Jurnal Hukum & Pembangunan Masyarakat

Vol. 17 No. 11, November 2025

ANALISIS CYBER CRIME DALAM PENDEKATAN UUD ITE

Komang Widiantara Saputra[1], Dina Ayu Wardani[2], Musdalifa[3], Wiwi Pratiwi[4], Dina Ariska Anggraeni[5], Nur Faisah[6], Linda Lestari[7], Herlinda[8]
Universitas Sembilanbelas November Kolaka
Email: komangsaputra701@gmail.com[1], dinaayuwardani13@gmail.com[2], musdalifahmjsdalifah@gmail.com[3], wiwipratiwi340@gmail.com[4], ariskadina240@gmail.com[5], ichai2924@gmail.com[6], iis896631@gmail.com[7], herlindarinda15@gmail.com[8]

Abstrak

Perkembangan pesat teknologi informasi dan komunikasi telah mengubah peradaban manusia, namun juga berfungsi sebagai "senjata dua mata" yang memicu munculnya berbagai bentuk kejahatan siber (cybercrime). Kejahatan digital ini telah menunjukkan peningkatan yang signifikan di Indonesia, di mana kasusnya tercatat melonjak drastis. Penelitian ini bertujuan untuk menganalisis bentuk dan jenis kejahatan siber di Indonesia, penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta mengevaluasi efektivitas UU ITE dalam menanggulangi kejahatan tersebut. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan konseptual dan studi kepustakaan, mengumpulkan data dari berbagai jurnal, artikel, dan peraturan perundang-undangan. Hasil analisis menunjukkan bahwa kejahatan siber di Indonesia mencakup berbagai bentuk, yang dikategorikan oleh aparat penegak hukum (Polri) sebagai computer crime (kejahatan yang menargetkan sistem komputer) dan computer-related crime (kejahatan yang menggunakan komputer sebagai alat bantu). UU ITE merupakan dasar hukum utama dalam penanganan kejahatan siber di Indonesia, yang secara spesifik mengatur tindak pidana seperti penyebaran konten ilegal (Pasal 27), penyebaran berita bohong dan ujaran kebencian (Pasal 28), serta akses ilegal (Pasal 30). Sebelum UU ITE diberlakukan, penegakan hukum mengandalkan interpretasi ekstensif dari Kitab Undang-Undang Hukum Pidana (KUHP) untuk kasus seperti penipuan (Pasal 378) dan pencurian (Pasal 362). Meskipun UU ITE telah menjadi payung hukum utama, regulasi ini masih dianggap belum mampu mengakomodasi semua jenis kejahatan siber yang terus berkembang dan memiliki celah yang dapat disalahgunakan. Oleh karena itu, diperlukan adanya reformasi UU ITE untuk memperkuat upaya penegakan hukum dan menciptakan instrumen hukum yang lebih efektif serta adaptif guna memberikan efek jera terhadap pelaku.
Kata Kunci: Cyber Criem, UU ITE, Hukum Siber, Kejahatan Digital, Dan Penegakan Hukum.

Abstract

The rapid development of information and communication technology has transformed human civilization, but it has also served as a "double-edged sword," triggering the emergence of various forms of cybercrime. This digital crime has shown a significant increase in Indonesia, with cases recorded as soaring dramatically. This study aims to analyze the forms and types of cybercrime in Indonesia, the implementation of the Electronic Information and Transactions Law (UU ITE), and evaluate the effectiveness of the ITE Law in combating these crimes. This study uses a normative legal research method with a conceptual approach and literature review, collecting data from various journals, articles, and laws and regulations. The analysis shows that cybercrime in Indonesia encompasses various forms, categorized by law enforcement officials (the Indonesian National Police) as computer crime (crimes targeting computer systems) and computer-related crime (crimes using computers as a tool). The ITE Law is the primary legal basis for handling cybercrime in Indonesia, specifically regulating crimes such as the distribution of illegal content (Article 27), the spread of fake news and hate speech (Article 28), and illegal access (Article 30). Before the enactment of the ITE Law, law enforcement relied on extensive interpretations of the Criminal Code (KUHP) for cases such as fraud (Article 378) and theft (Article 362). Although the ITE Law has become the primary legal umbrella, this regulation is still considered inadequate to accommodate all types of cybercrime, which continues to evolve and has loopholes that can be abused. Therefore,

reform of the ITE Law is needed to strengthen law enforcement efforts and create more effective and adaptive legal instruments to provide a deterrent effect on perpetrators.

Keywords: *Cyber Crime, ITE Law, Cyber Law, Digital Crime, And Law Enforcement.*

PENDAHULUAN

Teknologi informasi dan komunikasi telah mengubah cara hidup masyarakat dan perkembangan peradaban manusia di seluruh dunia. Selain itu, kemajuan di bidang teknologi informasi membuat dunia menjadi tak terbatas dan mendorong perubahan sosial yang terjadi sangat cepat. Saat ini, teknologi informasi berfungsi sebagai senjata dua mata, karena selain membantu meningkatkan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana yang efektif untuk melakukan tindak kejahatan. Perkembangan internet telah menimbulkan dampak negatif, seperti yang diungkapkan oleh Roy Suryo 2002, seorang ahli teknologi informasi dalam penelitiannya, bahwa "kejahatan siber kini semakin marak di lima kota besar di Indonesia dan cukup menyita perhatian. Kejahatan ini dilakukan oleh para hacker yang umumnya anak muda yang terlihat kreatif, tetapi sebenarnya mereka mencuri nomor kartu kredit melalui internet". Kejahatan siber dibagi menjadi dua kategori, yaitu kejahatan siber dalam arti sempit dan kejahatan siber dalam arti luas. Kejahatan siber dalam arti sempit adalah tindak kejahatan terhadap sistem komputer, sedangkan kejahatan siber dalam arti luas mencakup tindak kejahatan terhadap sistem atau jaringan komputer serta kejahatan yang menggunakan media komputer. Dilihat dari fakta hukum saat ini, dampak dari penggunaan ilmu pengetahuan dan teknologi yang salah digunakan sebagai sarana kejahatan telah sangat penting untuk dipertimbangkan bagaimana kebijakan hukumnya, sehingga kejahatan siber yang terjadi bisa ditangani dengan hukum pidana, termasuk dalam hal ini adalah mengenai cara membuktikan tindak pidana tersebut. Dikatakan sangat penting karena dalam menegakkan hukum pidana, dasar untuk menentukan seseorang bersalah atau tidak melakukan tindak pidana, selain tindakan yang dapat dihukum berdasarkan undang-undang yang sudah ada sebelumnya (asas legalitas), juga tindakan tersebut harus didukung oleh bukti yang sah dan dapat dipertanggungjawabkan (unsur kesalahan). Pandangan ini sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP), seperti diatur secara jelas dalam Pasal 1 ayat (1) KUHP yang berbunyi "Nullum delictum nulla poena sine praevia lege poenali" atau dalam bahasa Indonesia dapat diartikan sebagai "tidak ada tindak pidana dan tidak ada hukuman tanpa adanya peraturan hukum pidana sebelumnya".

Jenis-jenis kejahatan mayatara atau cybercrime yang muncul akibat kemajuan teknologi adalah peretasan. Hal ini diatur dalam Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 30 ayat (1), (2), dan (3). Sanksi pidana untuk tindak pidana ini juga dijelaskan dalam Pasal 46 UU ITE. Teknologi bisa memberi manfaat, tetapi juga bisa membawa bahaya bagi masyarakat. Semua negara mengalami peningkatan kasus kejahatan siber. Pada Kongres PBB ke-8 tahun 1990 di Havana, Kuba, dan Kongres ke-10 tahun 1990 di Wina, Austria, cybercrime menjadi topik pembicaraan. Karena banyaknya aktivitas peretas di Indonesia, negara ini memiliki kasus cybercrime terbanyak di dunia. Kejahatan siber terhadap anak-anak semakin menjadi tren baru di berbagai negara, termasuk Indonesia. Penggunaan internet yang tidak terbatasi meningkatkan risiko anak-anak menjadi korban kejahatan online. Jenis kejahatan yang terjadi secara daring seperti kejahatan seksual, pornografi, trafficking, bullying, serta kejahatan lainnya semakin mengancam generasi muda. Selain itu, pentingnya memastikan pelaku tahu tanggung jawab atas perbuatan mereka agar kejahatan siber dapat dicegah melalui hukum pidana, termasuk dalam proses pembuktian. (Waliadin, 2024)

Berikut beberapa contoh tindak pidana cyber crime, antara lain:

1. Pencurian Pasal 362: Siapa pun yang mengambil barang yang sepenuhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, akan diancam dengan hukuman penjara paling lama lima tahun atau denda paling banyak sembilan ratus rupiah. Pasal ini bisa diterapkan dalam kasus pencurian nomor kartu kredit orang

lain melalui internet untuk melakukan transaksi. Setelah barang dikirimkan, penjual tidak bisa mengambil uangnya karena pemilik kartu bukanlah orang yang melakukan transaksi.

2. Penipuan Pasal 378: Siapa pun yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum, menggunakan nama palsu atau martabat palsu, dengan tipu muslihat atau rangkaian kebohongan, agar orang lain menyerahkan barang, memberi hutang, atau menghapuskan piutang, akan diancam dengan hukuman penjara paling lama empat tahun. Pasal ini bisa digunakan dalam kasus penipuan, misalnya dengan menawarkan dan menjual produk atau barang melalui iklan di salah satu website sehingga orang tertarik membelinya dan mengirimkan uang kepada pemasang iklan. Namun, pada kenyataannya barang tersebut tidak ada. Hal ini baru diketahui setelah uang dikirim dan barang yang dipesan tidak datang, sehingga pembeli menjadi tertipu.
3. Pemerasan dan Pengancaman Pasal 335 (1) Seseorang yang melanggar hukum dengan memaksa orang lain melakukan, tidak melakukan, atau membiarkan sesuatu, dengan menggunakan kekerasan, tindakan lain, atau perlakuan yang tidak menyenangkan, baik kepada diri sendiri maupun orang lain, bisa diancam dengan pidana penjara paling lama satu tahun atau denda paling banyak empat ribu lima ratus rupiah. Seseorang yang memaksa orang lain melakukan, tidak melakukan, atau membiarkan sesuatu dengan ancaman pencemaran atau pencemaran tertulis juga bisa diancam dengan pidana yang sama. (2) Dalam hal seperti yang disebutkan dalam butir 2, tuntutan atas tindakan tersebut hanya bisa diajukan jika ada pengaduan dari orang yang terkena. Ketentuan dalam pasal ini bisa digunakan dalam kasus pemerasan atau pengancaman yang dilakukan melalui email yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan kemauan pelaku, dan jika tidak dilakukan, akan menyebabkan bahaya. Biasanya tindakan ini dilakukan karena pelaku mengetahui rahasia korban.

Masalah yang muncul dari aktivitas online bisa menyebabkan kebocoran data pribadi. Hal ini menunjukkan adanya kelemahan dalam sistem dan kurangnya pengawasan, sehingga data pribadi bisa disalahgunakan dan menimbulkan kerugian bagi pemiliknya. Penyalahgunaan, pencurian, atau menjual data pribadi merupakan pelanggaran hukum di bidang teknologi informasi. Selain itu, hal ini juga bisa dianggap sebagai pelanggaran hak asasi manusia, karena data pribadi merupakan bagian dari hak yang harus dilindungi. Berikut beberapa contoh kasus penyalahgunaan data pribadi:

1. Penyalinan data kartu ATM nasabah (skimming), dimana pelaku mengambil uang dari kartu tersebut di tempat lain.
2. Pinjaman online, di mana pengisian data dilakukan secara online. Namun, ketika terjadi keterlambatan pembayaran, ada kasus kolektor yang melakukan intimidasi ke nasabah, keluarga nasabah, atasan tempat kerja, bahkan bisa mengakses data dari ponsel nasabah.
3. Transportasi online, di mana konsumen mengalami pelecehan seksual melalui nomor WhatsApp. (Situmeng & Tua, 2021)

UU Nomor 11 Tahun 2008 tentang Informasi Elektronik dan Transaksi (UU ITE) merupakan dasar hukum utama dalam menangani tindak pidana di dunia maya di Indonesia. Namun, hingga saat ini UU ITE masih dianggap belum bisa mengakomodasi semua jenis kejahatan maya yang terus berkembang. Adanya celah dalam UU ITE bisa menyebabkan penyalahgunaan hukum, hukuman berlebihan, serta ketidakadilan terhadap hak asasi manusia. Oleh karena itu, dibutuhkan reformasi UU ITE agar bisa beradaptasi dengan perkembangan teknologi dan mengatasi kelemahan yang ada. Tujuan utama dari revisi UU ITE adalah untuk memperkuat upaya penegakan hukum terhadap kejahatan dunia maya. Diharapkan revisi ini bisa menciptakan instrumen hukum yang lebih efektif, sekaligus mampu mengikuti perkembangan saat ini, sehingga membentuk efek jera terhadap pelaku cyber crime. (Liviani & Habibi-isnatul, 2020)

TINJAUAN PUSTAKA

1. Definisi Cybercrem Menurut Parah Ahli, Contoh Kepolisian

Kejahatan siber, atau cybercrime, adalah tindakan kriminal yang melibatkan penggunaan komputer dan jaringan internet. Semakin berkembangnya teknologi, semakin banyak dampak baik dan buruk yang ditimbulkan bagi masyarakat. Meski teknologi ini memberikan banyak manfaat, di sisi lain juga menghadirkan ancaman baru, seperti kejahatan digital yang bisa merugikan individu maupun masyarakat secara luas Cybercrime sudah ada sejak lama, mulai dari peretas yang mencoba masuk ke jaringan komputer. Beberapa hanya ingin merasa hebat dengan akses ke jaringan yang aman, tetapi ada juga yang mencari informasi rahasia. Kemudian, pelaku mulai menggunakan virus dan malware untuk merusak sistem komputer pribadi maupun bisnis. Kesulitan mengatasi kejahatan ini disebabkan oleh beberapa faktor, seperti kurangnya alat yang memadai, korban yang enggan melaporkan ke polisi, sistem keamanan yang lemah, dan kesulitan menemukan lokasi pelaku (Dirjosisworo & Soedjono, 2022)

Cybercrime dapat diartikan sebagai tindakan kriminal yang sengaja dilakukan terhadap seseorang atau kelompok orang dengan tujuan merusak reputasi, menyebabkan kerugian fisik atau mental, atau merugikan secara langsung dan tidak langsung. Tindakan ini dilakukan menggunakan jaringan telekomunikasi modern seperti internet (termasuk ruang chat, email, forum, dan grup) serta ponsel (melalui Bluetooth, SMS, atau MMS). Debarati Halder dan K. Jaishankar memberikan definisi cybercrime dengan perspektif gender, yaitu kejahatan yang ditujukan pada wanita dengan maksud merugikan secara psikologis dan fisik menggunakan teknologi internet dan ponsel.Secara sengaja, pemerintah maupun perusahaan swasta terlibat dalam berbagai bentuk cybercrime, seperti spionase, pencurian uang, dan kejahatan lintas batas.Kegiatan yang melewati batas negara dan melibatkan kepentingan setidaknya satu negara sering disebut cyberwarfare (G.Gani & Alcianno, 2020)

Namun demikian, aturan tentang kejahatan siber di berbagai negara menggunakan kata yang berbeda-beda, tergantung tujuannya dan cakupan hukumnya. Kata "kejahatan dunia maya" berasal dari gabungan kata "cyber" dan "crime". "Crime" berarti tindak pidana, kejahatan, atau peristiwa yang melanggar hukum, sedangkan "cyber" berarti dunia maya, ruang maya, atau ruang mayantara. Dalam bukunya, Barda Nawawi Arief mengatakan bahwa cybercrime merupakan bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian besar di dunia internasional. Vodymyr Golubev menyebutnya sebagai bentuk baru perilaku anti-sosial. Ada beberapa julukan lain untuk jenis kejahatan ini yang digunakan dalam berbagai tulisan, seperti kejahatan dunia maya (cyber space/virtual space offence), dimensi baru dari high tech crime, dimensi baru dan transnasional crime, serta dimensi baru dari white collar crime. Dari beberapa definisi tersebut, cybercrime dirumuskan sebagai tindakan yang melanggar hukum dan dilakukan dengan menggunakan internet yang berbasis pada kemajuan teknologi komputer dan telekomunikasi, baik untuk memperoleh keuntungan atau tidak, dengan merugikan pihak lain.

Berikut adalah beberapa definisi mengenai kejahatan siber menurut para ahli:

a. Andi Hamzah menyatakan bahwa kejahatan komputer tidak tergolong sebagai kejahatan yang baru, melainkan kejahatan biasa, karena masih dapat diselesaikan berdasarkan hukum yang berlaku.
b. Forester dan Morrison menjelaskan kejahatan komputer sebagai tindakan kriminal di mana komputer berfungsi sebagai alat utama.
c. Girasa memberikan definisi cybercrime sebagai tindakan kriminal yang memanfaatkan teknologi komputer sebagai elemen utama.
d. Susanto mengemukakan bahwa secara umum, cybercrime terbagi menjadi dua kategori yaitu:

- Kejahatan yang memanfaatkan teknologi informasi sebagai sarana. Contoh aktivitas dari

jenis cybercrime pertama ini mencakup pembajakan (hak cipta), pornografi, pemalsuan, pencurian kartu kredit (carding), penipuan melalui e-mail, penipuan dan peretasan rekening bank, perjudian daring, terorisme, konten internet yang berkaitan dengan isu SARA (seperti penyebaran kebencian terhadap tertentu etnis, ras atau agama), transaksi dan penyebaran obat-obatan terlarang, transaksi seks dan lain-lain.

- Kejahatan yang menargetkan sistem dan fasilitas teknologi informasi. Cybercrime jenis ini tidak hanya memanfaatkan komputer dan internet sebagai media, tetapi menjadikannya sebagai objek sasaran. Contoh dari tindak kejahatan ini termasuk akses ilegal ke suatu sistem (hacking), merusak situs web dan server data (cracking), serta defacing. (Achmad Allang S & Abu, 2022)

Berikut adalah contoh kasus kepolisian:

1) Kasus Hacker Bjorka Mengenai Pembocoran Data

Seseorang yang menggunakan nama samaran Bjorka adalah salah satu anggota forum Breached. Breached Forums adalah sebuah situs yang berfungsi sebagai platform diskusi daring. Situs ini dapat diakses publik melalui alamat “breached. to”. Dalam komunitas tersebut, Bjorka diakui sebagai figur penting atau "God" dan telah memperjualbelikan miliaran data pribadi hasil dari aksinya. Dia pertama kali melakukan peretasan pada tahun 2020 dengan membobol data pengguna aplikasi Tokopedia. Data yang berhasil dicuri meliputi ID pengguna, nomor telepon, kata sandi, dan alamat email. Akibatnya, Tokopedia mengalami kerugian signifikan karena data yang dibocorkan itu terjual di dark web dengan nilai mencapai Rp74 juta. Selanjutnya, pada bulan Juni 2020, Bjorka juga berhasil membobol data dari 270 juta pengguna Wattpad. Ia juga meretas 1,3 miliar kartu SIM, yang menimbulkan kekhawatiran di kalangan masyarakat Indonesia tentang keamanan data pribadi mereka. Selain itu, situs resmi KPU (Komisi Pemilihan Umum) juga menjadi sasaran peretasan oleh Bjorka, di mana ia berhasil mendapatkan data NIK, KK, dan nama lengkap dari individu. (Aditama, Sinaga, & Dkk, 2025)

2. Hubungan UU Ite dan keamanan KUHP

hubungan Uu Ite dengan keamanan siber Uu Ite merupakan undang-undang mengenai siber yang pertama kali di Indonesia, dengan tujuan memberikan perlindungan secara hukum kepada masyarakat yang melakukan transaksi secara elektronik, mencegah kejahatan yang berfokus pada teknologi informasi, serta melindungi pengguna layanan teknologi informasi dan komunikasi. Keterkaitan antara UU ITE dan penanganan kejahatan siber oleh aparat penegak hukum sangat dipengaruhi oleh regulasi yang ada. Sebelumnya, terdapat sejumlah regulasi yang berkaitan dengan teknologi informasi, khususnya kejahatan yang berkaitan dengan internet sebelum UU ITE diberlakukan. Penegakan hukum terkait kejahatan siber sebelum adanya UU ITE dilakukan dengan cara menerapkan prinsip-prinsip cyber crime dalam ketentuan dalam Kitab Undang-Undang Hukum Pidana, serta undang-undang yang berkaitan dengan perkembangan teknologi informasi seperti:

Undang-Undang No. 14 Tahun 2008 mengenai Keterbukaan Informasi Publik;

a. Undang-Undang No. 36 Tahun 1999 mengenai Telekomunikasi;
b. Undang-Undang No. 19 Tahun 2002 yang telah diubah oleh Undang-Undang No. 28 Tahun 2014 mengenai Hak Cipta;
c. Undang-Undang No. 25 Tahun 2003 tentang perubahan Undang-Undang No. 15 Tahun 2002 mengenai Tindak Pidana Pencucian Uang yang telah digantikan oleh Undang-Undang No. 8 Tahun 2010 mengenai Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang (Riani, Firmansyah, & Dkk, 2023)

Keamanan dalam KUHP yang dapat digunakan untuk mengadili cybercrime dengan cara melakukan penafsiran extensif adalah ketentuan tentang tindak pidana pemalsuan (sebagaimana diatur dalam Pasal 263 sampai dengan Pasal 276), tindak pidana pencurian (sebagaimana diatur dalam Pasal 362 sampai dengan 367), tindak pidana penipuan

(bagaimana diatur dalam Pasal 378 sampai dengan Pasal 395), dan tindak pidana perusakan barang (sebagaimana diatur dalam Pasal 407 sampai dengan Pasal 412). Aturan yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang bisa dipakai untuk menangani kejahatan siber melalui penafsiran yang luas mencakup peraturan tentang pemalsuan (tercantum dalam Pasal 263 hingga Pasal 276), pencurian (yang diatur antara Pasal 362 hingga 367), penipuan (berdasarkan Pasal 378 sampai Pasal 395), dan perusakan barang (diatur dalam Pasal 407 hingga Pasal 412).

Berikut diuraikan tentang penerapan ketentuan hukum pidana untuk mengadili pelaku cybercrime di Indonesia

Penerapan pasal-pasal KUHP dalam perkara yang menjadikan komputer sebagai sasaran kejahatan dan perkara yang menggunakan komputer sebagai sarana kejahatan;

1) Kategori perusakan barang yang digunakan untuk pembuktian dihadapan pihak berwajib; Dalam kasus Unauthorized Transfer Payment di Bank Negara Indonesia (BNI) Cabang New York Agency (Tahun 1986), Pengadilan Negeri Jakarta Pusat selain menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 KUHP, yaitu pencurian yang dilakukan oleh lebih dari dua orang atau lebih secara bersama-sama, juga membuktikan bahwa terdakwa terbukti secara sah dan meyakinkan melanggar Pasal 233 KUHP, yaitu merusak barang yang digunakan untuk membuktikan sesuatu dihadapan pihak yang berwajib. Putusan itu dikuatkan Putusan Pengadilan Tinggi Jakarta, dan Putusan Mahkamah Agung.
2) Jenis perusakan barang yang digunakan sebagai alat bukti di hadapan penegak hukum; Dalam kasus transfer dana yang tidak sah di Bank Negara Indonesia (BNI) Cabang New York (Tahun 1986), Pengadilan Negeri Jakarta Pusat menghukum terdakwa dengan penjara setelah terbukti secara sah dan jelas melakukan pelanggaran Pasal 363 KUHP, terkait pencurian oleh sekelompok orang. Di samping itu, terbukti pula bahwa tergugat melanggar Pasal 233 KUHP yang menyatakan bahwa merusak barang untuk keperluan pembuktian di hadapan otoritas adalah pelanggaran. Keputusan ini diperkuat oleh Pengadilan Tinggi Jakarta dan Mahkamah Agung.
3) Kategori pencurian; Dalam kasus anauthirized Transfer Payment di Bank Negara Indonesia (BNI) Cabang New York agency (Tahun 1986), Pengadilan Negeri Jakarta Pusat menjatuhkan pidana penjara terhadap terdakwa karena terbukti secara sah dan meyakinkan melanggar Pasal 363 ayat (1) KUHP, yaitu pencurian yang dilakukan oleh lebih dari 2 orang secara bersama-sama. Putusan tersebut dikuatkan oleh putusan Pengadilan Tinggi Jakarta, dan Putusan Mahkamah Agung.
4) Kategori pencurian; Pada kasus transfer dana ilegal di Bank Negara Indonesia (BNI) Cabang New York (Tahun 1986), Pengadilan Negeri Jakarta Pusat menjatuhkan hukuman penjara kepada terdakwa karena terbukti dengan jelas melakukan pelanggaran terhadap Pasal 363 ayat (1) KUHP, terkait pencurian yang dilakukan oleh lebih dari dua orang secara bersama-sama. Keputusan ini diperkuat oleh Pengadilan Tinggi Jakarta dan Putusan Mahkamah Agung.

3. Penerapan UU di luar KUHP

Penerapan undang-undang di luar KUHP dalam menangani kasus yang menggunakan komputer sebagai alat untuk melakukan kejahatan. Untuk kasus kejahatan yang menyasar data atau sistem komputer hingga 31 Januari 2005, ditetapkan berdasarkan regulasi yang berada di luar KUHP. Undang-Undang yang dimaksud adalah Undang-Undang Nomor 7 Tahun 1987 tentang Hak Cipta, serta Undang-Undang Nomor 36 Tahun 1999 mengenai Telekomunikasi.

a. Undang-Undang Nomor 7 Tahun 1987 Tentang Hak Cipta; Aturan dari Undang-

Undang Nomor 7 Tahun 1987 tentang Hak Cipta diterapkan dalam peristiwa pembajakan perangkat lunak Word Star versi 5. 0 pada tahun 1990. Pengadilan Negeri Bandung menghukum terdakwa dengan penjara dan denda, setelah terbukti melanggar Pasal 11 ayat (1) huruf k, bersamaan dengan Pasal 14 huruf g, dan Pasal 44 ayat (1) dari Undang-Undang Nomor 7 Tahun 1987 tentang Hak Cipta, serta Keputusan Presiden RI Nomor 25 Tahun 1989 dan Pasal 55 ayat (1) dan Pasal 64 KUHP. Keputusan ini disetujui oleh Pengadilan Tinggi Bandung. Pasal 11 ayat (1) huruf k mengatur mengenai perangkat lunak komputer sebagai karya cipta eksklusif.

b. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi. Aturan dari Undang-Undang Nomor 36 Tahun 1999 mengenai Telekomunikasi diterapkan pada perkara pembobolan situs Komisi Pemilihan Umum (KPU) yang terjadi pada tahun 2004. Pengadilan Negeri Jakarta Pusat memberikan hukuman penjara kepada Dani Firmansyah setelah terbukti secara sah dan meyakinkan melanggar Pasal 22 huruf c, bersamaan dengan Pasal 50 dari Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

4. Implementasi UU Ite dari dulu sampai sekarang

Implementasi uu ite dari dulu sampai sekarang Tindak kejahatan siber di Indonesia telah ada sejak tahun 1983, terutama di sektor perbankan. Dalam beberapa tahun berikutnya hingga kini, kejahatan siber di Indonesia semakin banyak, termasuk peretasan program komputer, cracking, penyalahgunaan kartu kredit orang lain (carding), penipuan bank (banking fraud), serta pornografi, termasuk kejahatan yang terkait dengan nama domain. Selain itu, terdapat kasus lain yang melibatkan komputer di Indonesia seperti penyelundupan konten pornografi lewat internet (cyber smuggling), pagejacking (moustrapping), spam (surat sampah), penyadapan, cybersquatting, dan typosquatting. Sementara itu, kejahatan yang menargetkan sistem atau jaringan komputer meliputi cracking, defacing, serangan denial of service (DoS), serangan distributed denial of service (DDoS), penyebaran virus (worm), dan pemasangan logic bomb. Memerangi kejahatan siber telah menjadi fokus penting bagi lembaga penegak hukum dan intelijen, baik di tingkat nasional maupun internasional, serta untuk para praktisi bisnis, merchant, konsumen, serta pengguna akhir. Dalam banyak kasus, tindakan kejahatan siber diawali dengan mengeksploitasi host dan jaringan komputer. Oleh karena itu, penipu dan peretas bisa masuk ke dalam jaringan, khususnya yang menggunakan protokol TCP/IP. Dalam praktiknya, transaksi elektronik dilakukan melalui jaringan yang terhubung (internet), yaitu jaringan komputer dengan berbagai ukuran yang saling terhubung satu sama lain melalui media komunikasi elektronik, memungkinkan akses ke semua layanan yang ditawarkan oleh jaringan lainnya. (Laksana & Wijaya, 2019)

Teori-teori hukum pidanacyber dan teknologi informasi ada beberapa teori hukum pidana yang berhubungan dan digunakan dalam konteks kejahatan siber serta teknologi informasi, yang diuraikan dalam berbagai jurnal, antara lain:

a. Teori Kriminologi dalam Kejahatan Siber: Jurnal sering menjelaskan bagaimana teori kriminologi klasik, seperti teori pilihan rasional dan teori aktivitas rutin, diadaptasi dalam dunia siber. Teori-teori ini membantu memahami alasan di balik keputusan individu untuk melakukan kejahatan online serta bagaimana adanya target yang rentan dan kurangnya pengawasan mempermudah tindakan tersebut.
b. Teori Perlindungan Hukum: Teori ini menyoroti peran hukum pidana dalam memberikan perlindungan serta keadilan bagi para korban kejahatan siber, sekaligus menciptakan kepastian hukum dan rasa aman di masyarakat. Jurnal membahas pentingnya perlindungan data pribadi serta hak-hak korban dengan lebih detail.
c. Teori Efek Gentar: Teori ini berkaitan dengan peran sanksi hukum dalam menghindarkan individu dari melakukan tindakan kriminal. Dalam jurnal, dilakukan

analisis terhadap efektivitas Undang-Undang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana dalam memberikan efek jera kepada pelaku kejahatan siber, yang umumnya bersifat anonim dan melintasi batas.

d. Teori Fungsional Hukum Pidana: Teori ini membahas peranan hukum pidana dalam menjaga ketertiban sosial dan stabilitas, termasuk di ruang digital. Jurnal mengeksplorasi bagaimana kerangka hukum pidana berfungsi sebagai sarana untuk mendeteksi, menyelidiki, dan menuntut pelaku kejahatan yang semakin kompleks.

(Quintarti & Liza, 2024)

METODE PENELITIAN

Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundang undangan terkait cyber-crime. Metode pengumpulan data dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain. Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan cyber law di Indonesia.

pendekatan konseptual menurut para ahli berpendapat bahwa hukum pidana tidak mengenal penerapan analogi, meskipun tindakan yang dimaksud memiliki kesamaan konsep dengan kejahatan atau pelanggaran yang diatur dalam KUHP. Selain itu, karena tidak semua kejahatan memiliki karakteristik definisi yang serupa, dimungkinkan untuk menciptakan jenis kejahatan baru dengan kerangka hukumnya sendiri guna menghasilkan formulasi hukum pidana yang lebih efisien. Isu mengenai kejahatan siber masih menjadi topik hangat di kalangan akademisi hukum, dikarenakan bentuk kejahatan ini tergolong baru. Hukum pidana yang berlaku saat ini, seperti KUHP dan KUHAP, mengalami kritik dan pembelaan terkait seberapa baik mereka dapat menangani jenis kejahatan ini. Penegak hukum akan menangkap pelanggar kejahatan siber. Tindak pidana ini tetap diadili berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama yang sesuai dengan ketentuan pasal-pasal yang tidak biasa dalam KUHP. Para ahli telah memperkenalkan istilah "kejahatan siber", dan dalam kajian ini, peneliti akan mengusulkan beragam kategori dari kejahatan siber, mengingat istilah tersebut mencakup banyak aktivitas. (Pansariadi & Soekorini, 2023) Hukum pidana yang berlaku saat ini (KUHP dan KUHAP) telah mendapat kritik dan dukungan terkait kemampuannya dalam menangani kejahatan ini. Penegak hukum akan menangkap para pelaku kejahatan di dunia maya. Kejahatan siber masih dapat diadili berdasarkan Kitab Undang-Undang Hukum Pidana (KUHP), terutama untuk tindakan yang termasuk dalam kategori pasal-pasal yang tidak biasa di KUHP. Ketika regulasi ini dianggap kurang efektif untuk mencegah berbagai tipe kejahatan daring, terdapat banyak alat hukum pidana di luar KUHP yang bisa diterapkan untuk mengatasi kejahatan melalui pemanfaatan teknologi. Alat-alat ini melibatkan berbagai pendekatan terhadap undang-undang yang berbeda. Untuk mengeksplorasi bagaimana hukum Indonesia menangani kejahatan siber.

A. teori-teori penjelasan kejahatan cyber crime

1. Teori Anomie yang diusulkan oleh J. J. M. van Dick, H. I. Sagel Grande, dan L. G.

Toornvliet (1996: 133-143) menyatakan bahwa teori ini termasuk dalam kelompok teori yang membahas ketertinggalan sosial. Teori lain yang juga masuk dalam kategori ini adalah teori subkultur delinkuen, teori Cloward dan Ohlin, serta teori kriminologi ekologis. Teori anomi berasal dari pemikiran Sosiolog Perancis, Emille Durkheim (1858-1917), dan Robert Merton. Pendapat Durkheim disampaikan lebih awal daripada Merton. Durkheim memperkenalkan konsep anomi untuk menggambarkan keadaan yang ditandai dengan deregulasional. Ia berpendapat bahwa perubahan sosial yang cepat dan menekan dapat memberikan dampak besar kepada semua kelompok masyarakat. Nilai-nilai yang dulunya dianggap penting dapat menjadi tidak jelas atau hilang.

2. Teori Asosiasi Diferensial diperkenalkan oleh sosiolog dari Amerika Serikat, Edwin H.

Sutherland pada tahun 1939 dan kemudian disempurnakan pada tahun 1947. Teori ini

didasarkan pada tiga konsep, yaitu Teori Transmisi Ekologis dan Budaya dari Shaw dan McKay; Interaksionisme Simbolik dari George Mead; serta Teori Konflik Budaya (William III dan McShane, 1998:49-50). Pada tahun 1939, Sutherland membahas tentang perilaku kriminal yang sistematis, konflik budaya, disorganisasi sosial, dan asosiasi diferensial. Romli Atmasasmita menjelaskan bahwa pengertian sistematik berkaitan dengan kejahatan yang terorganisasi atau praktik-praktik yang terkoordinasi dalam aktivitas kriminal. Definisi praktik terorganisasi dalam kejahatan adalah perilaku yang mendukung norma-norma yang telah ada di Masyarakat. Pada tahun 1947, Sutherland mengganti istilah "disorganisasi sosial" dengan "organisasi sosial diferensial". Dengan perubahan istilah ini, Sutherland ingin menegaskan bahwa terdapat berbagai macam kondisi sosial dengan nilai-nilai dan tujuan masing-masing yang berfungsi sebagai alat berbeda dalam mencapai tujuan. Teori ini mengakui adanya beragam organisasi kemasyarakatan yang terpisah tetapi bersaing satu sama lain berdasarkan norma dan nilai mereka sendiri. (Djanggih & Qamar, 2018)

B. Pendekatan perundang-undangan, Pancasila, uuu 1945, uu, pp, pepres,

a. Undang-Undang

Selain hukum pidana dan prosedur hukum yang substantif, undang-undang mengenai kejahatan siber mungkin mencakup isu-isu yang terkait dengan kolaborasi internasional, bukti digital, dan tanggung jawab Penyedia Layanan Internet (ISP). Di banyak negara, elemen-elemen dari regulasi semacam ini mungkin telah ada, seringkali dalam konteks hukum yang berbeda. Aturan terkait kejahatan siber tidak harus diterapkan dalam satu undang-undang tunggal. Berkenaan dengan struktur yang sudah ada, mungkin perlu untuk memperbarui beberapa bagian dari undang-undang yang berbeda (seperti melakukan perubahan pada Undang-Undang Bukti agar dapat diterapkan dalam konteks penerimaan bukti elektronik dalam proses pidana) atau untuk menghapus ketentuan dari undang-undang yang sudah usang (misalnya dalam Undang-Undang Telekomunikasi) saat memperkenalkan regulasi baru (translasi oleh peneliti).

b. Pancasila

Pancasila berfungsi sebagai cita hukum dan gagasan untuk mewujudkan hukum yang ideal. Dalam hal ini, Rudolf Stamler menyatakan bahwa cita hukum bisa dianggap sebagai panduan dalam mencapai ideal masyarakat. Dari cita hukum ini, diperoleh pengertian dan politik hukum dalam suatu negara. Cita hukum tersebut memiliki sifat normatif dan konstitutif. Normatif berarti berfungsi sebagai syarat transcendental yang menjadi dasar bagi hukum positif yang bermartabat, serta jalur etika hukum dan ukuran sistem hukum positif. Sementara itu, cita hukum yang konstitutif berarti bahwa rechtsidee bertujuan untuk mengarahkan hukum kepada tujuan yang hendak dicapai.

3. Pepres

Badan Siber dan Sandi Nasional (BSSN) resmi didirikan dengan adanya Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Nasional, yang ditetapkan pada 19 Mei 2017. Dalam regulasi tersebut, BSSN dibentuk dengan mempertimbangkan bahwa keamanan siber merupakan salah satu sektor pemerintahan yang harus ditingkatkan dan diperkuat untuk mendukung pertumbuhan ekonomi nasional serta mencapai keamanan nasional. Pembentukan BSSN merupakan langkah untuk merestrukturisasi Lembaga Sandi Negara menjadi Badan Siber dan Sandi Negara agar kebijakan dan program pemerintah di bidang keamanan siber dapat dijalankan dengan baik.

4. Pendekatan perundang-undangan

Studi ini mengaplikasikan metode normatif untuk meneliti aspek-aspek hukum yang relevan, dengan fokus pada hukum tertulis serta pendekatan perundang-undangan yang mengatur informasi dan teknologi. Data dianalisis secara deskriptif melalui pengumpulan informasi hukum dari berbagai literatur dan peraturan yang terkait. Temuan menunjukkan bahwa ada kebutuhan untuk tindakan resmi dari pemerintah, seperti dari Kementerian Komunikasi dan Informatika, dalam memblokir nomor yang digunakan oleh pelaku penipuan. Pendekatan sosial juga disarankan sebagai alternatif untuk menekan risiko kejahatan ini. Oleh karena itu, pencegahan kejahatan siber membutuhkan keterlibatan pemerintah dan pendekatan sosial yang menyeluruh. (Tua & Situmeang, 2020)

HASIL DAN PEMBAHASAN

A. Statistika kasus cyber crime kepolisian dan bentuk, jenis cyber crem di Indonesia

Tindak pidana terkait kejahatan siber mengalami peningkatan yang signifikan pada tahun 2022 jika dibandingkan dengan tahun sebelumnya. Bahkan, jumlah kejadian kejahatan siber melesat hingga 14 kali lipat. Informasi dari e-MP Robinopsnal Bareskrim Polri menunjukkan bahwa pihak kepolisian menangani 8. 831 kasus kejahatan siber dari tanggal 1 Januari sampai 22 Desember 2022. Semua unit di Bareskrim Polri dan polda di seluruh Indonesia terlibat dalam penanganan kasus-kasus ini. Polda Metro Jaya mencatatkan jumlah penanganan tertinggi, yaitu 3. 709 kasus kejahatan siber. Sementara itu, pada periode yang sama di tahun 2021, total penanganan di seluruh Indonesia hanya mencapai 612 kasus, dengan hanya 26 unit yang melaksanakan tindakan.

Tabel 1 peningkatan kehatan siber

No	Satker (2021)	Kasus(2021)	Satker (2022)	Kasus (2022)
1.	Polda Metro Jaya	293	Polda Metro Jaya	3.709
2.	Polda Jatim	66	Polda Sulsel	964
3.	Polda Sulsel	58	Polda Sumut	896
4.	Polda Jabar	48	Polda Jatim	648
5.	Polda Sumut	29	Polda Jabar	499
6.	Barsekrim Polri	21	Polda Lampung	295
7.	Polda Lampung	18	Polda Sultra	167

Sumber Data: e-MP Robinopsnal Bareskrim Polri diakses pada jumat 23 Desember 2022 pukul 10:30 WIB.

Data penindakan kejahatan siber di Indonesia menunjukkan peningkatan yang substansial dan mengkhawatirkan antara tahun 2021 dan 2022. Dalam periode satu tahun (1 Januari s/d 22 Desember), jumlah penindakan kasus meningkat drastis hingga 14 kali lipat, melonjak dari 612 kasus di tahun 2021 menjadi 8.831 kasus di tahun 2022. Peningkatan eksponensial ini didukung oleh perluasan jangkauan penegakan hukum, di mana jumlah Satuan Kerja (Satker) yang terlibat dalam penindakan mencapai 35 (seluruh Satker) pada tahun 2022, naik signifikan dari 26 Satker pada tahun sebelumnya. Secara geografis, dominasi penindakan terpusat di wilayah dengan aktivitas digital tinggi, sebagaimana tercermin dari perbandingan 7 Satker terbanyak; Polda Metro Jaya, sebagai contoh, melaporkan peningkatan penindakan dari 293 kasus menjadi 3.709 kasus, mengindikasikan bahwa laju pertumbuhan kasus kejahatan siber telah melampaui kapabilitas pencegahan, sehingga menuntut evaluasi mendalam terhadap efektivitas regulasi dan strategi keamanan siber nasional.

Tabel 2 jenis kejahatan siber

Kategori kejahatan siber	Deskripsi	Jenis Kasus
Computer crime	Kejahatan siber yang mengunakan computer sebagai alat utama untuk melakukan tindak pidana.	Peretasan sistem elektronik (Hacking).
		Intersepsi atau penyadapan illegal (illegal interception).
		Perusakan tampilan situs web (web defacement)
		Gangguan sistem

		(system interference)
		Menipulasi data (data manipulation)
Computer Related crime	Kejahatan siber yang mengunakan computer sebagai alat bantu untuk menfasilitasi tindak pidana.	Pornografi dalam jaringan (Online Pornograhy)
		Perjudian dalam jaringan (online Gamble)
		Pencemaran nama baik (online defamation)
		Pemerasan dalam jaringan (online extortion)
		Penipuan dalam jaringan (online fraud)
		Ujaran kebencian (hate speech)
		Pengancaman dalam jaringan (Online Threat)
		Akses illegal (Illegal Access)
		Pencurian data (Data Theft)

Sumber Data : e-MP Robinopsnal Bareskrim Polri diakses pada jumat 23 Desember 2022 pukul 10:30 WIB.

Analisis taksonomi kejahatan siber yang ditangani oleh Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri mengklasifikasikannya menjadi dua kategori utama, yang merefleksikan peran teknologi dalam tindak pidana tersebut. Pertama, Computer Crime didefinisikan sebagai kejahatan yang secara esensial menggunakan komputer sebagai alat utama (instrument) dalam pelaksanaan aksinya, mencakup aktivitas destruktif dan invasif seperti peretasan sistem (hacking), intersepsi ilegal, perusakan tampilan situs (web defacement), dan manipulasi data. Kedua, Computer Related Crime melibatkan penggunaan komputer sebagai alat bantu (facilitator) untuk mempermudah tindak pidana yang secara tradisional sudah eksis, seperti penipuan daring (online fraud), pencemaran nama baik, penyebaran pornografi, dan ujaran kebencian (hate speech). Diferensiasi ini menunjukkan bahwa lanskap kejahatan siber bukan hanya tentang serangan teknis terhadap sistem, tetapi juga tentang eksploitasi infrastruktur digital untuk memperluas jangkauan dan efektivitas kejahatan konvensional, menuntut kerangka regulasi dan penegakan hukum yang mampu mengadaptasi kedua dimensi ancaman tersebut.

Tabel 3 jenis kejahatan siber

No	Jenis kasus kejahatan siber	Jumlah penindakan (kasus)
1.	Manipulasi data autentik	3.723
2.	Penipuan melalui media elektronik	2. 131
3.	cybercrime	1. 098

4.	Pencemaram nama baik melalu media elektronik dan juga berbentuk persekusi	835
5.	Mengakses sistem secara tidak sah	358
6.	Judi Online	164
7.	Pengancaman melalu media elektronik atau medsos dan juga berbentuk persekusi	145
8.	Pornografi atau prostitusi melalui media elektronik	143
9.	Penghinaan melalui media elektronik dan yang juga berbentuk perskusi	59
10.	Hate speech melalui media elektronik	43

Sumber Data : e-MP Robinopsnal Bareskrim Polri diakses pada jumat 23 Desember 2022 pukul 10:30 WIB.

Analisis terhadap 10 jenis kasus kejahatan siber dengan penindakan terbanyak di Indonesia pada tahun 2022 menunjukkan adanya pergeseran fokus ancaman ke ranah integritas data dan penipuan digital. Data Bareskrim Polri mengindikasikan bahwa jenis kasus yang paling dominan adalah Manipulasi data otentik, yang mencatat 5.123 kasus; jumlah ini hampir dua kali lipat lebih tinggi dari Penipuan melalui media elektronik (2.115 kasus) yang menempati posisi kedua. Tingginya angka manipulasi data ini merefleksikan kerentanan serius pada sistem informasi dan proses otentikasi digital, sementara tingginya kasus penipuan menegaskan bahwa aspek kejahatan berbasis rekayasa sosial (social engineering) tetap menjadi vektor serangan yang masif. Secara kolektif, temuan ini menyiratkan bahwa tantangan keamanan siber utama di Indonesia kini bukan hanya terkait dengan peretasan atau serangan teknis murni (seperti Cybercrime yang berada di posisi ketiga dengan 1.890 kasus), tetapi lebih terpusat pada perlindungan integritas data dan mitigasi penipuan yang memanfaatkan infrastruktur elektronik, sehingga menuntut prioritas kebijakan yang lebih kuat pada aspek otentikasi dan edukasi literasi digital.

Bentuk dan jenis cyber crem di Indonesia

Hukum siber adalah bidang hukum yang berfungsi untuk mengatur interaksi antara individu atau entitas hukum yang memanfaatkan teknologi internet, dimulai saat mereka mulai terhubung dan memasuki dunia maya. Hukum siber juga dikenal dengan istilah Hukum Ruang Siber. Kejahatan siber adalah bentuk tindakan kriminal yang terjadi di dunia virtual dengan menggunakan perangkat yang terhubung ke internet. Kejahatan ini tidak hanya dapat dilakukan melalui komputer atau laptop, tetapi juga bisa terjadi di smartphone dengan syarat harus terhubung ke jaringan internet.

Ada berbagai tipe kejahatan siber yang sangat terkait dengan pemanfaatan teknologi berbasis komputer dan jaringan telekomunikasi, diantaranya adalah:

a. Akses Tidak Sah ke Sistem dan Layanan Komputer, yang merupakan kejahatan yang terjadi di dalam suatu jaringan komputer tanpa izin atau pengetahuan dari pemilik sistem tersebut. Umumnya, pelaku kejahatan (hacker) melakukan ini dengan tujuan merusak atau mencuri data penting yang bersifat rahasia. Namun, ada juga yang melakukannya hanya karena tantangan untuk menguji kemampuan mereka menembus sistem yang memiliki tingkat keamanan lebih tinggi. Jenis kejahatan ini semakin meningkat seiring dengan kemajuan teknologi internet. Beberapa contoh yang relevan adalah:
    - Pada tahun 1999, saat isu Timor Timur sedang hangat dibicarakan di kancah internasional, sejumlah situs web pemerintah Indonesia telah disabotase oleh hacker.
    - Di tahun 2000, hacker berhasil mengakses database perusahaan Amerika yang

bergerak di bidang e-commerce dan memiliki tingkat kerahasiaan yang tinggi.
- Tahun 2004, situs Komisi Pemilihan Umum (KPU) berhasil diretas oleh hacker meskipun memiliki sistem keamanan yang sangat ketat.

b. Konten Ilegal, yaitu kejahatan yang terjadi dengan memasukkan data atau informasi ke dalam internet mengenai sesuatu yang salah, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh dari ini adalah:
   - Penyebaran berita palsu atau fitnah yang dapat merusak reputasi atau harga diri orang lain.
   - Penyebaran hal-hal yang berkaitan dengan pornografi.
   - Penyampaian informasi yang bersifat rahasia negara, agitasi, dan propaganda yang ditujukan untuk melawan pemerintah yang sah, dan sebagainya.

c. Pemalsuan Data, yaitu tindakan kriminal di mana data pada dokumen penting yang disimpan sebagai dokumen tanpa skrip di internet dipalsukan. Kejahatan ini biasanya menyasar dokumen di bidang e-commerce dengan menciptakan ilusi adanya "kesalahan pengetikan" yang dapat menguntungkan pelaku.

d. Spionase Siber, yaitu tindakan kejahatan yang menggunakan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara mengakses sistem jaringan komputer target. Kejahatan ini sering kali ditujukan kepada perusahaan pesaing yang menyimpan dokumen atau data penting di sistem komputer mereka. (Winarti, 2016)

B. Analisis pasal penting mengenai penerapan undang-undang ITE terkait kejahatan siber (pasal 27-37) Dan Contoh kasus nyata dan penerapan hukum

Berikut adalah berbagai tindakan kejahatan siber yang diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan dari Undang-Undang No. 11 Tahun 2008 terkait informasi dan transaksi elektronik, yaitu:

a. Tindakan yang melanggar norma kesopanan.

Dalam Pasal 27 ayat (1) Undang-Undang No. 11 Tahun 2008 dinyatakan bahwa “Setiap individu dengan sengaja dan tanpa hak menyebarluaskan atau membagikan, maupun membuat informasi elektronik atau dokumen elektronik yang mengandung konten yang melanggar norma kesusilaan”. Namun, penjelasan lebih lanjut terkait penyebaran konten yang melanggar kesopanan tidak terdapat secara eksplisit dalam Undang-Undang No. 11 Tahun 2008. Pelanggaran norma kesusilaan melalui internet mengacu pada Kitab Undang-Undang Hukum Pidana (KUHP).

a. Perjudian

Perjudian secara daring diatur dalam Pasal 27 ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Dalam ketentuan ini dijelaskan bahwa: “Setiap individu dengan sengaja dan tanpa hak menyebarkan atau membagikan, maupun membuat informasi elektronik atau dokumen elektronik yang mengandung unsur perjudian. ”

b. Pencemaran nama baik atau penghinaan

Pencemaran nama baik atau penghinaan di ranah daring adalah larangan yang tertuang dalam Pasal 27 ayat (3) Undang-Undang No. 11 Tahun 2008, yang menyatakan: “Setiap individu dengan sengaja, dan tanpa hak menyebarluaskan atau membagikan, maupun membuat dapat diakses informasi elektronik atau dokumen elektronik yang mengandung unsur penghinaan atau pencemaran nama baik. ” Para pembuat undang-undang menyamakan konsep penghinaan dan pencemaran nama baik. Penghinaan merupakan sebuah tindakan, sedangkan salah satu bentuk dari penghinaan adalah pencemaran. Sepertinya, para pembuat undang-undang ingin mengarahkan tindakan penghinaan yang dilakukan di media internet ini untuk dianggap sebagai pencemaran. Dalam Bab XVI Buku II diatur mengenai perbuatan penghinaan dan pencemaran.

c. Pemerasan atau pengancaman

Pada Pasal 27 ayat (4) Undang-undang No. 11 Tahun 2008 terdapat larangan mengenai tindakan pemerasan atau ancaman di ruang digital. Dalam pasal tersebut dijelaskan: "Setiap individu yang secara sengaja dan tanpa izin menyebarluaskan dan/atau mengirimkan dan/atau membuat akses terhadap informasi atau dokumen elektronik yang mengandung unsur pemerasan atau ancaman".

d. Penguntitan (cyberstalking)

Undang-undang No. 11 Tahun 2008 Pasal 29 menetapkan bahwa: "Setiap orang yang dengan sengaja dan tanpa hak mengirimkan informasi atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti secara pribadi". Ketentuan mengenai informasi dan transaksi elektronik dalam Pasal 29 membahas perilaku pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan rasa takut, termasuk kata-kata atau tindakan tertentu. Aturan ini serupa dengan pengaturan terkait cyberstalking di Amerika Serikat, Kanada, Inggris, dan negara lain. Tindakan ini dilakukan dengan menggunakan teknologi informasi dan komunikasi, seperti melalui mail bombs, surat kebencian yang tidak diminta, email yang cabul atau mengancam, dan lain-lain.

e. Penyebaran berita palsu (hoax)

Penyebaran informasi palsu diatur dalam Undang-undang No. 11/2008 Pasal 28 ayat (1), yang berbunyi: "Setiap orang dengan sengaja dan tanpa izin menyebarkan berita yang tidak benar dan menyesatkan, yang berdampak negatif terhadap konsumen dalam transaksi elektronik. "

f. Ujaran kebencian

Pasal 28 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentang tindakan pidana ini, yang menyatakan: "Setiap orang yang dengan sengaja dan tanpa izin menyebarkan informasi yang dibuat untuk menimbulkan kebencian atau permusuhan terhadap individu atau kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA)".

g. Akses ilegal

Undang-undang No. 11 Tahun 2008, dalam Pasal 30 mengatur hal-hal berikut:

- Setiap individu yang dengan sengaja, tanpa izin atau secara ilegal mengakses komputer atau sistem elektronik milik orang lain dengan cara apapun.
- Setiap individu yang secara sengaja, tanpa izin atau ilegal mengakses (membuka) komputer atau sistem elektronik dengan tujuan untuk mendapatkan informasi elektronik atau dokumen elektronik.
- Setiap individu yang melanggar, menerobos, melampaui, atau merusak sistem pengamanan dengan sengaja, tanpa izin atau secara ilegal mengakses komputer atau sistem elektronik" (Liviani & Habibi-isnatul, 2020)

C. Penerapan UU ITE

Penerapan Undang-Undang ITE dapat dilihat dari segi isi dan struktur hukumnya, termasuk penegak hukum, sumber daya yang ada pada aparat penegak hukum, partisipasi masyarakat dalam penegakan hukum, serta perlunya dukungan dari sarana dan prasarana agar penegakan hukum dapat terwujud. Secara terang-terangan, di zaman globalisasi ini kita menikmati kemudahan dan keuntungan besar yang dihasilkan dari perpaduan antara telekomunikasi, informasi, dan komputer, yang sering disebut sebagai revolusi teknologi informasi. Salah satu hasil dari perpaduan itu adalah aktivitas di dunia maya yang memiliki dampak luas pada berbagai aspek kehidupan dan berpotensi menimbulkan berbagai masalah hukum. Hal ini terlihat dari adanya penyalahgunaan dalam berbagai aktivitas teknologi informasi, yang menunjukkan bahwa teknologi informasi sering dipakai sebagai alat untuk melakukan tindakan kriminal, atau sebaliknya. Individu yang menggunakan teknologi informasi menjadi target, contohnya adalah data yang tersimpan dalam CPU, di mana data

ini sangat rentan untuk dimodifikasi, disadap, dipalsukan, dan dikirimkan ke berbagai negara dalam waktu singkat, dengan dampak yang sangat besar. Perkembangan teknologi informasi tidak memberikan manfaat optimal bagi masyarakat. Teknologi digital memberikan peluang untuk penyalahgunaan informasi dengan mudah, sehingga isu keamanan sistem informasi menjadi sangat krusial.

D. Kewenangan APH

a. Pengadilan

Pengadilan sebagai lembaga resmi negara memiliki tanggung jawab untuk melakukan analisis, memberikan keadilan melalui pengadilan, mengeluarkan keputusan, dan menyelesaikan semua perkara atau masalah yang dihadapkan oleh masyarakat. Proses penyelesaian perkara di pengadilan dapat berjalan dengan baik apabila semua pihak yang terlibat, termasuk hakim, mengikuti tata cara yang berlaku dengan jujur dan sesuai dengan hukum yang ada.

b. Kejaksaan

Kejaksaan memiliki peran penting sebagai institusi penegak hukum dalam sistem peradilan pidana di Indonesia. Tugas utamanya adalah melakukan penuntutan dan sebaliknya. Penuntutan merupakan hak eksklusif yang hanya dimiliki oleh kejaksaan dan tidak dimiliki oleh lembaga penegak hukum lainnya. Dalam menjalankan fungsi, tugas, dan wewenangnya, kejaksaan bebas dari segala bentuk intervensi kekuasaan pemerintah maupun pengaruh lainnya. Negara memberikan perlindungan kepada jaksa dalam menjalankan profesinya tanpa adanya ancaman, gangguan, bujukan, atau campur tangan yang tidak sesuai, serta tanpa tekanan terkait hal-hal yang belum terbukti kebenarannya, baik dalam aspek perdata maupun pidana.

c. Kepolisian

Kepolisian adalah salah satu bagian dari aparat penegak hukum. Tugas kepolisian adalah menjaga keamanan dan ketertiban masyarakat, menegakkan hukum, serta memberikan perlindungan, bantuan, dan pelayanan kepada masyarakat. Semua ketentuan mengenai fungsi kepolisian diatur dalam Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Peraturan tersebut menjelaskan bahwa salah satu tugas kepolisian adalah melaksanakan fungsi pemerintahan negara yang memberikan perlindungan, menciptakan atau menjaga ketertiban, memberikan pelayanan dan perlindungan kepada masyarakat, serta melakukan penegakan hukum. Hal ini dijelaskan secara gamblang dalam Pasal 14 ayat (1) Undang-Undang Kepolisian

KESIMPULAN

Kejahatan siber atau cybercrime merupakan fenomena hukum yang berkembang seiring dengan kemajuan teknologi informasi. Meskipun membawa banyak manfaat, digitalisasi juga menghadirkan tantangan baru bagi sistem hukum Indonesia. Bentuk kejahatan siber semakin beragam, mulai dari peretasan, pencurian data pribadi, penyebaran konten ilegal, hingga penipuan daring. Kejahatan ini tidak hanya menimbulkan kerugian ekonomi, tetapi juga berdampak pada stabilitas sosial dan kepercayaan publik terhadap sistem digital. Pemerintah Indonesia telah berupaya menanggulangi masalah ini melalui pengesahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta revisinya pada UU Nomor 19 Tahun 2016. UU ITE berfungsi sebagai dasar hukum untuk mengatur aktivitas di dunia maya dan menindak pelaku kejahatan siber. Namun, efektivitas UU ini masih menghadapi beberapa hambatan, terutama dalam hal multitafsir pasal, ketimpangan penerapan, dan keterbatasan kemampuan aparat dalam memahami bukti digital. Beberapa kasus besar seperti peretasan oleh kebocoran data lembaga pemerintah menunjukkan bahwa sistem keamanan digital nasional masih lemah. Di sisi lain, masyarakat juga belum sepenuhnya memahami pentingnya menjaga privasi dan

keamanan data pribadi. Hal ini menandakan perlunya sinergi antara pemerintah, aparat penegak hukum, dan masyarakat untuk membangun kesadaran hukum digital yang lebih kuat.

Ucapan Terimasih

"Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga jurnal berjudul "Analisis Kasus Cyber Crime dalam Pendekatan Undang-Undang ITE" dapat diselesaikan dengan baik. Penulis mengucapkan terima kasih kepada dosen pembimbing, rekan-rekan, serta semua pihak yang telah memberikan dukungan, arahan, dan bantuan selama proses penyusunan jurnal ini. Semoga karya ini dapat memberikan manfaat dan menambah wawasan bagi pembaca."

DAFTAR PUSTAKA

Achmad Allang S, H., & Abu, H. N. (2022). "TINJAUAN YURIDIS TERHADAP CYBER CRIME". 4-5.

Aditama, P., Sinaga, E. A., & Dkk. (2025). perbandingan hukum pidana cyber crime dan pengaruhnya dalam penangana hukum anatara indonesia dan amerika. Jurnal Kompilasi Hukum, 65-69.

Dirjosisworo, & Soedjono. (2022). Respon terhadap kejahatan, introduksi hukum penangulanggan kejahatan(introducti to the of crime prevention).

Djanggih, H., & Qamar, N. (2018). penerapan teori-teori keriminologi dan penanggulangan kejahatan sibe(cyber crime). 12-15.

G.Gani, & Alcianno. (2020). kejahatan berbasis komputer.

Laksana, & Wijaya, A. (2019). pemindaan cyber crime dalam prespektif hukum pidana positif. Jurnal Hukum UNISSULA, 54-55.

Liviani, & Habibi-isnatul, M. R. (2020). kejahatan teknologi dan informasi cyber crime dan penanggulangannya dalam sistem hukum indonesia. Jurnal Pemikiran Dan Pembaharuan Hukum Islam, 414-415.

Pansariadi, R. S., & Soekorini, N. (2023). Tindakan Pidana Cyber Crime dan Penegakan Hukumnya. 292.

Quintarti, & Liza, M. A. (2024). The Role of Criminal Law in Handling Cyber Crimes: Challenges and solutions.

Riani, Firmansyah, & Dkk. (2023). Konstruksi Hukum Dalam Cybercrime Pelaku Kejahatan Teknologi Informasi. Jurnal Hukum Tata Negara, 227.

Situmeng, & Tua, S. M. (2021). penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam presfektif hukum pidana. Jurnal Terakreditasi Hukum, 38-39.

Suhaili, A. (2022, September 16). Marak Kejahatan Siber, Polri Akan Kembangaka Struktur Ditsiber Di Polda. Retrieved from www.polri.go.id.

Tua, S. M., & Situmeang. (2020). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. Jurnal Terakreditasi Nasional, 47-48.

Winarti, R. R. (2016). EFEKTIVITAS PENERPAN UNDANG-UNDANG ITE DALAM TINDAK PIDANA CYBER CRIME. HUKUM DAN DINAMIKA MASYARAKAT, 19-20.