh seorang *cracker* sebagai bentuk lain dari kejahatan siber.[6] Walaupun hacking dan *cracking* memiliki sejumlah kesamaan, keduanya tetap memiliki karakteristik yang berbeda. Salah satu aktivitas ilegal yang kerap dilakukan oleh para *cracker* adalah *phishing*, yakni tindakan penipuan digital yang bertujuan memperoleh keuntungan pribadi dengan cara mengeksploitasi kerentanan korban. Praktik ini merugikan pihak lain dan termasuk dalam kategori *cyber crime* yang bersifat manipulatif dan merusak kepercayaan pengguna dunia maya.

Dalam hal kejahatan hacking, pelaku dapat dikenai sanksi pidana jika mencukupi unsur delik sejalan dengan UU yang relevan. Kemajuan pesat di bidang teknologi informasi telah mengubah paradigma masyarakat dengan kemunculan dunia maya (*cyber space*), yang ialah hasil dari terhubungnya jaringan komputer secara global, termasuk di

[5] Tomi Wicaksono Putra, S.H., Et. Al. 2023. "*Pertanggungjawaban Pidana Terhadap Kejahatan Hacking.*" PT Nasya Expanding Management. Pekalongan. Hal. 28-30.

[6] Ridwan, Muhammad Nur, Sulaiman. 2023. *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik*. Jurnal Ilmiah Mahasiswa (JIM FH). Vol. VI. No. 1. Hal. 2-3

dalamnya internet.[7] Peretasan atau hacking merupakan aktivitas mengakses sistem komputer, jaringan, atau data secara ilegal tanpa persetujuan dari pemiliknya. Tujuan dari tindakan ini dapat beragam, mulai dari sekadar mengeksplorasi teknologi hingga melakukan kejahatan seperti pencurian data, sabotase sistem, atau spionase siber. Para peretas atau hacker biasanya diklasifikasikan ke dalam beberapa jenis, antara lain ***White Hat Hackers***, ***Black Hat Hackers***, dan ***Grey Hat Hackers***.[8]

1. *White Hat Hackers* adalah peretas etis yang beroperasi secara legal dengan tujuan meningkatkan keamanan sistem. Mereka umumnya direkrut oleh perusahaan atau instansi pemerintah untuk menemukan celah keamanan dan membantu menutupnya sebelum dimanfaatkan oleh pihak yang berniat jahat. Melalui kegiatan seperti *penetration testing* atau simulasi serangan, mereka memastikan sistem tetap aman dan terlindungi. Seluruh aktivitas mereka dilakukan dengan izin dari pemilik sistem serta mematuhi hukum dan kode etik keamanan siber.
2. *Black Hat Hackers* adalah peretas yang melakukan tindakan ilegal dengan tujuan mengeksploitasi sistem demi keuntungan pribadi atau untuk merugikan suatu pihak. Mereka kerap terlibat dalam pencurian data, penyebaran malware, atau penghancuran sistem tanpa izin pemilik. Berbagai teknik digunakan, seperti *phishing*, *malware injection*, dan serangan *ransomware*. Aksi mereka sering menimbulkan kerugian besar bagi individu maupun perusahaan, baik dalam bentuk kerugian finansial maupun kebocoran data penting.
3. *Grey Hat Hackers* berada pada posisi "zona abu-abu" karena mereka mengakses sistem tanpa izin, namun tidak selalu dengan tujuan jahat. Mereka kerap menemukan celah keamanan dan memberitahukannya kepada pemilik sistem, tetapi dalam beberapa kasus juga meminta imbalan sebagai kompensasi atas informasi tersebut. Meskipun tindakan mereka tidak selalu menimbulkan kerusakan, tetap saja hal itu melanggar hukum karena dilakukan dengan masuk ke dalam sistem tanpa persetujuan.[9]

Dalam pertanggungjawaban pidana terhadap tindakan peretasan (*hacking*) merujuk pada ketentuan Pasal 30 UU ITE. Pada pasal tersebut, seseorang dapat dikenakan sanksi pidana apabila mengakses sistem elektronik atau komputer milik orang lain tanpa izin. Pasal ini menegaskan bahwa bentuk akses yang dilakukan dengan cara apa pun,

[7] Yudha Pratama, "Urgensi Keamanan Siber dalam Perspektif Hukum Nasional," *Dialektika Hukum*, Vol. 3, No. 1 (2022): 86

[8] Fithriatus Shalihah, "Tindak Pidana Peretasan (Hacking) dalam Perspektif Hukum Pidana Indonesia," *Jurnal Penelitian Hukum De Jure*, Vol. 19, No. 3, 2019, hlm. 317;

[9] Dr. Budiyanto, S.H., M.H., 2023. "*Pengantar Cybercrime Dalam Sistem Hukum Pidana Di Indonesia*." Sada Kurnia Pustaka. Banten. Hlm. 23-27.

termasuk peretasan, tetap dianggap melanggar hukum jika dilakukan tanpa hak.[10] Pertanggungjawaban pidana pada hakikatnya merupakan mekanisme hukum yang berfungsi menilai sejauh mana seseorang dapat dimintai pertanggungjawaban atas suatu perbuatan yang dikualifikasikan sebagai tindak pidana. Dengan kata lain, konsep ini berperan sebagai tolok ukur untuk menetapkan apakah individu yang diduga melakukan pelanggaran dapat dibebaskan dari tuntutan hukum atau justru dikenai sanksi pidana. Kewajiban pidana tersebut hanya dibebankan kepada pihak yang secara sah dan meyakinkan terbukti melakukan perbuatan melawan hukum, sehingga menjadi dasar utama dalam penjatuhan hukuman.[11]

Seseorang dapat dimintai pertanggungjawaban pidana apabila tindakannya memenuhi unsur melawan hukum. Namun, pertanggungjawaban tersebut dapat gugur apabila terdapat kondisi internal yang menyebabkan hilangnya kemampuan untuk bertanggung jawab secara hukum. Landasan utama suatu perbuatan dapat dipidana didasarkan pada asas legalitas sebagaimana ditegaskan dalam ketentuan Pasal 1 Ayat (1) KUHP, yang mengatakan bahwasanya "tidak ada perbuatan yang dapat dikenai pidana tanpa adanya ketentuan peraturan perundang-undangan yang telah berlaku sebelumnya. Unsur kesalahan menjadi elemen pokok dalam pembebanan pertanggungjawaban pidana, sementara konsep tindak pidana sendiri tidak serta-merta mencakup aspek pertanggungjawaban pidana."

Dalam ketentuan Pasal 30 Ayat (1) menjelaskan bahwa:

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun. Perbuatan pidana hacking telah mendapatkan pengaturan dan perumusan dalam sejumlah pasal yang memungkinkan pelaku dikenai sanksi hukum."

Secara umum, ketentuan mengenai tindak pidana hacking tercantum dalam Pasal 30 UU No 1 Tahun 2024 tentang Perubahan Kedua atas UU No 11 Tahun 2008 tentang ITE.[12] Unsur-unsur tindak pidana yang tercantum dalam ketentuan Pasal 30 Ayat (2) pada dasarnya serupa dengan Ayat (1). Namun pada ketentuan Ayat (2) menambahkan elemen tujuan, yakni "dengan maksud untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Pernyataan tersebut menegaskan bahwa individu yang masuk atau memanfaatkan komputer maupun sistem elektronik milik pihak lain tanpa memperoleh persetujuan, melalui metode apa pun, melakukannya dengan maksud

[10] Putri Lestari, "*Analisis Hukum Terhadap Tindak Pidana Peretasan Berdasarkan UU ITE*," Skripsi, Fakultas Hukum Universitas Diponegoro, 2020, hlm. 40.

[11] Eddy O.S. Hiariej, "*Prinsip-Prinsip Hukum Pidana*," Jakarta: Cahaya Atma Pustaka, 2016, hlm. 128;

[12] Yahya Ahmad Zein, "*Hukum Pidana Siber di Indonesia*," Jakarta: Sinar Grafika, 2020, hlm. 89; Fithriatus Shalihah, "Tindak Pidana Peretasan (Hacking) dalam Perspektif Hukum Pidana Indonesia," *Jurnal Penelitian Hukum De Jure*, Vol. 19, No. 3, 2019, hlm. 319;

tertentu, yakni untuk memperoleh informasi elektronik dan/atau dokumen elektronik. Pasal 30 ayat (3) menambahkan unsur "dengan tujuan untuk merugikan orang lain".

Sanksi terhadap pelaku hacking dijelaskan dalam pasal 46 UU ITE, Yaitu:

- "Pelanggaran Pasal 30 ayat (1) dipidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600 juta"
- "Pelanggaran Pasal 30 ayat (2) dipidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700 juta"
- "Pelanggaran Pasal 30 ayat (3) dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800 juta."

Selain itu, pelaku hacking juga dapat dijerat dengan ketentuan Pasal 32 UU ITE apabila perbuatannya disertai dengan manipulasi, penghapusan, atau perusakan data elektronik milik pihak lain. Selain sanksi pidana pokok, pelaku hacking juga dapat dikenai pertanggungjawaban tambahan seperti:

1. **Penyitaan barang bukti** (perangkat elektronik, server, atau alat bantu lainnya)
2. **Pemulihan kerugian korban melalui ganti rugi** (jika dituntut secara perdata)
3. **Pencabutan hak-hak tertentu**, seperti akses terhadap sistem tertentu, atau larangan profesi bagi pelaku dengan jabatan IT tertentu.[13]

Dengan demikian, penegakan hukum yang efektif memerlukan kombinasi antara penguatan regulasi, peningkatan kapasitas aparat penegak hukum, serta kerja sama antarnegara melalui mekanisme *mutual legal assistance* (MLA). Penerapan penegakan hukum yang berkesinambungan tidak semata-mata menimbulkan rasa jera bagi para pelanggar, tetapi juga berperan signifikan dalam memperkuat kepercayaan masyarakat terhadap efektivitas perlindungan hukum di ruang siber Indonesia. Dengan demikian, meskipun secara normatif perbuatan Bjorka dapat dikenai pertanggungjawaban pidana sesuai UU ITE dan KUHP, faktor teknis dan koordinasi antarnegara menjadi kendala besar dalam realisasi penegakan hukumnya.

Peran Pemerintah Dalam Menangani Kejahatan *Hacking*

Secara garis besar, hukum dapat dipahami sebagai seperangkat aturan atau pedoman yang mengarahkan serta membatasi perilaku individu dalam lingkup masyarakat maupun negara. Asal-usul terbentuknya hukum dipengaruhi oleh beragam faktor yang membentuk karakteristik dan wujudnya. Sumber hukum sendiri dapat ditelusuri dari aspek yang bersifat material, seperti kondisi sosial, ekonomi, dan politik, maupun dari

[13] Gusti Ngurah Agung Darmaputra, "Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan Dunia Maya (Cyber Crime) Berdasarkan UU ITE," *Kertha Wicaksana: Jurnal Ilmu Hukum*, Vol. 15, No. 2, 2021, hlm. 225;

aspek immaterial, seperti nilai-nilai moral, etika, dan keyakinan yang berkembang dalam masyarakat.[14] Strategi nasional Indonesia mencakup enam area utama, yaitu:

1. Nilai budaya dan kemampuan dalam menjaga keamanan informasi.
2. Potensi ancaman terhadap keamanan informasi.
3. Upaya untuk mengurangi risiko terkait keamanan informasi.
4. Proses penanganan insiden yang berkaitan dengan keamanan informasi.
5. Tingkat kinerja dalam pengelolaan keamanan informasi.
6. Kemampuan penegakan hukum di sektor Informasi dan Transaksi Elektronik (ITE).

Pemerintah Indonesia berupaya menangani kasus peretasan ini dengan membentuk sejumlah payung hukum, antara lain "UU No. 36 Tahun 1999 tentang Telekomunikasi, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik", Peraturan-peraturan tersebut mengatur dan mengkriminalisasi berbagai bentuk kejahatan siber, di mana para pelanggarnya dapat dikenakan sanksi pidana. Selanjutnya, Undang-Undang No. 27 Tahun 2022 merupakan regulasi yang mengatur perlindungan data pribadi, yang disosialisasikan kepada masyarakat guna menjamin terpenuhinya hak warga negara dalam hal keamanan data pribadi.[15] Dengan demikian, sebagai bagian dari masyarakat Indonesia, kita dituntut untuk meningkatkan perlindungan terhadap data pribadi guna meminimalisasi risiko kejahatan siber, khususnya peretasan. Upaya yang dapat dilakukan meliputi pemanfaatan VPN ketika terhubung dengan *home network*, melakukan pembaruan perangkat lunak secara rutin, menetapkan kata sandi Wi-Fi dengan tingkat keamanan tinggi, serta menghindari interaksi dengan email atau tautan yang berasal dari sumber tidak terpercaya.

Pihak Kepolisian Republik Indonesia melakukan berbagai strategi preventif guna meminimalisasi kemungkinan terulangnya insiden serupa. Salah satunya adalah dengan mengirimkan personel Polri untuk mengikuti program pelatihan tingkat internasional di berbagai negara maju agar pengetahuan dan keterampilan yang diperoleh dapat diaplikasikan di Indonesia, seperti kursus *CETS* di Kanada, pelatihan *Computer Forensic* di Jepang, serta program *Virtual Undercover* di Washington. Selain meningkatkan kompetensi sumber daya manusia, Polri juga melakukan modernisasi infrastruktur dan teknologi agar selaras dengan perkembangan dunia digital. Di sisi lain, mengingat tindak kejahatan siber bersifat lintas batas negara, kepolisian secara aktif memperkuat jejaring kerja sama dan koordinasi dengan lembaga penegak hukum internasional. Dalam konteks yang lebih luas, pemerintah Indonesia juga perlu mengambil langkah-langkah strategis, seperti merancang kerangka kebijakan dan peraturan perundang-undangan

[14] Sudikno Mertokusumo, "*Mengenal Hukum: Suatu Pengantar*," Yogyakarta: Liberty, 2014, hlm. 1–3;

[15] Afif Fahmi, "*Analisis Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia*," Skripsi, Fakultas Hukum Universitas Indonesia, 2023, hlm. 40.

yang tegas, komprehensif, dan adaptif sebagai pedoman utama bagi aparat penegak hukum dalam menindak serta memberantas pelaku *cybercrime*.[16]

Pemerintah juga dapat membentuk badan khusus keamanan siber yang berfokus pada peningkatan koordinasi dan penguatan pertahanan jaringan nasional, sehingga keamanan sistem lebih terjamin. Upaya lainnya meliputi identifikasi potensi ancaman siber beserta strategi pencegahannya, menjalin kerja sama dengan lembaga internasional ataupun nasional, serta menjalankan klasifikasi data untuk menentukan informasi yang memerlukan perlindungan khusus, baik yang terkait dengan perusahaan, instansi pemerintah, maupun data pribadi warga negara.[17] Sementara itu, langkah yang dapat dilakukan oleh masyarakat secara individu di Indonesia antara lain dengan rutin memperbarui kata sandi pada akun-akun pribadi, sehingga kata sandi menjadi lebih sulit ditebak dan diakses pihak lain. Lebih jauh, pengguna disarankan untuk tidak mengakses tautan mencurigakan, khususnya yang dikirim oleh pihak tidak dikenal, mengingat semakin banyaknya penyebaran link berbahaya dengan kedok undangan pernikahan, informasi perbankan, maupun pemberitahuan hadiah, yang berpotensi menyisipkan malware ke dalam akun atau perangkat. Selain itu, pembaruan sistem sebaiknya hanya dilakukan melalui perangkat lunak resmi agar celah keamanan tidak dimanfaatkan oleh peretas. Penggunaan jaringan *Wi-Fi* publik juga perlu dihindari, karena umumnya tidak menyediakan perlindungan memadai terhadap kerahasiaan data pengguna. Terakhir, informasi pribadi sebaiknya tidak dipublikasikan atau dibagikan melalui media sosial, mengingat data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Dengan demikian, meskipun pemerintah telah memiliki instrumen hukum dan strategi teknis, efektivitasnya masih terbatas. Ke depan, diperlukan pendekatan yang lebih komprehensif, yaitu menggabungkan aspek hukum, teknologi, diplomasi internasional, dan literasi siber masyarakat untuk menanggulangi kejahatan hacking secara berkelanjutan.

[16] Barda Nawawi Arief, "*Bunga Rampai Kebijakan Hukum Pidana"*, Jakarta: Kencana, 2017, hlm. 112;

[17] Dian Nurdiansyah, *Analisis Strategi Nasional Keamanan Siber Indonesia*, Skripsi, Fakultas Hukum Universitas Airlangga, 2021, hlm. 62.

Conclusion

Bentuk pertanggungjawaban pidana terhadap pelaku hacking menurut hukum pidana Indonesia Pelaku hacking dapat dimintai pertanggungjawaban pidana berdasarkan ketentuan "Pasal 30 dan Pasal 46 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)". Ketentuan ini menegaskan pelarangan terhadap tindakan memasuki, menggunakan, atau mengakses komputer maupun sistem elektronik milik pihak lain secara tanpa izin atau bertentangan dengan ketentuan hukum. Larangan tersebut mencakup upaya memperoleh informasi elektronik ataupun dokumen elektronik secara tidak sah, serta tindakan yang ditujukan untuk menimbulkan kerugian bagi pihak lain. Pelanggaran atas ketentuan ini dapat dikenakan sanksi pidana berupa penjara dengan durasi maksimum 6 hingga 8 tahun dan/atau denda yang mencapai Rp600 juta hingga Rp800 juta, bergantung pada unsur pelanggaran yang terbukti. Selain sanksi pidana pokok, pelaku juga dapat dikenai sanksi tambahan seperti penyitaan barang bukti, ganti rugi secara perdata, dan pencabutan hak tertentu. Pertanggungjawaban pidana ini tetap berlaku meskipun pelaku beroperasi secara anonim atau lintas yurisdiksi, selama dapat dibuktikan memenuhi unsur delik dan asas legalitas sebagaimana diatur dalam KUHP. Pemerintah Indonesia telah mengambil langkah melalui pembentukan regulasi seperti UU ITE, UU Perlindungan Data Pribadi, dan UU Telekomunikasi, serta melalui peningkatan kapasitas aparat penegak hukum, pelatihan forensik digital, dan kerja sama internasional. Strategi ini meliputi pencegahan, penindakan, serta edukasi masyarakat terkait keamanan siber. Pemerintah juga mendorong pembentukan badan khusus keamanan siber yang fokus pada koordinasi dan penguatan pertahanan jaringan nasional. Namun, efektivitas penegakan hukum masih terkendala oleh faktor teknis seperti kesulitan mengungkap identitas pelaku, keterbatasan sumber daya manusia, dan lemahnya koordinasi lintas negara. Ke depan, dibutuhkan pendekatan terpadu yang menggabungkan instrumen hukum, teknologi, diplomasi internasional, dan literasi siber masyarakat untuk menanggulangi kejahatan hacking secara berkelanjutan.

References

Books

Barda Nawawi Arief, S. H. (2016). *Bunga rampai kebijakan hukum pidana*. Prenada Media.

Budiyanto, S. H. (2023). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Eddy O.S. Hiariej, (2016). *Prinsip-Prinsip Hukum Pidana*. Cahaya Atma Pustaka.

Mertokusumo, S. (2014). Mengenal hukum: Suatu pengantar. Liberty.

Putra, T. W., Abdurrachman, H., & Hamzani, A. I. (2023). *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Penerbit NEM.

Journal

Afif Fahmi, Analisis Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia, Skripsi, Fakultas Hukum Universitas Indonesia, 2023.

Dian Nurdiansyah, Analisis Strategi Nasional Keamanan Siber Indonesia, Skripsi, Fakultas Hukum Universitas Airlangga, 2021.

Fithriatus Shalihah, "Tindak Pidana Peretasan (Hacking) dalam Perspektif Hukum Pidana Indonesia," Jurnal Penelitian Hukum De Jure, Vol. 19, No. 3, 2019.

Gusti Ngurah Agung Darmaputra, "Pertanggungjawaban Pidana Terhadap Pelaku Kejahatan Dunia Maya (Cyber Crime) Berdasarkan UU ITE," Kertha Wicaksana: Jurnal Ilmu Hukum, Vol. 15, No. 2, 2021.

Putri Lestari, Analisis Hukum Terhadap Tindak Pidana Peretasan Berdasarkan UU ITE, Skripsi, Fakultas Hukum Universitas Diponegoro, 2020.

Ridwan, Muhammad Nur, Sulaiman. 2023. Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Jurnal Ilmiah Mahasiswa (JIM FH). Vol. VI. No. 1.

Ridwan, Muhammad Nur, Sulaiman. 2023. Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Peretasan (Hacking) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Jurnal Ilmiah Mahasiswa (JIM FH). Vol. VI. No. 1.

Yahya Ahmad Zein, Hukum Pidana Siber di Indonesia, Jakarta: Sinar Grafika, 2020, hlm. 89;

Fithriatus Shalihah, "Tindak Pidana Peretasan (Hacking) dalam Perspektif Hukum Pidana Indonesia," Jurnal Penelitian Hukum De Jure, Vol. 19, No. 3, 2019.

Yudha Pratama, "Urgensi Keamanan Siber dalam Perspektif Hukum Nasional," Dialektika Hukum, Vol. 3, No. 1 (2022).

Regulations

Undang – Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik

Kitab Undang – Undang Hukum Pidana (KUHP)

Website

Kompas.Com, "Rekap Kasus Kebocoran Data hacker Bjorka Hingga Pelacakan Keberadaan dan Identitasnya". https://www.kompas.com/tren/read/2022/09/15/093000865/rekap-kasus-kebocoran-data-hacker-bjorka-hingga-pelacakan-keberadaan-dan, Diakses pada tanggal 15 Juli 2025.

Liputan6.com "Keamanan Siber Indonesia Peringkat 3 Terbawah di G20, Ego Sektoral Kronis Jadi Biang Keladinya". https://www.liputan6.com/bisnis/read/5243523/keamanan-siber-indonesia-peringkat-3-terbawah-di-g20-ego-sektoral-kronis-jadi-biang-keladinya?page=2 Diakses pada tanggal 7 Agustus 2025.