Pengantar [CYBERCRIME]

dalam Sistem Hukum Pidana di Indonesia

Dr. Budiyanto, S.H., M.H.

PENGANTAR *CYBERCRIME*

dalam Sistem Hukum Pidana di Indonesia

Dr. Budiyanto, S.H., M.H.

sada kurnia pustaka

PENGANTAR *CYBERCRIME*

dalam Sistem Hukum Pidana di Indonesia

Penulis:

Dr. Budiyanto, S.H., M.H.

Editor : Anik Iftitah, S.H., M.H.
Tata Letak : Lilis Khalisatul Karimah, S.H.
Desain Cover : Septimike Yourintan Mutiara, S.Gz.
Ukuran : UNESCO 15,5 x 23 cm
Halaman : vii, 182
ISBN : 978-634-7021-15-1
Terbit Pada : Januari 2025
Anggota IKAPI : No. 073/BANTEN/2023

PENERBIT PT SADA KURNIA PUSTAKA
Jl. Warung Selikur Km.6 Sukajaya – Carenang, Kab. Serang Banten
Email : sadapenerbit@gmail.com
Website : sadapenerbit.com & repository.sadapenerbit.com
Telpon/WA : +62 838 1281 8431

KATA PENGANTAR

"Keberhasilan dalam memerangi kejahatan siber tidak hanya terletak pada penguasaan teknologi, tetapi juga pada penerapan hukum yang adaptif dan efektif." – Ahmad M. Ramli, Pakar Hukum Siber Indonesia.

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga buku *"Pengantar Cybercrime: dalam Sistem Hukum Pidana di Indonesia"* ini dapat diselesaikan. Buku ini hadir sebagai wujud kepedulian terhadap isu *cybercrime* yang semakin kompleks dan dinamis di era digital. Kajian dalam buku ini dirancang untuk memberikan pemahaman mendalam tentang fenomena *cybercrime* dalam konteks sistem hukum pidana di Indonesia, termasuk tantangan yang dihadapi dalam penegakkan hukum serta solusi untuk mengatasi hambatan tersebut.

"Cybercrime is the greatest threat to every profession, every industry, and every country." – Ginni Rometty, Mantan CEO IBM.

Buku ini terdiri atas delapan bab yang saling terintegrasi untuk memberikan gambaran menyeluruh mengenai *cybercrime*. Bab pertama, *Pendahuluan*, menguraikan latar belakang dan urgensi pembahasan isu ini, terutama dalam kaitannya dengan perkembangan teknologi dan hukum di Indonesia. Bab ini menjadi pintu masuk bagi pembaca untuk memahami pentingnya sinergi antara teknologi dan hukum dalam memerangi kejahatan siber.

Bab kedua, *Definisi dan Jenis-Jenis Kejahatan Siber*, mengupas berbagai bentuk *cybercrime*, seperti *hacking*, pencurian data, *phishing*, hingga *cyber-terrorism*. Pemahaman ini penting untuk membangun kerangka analisis yang kokoh dalam upaya penegakan hukum.

Bab ketiga, *Cybercrime di Indonesia*, mengulas perkembangan kasus-kasus kejahatan siber di Indonesia, termasuk upaya regulasi yang telah dilakukan. Bab ini juga mengidentifikasi celah hukum yang masih menjadi tantangan utama dalam penegakan hukum terhadap *cybercrime*.

"Without rules and regulations, it is impossible to tackle crimes that transcend borders." – Eugene Kaspersky, Pakar Keamanan Siber Dunia.

Pada Bab keempat, *Tantangan Penegakan Hukum dalam Kasus Cybercrime*, pembahasan difokuskan pada hambatan yang dihadapi lembaga penegak hukum di Indonesia, Kepolisian, Kejaksaan, Peradilan, dan Pemasyarakatan. Bab ini menyoroti tantangan teknis, kelemahan koordinasi, serta keterbatasan sumber daya manusia yang berpengaruh terhadap efektivitas penanganan kasus *cybercrime*.

Bab kelima, *Bukti Elektronik dalam Proses Pembuktian Pidana*, membahas pentingnya bukti elektronik dalam sistem peradilan pidana modern. Aspek legalitas, validitas, serta tantangan teknis dalam pengumpulan dan pembuktian bukti elektronik dibahas secara mendalam dalam bab ini.

Bab keenam, *Kolaborasi Internasional dalam Penanggulangan Cybercrime*, menyoroti pentingnya kerja sama lintas negara untuk mengatasi sifat *cybercrime* yang sering kali melampaui batas yurisdiksi nasional. Bab ini memberikan perspektif tentang bagaimana Indonesia dapat memanfaatkan perjanjian internasional dan kolaborasi global untuk memperkuat sistem penegakan hukum siber.

"In a digital world, cyber justice must ensure that human rights are preserved even in the pursuit of security." – Tim Berners-Lee, Penemu World Wide Web.

Bab ketujuh, *Pelindungan Hak Asasi Manusia dalam Penegakan Hukum Cybercrime*, menekankan pentingnya menjaga keseimbangan antara keamanan dan pelindungan hak asasi manusia. Bab ini mengulas potensi pelanggaran hak dalam proses hukum kasus *cybercrime* dan cara untuk meminimalkan risiko tersebut.

Bab kedelapan, *Penutup*, menyajikan rangkuman serta rekomendasi strategis untuk meningkatkan efektivitas penegakan hukum terhadap kasus *cybercrime* di Indonesia.

Penulis berharap buku ini dapat menjadi referensi yang bermanfaat bagi akademisi, mahasiswa, praktisi hukum, dan pembaca umum yang memiliki minat terhadap isu *cybercrime*.

Terima kasih penulis sampaikan kepada semua pihak yang telah memberikan dukungan, baik langsung maupun tidak langsung, dalam proses penyusunan buku ini. Semoga buku ini dapat memberikan kontribusi nyata dalam pengembangan ilmu hukum pidana dan praktik penegakan hukum di Indonesia.

Penulis

DAFTAR ISI

BAB 1
PENDAHULUAN

Mengapa *Cybercrime* Penting untuk dipahami?

Transisi ekonomi Indonesia saat ini dibangun di atas prinsip-prinsip yang mendukung pertumbuhan di berbagai sektor, sekaligus membuka kesempatan yang setara bagi seluruh rakyat Indonesia. Prinsip-prinsip ini menekankan pentingnya inklusivitas dan pemerataan dalam pembangunan ekonomi, sehingga setiap lapisan masyarakat dapat berkontribusi dan merasakan manfaat dari kemajuan yang dicapai. Dengan demikian, Indonesia berupaya menciptakan ekosistem ekonomi yang berkelanjutan terhadap berbagai tantangan global. Indonesia adalah bangsa yang memiliki kekayaan budaya yang luar biasa, dengan keragaman suku, bahasa, dan tradisi yang menjadi aset penting dalam pembangunan nasional. Kekayaan budaya ini tidak hanya menjadi identitas bangsa, tetapi juga sumber inspirasi dalam menciptakan ekonomi bernilai tambah. Pertumbuhan ekonomi yang terus meningkat didorong oleh sektor manufaktur dan jasa, yang memanfaatkan kreativitas dan inovasi berbasis budaya lokal untuk bersaing di pasar internasional. Dengan potensi yang dimiliki, Indonesia bercita-cita untuk menjadi salah satu dari lima ekonomi terbesar dunia pada tahun 2045 dan menjadi pemimpin di panggung internasional. Visi ini menuntut akselerasi pembangunan di berbagai bidang, termasuk peningkatan kualitas sumber daya manusia, penguatan infrastruktur, dan pengembangan teknologi. Peran aktif Indonesia dalam forum-forum global juga menjadi strategi penting untuk memperkuat posisi dan pengaruhnya di kancah internasional.

Oleh sebab itu, transformasi digital akan menjadi katalis yang sangat penting dalam perjalanan ini, yang akan mendorong Indonesia

berubah dari negara konsumen menjadi negara produsen. Digitalisasi diharapkan dapat meningkatkan efisiensi, produktivitas, dan daya saing di berbagai sektor ekonomi. Selain itu, transformasi digital membuka peluang bagi lahirnya industri-industri baru yang berbasis teknologi dan inovasi, yang dapat menjadi motor penggerak pertumbuhan ekonomi di masa depan.

Pandemi Covid-19 pada tahun 2020 telah mendorong kebutuhan transformasi digital nasional menjadi semakin krusial. Koneksi internet yang memadai telah menjadi kebutuhan primer bagi masyarakat untuk mendukung aktivitas sehari-hari, seperti bekerja, belajar, dan berinteraksi sosial secara daring. Potensi resesi ekonomi akibat perlambatan aktivitas ekonomi memaksa pelaku usaha industri dan sektor ekonomi untuk segera mengadopsi digitalisasi agar bisnisnya dapat terus beroperasi. Digitalisasi tidak hanya menjadi solusi sementara, tetapi juga strategi jangka panjang untuk meningkatkan ketahanan dan adaptabilitas ekonomi Indonesia dalam menghadapi berbagai dinamika global.

Situasi ini mendesak Kementerian Informasi dan Informasi (Kominfo) untuk secara optimal akan melakukan percepatan penyediaan infrastruktur Teknologi Informasi dan Komunikasi (TIK) dan percepatan digitalisasi (Peraturan Presiden Republik Indonesia Nomor 139 Tahun 2024 tentang Penataan Tugas dan Fungsi Kementerian Negara Kabinet Merah Putih Periode Tahun 2024-2029 menyebutkan bahwa nomenklatur Kementerian Komunikasi dan Informatika telah diubah menjadi Kementerian Komunikasi dan Digital (Komdigi) pada periode Presiden Prabowo Subianto. Perubahan ini mencerminkan fokus baru pemerintah terhadap transformasi digital dan pengelolaan komunikasi di era teknologi).

Oleh karena itu, Renstra Kominfo Tahun 2020—2024 diarahkan untuk mendukung percepatan transformasi digital nasional, dimana pada 5 (lima) tahun ke depan fokus Komdigi adalah untuk menuntaskan penyediaan infrastruktur TIK ke seluruh wilayah Indonesia, mendorong percepatan transformasi digital dalam 3 (tiga) kerangka nasional yaitu industri, pemerintahan, dan masyarakat, serta mengoptimalkan pengelolaan komunikasi publik. Kondisi perkembangan TIK secara nasional direpresentasikan melalui ICT

Development Index (IDI) dikeluarkan oleh International Telecommunication Union (ITU) dan *Mobile Connectivity Index* yang dikeluarkan *Global System for Mobile Communications Association* (GSMA). Jika dilihat pada MCI, Indonesia memiliki pertumbuhan yang signifikan, dimana Indonesia menjadi salah satu dari 10 negara yang mengalami kemajuan paling signifikan dengan skor 46 di tahun 2014 menjadi 61 di tahun 2018. Akan tetapi, jika dilihat dari skor IDI terakhir tahun 2017, Indonesia menduduki peringkat ke 111 dari 176 negara di dunia dengan nilai 4,33 dari 10. Posisinya masih berada jauh di bawah Thailand yang menempati peringkat 78 (Kementerian Komunikasi dan Informatika Republik Indonesia, 2020).

Perkembangan TIK juga memunculkan tren industri 4.0 secara global, ditandai dengan berkembangnya terobosan-terobosan teknologi, meliputi *Artificial Intelligence (AI), robotic, Internet of Things (IoT), autonomous vehicles, 3D printing*. Perkembangan industri 4.0 ini juga mengakibatkan terjadi *shifting* di bidang SDM. Banyak pekerjaan *low-level/repetitive* yang akan tergantikan oleh sistem atau otomasi. Dari penelitian Oxford Economics 2018, yang menemukan bahwa pada negara-negara di Asia Tenggara, akan terjadi *job displacement* yang cukup besar. Dari studi tersebut, diperkirakan Indonesia akan kehilangan 9,5 juta pekerjaan akibat otomasi dan disrupsi digital (Oxford Economics, 2018).

Menurut penilaian *National Cyber Security Index* (NCSI) tahun 2022, kapasitas keamanan siber Indonesia berada di kategori kurang baik. Indonesia memiliki skor NCSI 38,96 yang berada di bawah rerata global. Delapan kapasitas keamanan siber, yakni kebijakan, ancaman, pendidikan, kontribusi global, layanan digital, layanan esensial, data pribadi, dan manajemen krisis. Di sisi lain, Indonesia memiliki skor di atas rerata global untuk empat kapasitas, yakni Identitas Digital dan Layanan Kepercayaan (E-ID & TS), Respons Insiden, Penindakan Kejahatan, dan Operasi Militer (Lemhannas RI, 2023). Pada tahun 2022, Indonesia mengalami lonjakan signifikan dalam jumlah kasus kejahatan siber yang ditangani oleh Kepolisian Republik Indonesia (Polri). Data dari e-MP Biro Pembinaan dan Operasional Badan Reserse Kriminal Kepolisian Republik Indonesia

(Robinopsnal Bareskrim Polri) mencatat bahwa Polri menangani sebanyak 8.831 kasus kejahatan siber sejak 1 Januari hingga 22 Desember 2022. Jumlah ini menunjukkan peningkatan hingga 14 kali lipat dibandingkan periode yang sama di tahun 2021, di mana hanya tercatat 612 kasus yang ditangani di seluruh Indonesia. Polda Metro Jaya tercatat sebagai satuan kerja dengan jumlah penindakan tertinggi, yaitu sebanyak 3.709 kasus, mencerminkan tingginya intensitas kasus kejahatan siber di wilayah tersebut (Pusiknas Polri, n.d.).

Cybercrime merupakan bentuk kejahatan baru yang timbul akibat kemajuan dalam teknologi informasi. Dalam kejahatan ini, komputer berperan sebagai sarana pelaksanaan. Tindakan yang berkaitan dengan kerahasiaan, integritas, dan keberadaan data serta sistem komputer memerlukan perhatian khusus karena karakteristiknya yang berbeda dengan kejahatan konvensional. Seiring pesatnya perkembangan teknologi, khususnya teknologi informasi di Indonesia, *cybercrime* menjadi salah satu masalah yang perlu kita perhatikan dan waspadai secara serius. Kejahatan seperti ini kemungkinan besar akan terjadi di suatu wilayah atau negara, dan pencegahan serta penanganannya sangat bergantung pada upaya yang dilakukan oleh negara atau wilayah tersebut (Chintia, E., Nadiah, et.al, 2019).

Menurut *Crown Prosecution Service* (CPS) di Inggris dan Wales, kejahatan siber dibagi menjadi dua kategori utama: *cyber-dependent crime* dan *cyber-enabled crimes*. *Cyber-dependent crimes* adalah jenis kejahatan yang hanya dapat dilakukan dengan menggunakan perangkat online, di mana perangkat tersebut berfungsi sebagai alat sekaligus target kejahatan. Contoh dari kategori ini adalah serangan *Distributed Denial of Service* (DDoS), di mana sistem komputer diserang hingga tidak dapat berfungsi. Sementara itu, *cyber-enabled crimes* adalah kejahatan tradisional yang dapat diperbesar skala dan dampaknya melalui penggunaan komputer, seperti penipuan atau pencurian identitas yang dilakukan secara daring. Pendekatan yang digunakan oleh CPS ini sejalan dengan *National Cyber Security Strategy 2016–2021* dari pemerintah Inggris, yang menerapkan definisi luas tentang kriminalitas siber. Definisi ini mencakup baik

kejahatan komputer *de facto* maupun kejahatan tradisional yang melibatkan unsur digital atau siber dalam pelaksanaannya. Selain itu, pandangan Karyda dan Mitrou memberikan perspektif bahwa kejahatan siber tidak selalu merupakan kejahatan baru. Banyak kasus kejahatan siber merupakan bentuk adaptasi dari kejahatan klasik yang menggunakan kekuatan komputasi dan aksesibilitas informasi melalui internet. Pandangan ini menekankan bahwa kemajuan teknologi informasi telah memungkinkan kejahatan lama muncul dengan bentuk dan metode yang lebih kompleks dalam ruang lingkup digital (Brants, C., Jackson, A., & Wilson, T. J., 2020).

Tulisan ini menggarisbawahi bahwa meskipun keberadaan kejahatan siber diakui secara universal, tidak ada definisi tunggal yang diterima secara global mengenai istilah ini. Berbagai istilah seperti *cybercrime*, *computer crime*, *cloud-crime*, dan *computer misuse* sering digunakan secara bergantian untuk merujuk pada aktivitas kriminal yang berkaitan dengan internet atau komputer. Dalam tulisan ini, semua perilaku kriminal yang menggunakan internet akan disebut sebagai "*cybercrime*," kecuali ketika mengacu pada penelitian khusus yang menggunakan istilah lain. Untuk tujuan buku ini, definisi kejahatan siber (*cybercrime*) yang diadopsi mencakup kejahatan yang dilakukan secara eksklusif melalui media digital maupun kejahatan tradisional yang dampaknya diperbesar oleh perangkat digital. Definisi ini mencakup regulasi dan penegakan hukum terhadap kejahatan baik di web terbuka (*clear web*) maupun di web gelap (*dark web*), termasuk "kejahatan baru" yang hanya dapat dilakukan melalui sarana digital serta kejahatan tradisional yang dipengaruhi oleh perangkat digital.

Terbayang betapa pedihnya melihat teknologi digital, yang mestinya membantu anak-anak Indonesia menjadi lebih cerdas dan berwawasan, justru menjadi ruang yang tidak aman dan melukai hingga merenggut nyawa. Selain perundungan, kasus kekerasan lainnya juga kerap terjadi kepada perempuan dan kelompok rentan lainnya. Dengan berbagai tekanan sosial tersebut, tentu sangat diharapkan bahwa pemerintah bisa hadir dalam dunia digital secara lebih baik. Akan tetapi, sebelum pemerintah dapat hadir secara maksimal di dunia digital, layanan-layanan publik yang diberikan

juga belum maksimal. Isu-isu seperti simpang siur koordinasi, duplikasi aplikasi, serta data yang masih belum tertata dengan baik menyebabkan pemerintah belum dapat maksimal dalam memberi rasa aman dan nyaman kepada seluruh elemen masyarakat Indonesia. Salah satu contoh yang menjadi sorotan publik adalah bagaimana pemerintah menghadapi berbagai serangan siber, terutama pada aset-aset vital negara. Serangan siber terbukti dapat melumpuhkan berbagai layanan publik, seperti layanan beasiswa maupun layanan imigrasi, selama beberapa hari. Pemerintah telah berusaha untuk memulihkan layanan yang terdampak serta memastikan perbaikan maupun peningkatan keamanan agar kejadian serupa tidak terulang kembali di masa depan. Meski demikian, berbagai insiden serangan siber terhadap berbagai layanan publik telah menurunkan kepercayaan masyarakat terhadap pemerintah, sekaligus menunjukkan pola koordinasi yang kurang optimal, khususnya dalam merespons insiden maupun melakukan mitigasi risiko atas serangan siber tersebut (Audrina et al., 2024).

Dalam konteks keamanan internet misalnya, pengguna internet sering kali merupakan elemen paling rentan, dengan kelemahan yang dapat dieksploitasi oleh pelaku kejahatan siber melalui berbagai metode, sehingga korban secara tidak langsung turut berperan dalam kejahatan yang menimpa dirinya sendiri. Teknik-teknik eksploitasi yang digunakan meliputi rekayasa sosial (*social engineering*), manipulasi dalam pengambilan keputusan dengan memanfaatkan persepsi urgensi atau otoritas, serta pemanfaatan kebiasaan yang mudah diprediksi, seperti penggunaan situs *web*, unduhan, kata sandi, dan aktivitas jaringan sosial atau profesional. Konsekuensinya, korban sering kali merasa bersalah atau dipersalahkan oleh pihak lain, di samping mengalami dampak yang signifikan seperti kerugian finansial, kerusakan reputasi, hingga dampak buruk terhadap karier. Sebagian besar korban kejahatan siber melaporkan dampak emosional, mulai dari perasaan terganggu hingga depresi, insomnia, kecemasan, dan serangan panik. Dalam kasus penipuan siber, persentase korban yang mengalami dampak emosional lebih tinggi daripada korban penipuan konvensional, dengan sebagian korban

menderita dampak jangka panjang seperti PTSD, yang juga dapat mempengaruhi kesehatan fisik (Curtis, J., & Oxburgh, G., 2023).

Oleh karena itu, kejahatan siber merupakan tantangan serius yang memerlukan perhatian mendalam dari pemerintah, penegak hukum, dan seluruh lapisan masyarakat. Kompleksitas dan sifat dinamis dari kejahatan siber menuntut kerangka hukum yang adaptif serta penegakan hukum yang efektif dan efisien. Tanpa upaya terpadu dan strategis, dampak negatif dari kejahatan siber akan terus meningkat, mengancam stabilitas ekonomi, keamanan nasional, dan kesejahteraan sosial. Buku ini hadir sebagai respons atas urgensi tersebut, dengan tujuan menganalisis tantangan dalam penegakan hukum pidana terhadap kejahatan siber di Indonesia dan menawarkan solusi praktis. Diharapkan, melalui pemahaman yang lebih komprehensif, berbagai pihak dapat berkolaborasi untuk memperkuat sistem hukum dan menciptakan lingkungan digital yang aman dan kondusif bagi seluruh masyarakat Indonesia.

BAB 2
DEFINISI DAN JENIS-JENIS KEJAHATAN SIBER

Cybercrime dalam Perspektif Hukum Pidana

1. Definisi Kejahatan Siber Menurut KUHP dan UU ITE

Kejahatan siber atau sering disebut sebagai *cybercrime* adalah setiap kegiatan kriminal yang dilakukan dengan menggunakan komputer, jaringan komputer atau internet. Ini berarti menggunakan teknologi untuk melakukan aktivitas ilegal, menargetkan korban, atau mengeksploitasi kerentanan dalam sistem digital (Butarbutar, 2023).

Pada dasarnya *cybercrime* meliputi semua tindak pidana yang berkenaan dengan sistem informasi (*information system*) itu sendiri, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya (*transmitter/originator to recipient*) (Suhariyanto, Budi., 2014).

Cybercrime bukan hanya masalah teknologi, tetapi juga permasalahan sosial dan hukum yang memiliki dampak luas pada keamanan ekonomi dan privasi masyarakat. Di Indonesia, meskipun telah memiliki landasan hukum untuk mengatur tindak pidana, Kitab Undang-Undang Hukum Pidana (KUHP) awalnya tidak dirancang untuk menangani kejahatan siber karena ruang lingkupnya yang masih terbatas pada tindak pidana konvensional. Oleh sebab itu, perubahan KUHP dan lahirnya Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjadi penting untuk melindungi keamanan di ruang digital.

Menurut KUHP, tindak pidana umumnya mengacu pada suatu perbuatan yang diancam dengan sanksi pidana dan/atau tindakan oleh peraturan perundang-undangan harus bersifat melawan hukum atau bertentangan dengan hukum yang hidup dalam masyarakat. Sanksi yang dimaksud baik berupa denda maupun hukuman penjara. Namun definisi ini belum mencakup kejahatan berbasis teknologi yang lebih kompleks, seperti kejahatan siber. Maka dari itu, definisi dan regulasi untuk *cybercrime* diatur dalam undang-undang khusus.

Pada KUHP terbaru (UU No. 1 Tahun 2023), beberapa pasal mulai mencakup tindakan ilegal di ranah digital. Hal tersebut diatur pada Bagian Kelima tentang Tindak Pidana terhadap Informatika dan Elektronika (Pasal 332 sampai Pasal 334 KUHP).

a. Pasal 332 tentang akses ilegal ke komputer atau sistem elektronik. Pasal ini menyebutkan bahwa setiap orang yang secara sengaja dan tanpa izin memasuki sistem komputer milik orang lain akan dikenakan pidana hingga 6 tahun penjara atau denda.
b. Pasal 333 tentang penggunaan tanpa hak terhadap sistem elektronik untuk merusak atau mencuri informasi penting, yang diancam dengan hukuman hingga tujuh tahun penjara.
c. Pasal 334 khususnya mengenai keuntungan finansial yang diperoleh secara ilegal dari sistem elektronik. Pelaku yang terbukti melanggar pasal ini dapat dikenai sanksi hingga sepuluh tahun penjara.

UU ITE memperjelas cakupan tindak pidana siber dengan menyebutkan jenis-jenis kejahatan yang secara spesifik berkaitan dengan aktivitas di ruang digital. Pasal 27 hingga Pasal 37 UU ITE secara spesifik mengatur tentang kejahatan terkait konten ilegal, akses tidak sah, penyadapan, dan serangan terhadap integritas sistem lainnya.

UU ITE menganggap kejahatan siber sebagai pelanggaran serius dengan dampak yang besar. Oleh sebab itu, sanksi yang dikenakan terhadap pelaku *cybercrime* cukup berat, dengan ancaman pidana hingga delapan tahun penjara atau denda

maksimal Rp 1 miliar, tergantung pada jenis dan tingkat kejahatannya.

Pengertian lain *cybercrime* dalam *Draft International Convention to Enhance Protection from Cybercrime and Terrorism*, "*cybercrime means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention*" (Draft International Convention to Enhance Protection from Cybercrime and Terrorism, n.d.). Artinya kejahatan dunia maya (*cybercrime*) berarti tindakan yang berkaitan dengan sistem dunia maya yang diklasifikasikan sebagai tindak pidana yang dapat dihukum berdasarkan konvensi ini. Dalam arti sempit *cybercrime* dapat disebut sebagai *computer crime*, yaitu perilaku ilegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer. Sedangkan dalam arti luar, *cybercrime* dapat disebut *computer relate crime*, yaitu merupakan perilaku ilegal/melanggar yang berkaitan dengan sistem komputer atau jaringan (Maskun & Meilarati, 2017, p. 21).

Secara internasional, kejahatan siber juga diatur dalam berbagai instrumen hukum seperti *Budapest Convention on Cybercrime*. Konvensi ini menjadi perjanjian internasional yang khusus menangani kejahatan siber, sehingga menjadi pedoman dalam menangani kejahatan siber secara global dengan fokus pada harmonisasi aturan hukum dan kerja sama antarnegara untuk melawan kejahatan siber lintas batas (Nabila et al., 2024).

Menurut *Convention on Cybercrime* 2001 di Budapest, Hungaria, terdapat beberapa jenis kejahatan yang sering terjadi di dunia maya, yaitu (Fitriani, Y., & Pakpahan, R. (2020):

a. *Illegal Access*/Akses Tanpa Izin ke Sistem Komputer dan Layanan

   Illegal access adalah bentuk kejahatan yang dilakukan dengan meretas atau memasuki sistem jaringan komputer secara tidak sah, tanpa izin atau sepengetahuan pemilik sistem.

b. *Illegal Contents*

   Illegal contents merupakan modus kejahatan *cybercrime* di mana pelaku mengunggah data atau informasi di internet yang

tidak benar, tidak etis, dan berpotensi melanggar hukum atau mengganggu ketertiban umum.

c. *Data Forgery*
   Data forgery adalah modus kejahatan yang dilakukan dengan memalsukan data pada dokumen-dokumen penting yang disimpan sebagai *scripless document* melalui internet. Biasanya, kejahatan ini menyasar dokumen *e-commerce* dengan menciptakan "kesalahan ketik" yang menguntungkan pelaku, seperti pencurian data pribadi dan nomor kartu kredit korban.
d. *Cyber Espionage* (Spionase Dunia Maya)
   Cyber espionage adalah kejahatan di mana pelaku menggunakan jaringan internet untuk memata-matai pihak lain dengan menyusup ke dalam *computer network system* milik pihak yang menjadi target.
e. *Cyber Sabotage and Extortion* (Sabotase dan Pemerasan di Dunia Maya)
   Kejahatan ini biasanya dilakukan dengan mengganggu, merusak, atau menghancurkan data, program komputer, atau sistem jaringan komputer yang terhubung ke internet. Modusnya termasuk menyusupkan *logic bomb*, virus komputer, atau program tertentu, sehingga data atau sistem komputer tidak dapat berjalan sebagaimana mestinya atau bahkan dikendalikan oleh pelaku.
f. *Offense Against Intellectual Property* (Pelanggaran Hak Kekayaan Intelektual)
   Kejahatan ini menargetkan hak kekayaan intelektual pihak lain di internet. Contohnya adalah peniruan tampilan *web page* milik orang lain secara ilegal.
g. *Infringements of Privacy* (Pelanggaran Privasi)
   Infringements of privacy menargetkan data pribadi yang tersimpan dalam formulir komputerisasi. Jika bocor, data ini dapat merugikan korban secara material maupun immaterial, seperti kebocoran nomor kartu kredit atau PIN ATM.

Peraturan *cybercrime* dalam KUHP, UU ITE, dan *Budapest Convention On Cybercrime* menunjukkan pendekatan yang

berbeda. Indonesia, dengan UU ITE berfokus pada pengaturan tindak pidana yang merusak ketertiban umum, melanggar privasi, dan merugikan ekonomi digital. Sementara itu, *Budapest convention* lebih bersifat global, berfokus pada upaya harmonisasi regulasi dan peningkatan kerja sama antar negara untuk menangani kasus lintas batas yang lebih sulit diselesaikan oleh suatu negara.

2. Kejahatan Siber sebagai Tindak Pidana di Ranah Digital

Kejahatan siber merupakan fenomena yang muncul seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi. Dalam ranah hukum pidana, kejahatan siber dianggap sebagai tindak pidana yang terjadi di ruang digital. Perbedaan utama antara kejahatan siber dengan kejahatan tradisional terletak pada alat dan sarana yang digunakan, tidak lagi dengan cara tradisional, namun sudah memanfaatkan dan menggunakan peluang yang disediakan oleh kemudahan instrumen modern dengan peralatan yang canggih (Habibi, M. R., & Liviani, I., 2020).

Hukum pidana Indonesia, yang awalnya tidak mengakomodasi perkembangan teknologi, kemudian secara bertahap menyesuaikan diri melalui UU ITE. Kejahatan siber mencakup berbagai aktivitas kriminal yang dilakukan melalui jaringan komputer dan internet, termasuk penipuan *online*, pencurian identitas, serangan *malware*, peretasan, dan eksploitasi data pribadi (Widianingrum, A. R. (2024).

Beberapa bentuk kejahatan siber yang diatur dalam Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mencakup:

a. Pasal 27

   Pasal ini mengatur mengenai berbagai tindakan distribusi konten ilegal di ruang digital, antara lain:

   1) Konten yang Melanggar Kesusilaan

      Setiap orang dilarang untuk menyebarluaskan, mentransmisikan, atau membuat dapat diaksesnya

informasi elektronik yang mengandung muatan yang melanggar kesusilaan secara sengaja dan tanpa hak. Muatan ini mencakup konten yang mengandung unsur pornografi, eksploitasi seksual, atau tindakan tidak senonoh yang dapat merusak moral masyarakat.

2) Konten Perjudian
   Melarang distribusi atau transmisi informasi elektronik yang mengandung unsur perjudian. Tindakan ini bertujuan untuk mencegah penyebaran aktivitas perjudian yang dapat diakses dengan mudah melalui media digital.
3) Pencemaran Nama Baik dan Kehormatan
   Pasal 27A yang disisipkan setelah Pasal 27 menjelaskan bahwa tindakan menyerang kehormatan atau nama baik orang lain melalui tuduhan atau informasi palsu juga dianggap pelanggaran. Pelanggaran ini ditujukan pada mereka yang menggunakan media digital untuk menyebarkan tuduhan yang dapat merusak reputasi seseorang.
4) Pemaksaan dengan Ancaman
   Pasal 27 B menambahkan larangan terhadap tindakan distribusi informasi yang digunakan untuk memeras atau mengancam orang lain. Tindakan ini mencakup ancaman untuk meminta barang, uang, atau pengakuan utang dengan menggunakan dokumen elektronik untuk menakut-nakuti korban.

b. Pasal 28
   Pasal ini mengatur penyebaran informasi elektronik yang berpotensi menimbulkan kerugian pada pihak lain, dengan dua fokus utama:
   1) Penyebaran Informasi Palsu atau Menyesatkan
      Melarang distribusi informasi yang berisi berita bohong atau informasi yang dapat menyesatkan masyarakat. Pelanggaran ini bertujuan untuk mencegah kerugian materiil pada konsumen dalam transaksi elektronik yang mengandalkan informasi akurat.

2) Penyebaran Kebencian atau Hasutan
   Melarang tindakan menyebarkan informasi yang menghasut atau mengajak orang lain untuk melakukan permusuhan atau kebencian terhadap kelompok berdasarkan ras, agama, etnis, dan sebagainya. Pasal ini melindungi masyarakat dari konten digital yang dapat memicu konflik atau diskriminasi.

c. Pasal 29
   Pasal ini mengatur mengenai larangan mengirimkan ancaman kekerasan atau ancaman lainnya secara langsung melalui dokumen elektronik. Setiap orang yang secara sengaja dan tanpa hak mengirimkan informasi yang berisi ancaman kekerasan kepada orang lain dapat dikenakan sanksi. Tujuan utama dari pasal ini adalah untuk melindungi individu dari intimidasi atau teror melalui pesan digital.

d. Pasal 30
   Pasal ini mengatur tentang akses tidak sah (*unauthorized access*) ke dalam sistem elektronik, yaitu:
   1) Akses Tanpa Izin ke Sistem Elektronik
      Setiap orang dilarang untuk memasuki atau menyusup ke dalam sistem elektronik milik orang lain tanpa izin yang sah. Tindakan peretasan atau penyusupan ke dalam perangkat atau jaringan digital yang bukan miliknya, untuk mengakses data atau informasi pribadi, adalah bentuk kejahatan siber yang diatur dalam pasal ini.
   2) Kontrol Ilegal atas Sistem
      Selain mendapatkan akses, seseorang yang tanpa izin mencoba mengendalikan atau menguasai sistem elektronik orang lain juga dianggap melanggar hukum. Ini mencakup upaya untuk memanfaatkan sistem pihak lain untuk keuntungan pribadi atau untuk kepentingan jahat.

e. Pasal 31
   Pasal ini mengatur tentang penyadapan atau intersepsi informasi elektronik yang dilakukan secara ilegal, dengan ketentuan sebagai berikut:

1) Larangan Penyadapan Komunikasi Digital
   Setiap orang yang melakukan intersepsi atau penyadapan informasi elektronik orang lain tanpa izin dinyatakan melanggar hukum. Tindakan ini mencakup pengawasan terhadap komunikasi digital seperti email, pesan instan, atau panggilan suara tanpa persetujuan pihak yang bersangkutan.
2) Hak atas Privasi dalam Komunikasi Digital
   Pasal ini menguatkan prinsip privasi dengan memastikan bahwa informasi elektronik individu tidak dapat diakses, direkam, atau dipantau oleh pihak lain tanpa alasan hukum yang jelas. Setiap bentuk penyadapan harus dilakukan berdasarkan ketentuan hukum untuk menjaga hak asasi dan kebebasan berkomunikasi.

f. Pasal 32
   Pasal ini mengatur tentang tindakan perusakan, pengubahan, penghilangan, atau pemindahan informasi elektronik atau dokumen elektronik tanpa izin, yang secara rinci mencakup:
   1) Pengubahan, Penghilangan, atau Pemindahan Data Elektronik Tanpa Izin
      Setiap orang yang sengaja dan tanpa hak melakukan tindakan perusakan, pengubahan, penghilangan, atau pemindahan data elektronik dianggap melanggar hukum. Ini termasuk segala upaya untuk mengubah isi data tanpa sepengetahuan atau izin pemiliknya, seperti menghapus atau merusak data milik orang lain di sistem elektronik.
   2) Penguasaan Data secara Melawan Hukum
      Tindakan yang berupaya memindahkan data elektronik dari satu sistem ke sistem lain tanpa izin juga diatur dalam pasal ini. Misalnya, memindahkan atau mencuri data dari sistem perusahaan atau individu untuk keuntungan pribadi atau tujuan jahat adalah tindakan ilegal.

g. Pasal 33

Pasal ini melarang setiap orang yang secara sengaja dan tanpa hak melakukan tindakan yang menyebabkan terganggunya sistem elektronik.

Beberapa bentuk tindakan yang diatur dalam pasal ini meliputi:

1) Mengganggu Sistem Elektronik

Tindakan ini mencakup setiap usaha yang dapat mengganggu fungsi, aksesibilitas, atau efektivitas sistem elektronik, seperti serangan *Distributed Denial of Service* (DDoS) atau serangan lain yang menargetkan sistem agar tidak berfungsi secara normal.

2) Mencegah Akses terhadap Sistem

Pasal ini juga melarang tindakan yang bertujuan untuk memblokir atau mencegah akses ke sistem elektronik oleh pihak yang berhak. Misalnya, melakukan pemblokiran terhadap situs atau jaringan tertentu tanpa izin merupakan tindakan ilegal.

h. Pasal 34

Pasal 34 melarang setiap orang yang dengan sengaja dan tanpa hak memproduksi, menjual, atau menyebarkan perangkat lunak yang dirancang khusus untuk menyerang atau merusak sistem elektronik. Rinciannya mencakup:

1) Produksi dan Distribusi Perangkat Lunak Berbahaya (*Malware*)

Melarang pembuatan dan penjualan perangkat lunak yang dirancang untuk merusak, mencuri data, atau mengganggu sistem elektronik. Contoh perangkat lunak ini termasuk virus, trojan, dan *spyware* yang sering digunakan untuk tujuan peretasan atau pencurian data.

2) Penggunaan Perangkat untuk Menyerang Sistem

Pasal ini juga melarang setiap bentuk distribusi atau pemanfaatan alat yang dapat digunakan untuk menyerang sistem elektronik, termasuk alat yang dapat menembus sistem keamanan tanpa izin.

i. Pasal 35

Pasal 35 melarang setiap orang untuk memalsukan data elektronik atau dokumen elektronik. Rincian dari pasal ini mencakup:

1) Pemalsuan Data Elektronik atau Dokumen
   Setiap orang yang dengan sengaja dan tanpa hak memalsukan atau mengubah data atau dokumen elektronik untuk keuntungan pribadi atau tujuan tertentu dianggap melanggar hukum. Ini termasuk tindakan memalsukan tanda tangan elektronik atau dokumen resmi secara digital.
2) Keamanan Identitas Digital dan Transaksi Elektronik
   Pasal ini bertujuan untuk menjaga keaslian dan integritas data serta dokumen elektronik, yang penting dalam transaksi digital atau komunikasi resmi. Pelanggaran terhadap keaslian dokumen dapat mengakibatkan kerugian bagi individu maupun entitas bisnis.

j. Pasal 36 dan Pasal 37

Pasal 36 dan Pasal 37 mengatur bahwa setiap tindakan yang melanggar pasal-pasal sebelumnya (Pasal 27-35) dan menimbulkan kerugian bagi orang lain dapat dikenakan sanksi. Fokus dari pasal ini adalah pada:

1) Akibat Hukum bagi Pelanggaran yang Merugikan Pihak Lain
   Setiap tindakan yang terbukti melanggar ketentuan dalam Pasal 27 hingga Pasal 35, dan menyebabkan kerugian materiil atau immateriil bagi orang lain, dapat dikenakan sanksi pidana. Dengan kata lain, jika tindakan tersebut terbukti berdampak pada kerugian korban, maka pelaku dapat dihukum lebih berat.
2) Sanksi sebagai Bentuk Perlindungan Hukum
   Pasal ini memperkuat perlindungan hukum terhadap korban kejahatan siber dengan memastikan bahwa pelaku yang menyebabkan kerugian pada orang lain melalui tindakan ilegal di dunia digital dapat dituntut dan dihukum.

Bentuk-bentuk kejahatan siber yang tercantum dalam UU ITE ini menunjukkan bahwa undang-undang telah mencakup berbagai aspek tindakan ilegal di ranah digital, baik yang berdampak langsung maupun tidak langsung terhadap individu, masyarakat, atau negara. Setiap pasal dalam UU ITE memberikan landasan hukum yang jelas untuk menindak berbagai aktivitas kriminal di ruang digital yang terus berkembang (Pratama et al., 2024).

Misalnya, ketentuan tentang distribusi konten ilegal, penyebaran kebencian, dan ancaman kekerasan (Pasal 27-29) dirancang untuk menjaga ketertiban sosial serta mencegah penyebaran konten yang dapat memicu konflik atau kerusuhan dalam masyarakat. Pasal-pasal ini menegaskan larangan terhadap penyebaran informasi elektronik yang mengandung muatan kesusilaan, perjudian, fitnah, atau ujaran kebencian yang mengarah pada diskriminasi berbasis ras, agama, etnis, dan karakteristik lainnya.

Selain itu, ketentuan mengenai akses tidak sah (Pasal 30) melindungi sistem elektronik dari peretasan atau penyusupan tanpa izin yang dapat membahayakan keamanan data dan integritas sistem. Pasal 31 juga mengatur larangan penyadapan dan intersepsi informasi elektronik yang bertujuan untuk menjaga hak privasi dalam komunikasi digital dari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Pasal-pasal yang mengatur gangguan data (Pasal 32) dan sistem (Pasal 33) berfungsi untuk melindungi integritas data dan operasional dari upaya peretasan yang dapat mengakibatkan kerugian finansial atau operasional pada lembaga yang diserang. Selain itu, UU ITE juga mengantisipasi penyebaran perangkat lunak berbahaya (Pasal 34) yang sering kali digunakan dalam serangan siber untuk mengendalikan atau merusak sistem komputer milik orang lain. Dalam hal ini, UU ITE tidak hanya menindak pelaku yang menggunakan teknologi secara ilegal, tetapi juga mereka yang memproduksi dan mendistribusikan perangkat atau perangkat lunak dengan tujuan kriminal.

Selanjutnya, pasal tentang manipulasi data dan informasi elektronik (Pasal 35) memberikan perlindungan terhadap

keaslian data, yang sangat penting dalam transaksi bisnis dan legalitas dokumen digital. Tindakan manipulasi data ini dapat mengakibatkan kerugian besar bagi korban yang datanya diubah atau disalahgunakan. Akhirnya, ketentuan yang mengatur perbuatan yang merugikan pihak lain (Pasal 36-37) menunjukkan bahwa UU ITE melindungi semua pihak yang dirugikan, baik secara materiil maupun immateriil, akibat pelanggaran hukum siber.

Dengan adanya berbagai ketentuan ini, UU ITE berfungsi sebagai instrumen yang komprehensif untuk menindak berbagai bentuk kejahatan siber di Indonesia dan memastikan keamanan digital bagi masyarakat luas. Selain itu, dalam UU ITE tindak pidana di ranah digital diatur dalam Pasal 45 sampai Pasal 51 di mana pelaku kejahatan siber dapat dijerat dengan sanksi yang cukup berat berupa penjara maupun denda maksimal Rp1 miliar tergantung dengan tingkat kejahatan yang dilakukan.

3. Tindak Pidana terhadap Informatika dan Elektronika

Selain dalam UU ITE, kejahatan siber juga telah diatur dalam KUHP baru yaitu Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Dalam KUHP baru, tindak pidana siber didefinisikan lebih rinci untuk memberikan perlindungan hukum yang lebih kuat terhadap kejahatan di ruang digital. KUHP ini memuat berbagai pasal yang mencakup perbuatan-perbuatan ilegal dalam penggunaan sistem elektronik, termasuk komputer dan jaringan komputer. Fokus utamanya adalah untuk memberikan sanksi terhadap perbuatan yang mengakses, memanipulasi, atau menggunakan data elektronik tanpa hak dengan cara yang merugikan individu, institusi, atau negara. Hal tersebut diatur dalam BAB VIII tentang Tindak Pidana yang Membahayakan Keamanan Umum Bagi Orang, Kesehatan, dan Barang.

Bagian kelima tindak pidana terhadap informatika dan elektronika yang diuraikan sebagai berikut (Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana):

a. Pasal 332 KUHP

Pasal ini mengatur sanksi bagi siapa saja yang melakukan akses ilegal atau tanpa izin ke dalam komputer dan sistem elektronik milik orang lain.

1) Ayat (1) Setiap orang yang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain dapat dipidana dengan pidana penjara paling lama 6 tahun atau denda kategori V.
2) Ayat (2) Jika akses dilakukan dengan tujuan untuk memperoleh informasi elektronik atau dokumen elektronik, pelaku dapat dipidana dengan pidana penjara paling lama 7 tahun.
3) Ayat (3) Jika akses dilakukan dengan cara melanggar, menerobos, atau menjebol sistem pengamanan, pelaku dapat dipidana dengan pidana penjara paling lama 8 tahun.

Aturan ini untuk melindungi hak privasi dan keamanan sistem elektronik dari akses yang tidak sah, baik dengan niat eksplorasi pribadi maupun tujuan pencurian informasi. Pasal ini menanggapi perkembangan teknologi keamanan dan mendorong pelaku usaha atau individu untuk menjaga sistem mereka dengan proteksi yang lebih baik, seperti penggunaan enkripsi dan keamanan jaringan.

b. Pasal 333

Pasal ini mengatur tentang penggunaan tanpa hak terhadap komputer dan sistem elektronik. Setiap orang yang tanpa hak menggunakan atau mengakses komputer atau sistem elektronik dengan maksud untuk merusak atau menghilangkan informasi penting dapat dipidana dengan pidana penjara paling lama 7 tahun.

Pasal ini melindungi keamanan data yang bernilai tinggi dari tindakan sabotase digital yang dapat merugikan pemilik data. Penggunaan tanpa hak ini seringkali merugikan perusahaan atau individu, karena bisa berakibat pada hilangnya informasi penting yang berharga. Aturan ini mencakup berbagai bentuk kerusakan, termasuk penghapusan

data penting yang berpotensi mengganggu bisnis atau operasi organisasi yang terkena dampak.

c. Pasal 334
Mengatur tentang akses tanpa hak untuk mendapatkan keuntungan finansial. Setiap orang yang tanpa hak mengakses komputer atau sistem elektronik untuk memperoleh keuntungan dari lembaga keuangan dapat dipidana dengan pidana penjara paling lama 10 tahun.

Pasal ini menekankan bahwa akses tidak sah untuk keuntungan finansial adalah tindakan kriminal serius yang bisa merusak stabilitas ekonomi individu dan lembaga. Hal ini penting karena penipuan finansial melalui akses elektronik sering kali terjadi secara lintas negara.

d. Pasal 335
Mengatur tentang penggunaan tanpa hak terhadap informasi milik pemerintah. Setiap orang yang tanpa hak mengakses informasi milik pemerintah yang harus dirahasiakan dapat dipidana dengan pidana penjara paling lama 12 tahun.

Tindakan ini mencakup upaya untuk memperoleh informasi rahasia negara, yang bisa digunakan untuk tujuan spionase atau merusak reputasi negara di tingkat internasional. Pasal ini bertujuan untuk melindungi keamanan informasi penting negara dari upaya pencurian atau penyalahgunaan oleh pihak-pihak yang tidak berwenang. Dengan adanya aturan ini, diharapkan stabilitas keamanan nasional dan perlindungan terhadap informasi sensitif pemerintah dapat terjaga.

Jenis-jenis Kejahatan Siber

Kejahatan siber terbagi menjadi beberapa jenis berdasarkan modus operandi, target, dan teknologi yang digunakan. Berbagai jenis ini mencakup serangan terhadap sistem, penyebaran *malware*, hingga bentuk-bentuk penipuan daring. Setiap jenis kejahatan memiliki ciri khas dan potensi dampak yang berbeda, baik secara finansial, sosial, maupun psikologis bagi korban.

Departemen Komunikasi dan Informasi (Depkominfo) menetapkan 3 (tiga) jenis pelanggaran hukum yang terjadi dalam memanfaatkan sistem komunikasi teknologi informasi atau *cybercrime*. Kejahatan itu meliputi pelanggaran isi situs *web*, pelanggaran dalam perdagangan secara elektronik dan pelanggaran bentuk lain. Pelanggaran dalam bentuk lain tersebut terdiri dari *recreational hacker, cracker* atau *criminal minded hacker, denial of service attack (DoS), viruses, piracy* (pembajakan), *fraud, phising,* perjudian, dan *cyber stalking* (Riyadh, A., 2019).

Sementara itu, beragam serangan siber menurut data Balai Pelatihan dan Pengembangan Teknologi Informasi dan Komunikasi (BPPTIK) Kementerian Komunikasi dan Informatika RI tahun 2023, meliputi:

1. ***Phising***
   Penipuan *online* yang berusaha untuk mendapatkan informasi pribadi seperti kata sandi dan nomor kartu kredit.
2. **Serangan *Ransomware***
   Serangan yang mengenkripsi data dan mengharuskan korban membayar tebusan untuk mendapatkan akses kembali.
3. ***Malware***
   Perangkat lunak berbahaya yang dapat merusak sistem dan mencuri data.
4. **Serangan DDoS (*Distributed Denial of Service*)**
   Serangan terhadap *server* atau jaringan dengan membanjiri lalu lintas, mengakibatkan akses ke situs *web* menjadi sangat lambat atau macet bahkan membuatnya tidak tersedia untuk pengguna yang sah (Ahmad Riyadh, 2019).
5. **Serangan *Man in the Middle* (MITM)**
   Mencegat (*intercept*) komunikasi antara dua pihak yang sah dan mencuri informasi yang sedang ditransmisikan.
6. **Serangan *Zero-Day***
   Serangan yang mengeksploitasi kerentanan perangkat lunak yang belum ditemukan atau dilaporkan kepada pengembang. Serangan ini dapat sangat merusak karena tidak ada pembaruan keamanan yang tersedia.

7. **Serangan terhadap Identitas**
   Mencuri informasi pribadi seseorang, seperti nomor kartu kredit atau data identifikasi, dan menggunakannya untuk tujuan ilegal.
8. **Serangan terhadap Aplikasi *Web***
   Mengeksploitasi aplikasi web untuk mencuri data pengguna atau mendapatkan akses ke server.
9. **Serangan terhadap Pemerintah dan Infrastruktur Kritis**
   Upaya untuk meretas sistem pemerintah atau infrastruktur penting seperti sistem kelistrikan atau air.
10. **Serangan terhadap Bisnis**
    Serangan yang menargetkan perusahaan untuk melakukan termasuk pencurian data pelanggan dan kerugian finansial.

Sebelum memahami lebih jauh jenis-jenis serangan ini, penting untuk mengetahui bahwa kejahatan siber terus berkembang seiring kemajuan teknologi. Serangan-serangan ini tidak hanya menargetkan individu tetapi juga organisasi besar, pemerintah, dan infrastruktur penting. Dampaknya pun bervariasi, mulai dari kerugian finansial hingga gangguan pada kehidupan sehari-hari. Berikut ini beberapa bentuk serangan siber yang sering ditemui.

1. ***Hacking* dan *Cracking***
   Hacking dan *cracking* adalah dua bentuk kejahatan siber yang sering disalahpahami sebagai hal yang sama. Pada dasarnya, *hacking* adalah kegiatan menerobos program komputer milik orang/pihak lain dengan maksud tertentu secara melawan hak atau tanpa izin pemiliknya, sering kali dengan tujuan mengeksplorasi kelemahan keamanan sistem tersebut. Sementara itu, *cracking* adalah suatu kegiatan hacking untuk tujuan jahat dimana pelaku tidak hanya mengakses, tetapi juga mengubah, merusak, atau mencuri data dari sistem yang ditargetkan (Antoni, 2017)..

   Menurut Pasal 30 Ayat (1) UU ITE, tindakan akses ilegal (*hacking*) terhadap sistem komputer atau jaringan elektronik dengan sengaja dan tanpa hak atau melawan hukum dianggap sebagai tindak pidana. Sesuai Pasal 46 Ayat (1) UU ITE maka 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 Rp 600.000.000,00 (enam ratus juta rupiah). Jika tindakan tersebut disertai dengan perusakan atau manipulasi data, seperti yang sering dilakukan dalam *cracking* sebagaimana diatur dalam Pasal 30 Ayat (2) dan (3) UU ITE maka hukumannya dapat lebih berat.

Hacking meskipun ilegal, kadang kala dilakukan dengan niat baik untuk mengidentifikasi kelemahan dalam sistem keamanan siber (dikenal sebagai *ethical hacking* atau *hacking* yang bersifat etis). *Ethical hacking* adalah proses mengidentifikasi dan menguji kerentanan dalam sistem komputer, jaringan, dan aplikasi dengan izin dari pemilik untuk melakukannya (Fitroh et.al., 2023). Sebaliknya, *crackers* adalah individu secara ilegal menyusup, menembus, serta merusak situs *web*, dan sistem keamanan jaringan internet hanya untuk tujuan hiburan dan keuntungan (Miftakhur Rokhman Habibi, & Isnatul Liviani, 2020).

Secara hukum, *hacking* dan *cracking* diatur dalam UU ITE dalam pasal-pasal yang terkait dengan perlindungan data serta pelanggaran privasi yaitu Pasal 30 dan Pasal 32. Pelaku hacking bisa dijatuhi hukuman pidana, sedangkan pelaku *cracking* sering dikenakan hukuman yang lebih berat karena niat merusaknya sesuai Pasal 48 UU ITE. Sanksi hukum untuk hacking mencakup denda dan kurungan penjara, terutama jika kerusakan yang ditimbulkan berskala besar atau melibatkan data pribadi yang sensitif perspektif sosial.

2. *Malware* dan *Ransomware*

Malware adalah singkatan dari *malicious software*, yaitu program komputer yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem komputer tanpa izin pengguna (Berutu et al., n.d.). *Malware* mencakup berbagai jenis ancaman seperti *virus, worm, Trojan,* atau *ransomware,* serta cara mereka menyebar dan merusak data atau perangkat (Butarbutar, Russel., 2023). Salah satu jenis malware yang paling merusak dan sering ditemukan saat ini adalah *ransomware*, merupakan jenis perangkat lunak berbahaya (*malware*) yang

dirancang untuk memblokir atau mengenkripsi data pada sistem komputer korban (Salahdine, F., & Kaabouch, N., 2019).

Menurut Pasal 32 UU ITE, tindakan penyebaran *malware* termasuk dalam kategori kejahatan siber yang berkaitan dengan manipulasi dan pengubahan data elektronik secara ilegal. Menurut Bernadetta Septarini tahun 2024 dalam "*The Impact of Ransomware on Businesses and Individuals*" menjelaskan bahwa penyebaran *malware*, terutama *ransomware* telah menjadi salah satu ancaman terbesar dalam keamanan siber global, dengan banyak perusahaan besar, lembaga pemerintahan, dan individu menjadi korban.

Ransomware biasanya bekerja dengan cara memblokir atau mengenkripsi data pada sistem komputer korban (Salahdine, F., & Kaabouch, N., 2019). Penyerang kemudian menuntut pembayaran tebusan (*ransom*) kepada korban agar data mereka dapat dibuka atau dikembalikan. *Ransomware* biasanya menyebar melalui tautan atau lampiran yang meragukan dalam email phishing, situs web yang terinfeksi, atau menggunakan eksploitasi kelemahan dalam sistem komputer. Setelah *ransomware* berhasil menginfeksi sistem komputer, ia akan mengenkripsi file dan memberikan peringatan kepada korban dengan instruksi tentang bagaimana cara membayar tebusan agar mendapatkan kunci dekripsi atau pemulihan data. Biasanya, pembayaran ini harus dilakukan dalam bentuk mata uang digital seperti *Bitcoin* agar sulit dilacak. Beberapa *ransomware* terkenal yang pernah muncul adalah *WannaCry, Petya/NotPetya, dan Ryuk* (Alshaikh, H., Ramadan, N., & Hefny, H. A., 2020).

Dalam hukum siber, penyebaran *malware* dan *ransomware* dianggap sebagai tindakan kriminal khusus. Pelaku yang tertangkap dapat dikenai hukuman berat, mulai dari hukuman penjara hingga denda yang signifikan. Pasal 32 UU ITE menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak melakukan tindakan manipulasi, perubahan, hingga penghapusan informasi elektronik dapat dikenakan hukuman hingga 8 tahun penjara atau denda hingga Rp 2 miliar.

3. *Phising* dan Penipuan Daring

Phising adalah kegiatan memancing pemakai komputer di Internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu i yang sudah di-deface. *Phising* biasanya diarahkan kepada pengguna online banking, isian data pemakai dan password yang vital (Nuraini, 2017). Dalam "*Avoiding Social Engineering and Phishing Attacks*" dijelaskan Pelaku *phising* biasanya menggunakan kode rekayasa sosial (*social engineering*) dengan menyamar sebagai lembaga resmi, seperti bank atau perusahaan besar untuk menipu korban agar memberikan informasi pribadi mereka. Modus operandi ini sering dilakukan melalui *email,* situs web palsu, atau pesan teks yang tampak meyakinkan (Cybersecurity & Infrastructure Security Agency, 2021).

Phising adalah salah satu bentuk penipuan daring (*online fraud*) yang paling umum dan berbahaya karena dapat menyebabkan kerugian finansial besar bagi korban. Pasal 28 Ayat 1 UU ITE secara khusus mengatur tentang penyebaran berita bohong yang dapat menyesatkan publik dan merugikan konsumen dalam transaksi elektronik, yang termasuk dalam kategori penipuan digital. Tindakan *phising* juga dapat dikategorikan sebagai akses ilegal dan penyalahgunaan data pribadi, yang melanggar UU Pelindungan Data Pribadi.

Pelaku *phising* sering kali menggunakan berbagai metode untuk memanipulasi korban agar mereka secara sukarela memberikan informasi sensitif.

Beberapa jenis *phising* yang sering digunakan menurut data Laporan Tahunan Monitoring Keamanan Siber Tahun 2021:

a. *Email phising* merupakan salah satu jenis *phishing* yang banyak digunakan peretas untuk mengelabui korban. *Email Phishing* ditandai dengan peretas mengirimkan sebuah *email* dengan judul (*Subject*) yang menarik sehingga membuat korban menjadi penasaran dan tertarik untuk membuka email tersebut. *Email* tersebut biasanya berisikan *file* sisipan (*attachment*) atau *link* yang akan mengarahkan korban pada *website* untuk mengunduh program berbahaya. Apabila

program berbahaya ini terinstall, maka secara otomatis bekerja pada komputer korban dan mencuri *kredensial, password*, akun, dan informasi rahasia lainnya. Selain itu, peretas juga menggunakan frasa, tipografi, dan/atau logo yang sama sehingga membuat pesan tampak sah.

b. *Spear phishing* yaitu jenis *phishing* yang mirip seperti email phishing namun hanya menargetkan pada korban tertentu. Serangan *phising* ini lebih terarah, di mana pelaku menargetkan individu atau organisasi tertentu dengan menggunakan informasi pribadi untuk membuat serangan terlihat lebih kredibel.
c. *Smishing* merupakan jenis *phishing* yang mirip seperti *email phishing* namun dilakukan menggunakan SMS.
d. *Vishing* merupakan jenis *phishing* yang dilakukan menggunakan panggilan telepon untuk mengelabuhi korban. Penyerang akan menghubungi sejumlah nomor telepon dan kemudian mengarahkan korban untuk menyetujui klaim palsu seperti aktivitas transfer pada rekening, dan lainnya.

Phising sangat berbahaya karena serangan ini sering kali tidak disadari oleh korban sampai kerugian telah terjadi, misalnya ketika uang mereka diambil dari rekening bank atau identitas mereka digunakan untuk melakukan penipuan lebih lanjut (Cybersecurity & Infrastructure Security Agency. (n.d.).

Secara hukum, pelaku *phising* di Indonesia dapat dijerat dengan beberapa pasal pada UU ITE, terutama yang berkaitan dengan penipuan digital dapat mencapai 6 tahun penjara dan denda maksimal Rp 1 miliar. Selain itu, *phising* juga dapat dikategorikan sebagai pelanggaran terhadap hak privasi individu dan dapat menimbulkan tuntutan hukum tambahan.

4. *Cyberstalking* dan Perundungan Siber *(Cyberbullying)*

Cyberstalking dan perundungan siber (*cyberbullying*) adalah bentuk kejahatan siber yang menargetkan individu, terutama dengan tujuan mengintimidasi, melecehkan, atau menyakiti korban secara emosional. Kejahatan ini melibatkan penggunaan sarana digital, seperti media sosial, email, dan aplikasi pesan

untuk terus menerus mengganggu atau mengintimidasi seseorang. Berbeda dari ancaman fisik, kejahatan ini sering kali terjadi secara diam-diam (Farid, M., Febrianto, D., & Amalia, R. A. K., 2021), sehingga korban mungkin tidak langsung menyadari bahwa mereka sedang diawasi atau menjadi target pelecehan.

Federasi Serikat Guru Indonesia (FSGI) mencatat kasus perundungan di satuan pendidikan sejak Januari sampai September 2023 mencapai 23 kasus, dimana 50 persen terjadi di jenjang SMP, 23 persen di jenjang SD, 13,5 persen di jenjang SMA, dan 13,5 persen di jenjang SMK. Kasus perundungan juga telah memakan korban jiwa (Budiman, Ahmad., 2023).

Kasus perundungan siber (*cyber bullying*) yang dialami seorang anak berinisial FH, berusia 11 tahun, di Singaparna, Tasikmalaya, Jawa Barat, telah menjadi perhatian serius dari Komisi Perlindungan Anak Indonesia (KPAI). Kasus ini dianggap sebagai kasus yang berat dan kompleks karena korban mengalami kekerasan fisik, seksual, dan psikologis secara bersamaan. Berdasarkan penilaian KPAI, kasus ini perlu diproses melalui jalur hukum untuk mencegah terulangnya peristiwa serupa di masa mendatang, terutama karena anak-anak cenderung menjadi "peniru ulung." Menurut Kepolisian Daerah Jawa Barat, telah dilakukan pemeriksaan terhadap 15 saksi terkait peristiwa ini, termasuk keluarga korban. Komisioner KPAI, Jasra Putra, mengungkapkan keprihatinannya atas kasus ini, yang menunjukkan bahwa perundungan di kalangan anak-anak semakin serius dan kompleks. Peristiwa tersebut terungkap melalui video berdurasi 50 detik yang tersebar di media sosial, memperlihatkan tindakan yang sangat meresahkan, termasuk kekerasan seksual yang melibatkan hewan. Video tersebut pertama kali tersebar melalui aplikasi pesan WhatsApp di lingkungan warga setempat, sebelum akhirnya diunggah ke media sosial, yang menyebabkan perubahan perilaku pada korban. Setelah mengetahui bahwa dirinya menjadi viral, korban merasa malu dan mengalami tekanan psikis yang berat, hingga kondisi fisik serta psikologisnya mengalami kemunduran. Menurut keterangan Kepala Bidang Pelayanan Kesehatan RSUD SMC

Tasikmalaya, sebelum meninggal, korban mengalami berbagai komplikasi, termasuk depresi, *thypoid*, dan ensefalopati akibat tekanan psikologis. Jasra Putra menekankan bahwa perundungan biasanya terjadi secara berulang oleh pihak yang lebih dominan, serta mempertanyakan apakah kejadian yang terekam dalam video tersebut merupakan puncak dari serangkaian perundungan yang telah dialami korban. Ia juga menyesalkan lambatnya respon sehingga pendampingan terhadap korban dan keluarga tidak bisa dilakukan lebih cepat. Jasra menyarankan agar kasus ini menjadi catatan penting bagi pemerintah, mengingat bahwa akses bagi keluarga untuk melaporkan insiden perundungan masih sulit dijangkau. Terkait dengan latar belakang para pelaku, pihak Kepolisian Daerah Jawa Barat menduga bahwa mereka kemungkinan telah terpapar konten pornografi. Oleh karena itu, KPAI merekomendasikan keterlibatan psikolog anak dalam proses pemeriksaan, serta memberikan edukasi tentang reproduksi dan dampak perilaku seksual pada usia dini, sebagaimana diatur dalam Peraturan Pemerintah Nomor 78 Tahun 2021 tentang Perlindungan Anak. Dengan adanya pendekatan edukatif ini, diharapkan perilaku perundungan dapat dicegah dan dihentikan secara efektif (Kompas, 2022, July 24).

Menurut Pasal 27 Ayat (3) UU ITE, segala bentuk penghinaan, ancaman, atau perundungan melalui media digital yang ditujukan kepada individu atau kelompok, termasuk tindakan *cyberbullying*, merupakan tindak pidana yang dapat dikenai sanksi. Selain itu, *cyberstalking* juga dapat dikategorikan sebagai pelanggaran privasi yang diatur lebih lanjut dalam UU Pelindungan Data Pribadi.

Cyberstalking Ini melibatkan penelusuran, pengawasan, atau pengikutan yang tidak diinginkan terhadap seseorang secara online. Ini bisa mencakup pengawasan aktivitas media sosial, pengiriman pesan yang berlebihan, atau pembuatan akun palsu untuk mengamati dan mengganggu kehidupan pribadi korban (Butarbutar, Russel., 2023). Tindakan ini dapat menimbulkan rasa takut dan kecemasan pada korban, terutama jika diikuti dengan ancaman fisik atau pelecehan. Sedangkan perundungan siber

(cyber bullying) Ini adalah bentuk pelecehan yang berulang dan bertujuan untuk merendahkan, mengintimidasi, atau menyakiti seseorang secara emosional melalui pesan teks, komentar, atau konten yang diunggah di media sosial atau platform *online* lainnya (Butarbutar, Russel., 2023). Bentuk perundungan ini dapat mencakup penyebaran rumor palsu, penghinaan, atau ancaman di mana korban seringkali mengalami tekanan psikologis yang serius, hal tersebut dapat menyebabkan depresi, kecemasan, bahkan keinginan untuk bunuh diri.

Dalam konteks hukum, *cyberstalking* dan *cyberbullying* di Indonesia dapat dikenakan sanksi pidana berdasarkan UU ITE. Pelaku yang terbukti melakukan pelecehan, ancaman, atau perundungan siber dapat dijatuhi hukuman penjara hingga 4 tahun dan denda maksimal Rp 750 juta sesuai Pasal 27 Ayat 3 UU ITE. Selain itu, *cyberstalking* yang melibatkan pelanggaran privasi juga dapat dijerat dengan hukum privasi dan perlindungan data pribadi.

5. Penipuan Keuangan Daring

Penipuan keuangan daring adalah salah satu bentuk kejahatan siber yang paling merugikan, di mana pelaku memanfaatkan internet untuk menipu korban dengan janji keuntungan finansial, investasi fiktif, atau skema cepat kaya. Beberapa jenis kejahatan dan kategori ini termasuk pencucian uang, skema ponzi, dan penipuan investasi yang sering kali menargetkan individu maupun institusi finansial. Penipuan keuangan daring juga sangat berkaitan dengan kejahatan terkait identitas, juga dikenal sebagai kejahatan identitas atau pencurian identitas. Hal ini merujuk pada tindakan yang melibatkan penggunaan identitas seseorang secara tidak sah untuk tujuan penipuan atau keuntungan pribadi (Butarbutar, Russel., 2023). Dalam kejahatan ini, pelaku mencuri atau menggunakan informasi pribadi seseorang, seperti nama, nomor identitas, kartu kredit, atau informasi keuangan lainnya, dengan maksud menipu, melakukan penipuan, atau melakukan kegiatan ilegal lainnya.

Berikut ini beberapa bentuk umum dari kejahatan terkait identitas (Butarbutar, Russel., 2023):

a. Pencurian Identitas

   Ini terjadi ketika seseorang mengambil informasi pribadi seseorang tanpa izin, biasanya melalui pencurian fisik atau serangan siber, dan menggunakannya untuk tujuan ilegal. Informasi yang dicuri dapat digunakan untuk membuka rekening palsu, mengajukan pinjaman, melakukan transaksi finansial, atau melakukan tindakan ilegal lainnya atas nama korban.

b. Penipuan Kartu Kredit

   Pelaku menggunakan informasi kartu kredit yang dicuri untuk membuat pembelian *online* atau *offline* tanpa izin pemilik kartu. Mereka dapat membeli barang, makanan, atau layanan dengan menggunakan informasi kartu kredit yang sah namun tanpa sepengetahuan pemilik kartu.

c. Pembobolan Data

   Ini terjadi ketika pelaku berhasil memperoleh akses tidak sah ke basis data yang berisi informasi pribadi, seperti data pelanggan atau data keuangan perusahaan. Informasi yang dicuri kemudian dapat digunakan untuk melakukan penipuan atau dijual ke pasar gelap.

Beberapa kasus penipuan berbasis skema ponzi yang menimbulkan kerugian finansial besar misalnya pada kasus *Dream for Freedom* (D4F) dan kasus Sunmod Alkes yang menjanjikan keuntungan yang tinggi kepada investornya. Bahkan skema serupa juga masih terjadi di negara maju, seperti kasus Madof yang terjadi di Amerika Serikat dimana literasi Keuangan masyarakatnya sudah sangat tinggi. Jika menilik lebih jauh kasus-kasus tersebut, kita akan menemukan skenario *fraud* yang dikenal sebagai skema ponzi. Skema ini dicetuskan oleh Charles Ponzi pada tahun 1920.

Skema ponzi adalah skema kejahatan investasi dengan memberikan keuntungan kepada investor (anggota) menggunakan dana yang disetorkan oleh investor (anggota) lain. Alih-alih menginvestasikan dana yang sudah disetorkan oleh

investornya, skema ini hanya memberikan pembayaran keuntungan melalui dana investor lain. Sehingga, skema ini selalu membutuhkan aliran dana yang terus meningkat yang bersumber dari anggota-anggota baru. Saat aliran kebutuhan dana sudah terlalu besar dan sulit untuk menambah anggota baru, maka skema ini akan runtuh dan investor (anggota) akan kehilangan dananya.

Skema ponzi hadir dalam bentuk yang beragam. Bentuk yang paling sering muncul adalah dalam bentuk produk investasi seperti yang terjadi pada D4F dan Sunmod Alkes, dimana seseorang dijanjikan mendapatkan keuntungan yang konstan dan tanpa risiko. Secara sederhana dapat digambarkan, misalkan si A menyetorkan dana sebesar Rp 100 dan dijanjikan mendapatkan keuntungan sebesar 20%, maka pada saat jatuh tempo A mendapatkan pembayaran sebesar Rp 120. Keuntungan Rp 20 yang diperoleh A bersumber dari dana yang disetorkan oleh B yang dijanjikan keuntungan yang sama, dan begitu seterusnya (Saptono, Wahyudi., n.d.).

Dalam UU ITE, berbagai bentuk penipuan daring ini diatur melalui pasal-pasal yang mencakup manipulasi data, penyalahgunaan informasi yang menyesatkan. Selain itu, dalam beberapa kasus tindakan ini juga melibatkan pencucian uang yang melanggar Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Salah satu bentuk penipuan keuangan daring yang paling umum adalah skema ponzi, di mana pelaku menawarkan investasi dengan imbal hasil yang sangat tinggi dalam waktu singkat. Pelaku menggunakan uang yang diinvestasikan oleh investor baru untuk membayar keuntungan kepada investor lama, menciptakan ilusi bahwa investasi tersebut sah. Pada akhirnya, Ketika tidak ada lagi investor baru yang masuk, skema ini runtuh, dan para investor kehilangan seluruh uang mereka.

Pencucian uang atau *money laundering* adalah rangkaian kegiatan yang merupakan proses yang dilakukan oleh seseorang atau organisasi terhadap uang haram yaitu uang yang berasal dari kejahatan, dengan maksud untuk menyembunyikan atau

menyamarkan asal-usul uang tersebut dari pemerintah atau otoritas yang berwenang melakukan penindakan terhadap tindak pidana dengan cara terutama memasukkan uang tersebut ke dalam sistem keuangan (*financial system*) sehingga uang tersebut kemudian dapat dikeluarkan dari sistem keuangan itu sebagai uang yang halal (Rusli, Muhammad., 2016). Di era digital, internet telah menjadi sarana utama bagi pelaku untuk mencuci uang dengan cara mentransfer dana melalui berbagai rekening bank, menggunakan *cryptocurrency* atau melalui platform perdagangan daring. Tindakan ini melibatkan berbagai aktivitas digital yang sering kali sulit dilacak tanpa bantuan teknologi forensik yang canggih.

Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, mengatur tentang tindak pidana pencucian uang, termasuk yang dilakukan melalui sarana digital. Hukum ini mencakup segala upaya untuk mengidentifikasi, melacak, dan menyita aset yang diperoleh secara ilegal.

Penipuan keuangan daring dan pencucian uang di Indonesia dapat dijerat dengan berbagai undang-undang, termasuk UU ITE dan Undang-Undang Republik Indonesia Nomor 8 Tahun 2010. Hukuman untuk pelaku penipuan keuangan dapat mencapai 6 tahun penjara dan denda hingga Rp 1 miliar tergantung pada tingkat kerugian yang ditimbulkan pada korban.

DAFTAR PUSTAKA

Abdusallam, H. R., & Agung, R. (2006). *Prospek Hukum Pidana Indonesia dalam Mewujudkan Rasa Keadilan Masyarakat*. Jakarta, 13.

Almakki, H. M. (n.d.). Hak Asasi Manusia dalam Al-Quran. *Al-Furqan: Jurnal Agama, Sosial, dan Budaya, 2*(1), 23.

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware prevention and mitigation techniques. *International Journal of Computer Applications, 177*(40), 31–39.

Anggraini, Y. (2024). Kekuatan hukum alat bukti elektronik dan kredibilitasnya dalam pembuktian hukum pidana. *Jurnal Hukum dan Kewarganegaraan, 6*(8), 3.

Antoni. (2017). Kejahatan dunia maya (Cybercrime) dalam Simak Online. *Jurnal Nuraini, 17*(2), 264–265.

Arief, Barda Nawawi. (2006). *Tindak pidana mayantara: Perkembangan kajian cybercrime di Indonesia*. Jakarta: PT RajaGrafindo Persada.

Audrina, V., Washington, V., Harianto, S. K., Manjali, R., & Nadia, A. (2024). *Refleksi satu dekade 2014-2024: Menuju transformasi digital yang bermakna* (p. 6). Kementerian Komunikasi dan Informatika.

Avrizal, Dhevanda Ashar Evrast, & Lestari, Okti Indah. (2024). Mengungkap jejak digital: Studi kasus alat bukti elektronik kasus carding di Bali pada tahun 2023. *Jurnal Kritis Studi Hukum, 9*(6).

Berutu, S. P., Rizki, Heriyanti, Leonard, T., Tanjaya, W., Nainggolan, F., & Nababan, B. S. P. (n.d.). *Buku pembelajaran digital security* (hlm. 23). Cianjur: Unpi Press.

BPPTIK. (2023). Kementerian Komunikasi dan Informatika RI.

Brants, C., Jackson, A., & Wilson, T. J. (2020). A Comparative Analysis of Anglo-Dutch Approaches to 'Cyber Policing': Checks and Balances Fit for Purpose? *The Journal of Criminal Law, 84*(5), 451–473. https://doi.org/10.1177/0022018320952561

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.

Brown, A. (2017). Data protection and privacy in the United States. *Journal of Privacy Law, 8*(3), 46.

Budiman, Ahmad. (2023). Upaya mengatasi perubardandungan di media sosial. *Info Singkat: Pusat Analisis Keparlemenan Badan Keahlian DPR RI, XV*(20/II/Pusaka/Oktober), 1-10.

Budiman, Maman. (2020). *Kejahatan korporasi di Indonesia*. Malang: Setara Press.

Butarbutar, Russel. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. *Technology and Economics Law Journal, 2*(2), 307–311.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Chazawi, Adami. (2010). *Pelajaran Hukum Pidana 1*. Jakarta: PT Raja Grafindo Persada.

Chazawi, Adami. (2010). *Pelajaran Hukum Pidana 2*. Jakarta: PT Raja Grafindo Persada.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S.** (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology*, 65–66.

Clough, J. (2015). *Principles of Cybercrime*. Cambridge University Press.

Council of Europe. (2001). *Preamble of the Convention on Cybercrime*. Budapest, 23.XL2001.

Cryer, Robert, et al. (2007). *Universal jurisdiction: International and municipal legal perspectives* (hlm. 220).

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Cybersecurity & Infrastructure Security Agency. (n.d.). *National Terrorism Advisory System*. Retrieved from https://www.cisa.gov

Dianti, Flora. (2024). *Hukum pembuktian pidana di Indonesia: Perbandingan HIR dan KUHAP* (Edisi revisi). Jakarta: Sinar Grafika.

Dikdik, Elisatris. (2009). *Cyber law aspek hukum teknologi informasi*. Bandung: Refika Aditama.

Djanggih, H., & Qamar, N. (2018). Penerapan teori-teori kriminologi dalam penanggulangan kejahatan siber (cybercrime). *PANDECTA Research Law Journal, 3*(1), 20–21.

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining cyberbullying. *Pediatrics, 140*(2).

Erman, R. (1999). Peranan Hukum dalam Pembangunan pada Era Globalisasi. *Jurnal Hukum, 11*(6), 123.

Ersya, Muhammad Prima. (2017). Permasalahan hukum dalam menanggulangi cybercrime di Indonesia. *Journal of Moral and Civil Education, 1*(1), 60.

European Union Agency for Fundamental Rights and Council of Europe. (2014). *Handbook on European Data Protection Law* (p. 27). Belgium.

Fadhillah, Siti Aura, Matakupan, Michelle Sharon Anastasia, & Mingga, Britney Wilhelmina Berlian. (2023). Peran Interpol dalam penyelesaian kasus kejahatan siber berdasarkan Konvensi Budapest on Cybercrimes. *Journal on Education, 5*(4), 16553–16564.

Farid, M., Febrianto, D., & Amalia, R. A. K. (2021). Model pengaturan ketentuan hukum pidana dalam upaya kebijakan penanggulangan tindak pidana cyberbullying terhadap anak. *Laporan akhir penelitian dasar Universitas Lampung*. LPPM UNILA, 26.

Fitriani, Y., & Pakpahan, R. (2020). Analisa penyalahgunaan media sosial untuk penyebaran cybercrime di dunia maya atau cyberspace. *Cyberspace, 20*(1), 21–27.

Fitroh, Qotrunnada Ayu., & Sugiantoro, Bagus. (2023). Peran ethical hacking dalam memerangi cyberthreats. *Jurnal Ilmiah, 11*(1), 28.

Gillespie, Alisdair A. (2015). *Cybercrime: Key Issues and Debates*. Routledge.

Gollose, Petrus Reinhart. (2006). Perkembangan cybercrime dan upaya penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan, 4*(2).

Golose, Petrus Reinhard. (2008). *Seputar kejahatan hacking: Teori dan studi kasus*. Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable, and what we can do about it*. Anchor Books.

Goodman, M., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, 10(2), 139–163.

Habibi, M. R., & Liviani, I. (2020). Kejahatan teknologi informasi (cybercrime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23*(2), 2722–2075.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cybercrime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23*(2), 409.

Habibi, Muhammad Rizky., & Liviani, Indri. (2020). Kejahatan teknologi informasi (Cybercrime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23*(2), 409.

Hamzah, Andi. (1992). *Aspek-aspek pidana di bidang komputer*. Jakarta: Sinar Grafika.

Hamzah, Andi. (2016). *Hukum acara pidana Indonesia*. Jakarta: Sinar Grafika.

Harahap, M. Yahya. (2016). *Pembahasan permasalahan dan penerapan KUHAP* (Cetakan ke-15).

Hartono, Budi. (2023). Ransomware: Memahami ancaman keamanan digital. *Bincang Sains dan Teknologi, 2*(02), 55–62.

Hassanah, Hetty. (2023). Tindakan hukum terhadap pelaku penyebaran virus komputer melalui e-mail (cyber spamming) berdasarkan ketentuan tentang informasi dan transaksi elektronik. *Res Nullius Law Journal, 5*(1), 1–8.

Himawan, Irfan Sophan, et al. (2022). *Etika profesi teknologi informasi dan komunikasi*. TOHAR MEDIA.
Sidik, Suyanto. (2013). Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya, 1*(1), 1–7.

HukumOnline.com. (2003, terakhir diubah). *Tindak pidana cybercrime*. Diakses pada 6 November 2024, dari https://www.hukumonline.com/klinik/a/tindak-pidana-cyber-crime-cl2824/.

Hutabarat, Sumiaty Adelina, et al. (2023). *Cyber-law: Quo vadis regulasi UU ITE dalam revolusi industri 4.0 menuju era society 5.0*. PT. Sonpedia Publishing Indonesia.

Irawati, Arista Candra. (2019). Politik hukum dalam pembaharuan hukum pidana (RUU KUHP asas legalitas). *ADIL Indonesia Journal, 1*(2), 1–12.

Irwansyah, Irwansyah, & Yudiastuti, Helda. (2019). Analisis digital forensik rekayasa image menggunakan Jpegsnoop dan Forensically Beta. *Jurnal Ilmiah Matrik, 21*(1), 54–63.

Iskandar, T., et al. (2023). Kekuatan pembuktian alat bukti elektronik berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi Transaksi Elektronik (ITE). *Lexstricta: Jurnal Ilmu Hukum, 2*(1), 23–34.

Jhaver, S., Ghoshal, S., Bruckman, A., & Gilbert, E. (2018). Online harassment and content moderation: The case of blocklists. *ACM Transactions on Computer-Human Interaction, 25*(2), 6.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2020). *Rencana strategis Kementerian Komunikasi dan Informatika 2020–2024*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Kompas. (2022, July 24). Kasus "bullying" yang tewaskan siswa SD di Tasikmalaya, KPAI menduga pelaku terpapar konten pornografi. *Kompas*. https://regional.kompas.com/read/2022/07/24/060600878/kasus-bullying-yang-tewaskan-siswa-sd-di-tasikmalaya-kpai-menduga-pelaku?page=all. Diakses 5 November 2024.

Koto, Ismail. (2021). Cybercrime according to the ITE law. *International Journal Reglement & Society (IJRS), 2*(2), 103–110.

Kurniawan, Itok Dwi. (2024). Penegakan hukum terhadap tindak pidana perjudian: Tantangan dan solusi dalam era digital. *Complex: Jurnal Multidisiplin Ilmu Nasional, 1*(1), 4–5.

Kusnaidi, S. A., & Wijaya, A. U. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *Jurnal Al-Wasath, 2*(1), 21.

Laksana, T. G., & Mulyani, S. (2023). Faktor-faktor mendasar kejahatan siber terhadap kemanusiaan. *Jurnal Hukum Prioris, 11*(2), 141.

Laporan Tahunan Monitoring Keamanan Siber. (2021). *Laporan tahunan monitoring keamanan siber tahun 2021*.

Lemhannas RI. (2023). *Digital Transformation*. Retrieved October 26, 2024, from https://www.lemhannas.go.id/images/2023/Materi_KUP/2807_UIs_Digital_Transformation.pdf

Levin, James., et al. (1980). *Criminal justice: A public policy approach*. New York: Harcourt Brace Jovanovich, 63–64.

Mahmud, A. S., & Hamzah, A. (2016). *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika.

Manurung, E. A. P. (2023). The right to privacy based on the Law of the Republic of Indonesia Number 27 of 2022. *Journal of Digital Law and Policy, 2*(3), 109.

Marzuki, P. M. (2005). *Penelitian Hukum*. Prenada Media.

Maskun, & Meilarati, W. (2017). Aspek Hukum Penipuan Berbasis Internet. CV Keni Media.

Miftakhur Rokhman Habibi, & Isnatul Liviani. (2020). Kejahatan teknologi informasi (cybercrime) dan penanggulangannya dalam sistem hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran dan Pembaharuan Hukum Islam, 23*(2), 409.

Moeljatno. (2002). *Asas-Asas Hukum Pidana*. Jakarta: PT Rineka Cipta.

Moeljatno. (2015). *Asas-Asas Hukum Pidana*. Jakarta: Rhineka Cipta.

Muladi, & Barda, N. A. (1992). *Bunga Rampai Hukum Pidana*. Bandung: Alumni.

Muladi. (2017). *Kapita Selekta Sistem Peradilan Pidana*. Badan Penerbit Universitas Diponegoro.

Mursito, Danan, dkk. (2005). *Pendekatan hukum untuk keamanan dunia cyber serta urgensi cyber law di Indonesia*. Makalah, Program Magister Fakultas Ilmu Komputer, Universitas Indonesia.

Nabila, A. P., Manabung, N. A., & Ramadhansha, A. C. (2024). Peran hukum internasional dalam menanggulangi cybercrime pada kejahatan transnasional. *Indonesian Journal of Law, 1*(1), 27.

Naskah Akademik Rancangan Undang-Undang tentang Keamanan dan Ketahanan Siber. (n.d.).

Nirwana, M. A. (2022). Perlindungan hukum terhadap data pribadi sebagai hak privasi individual. *Jurnal Al-Wasath, 3*(2), 94.

Nitibaskara, Ronni R. (2005). *Cyber law: Aspek hukum teknologi informasi*. Bandung: PT Refika Aditama.

Nugraha, R. (2021). Perspektif hukum Indonesia (Cyberlaw) penanganan kasus cyber di Indonesia. *Jurnal Ilmiah Hukum Dirgantara, 11*(2).

Nugraha, Riko. (2021). Perspektif hukum Indonesia (Cyber law) penanganan kasus cyber di Indonesia. *Jurnal Ilmiah Hukum Dirgantara, 11*(2), 55.
Raharjo, Agus. (2002). *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Bandung: PT Citra Aditya Bakti.

Nugroho, A., & Chandrawulan, A. A. (2022). Research synthesis of cybercrime laws and COVID-19 in Indonesia: Lessons for developed and developing countries. *Security Journal, 2022*, 1–20.

Nugroho, Kristian Aji. (2018). Pengaruh cyber attack terhadap kebijakan cyber security Amerika Serikat. *Journal of International Relations, 3*(4).

Nuraini. (2017). Kejahatan dunia maya (cybercrime) dalam simak online. *Jurnal Nuraini, 17*(2), 265.

Oxford Economics. (2018). *Technology and the future of ASEAN jobs*. Oxford Economics.

Pahajow, Aan Andrew Johanes. (2016). Pembuktian terhadap kejahatan dunia maya dan upaya mengatasinya menurut hukum positif di Indonesia. *Jurnal Lex Crimen, 5*(2), 97.

Pambudi, Agung, & Yitawati, Krista. (2021). Dinamika dan tantangan cyber law di Indonesia. *Proceeding of Conference on Law and Social Studies*.

Pamungkas, Alief Tanding, Muliyono, Andi, & Lahangatubun, Nurjana. (2024, Mei). Krisis penegakan hukum cybercrime di Indonesia: Hambatan dan jalan keluar. *DJHPI*.

Parthiana, I Wayan. (1990). *Pengantar hukum internasional* (Edisi pertama). Bandung: Mandar Maju.

Peraturan Presiden Republik Indonesia Nomor 139 Tahun 2024 tentang Penataan Tugas dan Fungsi Kementerian Negara Kabinet Merah Putih Periode Tahun 2024–2029.

Perdana, P. I. (2024). *Pemenuhan hak-hak tersangka tindak pidana siber/cyber sebagai wujud pemenuhan hak asasi manusia di wilayah hukum kepolisian daerah Jawa Tengah* (Tesis, Universitas Darul Ulum Islamic Centre Sudirman Guppi Undaris). 59.

Praptono, Agung, & Yusuf, Hudi. (2024). Tinjauan kriminologi terhadap pelaku kejahatan pemerasan dengan menggunakan virus, ransomware WannaCry sebagai suatu kejahatan modern. *Jurnal Intelek dan Cendikiawan Nusantara, 1*(2), 1660–1669.

Pratama, A. Y., Nugroho, H. A. D., Astinda, A. N. R., & Adhipradana, Y. A. (2024). Penegakan tindak pidana cyberstalking dalam hukum positif Indonesia. *Legal Standing: Jurnal Ilmu Hukum, 8*(3), 703.

Pristiono, Agus. (2020). Kebijakan kriminal (criminal policy) dengan konsep mediasi dalam proses penyidikan tindak pidana umum (penipuan dan penggelapan) pada Bagwassidik Ditreskrimum Polda Sumut. *Jurnal Ilmiah Muqoddimah: Jurnal Ilmu Sosial, Politik dan Hummaniora, 4*(1), 34–43.

Prodjodikoro, R. W. (2014). *Asas-asas hukum pidana di Indonesia*. Refika Aditama, 1.

Pusiknas Polri. (n.d.). *Kejahatan Siber di Indonesia Naik Berkali-Kali Lipat*. Retrieved October 30, 2024, from https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Putra, A. S., & Prayudi, Y. (2021). Implementasi multi smart contract pada bukti digital dan chain of custody dalam meningkatkan keamanan dan integritas bukti digital. *JUSTINDO: Jurnal Sistem dan Teknologi Informasi Indonesia, 6*(2), 98–108.

Qibriya, M. R. D., Ambarwa, A., & Susilo, K. E. (2021). Analisis forensik digital pada aplikasi instant messaging di smartphone berbasis Android untuk bukti digital. *Jurnal Teknologi Informasi, 5*(2), 114–121.

Rahardjo, S. (2009). *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing.

Rahardjo, Satjipto. (1983). *Masalah Penegakan Hukum*. Bandung: Sinar Baru.

Rahardjo, Satjipto. (2009). *Hukum dan Perilaku: Hidup baik adalah dasar hukum yang baik*. Jakarta: Penerbit Buku Kompas.

Rajagukguk, Erman. (1999). Peranan hukum dalam pembangunan pada era globalisasi. *Jurnal Hukum, 11*(6), 123.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Republik Indonesia. (2023). *Kitab Undang-Undang Hukum Pidana*.

Riyadh, A. (2019). *Hukum Media Massa*. Sidoarjo: Indomedia Pustaka.

Rosadi, S. D. (2015). *Cyber law aspek data privasi menurut hukum internasional, regional dan nasional.* Refika Aditama.

Rosalina, Vidila, & Saputra, Dadang Herli. (2015). Pengembangan model tahapan digital forensic untuk mendukung Serang sebagai kota bebas cybercrime.

Ruddin, Isra, & Zein SGN, Subhan. (2023). Evolusi hukum cybercrime dalam perkembangan hukum dalam dunia digital. *Jurnal Hukum & Pembangunan, 53*(1), 143–150.

Rumampuk, A. M. (2015). Tindak pidana penipuan melalui internet berdasarkan aturan hukum yang berlaku di Indonesia. *Jurnal Lex Crimen, 6*(3), 34.

Rusli, Muhammad. (2016). Pencucian uang dalam transaksi perdagangan trade based money laundering. *Jurnal IUS, 4*(2), 68.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(89). https://doi.org/10.3390/fi11040089

Salim, Agus, & Muttaqin, Elfran Bima. (2020). Persidangan elektronik (e-litigasi) pada peradilan tata usaha negara. *Paulus Law Journal, 2*(1), 15–25.

Salsa, A. (n.d.). Tinjauan yuridis terhadap perlindungan hak asasi manusia dalam kasus cybercrime. *Triwikrama: Jurnal Ilmu Sosial, 1*(3), 24.

Sangalang, Rizki Setyobowo, et al. (2024). *Hukum pidana cyber: Buku referensi*.

Saptono, Wahyudi. (n.d.). Kepala divisi penunjang, skema Ponzi, ancaman bagi perkembangan industri jasa keuangan. *Indonesia Securities Investor Protection Fund*, 1.

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cybercrime prevention strategy in Indonesia. *SSRG International Journal of Humanities and Social Science, 3*(6), 22–26.

Setiyadi, Mas Wigrantoro Roes, & Siregar, Mirna Dian Avanti. (2003, November). *Naskah akademik rancangan undang-undang tindak pidana di bidang teknologi informasi*. Global Internet Policy Initiative Indonesia bekerja sama dengan Indonesia Media Law and Policy Center.

Simanjuntak, Shara Yosevina, & Utomo, Tri Cahyo. (2016). Analisis kerja sama bilateral Indonesia dengan Australia dalam penanggulangan terorisme sebagai kejahatan transnasional terorganisir (2002–2015). *Journal of International Relations Universitas Diponegoro, 2*(3), 117–127.

Sirait, Timbo Mangaranap, & SH, M. H. (2024). *Cyber law dalam teori dan perkembangannya (Cybercrime, privacy data, e-commerce)*. Deepublish.

Situmpul, Josua. (2012). *Cyberspace cyberlaw: Tinjauan aspek hukum pidana*. Jakarta: Tata Nusa.

Smith, J. C., & Hogan, Brian. (1988). *Criminal law*. English Language Book Society/Butterworths, 18.

Soejadi. (2017). *Refleksi mengenai hukum dan keadilan: Aktualisasinya di Indonesia*. Yogyakarta: Aswaja Pressindo.

Soekanto, S. (2014). *Faktor-Faktor yang Mempengaruhi Penegak Hukum*. Jakarta: Rajawali Pers.

Sofyan, A., & Azisa, N. (2016). *Hukum Pidana*. Nasional Republik Indonesia. 99.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564. https://doi.org/10.2307/40041279

Soraja, A. (2021). Perlindungan hukum atas hak privasi dan data pribadi dalam perspektif HAM. *Prosiding: Seminar Nasional Kota Ramah Hak Asasi Manusia, 1*, 1–[page numbers].

Sudarto. (1986). *Hukum dan hukum pidana*. Bandung: Alumni.

Sudarwanto, Al Sentot. (2009). Cyber bullying: Kejahatan dunia maya yang terlupakan. *Jurnal Hukum Pro Justitia, 27*(1).

Suhariyanto, Budi. (2014). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: PT. Raja Grafindo Persada.

Suseno, Sigid. (2012). *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama.

Syamsu, M. A. (2016). *Penjatuhan pidana dan dua prinsip dasar hukum pidana*. Kencana, 15.

Tanziilal, Altoof Aththobarani. (2024). Analisis pertimbangan hakim dalam tindak pidana peretasan informasi elektronik (Studi putusan PT Nomor 281/Pid. Sus/2022/PT DKI).

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Voigt, P., & Bussche, A. V. D. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Walies, M. H. (2021). Perspektif hukum positif dan hukum Islam terhadap kejahatan carding di Indonesia. *Guepedia*.

Wibowo, A. (2015). Tinjauan teoritis terhadap wacana kriminalisasi LGBT. *Jurnal Cakrawala Hukum, 11*(1), 99.

Wibowo, Arief, Wangsajaya, Yehu, & Surahmat, Asep. (2023). *Pemolisian digital dengan artificial intelligence*. Jakarta: PT. RajaGrafindo Persada-Rajawali Pers.

Widianingrum, A. R. (2024). Analisis implementasi kebijakan hukum terhadap penanganan kejahatan siber di era digital. *Jurnal Iuris Scientia, 2*(2), 2985–8836.

Widodo. (2013). *Aspek hukum pidana kejahatan mayantara*. Yogyakarta: Aswaja Pressindo.

Wiratama, A. B., & Gede, I. (2020). *Cybercrime & cyber law: Pengantar memahami kejahatan komputer*. Bandar Lampung: Anugrah Utama Raharja.

Yurizal, D. R., et al. (2018). *Penegakan hukum tindak pidana cybercrime di Indonesia*. Media Nusa Creative (MNC Publishing).

Yussuf, T. T., Muhammad, J. W., Olalekan, D. M., Yusuf, B., Unuriode, A., & Matti, B. H. (2023). Data protection and privacy as a tool to reduce financial loss from cybercrimes. *Global Scientific Journals, 11*(11), 1598.

Yustia, M. (2010). Pembuktian dalam hukum pidana Indonesia terhadap cybercrime. *Pranata Hukum, 5*(2), 26724.

PROFIL PENULIS

Dr. Budiyanto, S.H., M.H.

Buku ini berjudul "Pengantar *Cybercrime* dalam Sistem Hukum Pidana di Indonesia" merupakan hasil kajian berbagai literatur. Pembahasan buku ini difokuskan pada efektivitas penegakan hukum, tantangan yang dihadapi oleh keempat lembaga penegak hukum (Kepolisian, Kejaksaan, Peradilan, Pemasyarakatan) dan solusi mengatasi hambatan dalam penegakan hukum terhadap kasus *cybercrime* di Indonesia.

Penulis memiliki kepakaran di bidang ilmu Sistem Peradilan Pidana, sehingga buku ini diketengahkan mengenai kejahatan *cybercrime* yang dikaitkan dengan tugas dan kewenangan masing-masing dari ke-empat sub sistem dalam Sistem Peradilan Pidana *(Criminal Justice System).*

Penulis sebagai Dosen tetap pada Fakultas Hukum Universitas Cenderawasih di Jayapura - Papua. Jabatan Fungsional: Lektor Kepala, Pangkat Pembina Utama Muda, Golongan IV/c. Tempat dan tanggal lahir: Nganjuk, 24 Januari 1966. Pendidikan: Sekolah Dasar (1979), Sekolah Menengah Pertama (1982) dan Sekolah Menengah Atas (1985) di Kabupaten Nganjuk. Penulis melanjutkan kuliah Program Sarjana (S1) Ilmu Hukum pada Fakultas Hukum Universitas Cenderawasih (1991), Program Pascasarjana Magister Ilmu Hukum (S2) pada Fakultas Hukum Universitas Udayana (2000), Program Doktor (S3) pada Fakultas Hukum Universitas Hasanuddin (2015). Jabatan saat ini adalah sebagai Ketua Bagian Hukum Pidana periode 2021-2025 pada Fakultas Hukum Universitas Cenderawasih.

Email Penulis: budiyantofhuncen@gmail.com

Pengantar [CYBERCRIME] dalam Sistem Hukum Pidana di Indonesia

Buku ini hadir sebagai wujud kepedulian terhadap isu *cybercrime* yang semakin kompleks dan dinamis di era digital. Kajian dalam buku ini dirancang untuk memberikan pemahaman mendalam tentang fenomena *cybercrime* dalam konteks sistem hukum pidana di Indonesia, termasuk tantangan yang dihadapi dalam penegakkan hukum serta solusi untuk mengatasi hambatan tersebut. Buku ini terdiri atas delapan bab yang saling terintegrasi untuk memberikan gambaran menyeluruh mengenai *cybercrime*. Bab pertama, *Pendahuluan*, menguraikan latar belakang dan urgensi pembahasan isu ini, terutama dalam kaitannya dengan perkembangan teknologi dan hukum di Indonesia. Bab ini menjadi pintu masuk bagi pembaca untuk memahami pentingnya sinergi antara teknologi dan hukum dalam memerangi kejahatan siber.

Bab kedua, Definisi dan Jenis-Jenis Kejahatan Siber, mengupas berbagai bentuk *cybercrime*, seperti *hacking*, pencurian data, *phishing*, hingga *cyber-terrorism*. Pemahaman ini penting untuk membangun kerangka analisis yang kokoh dalam upaya penegakan hukum. Bab ketiga, *Cybercrime* di Indonesia, mengulas perkembangan kasus-kasus kejahatan siber di Indonesia, termasuk upaya regulasi yang telah dilakukan. Bab ini juga mengidentifikasi celah hukum yang masih menjadi tantangan utama dalam penegakan hukum terhadap cybercrime.

Pada Bab keempat, Tantangan Penegakan Hukum dalam Kasus *Cybercrime*, pembahasan difokuskan pada hambatan yang dihadapi lembaga penegak hukum di Indonesia, Kepolisian, Kejaksaan, Peradilan, dan Pemasyarakatan. Bab ini menyoroti tantangan teknis, kelemahan koordinasi, serta keterbatasan sumber daya manusia yang berpengaruh terhadap efektivitas penanganan kasus *cybercrime*. Bab kelima, *Bukti Elektronik dalam Proses Pembuktian Pidana*, membahas pentingnya bukti elektronik dalam sistem peradilan pidana modern. Aspek legalitas, validitas, serta tantangan teknis dalam pengumpulan dan pembuktian bukti elektronik dibahas secara mendalam dalam bab ini.

Bab keenam, *Kolaborasi Internasional dalam Penanggulangan Cybercrime*, menyoroti pentingnya kerja sama lintas negara untuk mengatasi sifat *cybercrime* yang sering kali melampaui batas yurisdiksi nasional. Bab ini memberikan perspektif tentang bagaimana Indonesia dapat memanfaatkan perjanjian internasional dan kolaborasi global untuk memperkuat sistem penegakan hukum siber. Bab ketujuh, *Pelindungan Hak Asasi Manusia dalam Penegakan Hukum Cybercrime*, menekankan pentingnya menjaga keseimbangan antara keamanan dan pelindungan hak asasi manusia. Bab ini mengulas potensi pelanggaran hak dalam proses hukum kasus *cybercrime* dan cara untuk meminimalkan risiko tersebut. Bab kedelapan, Penutup, menyajikan rangkuman serta rekomendasi strategis untuk meningkatkan efektivitas penegakan hukum terhadap kasus *cybercrime* di Indonesia.

ISBN 978-634-7021-15-1

9 786347 021151

sada kurnia pustaka