Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

KAJIAN HUKUM DAN REGULASI TERKAIT SERANGAN HACKING PADA PLATFORM DIGITAL DI INDONESIA

STUDY OF LAWS AND REGULATIONS RELATED TO HACKING ATTACKS ON DIGITAL PLATFORMS IN INDONESIA

Adelina Damayanti Anggarini [1*], Rina Arum Prastyanti[2]
[1*] Prodi S1-Hukum, Fakultas Hukum dan Bisnis, Universitas Duta Bangs
[2]Prodi S1-Hukum, Fakultas Hukum dan Bisnis, Universitas Duta Bangsa
*email Koresponden: anggariniadelina@gmail.com

DOI: 10.62567/micjo.v1i2.117

Article info:
Submitted: 28/04/24 Accepted: 30/04/24 Published: 30/04/24

Abstract

Hacking is a technique carried out by someone (hacker, cracker, intruder, or attacker) to attack a system, network, and application by exploiting weaknesses with the intention of gaining access rights to data and systems. Currently, the development of Information and Communication Technology (ICT) is experiencing very rapid growth. The development of information technology, especially the internet, has provided many positive benefits for its users. However, the use of internet technology also has negative impacts that cannot be ignored. The increase in Cybercrime cases in Indonesia is also caused by the impact of advances in Information Technology. Based on this explanation, the aim of this research is to find out how to study law enforcement procedures for hacking victims on digital platforms and how to ensure that digital platform users are more regulated regarding cyber security. The research method used is a descriptive analytical method. The results and discussion in this research are that handling crime cases in the field of information and electronic transactions is a responsibility that has been established for investigators, especially cyber patrols, to investigate and uncover these crimes. The investigation process has a very important and strategic role in determining the success of criminal law enforcement. The quality of a good investigation greatly determines the possibility of success in the prosecution process and makes it easier to reveal material truths during the trial. In order to prevent cybercrime, it is important for individuals and governments to have a deep understanding of crime patterns in the digital realm as well as current and ongoing internet trends and behavior carried out by perpetrators of these crimes.

Keywords **:** *Hacking, cyber, digital platform*

Abstrak

Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem. Saat ini, perkembangan Teknologi Informasi dan Komunikasi (TIK) sedang mengalami pertumbuhan yang sangat cepat, Perkembangan teknologi informasi, terutama internet, telah memberikan banyak manfaat positif bagi penggunanya, Namun, penggunaan teknologi internet juga membawa dampak negatif yang tidak bisa diabaikan.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com
E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

Peningkatan kasus Cybercrime di Indonesia juga disebabkan oleh dampak kemajuan Teknologi Informasi. Berdasarkan paparan tersebut tujuan penelitian ini adalah untuk mengetahui Bagaimana kajian prosedur penegakan hukum bagi korban hacking pada platform digital dan Bagaimana cara agar pengguna platform digital lebih terregulasi terkait dengan keamanan siber. Metode penelitian yang digunakan adalah metode deskriptif analitis. Hasil dan pembahasan dalam penelitian ini yaitu Penanganan kasus kejahatan di bidang informasi dan transaksi elektronik merupakan tanggung jawab yang telah ditetapkan bagi penyelidik, khususnya patroli siber, untuk menyelidiki dan mengungkap kejahatan tersebut. Proses penyidikan memiliki peran yang sangat penting dan strategis dalam menentukan keberhasilan penegakan hukum pidana. Kualitas penyidikan yang baik sangat menentukan kemungkinan sukses dalam proses penuntutan dan memudahkan pengungkapan kebenaran materiil selama persidangan. Agar dapat mencegah kejahatan siber, penting bagi individu dan pemerintah untuk memiliki pemahaman yang mendalam tentang pola kejahatan di ranah digital serta tren dan perilaku internet terkini dan berkelanjutan yang dilakukan oleh para pelaku kejahatan tersebut.

Kata Kunci : Hacking/peretasan, cyber, platform digital

1. PENDAHULUAN

Saat ini, perkembangan Teknologi Informasi dan Komunikasi (TIK) sedang mengalami pertumbuhan yang sangat cepat, baik di Indonesia maupun di seluruh dunia. Misi pokok dari kemajuan teknologi adalah untuk mempermudah, mempercepat, menekan biaya, dan meningkatkan keamanan dalam kehidupan manusia (Benny Cahyadi et al., 2024). Perkembangan teknologi informasi, terutama internet, telah memberikan banyak manfaat positif bagi penggunanya, seperti meningkatnya kecepatan dalam pengiriman dan penerimaan informasi, kemudahan dalam melakukan kegiatan online, mempermudah transaksi bisnis, menyediakan platform jejaring sosial yang menyenangkan, dan menyediakan beragam hiburan tanpa batas. Bentuk teknologi komunikasi berupa perangkat keras dan struktur organisasi yg berfungsi mengumpulkan, memproses, serta bertukar informasi dengan orang lain (Pudjiarti et al., 2023).

Platform digital merujuk pada struktur teknologi yang memungkinkan pengembangan fungsi komputasinya serta memfasilitasi integrasi berbagai platform teknologi informasi, komputasi, dan konektivitas yang tersedia bagi sebuah organisasi[1] (Juwita et al., 2022). Sebagai pengguna platform digital, tentunya perlu mengelola identitas digital dan data pribadi di dalam platform tersebut. Masalah yang masih timbul terkait dengan perlindungan identitas digital dan data pribadi. Indonesia termasuk negara yang belum memiliki undang-undang yang khusus mengatur perlindungan data pribadi, sehingga hak-hak warga negara tidak sepenuhnya dijamin oleh undang-undang. Peretasan akun dan kebocoran data pribadi adalah contoh ancaman keamanan digital yang bisa mengungkapkan identitas digital dan informasi pribadi kepada pihak yang tidak berwenang. Informasi ini bisa dimanfaatkan tanpa pengetahuan pengguna untuk tujuan yang tidak diketahui dan berpotensi merugikan mereka. Penggunaan luas platform digital menyebabkan akumulasi data besar dari informasi yang dikumpulkan, meningkatkan risiko bocornya identitas digital dan data pribadi selama proses penyimpanan dan pengolahan data[2] (Anak Agung Ayu Intan Wulandari & Komang Tri Werthi, 2023).

Digital platform diidealkan sebagai struktur digital yang berhubungan dengan sumber daya komputasi dan jaringan, memfasilitasi pihak-pihak yang terlibat untuk mengembangkan konten yang diperlukan. Dalam beberapa dekade terakhir, digital platform telah menjadi pilar utama dalam mengatur berbagai aspek kehidupan manusia, termasuk ekonomi, politik, dan interaksi sosial. Seiring dengan perkembangan ini, muncul berbagai platform seperti amazon.com untuk e-commerce, edmodo untuk pendidikan, gojek untuk transportasi, facebook dan instagram untuk media sosial, serta YouTube, dan sebagainya. Hal ini menunjukkan bahwa platform berbasis internet memiliki dampak yang besar tidak

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com
E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

hanya dalam ranah ekonomi, tetapi juga dalam hal-hal seperti kepemilikan intelektual, terutama hak cipta[3] (Asril et al., 2021).

Berikut data kasus kejahatan peretasan platform digital di Indonesia dalam 5 tahun terakhir :

Table 1 Kasus peretasan platform digital

No	Tahun	Jumlah Kasus	Keterangan
1	2019	20.048	Peningkatan 13% dari tahun 2018
2	2020	32.402	Peningkatan 61% dari tahun 2019
3	2021	28.232	Peningkatan 13% dari tahun 2020
4	2022	36.054	Peningkatan 28% dari tahun 2021
5	2023 (Jan-Sept)	24.109	Diperkirakan akan meningkat di akhir tahun

Sumber Data:

- Badan Siber dan Sandi Negara (BSSN)
- Kominfo: https://kominfo.go.id/
- Katadata: https://katadata.co.id/
- Media massa: Kompas, Tempo, CNN Indonesia

Hack dalam ahasa Indonesia adalah meretas yaitu menggunakan computer, atau perangkat teknologi lainnya untuk mengakses data milik orang lain atau organisasi lain secara tidak sah. Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem. Istilah "Hacking" dalam konteks keamanan informasi mengacu pada tindakan mengeksploitasi kelemahan dalam sebuah sistem dengan maksud untuk memperoleh akses dan kontrol yang tidak sah terhadap sumber daya sistem. Praktik ini berpotensi merusak keamanan sistem serta dapat dimanfaatkan untuk mengubah sumber daya sistem, mengganggu fitur dan layanan, dengan tujuan mencapai berbagai tujuan yang tidak sah. Selain itu, tindakan peretasan juga dapat dimanfaatkan untuk mencuri informasi rahasia yang kemudian dapat digunakan untuk berbagai kepentingan. Maka tidak kecil kemungkinan para hacker dapat terus menambah jumlah data pencurian atau peretasan (Pencurian et al., n.d.).

Perlindungan adalah esensi dari keamanan. Tujuan utama keamanan adalah melindungi dari ancaman, baik yang disengaja maupun tidak disengaja. Sebagai contoh, keamanan nasional merupakan rangkaian sistem yang kompleks untuk melindungi kedaulatan negara, asetnya, sumber daya, dan warganya. Untuk mencapai tingkat keamanan yang tepat bagi suatu organisasi, diperlukan beragam sistem. Organisasi yang berhasil harus memiliki berbagai lapisan keamanan yang melindungi operasionalnya, infrastruktur fisik, personel, fungsi, komunikasi, dan informasi.

Berdasarkan pendahuluan diatas maka terdapat dua rumusan masalah yaitu :

1. Bagaimana kajian prosedur penegakan hukum bagi korban hacking pada platform digital?
2. Bagaimana cara agar pengguna platform digital lebih terregulasi terkait dengan keamanan siber?

2. METODE PENELITIAN

Jenis penelitian ini adalah Penelitian pustaka, merupakan proses penelitian yang dilakukan dengan menggali informasi dari berbagai buku dan literatur yang relevan dengan topik yang sedang dibahas. Dalam konteks ini, peneliti akan membaca dan menganalisis buku-buku yang terkait dengan hacking untuk memperoleh pemahaman yang mendalam tentang hasil-hasil penelitian yang telah dilakukan sebelumnya dalam bidang tersebut. metode penelitian dengan menerapkan pendekatan hukum normatif, yang memeriksa informasi dari sumber sekunder dan mengacu pada prinsip-prinsip yang tercantum dalam peraturan hukum. Dengan menggunakan metode tersebut, penelitian dilakukan

E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

terhadap informasi sekunder yang terkait dengan perlindungan hukum bagi pengguna platform digital terhadap tindak kejahatan hacking dalam penggunaan platform digital.

Penulis menyelesaikan penulisan dengan menggunakan pendekatan hukum normatif yang menitikberatkan pada pemahaman konsep, teori, dan regulasi hukum yang terkait dengan penelitian yang dilakukannya. Dalam penelitian ini, penulis mengadopsi metode deskriptif analitis. Data lapangan dianalisis dengan merujuk pada peraturan hukum dan teori-teori yang relevan, kemudian disajikan secara kualitatif tanpa menggunakan rumus atau statistik, tetapi dengan mempertimbangkan hubungan aturan hukum positif secara kualitatif.

Teori Hukum

Teori Asosiasi Diferensial, yang juga dikenal sebagai Differential Association Theory, pertama kali diajukan oleh sosiolog Amerika Serikat, Edwin H. Sutherland, pada tahun 1939 dan kemudian diperbarui pada tahun 1947. Konsep ini terinspirasi oleh beberapa teori lain, termasuk Teori Transmisi Ekologis dan Budaya oleh Shaw dan McKay, Interaksionisme Simbolik oleh George Mead, serta Teori Konflik Budaya.

Teori ini memiliki dua versi. Pada tahun 1939, Sutherland mengusulkan teori tentang perilaku kriminal sistematis, konflik budaya, disorganisasi sosial, dan asosiasi diferensial. Konsep "sistematis" merujuk pada karier kriminal atau praktik terorganisir dari kejahatan. Praktik terorganisir kejahatan mengacu pada tindakan yang mendukung norma-norma yang telah ada dalam masyarakat. Dalam versi ini, teori berfokus pada proses komunikasi seseorang dengan kelompok pergaulan, menunjukkan bahwa kejahatan atau perilaku jahat muncul dari komunikasi dengan individu yang terlibat dalam perilaku kriminal. Versi kedua, diperbarui oleh Sutherland pada tahun 1947, mengganti istilah "Disorganisasi Sosial" dengan "Organisasi Sosial Diferensial." Perubahan istilah tersebut dimaksudkan untuk menunjukkan keberagaman kondisi sosial dengan nilai-nilai internal.

Teori asosiasi diferensial menyatakan bahwa individu menjadi pelaku kriminal karena mereka mempelajari perilaku kriminal dari lingkungan sosial mereka melalui interaksi dan komunikasi yang intim dan mendalam. Teori ini menekankan pentingnya proses pembelajaran seseorang, yang mengimplikasikan bahwa kejahatan, seperti halnya perilaku lainnya, dapat dipelajari. Proses pembelajaran ini terjadi dalam kelompok melalui interaksi dan komunikasi, di mana individu mempelajari teknik untuk melakukan kejahatan serta alasan yang mendukung tindakan tersebut, seperti nilai-nilai, motif, rasionalisasi, dan tingkah laku. Teori ini berlaku baik untuk kasus anak-anak maupun orang dewasa, dan tidak berkaitan dengan karakteristik individu atau sifat-sifat konkret yang terlihat secara langsung. Sutherland menekankan bahwa fakta dasar yang ditekankan adalah adanya variasi sosial dalam masyarakat, di mana asosiasi diferensial menyebabkan kriminalitas pada individu sebagai hasil dari prinsip pembelajaran sosial. Dengan demikian, konsep asosiasi diferensial berlaku baik untuk kelompok yang terlibat dalam kegiatan kriminal maupun kelompok yang menentangnya. Dari penjelasan diatas, dapat dipahami bahwa teori Asosiasi Diferensial mengakui bahwa lingkungan mempengaruhi perilaku seseorang dan memiliki efek tertentu. Selain itu, dapat disimpulkan bahwa Sutherland meyakini bahwa individu akan mengalami perubahan sesuai dengan harapan dan pandangannya.

3. HASIL DAN PEMBAHASAN

Dalam hal negara dan pertahanan, kemajuan teknologi informasi disertai oleh ancaman yang berpotensi dalam keamanan siber bagi negara (Putri et al., 2022). Namun, penggunaan teknologi internet juga membawa dampak negatif yang tidak bisa diabaikan. Munculnya kejahatan dunia maya (cyber crime) seperti pencurian kartu kredit dalam transaksi bisnis e-commerce, serangan ke situs web, terutama situs pemerintah, dan kasus plagiasi di dunia akademik, serta meningkatnya kasus pencemaran nama baik karena kemudahan akses dan publikasi berita dan keluhan di forum dan media sosial[4] (Hermawan, 2013). Teknologi menjadi perkembangan yang dikatakan pesat dari masa ke masa (Vol et al., 2023). Media sosial adalah platform online di mana pengguna dapat dengan mudah terlibat, berbagi,

dan menciptakan berbagai konten, termasuk blog, jejaring sosial, wiki, forum, dan dunia virtual. Blog, jejaring sosial, dan wiki merupakan jenis media sosial yang paling sering digunakan oleh masyarakat global. Sudut pandang lain menyatakan bahwa media sosial adalah platform online yang memfasilitasi interaksi sosial dan menggunakan teknologi berbasis web untuk mengubah komunikasi menjadi dialog interaktif (Rafiq, 2015).

Table 2 PENGGUNAAN TEKNOLOGI DAN TINGKAT KEPEDULIAN TERHADAP PRIVASI

No.	Perspektif pada masalah privasi TI	Persentase
1	Tingkat kepercayaan akan peluang TI dibandingkan resiko	71%
2	Penggunaan TI dalam menyelesaikan tugas	68%
3	Tingkat kepercayaan akan privasi data dan perlindungannya	79%
4	Penghapusan cookies pada browser Internet untuk melindungi privasi	57%
5	Penggunaan alat pemblokiran iklan untuk menghentikan iklan yang ditampilkan	50%

Kekhawatiran pengguna mengenai privasi berkaitan dengan risiko kehilangan privasi yang timbul dari penyingkapan informasi kepada pihak ketiga seperti pengembang platform digital (Akraman & Priyadi, 2018). Peningkatan kasus Cybercrime di Indonesia juga disebabkan oleh dampak kemajuan Teknologi Informasi dalam mempengaruhi budaya di Indonesia, seperti perubahan dalam peran gender, peningkatan rasa percaya diri, dan tekanan yang dirasakan. Budaya yang telah terakar kuat dalam masyarakat Indonesia dan sangat memengaruhi kehidupan sosialnya juga menjadi faktor dalam munculnya kasus Cybercrime ini, dimana kelemahan dalam budaya sosial masyarakat Indonesia menjadi celah bagi masuknya kasus-kasus ini. Oleh karena itu, pentingnya kesadaran masyarakat dalam menghadapi kasus Cybercrime harus diperkuat, termasuk perubahan dalam budaya masyarakat itu sendiri (Chintia et al., 2018).

Hacker bisa dikelompokkan ke dalam beberapa kategori yang berbeda. Secara umum, ada tiga kategori utama:

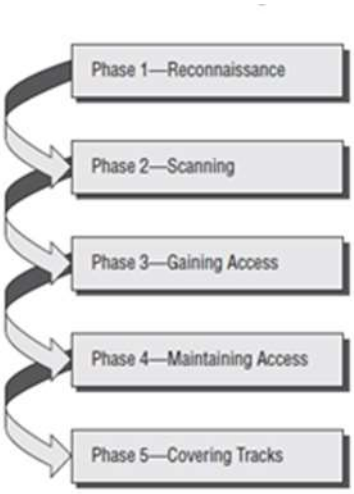
a. Black Hat Hacker adalah jenis hacker yang dianggap berbahaya dan jahat. Motivasi mereka biasanya berkisar pada keuntungan finansial, balas dendam, atau kegiatan kriminal lainnya. Mereka memperoleh akses ilegal ke dalam sistem, seringkali dengan tujuan merusaknya atau mencuri informasi sensitif.
b. White Hat Hacker, yang juga dikenal sebagai Ethical Hacker, bertindak dengan niat baik. Mereka tidak pernah bermaksud merusak sistem, melainkan mereka berusaha untuk menemukan kelemahan dalam komputer atau jaringan sebagai bagian dari pengujian penetrasi atau evaluasi kerentanan.
c. Grey Hat Hacker adalah kelompok hacker yang berada di antara Black Hat dan White Hat Hacker. Terkadang, mereka melakukan peretasan dengan memanfaatkan kelemahan sistem seperti yang dilakukan oleh Black Hat Hacker. Namun, di sisi lain, mereka juga dapat berperan sebagai konsultan keamanan, mirip dengan White Hat Hacker.[5]

Langkah-langkah hacking selanjutnya akan dijadikan pedoman untuk mengidentifikasi tindakan-tindakan hacking yang dapat dianggap sebagai kejahatan. Langkah-langkah hacking yang dimaksud mencakup:

a. Mengumpulkan dan mempelajari informasi tentang sistem operasi komputer atau jaringan komputer yang digunakan oleh target yang dituju.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com
E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

b. Meretas atau mengakses jaringan komputer yang menjadi target.
c. Mengeksplorasi sistem komputer dan mencari cara untuk mendapatkan akses yang lebih tinggi.
d. Membuat pintu belakang (backdoor) dan menghapus jejak yang ada (Ite et al., 2019).



Gambar 1 Metode Hacking

Terdapat lima metode hacking diantaranya :

1. Reconnaissance

Reconnaissance merupakan fase di mana informasi dikumpulkan, di mana seorang peretas akan menghimpun data tentang target dari berbagai sumber yang tersedia. Ini bisa mencakup nama-nama anggota keluarga, tanggal lahir, detail pekerjaan, dan informasi terkait lainnya. Namun, manfaat Reconnaissance tidak terbatas pada hal-hal tersebut saja. Reconnaissance dibagi menjadi dua jenis, yaitu Active Reconnaissance dan Passive Reconnaissance.

a. Active Reconnaissance melibatkan peretas dalam proses pengumpulan informasi secara langsung dengan korban atau entitas yang terhubung dengan korban. Hal ini dianggap berisiko karena interaksi langsung dengan target.
b. Passive Reconnaissance, di sisi lain, melibatkan pencarian informasi tanpa sepengetahuan langsung korban. Sebagai contoh, peretas akan melakukan profilisasi data korban di internet tanpa interaksi langsung dengan mereka.

2. Scanning

Scanning merupakan fase di mana secara aktif dilakukan penyelidikan terhadap kerentanan yang mungkin bisa dieksploitasi dari target.

3. Gaining access

Gaining access adalah tahapan proses penetrasi sudah dilakukan. Hacker akan berusaha menguasai sistem target dari kelemahan target sistem yang telah diperoleh dari hasil scanning.

4. Maintaining access

Menjaga akses merupakan langkah dalam proses di mana peretas telah berhasil memperoleh akses ke sistem. Setelah itu, peretas menempatkan backdoor ke dalam sistem agar dapat terus mempertahankan akses tersebut.

5. Clearing Tracks

Clearing Tracks adalah langkah di mana seorang peretas akan menghilangkan jejaknya dengan menghapus file log dan semua jejak yang mungkin telah ditinggalkannya. (Kelrey & Muzaki, 2019)

Kajian prosedur penegakan hukum bagi korban hacking pada platform digital

Penegak hukum adalah individu yang terlibat secara langsung atau tidak langsung dalam menjalankan proses penegakan hukum. Mereka memadukan nilai, norma, dan perilaku dalam tindakan mereka. Umumnya, penegak hukum berperan aktif dalam upaya untuk mencapai tujuan keadilan

melalui tindakan dan pemeliharaan hukum (Hukum & Yogyakarta, 2020). Permasalahan-permasalahan sebagaimana yang telah dijelaskan, membutuhkan pencarian solusi terutama pada ranah hukum. Hukum harus dapat menjadi solusi atas permasalahan-permasalahan yang hadir dalam kehidupan manusia. Penanganan kasus kejahatan di bidang informasi dan transaksi elektronik merupakan tanggung jawab yang telah ditetapkan bagi penyelidik, khususnya patroli siber, untuk menyelidiki dan mengungkap kejahatan tersebut. Proses penyidikan memiliki peran yang sangat penting dan strategis dalam menentukan keberhasilan penegakan hukum pidana. Kualitas penyidikan yang baik sangat menentukan kemungkinan sukses dalam proses penuntutan dan memudahkan pengungkapan kebenaran materiil selama persidangan. Dalam ranah hukum, kejelasan tentang bukti kejahatan, lokasi kejahatan, dan korban tindak kejahatan itu diperlukan untuk menegakkan hukum (Hartono, 2011).

Keamanan siber adalah serangkaian tindakan yang bertujuan untuk melindungi informasi, perangkat keras, perangkat lunak, serta elemen-elemen lain dalam ruang siber dari ancaman, gangguan, dan serangan jaringan computer (Aji, 2022). Dalam menghadapi kompleksitas komunikasi global melalui internet, dibutuhkan undang-undang yang responsif terhadap perkembangan teknologi dan proaktif dalam mengatasi masalah, termasuk penyalahgunaan internet dengan beragam motif yang berpotensi merugikan pengguna secara finansial maupun non-finansial (Mathilda et al., n.d.). Sesuai dengan Pasal 109 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP), penyidik wajib segera memberitahukan kepada Penuntut Umum setelah memulai penyidikan terhadap suatu tindak pidana. Hal ini bertujuan untuk mencegah penyidikan yang berkepanjangan tanpa adanya penyelesaian, di mana Penuntut Umum memiliki kewenangan untuk meminta klarifikasi mengenai perkembangan penyidikan yang sedang dilakukan.

Dari tiga kriteria umum yang berkaitan dengan jenis kejahatan di bidang informasi dan transaksi elektronik yang dikenal dalam masyarakat, salah satu aspek yang paling disoroti adalah tindakan melanggar privasi dengan cara mengakses sistem elektronik milik orang lain. Masih banyak masyarakat yang tidak mengetahui dasar hukum dan kepastian hukum penggunaan platfm digital (Murizqy & Dirkareshza, 2011). Secara hukum, tindakan tersebut dianggap sebagai perbuatan yang melanggar hukum, sebagaimana diatur dalam Pasal 30 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang menyatakan :

"(1) Setiap orang dengan sengaja tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun"

Selanjutnya, berbicara tentang potensi hukuman yang diatur dalam Pasal 46 ayat (1) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang menyatakan:

"(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)."

Norma tindak pidana pada Pasal 30 ayat (1) Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdiri dari unsur-unsur yaitu:

a. Subjek hukum : setiap orang
b. Kesalahan: dengan sengaja
c. Melawan hukum: tanpa hak atau melawan hukum
d. Perbuatan: mengakses
e. Objek: komputer atau sistem elektronik
f. Caranya: dengan cara apapun; Unsur (Pathavi & Prasetyo, 2023)

Dengan inklusi kejahatan mengakses sistem elektronik orang lain dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 sebagai revisi dari Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan langkah yang menunjukkan tanggung jawab aparat penegak hukum dalam memberikan perlindungan optimal terhadap penggunaan teknologi informasi dan komunikasi oleh masyarakat. Hal ini bertujuan untuk melindungi masyarakat dari potensi kejahatan dan penyalahgunaan teknologi, termasuk kasus seperti tindakan mengakses sistem elektronik orang lain yang terjadi di Wilayah Hukum Polres Batanghari (Whitt, 2020). Dalam konteks ini, penting bagi para korban untuk mendapatkan kompensasi atas

kerugian yang mereka alami. Hal tersebut akan mempengaruhi aktivitas manusia di berbagai bidang (Ismantara & Prianto, 2022). Oleh karena itu, hak mereka untuk mendapatkan restitusi harus dijamin dan dilindungi sebagai bagian dari tanggung jawab negara melalui penegakan hukumnya (Sahabuddin, 2023), dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya (Liviani, 2020).

Pasal 27 ayat 3 sering dikenal sebagai "pasal karet" oleh para ahli hukum dan praktisi ICT. Poin penting dalam pasal tersebut adalah frasa "dengan SENGAJA" dan "TANPA HAK". Banyak pakar berpendapat bahwa dalam kasus Prita, tindakannya tidak disengaja dalam upaya mencemarkan nama baik, melainkan sekadar menyampaikan keluhan terkait pengalamannya, yang sebenarnya dilindungi oleh UU Perlindungan Konsumen. Pertanyaan selanjutnya adalah, apakah Prita tidak memiliki hak? Sebenarnya, Prita memiliki hak untuk menyuarakan keluhannya mengenai pengalaman yang dia alami sebagai konsumen dan pasien di rumah sakit tersebut. Kasus ini memiliki potensi dampak yang negatif, karena dapat mendorong ketakutan masyarakat untuk menyampaikan pendapat, kritik, saran, atau komentar mereka secara daring. Oleh karena itu, penting untuk merevisi Pasal UU ITE, setidaknya untuk sementara waktu tidak menjadikannya sebagai dasar hukum, sampai ada penurunan hukum lebih lanjut seperti Peraturan Pemerintah (PP) dan Peraturan Menteri/Kepmen Kominfo.

Hukum Informasi dan Transaksi Elektronik (UU ITE) telah memperkenalkan alat bukti yang dapat digunakan sesuai dengan Pasal 5, yang meliputi Informasi Elektronik, Dokumen Elektronik, dan hasil cetaknya. Sejalan dengan adaptasi terhadap kondisi pasca-pandemi di Indonesia, Peraturan Mahkamah Agung (Perma) Nomor 4 Tahun 2020 tentang Administrasi dan Persidangan Perkara Pidana di Pengadilan secara Elektronik mengenalkan ketentuan baru terkait dengan Dokumen Elektronik yang disampaikan (von Briel & Davidsson, 2019). Persyaratan baru tersebut mengamanatkan bahwa dokumen harus dalam format Portable Document Format (PDF) dan harus melalui proses verifikasi untuk memastikan kesesuaian antara dokumen yang dibacakan dengan yang diunduh (Khalisah & Kirana, 2022). Keberhasilan penerapan aspek pidana dalam UU ITE dinilai dari segi substansi dan struktur hukumnya, termasuk ketersediaan penegak hukum, sumber daya manusia dalam penegakan hukum, partisipasi masyarakat dalam menegakkan hukum, serta dukungan sarana dan prasarana yang diperlukan untuk menjamin penegakan hukum yang efektif (Tindak & Cyber, 2016).

Cara pengguna platform digital lebih terregulasi terkait dengan keamanan siber

Saat platform digital diretas, respons yang cepat dan tepat sangat penting untuk mendapatkan kendali kembali atas akun tersebut. Tindakan-tindakan penting termasuk segera mengubah kata sandi untuk mencegah akses yang tidak sah serta memberitahukan platform media sosial tentang kejadian tersebut agar mereka dapat mengambil tindakan yang sesuai. Selain itu, meminta bantuan dari lembaga penegak hukum atau ahli keamanan cyber dapat menjadi langkah yang cerdas, terutama jika ada indikasi kejahatan yang terkait dengan peretasan tersebut. Berkolaborasi dengan pihak berwenang dapat membantu dalam penyelidikan lebih lanjut dan penegakan hukum terhadap pelaku. Dengan mengambil langkah-langkah ini secara proaktif, individu yang terdampak oleh peretasan dapat meningkatkan peluang pemulihan dan mengurangi risiko potensial yang timbul akibat akses yang tidak sah terhadap akun media sosial mereka (Puteri & Soesanto, 2023).

Agar dapat mencegah kejahatan siber, penting bagi individu dan pemerintah untuk memiliki pemahaman yang mendalam tentang pola kejahatan di ranah digital serta tren dan perilaku internet terkini dan berkelanjutan yang dilakukan oleh para pelaku kejahatan tersebut (Butarbutar, 2023). Ketiadaan pengaturan atau regulasi yang memadai mengenai keamanan siber dan perlindungan data pribadi menyebabkan kelemahan dalam dunia siber, menciptakan ketidakjelasan di kalangan masyarakat. Oleh karena itu, diperlukan sebuah sistem yang dapat mengatasi tantangan tersebut[6]. Kejahatan – kejahatan siber pada dasarnya merupakan kejahatan konvensional (Jurnal et al., 2024). Selain itu, perbaikan keamanan akun, hukuman yang tegas bagi pelaku kejahatan, kerjasama dengan platform, tim tanggap keamanan, hukum perlindungan data pribadi, pendidikan hukum digital, pengembangan teknologi keamanan, dan audit keamanan rutin juga menjadi langkah-langkah yang

disarankan untuk mengatasi peretasan pada platform digital (Fergie Brillian Arthaleza1 , Uzie Valerie2 , Najla Rafiki3, n.d.).

Jenis-jenis serangan hacking adalah :

1. Phising

Peretasan semacam ini sering terjadi, terutama di berbagai platform media sosial. Phishing adalah teknik peretasan yang bertujuan mencuri informasi email korban dengan membuat situs web palsu yang terlihat resmi dan seolah-olah berasal dari organisasi yang sah.

2. Dos dan DdoS

Jenis peretasan ini menyebabkan korban tidak bisa mengakses sistem, perangkat, atau teknologi informasi lainnya yang dimilikinya. Seorang peretas ilegal atau kriminal biasanya menggunakan metode serangan ini untuk merusak sistem, server web, dan mengganggu lalu lintas jaringan korban dengan serangan DDoS.

3. DNS Spoofing

Biasanya, tindakan peretasan ini dilakukan dengan memanfaatkan celah keamanan pada DNS dan server web klien untuk mengarahkan lalu lintas internet ke server yang palsu.

4. Injeksi Keylogger

Program keylogging biasanya disuntikkan atau disebarluaskan kepada korban menggunakan alat peretasan sebagai malware, yang dapat merekam atau memantau semua penekanan tombol yang dilakukan oleh korban. Ini dapat memberikan hacker banyak informasi penting, termasuk pencurian data pribadi seperti kredensial login, data perusahaan, dan banyak lagi.

5. Serangan brutal

Biasanya, tindakan peretasan ini menggunakan alat untuk menebak berbagai kombinasi seperti nama pengguna, kata sandi, atau kode kombinasi lainnya dengan tujuan meretas sistem.

6. Perbaikan UI

Peretas ini sering disebut juga sebagai clickjacking, di mana hacker menciptakan antarmuka pengguna palsu atau tautan palsu di dalam sebuah situs web resmi. Maksudnya adalah agar pengunjung situs tersebut mengklik tautan palsu tersebut, sehingga hacker dapat mengakses komputer korban tanpa sepengetahuan mereka (Sari, 2015).

Barikut cara mencegah terjadinya serangan kejahatan hacking :

1. Memasang Proteksi: Memastikan keamanan informasi dengan menginstal proteksi menjadi hal yang sangat penting. Proteksi ini bisa berupa antivirus atau firewall. Antivirus digunakan untuk mendeteksi program-program yang berpotensi merusak sistem atau data di dalam komputer, seperti virus.
2. Memantau Serangan: Sering kali serangan dari penyusup dilakukan tanpa sepengetahuan administrator jaringan, oleh karena itu, diperlukan sistem pemantauan terhadap serangan tersebut. Salah satu sistem tersebut adalah Intruder Detection System (IDS) yang memberikan peringatan langsung kepada administrator melalui alarm, sinyal, atau pesan email jika ada serangan. Contoh dari IDS adalah tcpdump untuk menganalisis paket data yang lewat.
3. Mengatur Keamanan Program: Saat merancang sistem keamanan jaringan komputer, penting untuk memperhatikan detail kecil yang bisa dimanfaatkan oleh penyusup. Diperlukan ketelitian dalam memilih karakter-karakter khusus dan perhitungan algoritma dalam pembuatan program.
4. Menutup Layanan yang Tidak Diperlukan: Layanan-layanan yang tidak diperlukan pada umumnya disertakan dan dijalankan secara default dalam sebuah sistem operasi. Namun, layanan-layanan tersebut dapat dimanfaatkan oleh penyusup untuk melakukan hacking. Oleh karena itu, sebaiknya layanan-layanan tersebut ditutup jika tidak diperlukan.
5. Menggunakan Public-Key Cryptography: Untuk menjaga keamanan data-data penting, digunakanlah Public-Key Cryptography. Program ini akan secara otomatis mengacak (encrypt) informasi yang dikirim dan memerlukan kata sandi (password) untuk membukanya (decrypt). Ini dilakukan menggunakan Public Key Infrastructures yang dimiliki oleh lembaga penyelenggara untuk mendukung Digital Signature.
6. Melakukan Backup: Mengingat perkembangan kejahatan hacking yang semakin kompleks, melakukan backup secara berkala menjadi sangat penting. Jika sistem pengamanan telah

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com
E.ISSN. 3032-2472
Vol. 1 No. 2 Edisi
April 2024

ditembus oleh penyusup, data-data di dalam komputer dapat menjadi sasaran selanjutnya. Dengan melakukan backup, kemungkinan data asli yang rusak atau dimanipulasi oleh penyusup dapat diminimalisir (Kejahatan et al., 2022).

Gambar 2 CIA Triangle

Prinsip keamanan informasi merupakan perlindungan terhadap aspek-aspek berikut:

a. Ketersediaan (Availability) adalah dimensi yang memastikan bahwa data tersedia saat diperlukan, memungkinkan pengguna yang berhak untuk mengakses informasi dan perangkat terkait sesuai kebutuhan.
b. Integritas (Integrity) adalah aspek yang menjamin bahwa data tidak mengalami perubahan tanpa izin dari pihak yang berwenang, menjaga keakuratan dan integritas informasi, serta prosesnya untuk memastikan bahwa integritas ini tetap terjaga.

Kerahasiaan (Confidentiality) adalah dimensi yang memastikan bahwa informasi tetap rahasia dan hanya diakses oleh pihak yang memiliki izin, serta memastikan kerahasiaan data saat dikirim, diterima, dan disimpan.

4. KESIMPULAN

Peningkatan kasus Cybercrime di Indonesia juga disebabkan oleh dampak kemajuan Teknologi Informasi dalam mempengaruhi budaya di Indonesia, seperti perubahan dalam peran gender, peningkatan rasa percaya diri, dan tekanan yang dirasakan. Pada platform digital diidealkan sebagai struktur digital yang berhubungan dengan sumber daya komputasi dan jaringan, memfasilitasi pihak-pihak yang terlibat untuk mengembangkan konten yang diperlukan. Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem. oleh sebab itu diperlukan Penegak hukum (individu yang terlibat secara langsung atau tidak langsung dalam menjalankan proses penegakan hukum). Karena masih banyak masyarakat yang tidak mengetahui dasar hukum dan kepastian hukum penggunaan platfm digital. Dengan inklusi kejahatan mengakses sistem elektronik orang lain dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 sebagai revisi dari Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, ini merupakan langkah yang menunjukkan tanggung jawab aparat penegak hukum dalam memberikan perlindungan optimal terhadap penggunaan teknologi informasi dan komunikasi oleh masyarakat.

5. DAFTAR PUSTAKA

Aji, M. P. (2022). *Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective*. https://doi.org/10.22212/jp.v13i2.3299

Akraman, R., & Priyadi, Y. (2018). *Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia*. *02*, 1–8.

Anak Agung Ayu Intan Wulandari, & Komang Tri Werthi. (2023). Peningkatan Kepedulian Terhadap Perlindungan Keamanan Data Pribadi di Platform Digital Bagi Warga Kelurahan Tonja. *Jurnal Pengabdian Masyarakat Bhinneka (JPMB)*, *1*(3), 188–194. https://doi.org/10.58266/jpmb.v1i3.41

Asril, F. A., Permata, R. R., & Ramli, T. S. (2021). Perlindungan Hak Cipta pada Platform Digital Kreatif YouTube. *Jurnal Jurisprudence*, *10*(2), 146–162. https://doi.org/10.23917/jurisprudence.v10i2.10368

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

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya. *Journal Technology and Economiacs Law*, *2*(2), 297–316.

Chintia, E., Nadiah, R., Ramadhani, H. N., & Haedar, Z. F. (2018). *Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya*. *02*.

Fergie Brillian Arthaleza1 , Uzie Valerie2 , Najla Rafiki3, N. S. H. M. R. (n.d.). *Perspektif Hukum Telematika Terhadap Kasus Cyber Crime Di Indonesia*.

Hartono, B. (2011). *Hacker dalam perspektif hukum indonesia*. *26*, 23–30.

Hermawan, R. (2013). Kesiapan Aparatur Pemerintah Dalam Menghadapi. *Jurnal Teknik Informatika*, *6*(1), 43–50.

Hukum, F., & Yogyakarta, U. M. (2020). *Penegakan Hukum terhadap Cyber Crime Hacker*. *1*(2), 162–169. https://doi.org/10.18196/ijclc.v1i3.11264

Ismantara, S., & Prianto, Y. (2022). Relevansi Hukum Perlindungan Konsumen Indonesia Di Era Ekonomi Digital. *Prosiding Serina*, *4*(3), 321–330. https://journal.untar.ac.id/index.php/PSERINA/article/view/18548%0Ahttps://journal.untar.ac.id/index.php/PSERINA/article/download/18548/10468

Ite, U., Hukum, D. A. N., & Islam, P. (2019). *No Title*.

Jurnal, H., Hukum, I., Februari, N., Hukum, F., & Padjadjaran, U. (2024). *Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia Salsabila Chairunnisa Tarsisius Murwadji Nun Harrieti Pelaku Usaha Jasa Keuangan (" PUJK ") d alam hal ini bank d*. *2*(1).

Juwita, O., Firdonsyah, A., Ali, M., Widodo, A. P., & Isnanto, R. R. (2022). Studi Literatur Platform Digital Sebagai Sarana Pembangunan Ekosistem Dalam Mengembangkan UMKM. *INFORMAL: Informatics Journal*, *7*(1), 59. https://doi.org/10.19184/isj.v7i1.31547

Kejahatan, A., Sebagai, H., Cyber, B., Dalam, C., & Hukum, S. (2022). *Jurnal Pendidikan dan Konseling*. *4*, 3029–3034.

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

Khalisah, A. M., & Kirana, P. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, *5*(6), 2117–2132. https://doi.org/10.20473/jd.v5i6.40073

Liviani, M. R. H. (2020). *Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia*. *23*(2).

Mathilda, F., Pengajar, S., Mku, U. P., & Negeri, P. (n.d.). *CYBER CRIME DALAM SISTEM HUKUM INDONESIA CYBER CRIME IN INDONESIA LAW SYSTEM*. 34–45.

Murizqy, M. A., & Dirkareshza, R. (2011). *Peninjauan Aspek Keamanan Dan Perlindungan Hukum Terhadap Investor Crpytocurrency*. *7*, 277–292.

Pathavi, W., & Prasetyo, M. H. (2023). *Tinjauan Hukum Pidana Cheat / Hacking dalam Game Online Berdasarkan Undang-Undang Nomor 11 Tahun 2008 dan Undang- Undang Nomor 19 Tahun 2015*. *5*(2), 2059–2080. https://doi.org/10.37680/almanhaj.v5i2.3110

Pencurian, A., Indonesia, B., Perlindungan, R. U., Pribadi, D., & Indonesia, B. (n.d.). *Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia) Aditama Candra Kusuma , Ayu Diah Rahmani Fakultas Hukum , Universitas Pembangunan Veteran Jakarta Kemajuan teknologi sangat membantu manu*. *5*(01), 46–63.

Pudjiarti, E., Faizah, S., & Hardani, S. (2023). Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi dan Media Sosial. *Bina Insani Ict Journal*, *10*(1), 210–223.

Puteri, A. A., & Soesanto, E. (2023). *IJM : Indonesian Journal of Multidisciplinary Pengamanan Cyber pada Media Sosial Instagram dalam Mengurangi Dampak Negatif Psikologis*. *1*, 1988–1996.

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

Rafiq, A. (2015). *dilengapi dengan fasilitas yang disediakan dalam berkomunikasi semakin beraneka macam, mulai dari*. 18–29.

Sahabuddin, S. (2023). *Legalitas*. *15*(2), 265–272. https://doi.org/10.33087/legalitas.v15i2.513

Sari, I. (2015). *MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA Indah Sari*. 169–186.

Tindak, D., & Cyber, P. (2016). *Issn : no. 0854-2031*. *14*(0854), 16–27.

Vol, T., Maret, N., Mesin, J. T., Dan, E., Komputer, I., & Whphisher, S. D. A. N. (2023). *ANALISIS KERENTANAN KEJAHATAN ONLINE PHISING MENGGUNAKAN TOOLS*. *3*(1), 23–31.

von Briel, F., & Davidsson, P. (2019). Digital platforms and network effects: Using digital nudges for growth hacking. *40th International Conference on Information Systems, ICIS 2019*, 1–9.

Whitt, R. S. (2020). Hacking the SEAMs: Elevating Digital Autonomy and Agency for Humans. *SSRN Electronic Journal*, 135–212. https://doi.org/10.2139/ssrn.3669914