BAB I
PENDAHULUAN

A. Latar Belakang Penelitian

Transformasi dalam bidang sosial dan kehidupan secara keseluruhan telah membentuk pola pikir manusia. Kemajuan signifikan dalam ilmu pengetahuan dan teknologi telah mentransformasikan metode konvensional menjadi modern, baik dalam cara berpikir maupun dalam interaksi sosial. Arus globalisasi yang cepat membawa pengaruh besar dan manfaat yang luar biasa, seolah tanpa batas. Dalam konteks perkembangan industri dan sosial ini, hukum harus mampu beradaptasi dan menerima kemajuan teknologi informasi, meskipun sering kali mengalami kesulitan untuk mengimbangi kecepatannya. Menurut Satjipto Rahardjo, "Hukum ada untuk memanusiakan, bukan manusia yang harus menyesuaikan dengan hukum."[1] Dengan kata lain, manusia tidak harus dipaksa menyesuaikan diri dengan hukum jika hukum tersebut sudah tidak relevan, melainkan hukum yang harus disesuaikan dengan perkembangan kebutuhan manusia.

Peran teknologi informasi sangat penting, teknologi ini dianggap sebagai katalis utama bagi kemajuan global, terutama dalam sektor ekonomi, didukung oleh dua aspek utama. Pertama, teknologi informasi meningkatkan permintaan untuk perangkat dan solusi teknologinya sendiri, seperti infrastruktur jaringan internet. Kedua, teknologi ini memfasilitasi pelaksanaan transaksi bisnis, khususnya dalam sektor perbankan dan bidang komersial lainnya. Implementasi teknologi informasi sangat penting dalam perdagangan dan pertumbuhan ekonomi nasional, yang pada gilirannya membantu meningkatkan kesejahteraan masyarakat. Pemerintah harus berperan aktif dalam mendukung teknologi ini, termasuk penyediaan infrastruktur hukum dan regulasi yang memastikan penggunaannya secara efektif dan aman, serta meminimalisir

[1] Satjipto Rahardjo, *Penegakan Hukum Progresif* (Kompas, 2010). Hlm 31

penyalahgunaan yang bertentangan dengan nilai-nilai agama dan budaya masyarakat Indonesia.

Era globalisasi membawa perubahan besar dalam teknologi informasi, tidak hanya mempercepat perkembangan teknologi tetapi juga mengubah perilaku sosial secara global. Pentingnya teknologi informasi terlihat dalam kemampuannya menghapus batasan ruang, waktu, dan jarak. Pertumbuhan internet yang signifikan dan mudah diakses telah membawa pengaruh besar bagi semua lapisan masyarakat. Meskipun memberi banyak manfaat, teknologi informasi juga memiliki sisi negatif, seperti meningkatnya potensi tindakan melanggar hukum.

Indonesia rentan terhadap serangan siber dari luar negeri, baik dari negara-negara yang bersaing secara geopolitik maupun dari kelompok kriminal transnasional. Jika Indonesia tidak mampu melindungi diri dari *cracking*, ada potensi bahwa negara bisa dimanfaatkan oleh pihak eksternal untuk tujuan yang lebih besar, seperti spionase, pencurian kekayaan intelektual, atau bahkan penyerangan siber terkoordinasi terhadap aliansi internasional yang lebih besar. Di Indonesia, isu *cybercrime* atau kejahatan siber diatur secara khusus dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diperbaharui oleh Undang-Undang No. 1 Tahun 2024. Undang-undang ini mencakup berbagai bentuk kejahatan siber, termasuk *cracking*. *Cracking* adalah tindakan ilegal yang bertujuan merusak sistem untuk kepentingan pribadi, yang diatur dalam undang-undang tersebut.[2] Pelaku *cracking* sering kali merusak sistem pengamanan untuk mencapai tujuan mereka, yang bisa meliputi pencarian keuntungan pribadi. *Cracker* menargetkan teknologi informasi (TI) untuk melakukan tindakan ilegal demi keuntungan materiil atau tujuan spesifik lainnya. *Cracking* adalah akses ilegal ke komputer, sistem elektronik, atau situs web milik individu, bisnis, bahkan pemerintah, dengan motif tertentu. Kejahatan ini sering

[2] Christiara Febriliani and Diana Lukitasari., "Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta.," *Hukum Pidana Dan Penanggulangan Kejahatan 8, No. 3* , 2019, 219–26.

menimbulkan kerugian finansial dan non-finansial yang signifikan.[3] *Cracker* biasanya menemukan dan mengeksploitasi celah keamanan dalam sistem atau jaringan situs web, menyebabkan gangguan operasional, pengurangan kepercayaan publik, dan biaya perawatan atau perbaikan yang tinggi.

Hacking dan *cracking* adalah dua istilah yang sering digunakan dalam dunia keamanan siber, tetapi memiliki perbedaan mendasar dalam motivasi, metode, dan legalitasnya. Secara umum, *hacking* adalah kegiatan mengakses sistem komputer atau jaringan dengan tujuan tertentu, yang bisa bersifat legal maupun ilegal, tergantung pada niat dan izin yang dimiliki oleh pelaku. Sementara itu, *cracking* adalah bentuk peretasan yang bersifat ilegal, di mana seorang *cracker* sengaja menembus sistem keamanan untuk tujuan merusak, mencuri, atau menyalahgunakan data tanpa izin.[4] Dalam dunia keamanan siber, hacker terbagi menjadi beberapa kategori, yaitu *white hat hackers* (*hacker etis*), *black hat hackers* (*hacker jahat*), dan grey hat hackers (*hacker di antara keduanya*).[5] *White hat hackers* biasanya bekerja sebagai profesional keamanan siber yang membantu organisasi dalam mengamankan sistem mereka melalui *penetration testing* (uji penetrasi). Sebaliknya, *black hat hackers* bertindak sebagai peretas ilegal yang memanfaatkan kelemahan sistem untuk keuntungan pribadi, seperti mencuri informasi sensitif atau melakukan serangan siber. *Grey hat hackers* berada di antara keduanya karena mereka dapat membobol sistem tanpa izin tetapi tidak selalu memiliki niat jahat, sering kali untuk mengungkap celah keamanan. Di sisi lain, *cracking* lebih berorientasi pada eksploitasi sistem untuk kepentingan pribadi atau kelompok tertentu, biasanya tanpa memperhatikan etika atau dampak hukum. *Cracker* sering kali menggunakan metode seperti *brute-force attacks*, *keylogging*, *reverse engineering*, dan *exploit kits* untuk membobol sistem keamanan.

---

[3] Anggrawan et al., Teori Dan Penerapan Komputer Masyarakat Era Industri 4.0 Dan Society 5.0. (PT. Sonpedia Publishing Indonesia, 2023). Hlm 69

[4] Vivi Kumalasari, *ETIKA PROFESI Dalam Bidang Teknologi Informasi* (YAYASAN PRIMA AGUS TEKNIK, 2021). Hlm 56

[5] Sultan Hajji Nst, "HACKER DALAM PERSPEKTIF AL-QUR'AN" (UNIVERSITAS PTIQ JAKARTA, 2023). Hlm 66

Beberapa bentuk *cracking* yang umum meliputi *cracking* perangkat lunak (*software cracking*), pembobolan password (*password cracking*), dan akses ilegal ke sistem komputer atau jaringan perusahaan.

Dari segi legalitas, *hacking* bisa menjadi tindakan yang sah atau tidak sah, tergantung pada apakah *hacker* memiliki izin untuk mengakses sistem tersebut.[6] Misalnya, perusahaan sering kali mempekerjakan ethical hackers untuk menguji kerentanan sistem mereka dan meningkatkan keamanan jaringan. Sebaliknya, *cracking* selalu bersifat ilegal karena melibatkan akses tanpa izin, pencurian data, atau perusakan sistem, yang dapat dikenai hukuman pidana berdasarkan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia serta berbagai regulasi keamanan siber di tingkat global. Perbedaan lain antara *hacking* dan *cracking* dapat dilihat dari tujuan akhir yang ingin dicapai. Seorang *hacker* biasanya berusaha memahami sistem dan meningkatkan keamanannya, sementara seorang *cracker* memiliki tujuan untuk mengeksploitasi kelemahan sistem demi keuntungan pribadi, seperti pencurian data, sabotase, atau spionase siber. Oleh karena itu, *hacking* dapat dianggap sebagai keahlian teknis yang dapat digunakan untuk kepentingan positif, sedangkan *cracking* lebih sering dikaitkan dengan aktivitas kriminal di dunia maya.[7] Dengan demikian, meskipun kedua istilah ini sering digunakan secara bergantian oleh masyarakat awam, *hacking* dan *cracking* memiliki perbedaan signifikan dalam motivasi, metode, dan dampaknya terhadap keamanan siber. *Hacking* dapat digunakan untuk melindungi dan memperkuat keamanan sistem, sedangkan *cracking* lebih banyak digunakan untuk tujuan ilegal yang dapat merugikan individu, organisasi, atau negara. Oleh karena itu, pemahaman yang jelas tentang perbedaan keduanya sangat penting, terutama dalam konteks hukum dan regulasi keamanan siber di era digital saat ini.

Data dari Badan Siber dan Sandi Negara (BSSN) mengonfirmasi eskalasi ancaman ini; sepanjang tahun 2023 saja tercatat lebih dari 403 juta anomali trafik yang

[6] Putra et al., *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking* (NEM, 2023). Hlm 32
[7] Indah Sari, "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya," *JSI (Jurnal Sistem Informasi) Universitas Suryadarma 10, No. 2*, 2023. Hlm 33

berpotensi serangan, dengan lebih dari satu juta di antaranya teridentifikasi sebagai aktivitas *ransomware* yang destruktif, sebuah kejahatan yang selalu diawali dengan tindak pidana *cracking* untuk mendapatkan akses ilegal. Angka ini meningkat 40% dibanding tahun sebelumnya, menunjukkan bahwa *cracking* bukan sekadar kejahatan individu, tetapi telah menjadi ancaman besar yang membutuhkan perhatian serius dari sistem hukum di Indonesia. Sementara itu, data dari Kementerian Komunikasi dan Informatika (Kominfo) 2023 mencatat bahwa terdapat lebih dari 11.000 kasus kejahatan siber, dengan akses ilegal (*cracking*), pencurian data (*phishing*), dan serangan *ransomware* sebagai kasus terbanyak. *Interpol's ASEAN Cybercrime Assessment Report* 2023 juga menempatkan Indonesia dalam 5 besar negara ASEAN yang paling sering menjadi target serangan siber, terutama terhadap lembaga keuangan dan pemerintahan. Skala ancaman siber di Indonesia telah mencapai tingkat yang mengkhawatirkan, menjadikannya isu keamanan nasional yang mendesak. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan gambaran lanskap ancaman yang masif. Sepanjang tahun 2023 saja, BSSN mencatat adanya 403.990.813 anomali lalu lintas internet yang berpotensi serangan. Angka ini mencakup berbagai jenis aktivitas berbahaya, termasuk lebih dari satu juta aktivitas ransomware dan empat juta aktivitas Advanced Persistent Threat (APT), yang seringkali diawali dengan teknik cracking untuk infiltrasi awal. Tingginya volume anomali ini mengindikasikan bahwa ruang siber Indonesia secara konstan berada di bawah kepungan serangan yang mencoba mencari dan mengeksploitasi celah keamanan. Ancaman tersebut bukan lagi sekadar angka statistik, melainkan telah bermanifestasi menjadi insiden-insiden nyata dengan dampak yang melumpuhkan. Laporan BSSN tahun 2024 mengidentifikasi 5.780 kasus *web defacement* (peretasan dengan mengubah tampilan situs), di mana 4.071 di antaranya menargetkan situs pemerintah yang seharusnya menjadi benteng pertahanan data publik. Lebih jauh lagi, insiden serangan ransomware terhadap Pusat Data Nasional (PDN) pada Juni 2024 menjadi bukti paling nyata dari kerentanan infrastruktur digital vital di Indonesia. Serangan ini tidak hanya mengganggu lebih dari 282 instansi pemerintah dan layanan publik, tetapi juga diproyeksikan menimbulkan

kerugian ekonomi hingga Rp 1 Triliun per hari selama masa pemulihan. Kasus PDN secara gamblang menunjukkan bagaimana tindak pidana cracking dapat berevolusi dari sekadar akses ilegal menjadi ancaman yang melumpuhkan kedaulatan data dan stabilitas pelayanan negara. Menurut Badan Siber dan Sandi Negara (BSSN) 2023, Indonesia

Indonesia sesungguhnya telah memiliki landasan hukum untuk menghadapi tindak pidana *cracking*. Pengesahan Undang-Undang Informasi dan Transaksi Elektronik, khususnya Pasal 30 yang mengkriminalisasi akses ilegal, dirancang sebagai respons legislatif untuk melindungi ruang siber. Kerangka ini, yang berjalan di atas hukum acara pidana dalam KUHAP, secara ideal seharusnya mampu memberikan landasan yang kokoh bagi aparat penegak hukum untuk melakukan investigasi, pembuktian, dan penuntutan terhadap pelaku cracking. Dengan demikian, hukum positif Indonesia menghendaki terciptanya sebuah sistem peradilan pidana yang efektif dalam memberikan perlindungan kepada korban dan menjamin keamanan transaksi digital bagi masyarakat. Namun, realitas di lapangan (*das Sein*) menunjukkan gambaran yang jauh dari kondisi ideal tersebut. Data dari Badan Siber dan Sandi Negara (BSSN) mengonfirmasi bahwa Indonesia berada dalam kepungan ancaman siber yang masif, dengan 403 juta anomali trafik tercatat sepanjang 2023. Ancaman ini telah bermanifestasi menjadi insiden nyata yang merugikan kepentingan nasional, seperti lumpuhnya layanan publik akibat serangan *ransomware* terhadap Pusat Data Nasional (PDN) pada Juni 2024. Di tingkat penyidikan, aparat penegak hukum dihadapkan pada tantangan berat berupa anonimitas pelaku yang bersembunyi di balik teknologi VPN, yurisdiksi kejahatan yang melintasi batas negara, serta sifat bukti digital yang mudah dimanipulasi dan dihapus.

Cracking memiliki dampak signifikan terhadap keamanan negara, di Indonesia tindakan ini dapat menargetkan institusi vital seperti lembaga militer, kepolisian, dan pemerintahan, yang menyimpan data penting terkait pertahanan dan keamanan negara.[8]

[8] Vitadiar, *Etika & Hukum Cyber.* (CV. AE MEDIA GRAFIKA, 2021). Hlm 21

Kebocoran informasi sensitif, seperti data intelijen atau strategi militer, bisa berdampak buruk bagi keamanan nasional, karena bisa digunakan oleh pihak asing atau organisasi kriminal untuk melakukan sabotase atau bahkan memicu konflik. *Cracking* juga dapat menyebabkan gangguan besar pada infrastruktur penting seperti sistem transportasi, energi, dan komunikasi. Serangan terhadap jaringan listrik, misalnya, dapat melumpuhkan aktivitas ekonomi dan sosial, sementara serangan pada sistem telekomunikasi dapat memutuskan jalur komunikasi penting yang dibutuhkan oleh pemerintah dan masyarakat. Infrastruktur ini sangat rentan, dan tindakan *cracking* yang menargetkan sistem-sistem tersebut dapat menimbulkan kerugian besar dan berpotensi menyebabkan kekacauan, dalam ranah politik, tindak pidana *cracking* dapat mempengaruhi stabilitas negara ketika *hacker* meretas situs-situs pemerintah atau mencuri data pejabat tinggi, informasi yang diperoleh bisa digunakan untuk kampanye disinformasi atau propaganda. Ini dapat menciptakan ketidakpercayaan masyarakat terhadap pemerintah, meningkatkan tensi politik, dan memperburuk kondisi stabilitas dalam negeri. Selain itu, *cracking* terhadap sistem pemilihan umum dapat merusak integritas proses demokrasi, menimbulkan kecurangan dan memengaruhi hasil pemilu.

Serangan *cracking* terhadap lembaga-lembaga negara atau perusahaan-perusahaan besar dapat merusak kepercayaan masyarakat. Jika publik merasa bahwa data pribadi mereka tidak aman atau jika mereka melihat bahwa sistem pemerintahan tidak dapat melindungi informasi sensitif, rasa percaya mereka terhadap institusi publik akan menurun. Krisis kepercayaan ini bisa mempengaruhi legitimasi pemerintah dalam jangka panjang. Dampak *cracking* pada ekonomi sangat signifikan, terutama ketika serangan diarahkan pada sektor keuangan atau perusahaan-perusahaan besar. Data dari bank, perusahaan investasi, atau pasar saham bisa dieksploitasi untuk mencuri uang atau mengubah transaksi keuangan. Kejahatan *cracking* dapat menyebabkan perusahaan kehilangan pendapatan akibat serangan terhadap sistem mereka. Sistem yang diretas bisa menyebabkan operasi terhenti atau layanan penting terganggu, yang

pada akhirnya merugikan perusahaan secara finansial.[9] Selain itu, biaya untuk memperbaiki kerusakan dan memperkuat keamanan sistem juga dapat sangat mahal, dan sering kali perusahaan harus menghadapi tuntutan hukum dari pelanggan yang terkena dampaknya dan mengguncang kepercayaan investor internasional terhadap stabilitas ekonomi Indonesia.

Industri teknologi di Indonesia juga bisa mengalami dampak serius akibat *cracking*. Perusahaan teknologi yang menjadi korban serangan *cracking* mungkin kehilangan data penting terkait inovasi atau riset yang sedang dilakukan. Hal ini dapat menghambat perkembangan industri teknologi nasional, karena perusahaan mungkin enggan berinvestasi lebih jauh dalam inovasi teknologi jika keamanan data mereka tidak terjamin. Keamanan siber yang lemah dapat membuat Indonesia kurang menarik bagi investor asing. Jika perusahaan-perusahaan besar khawatir tentang potensi serangan *cracking*, mereka mungkin enggan menanamkan modal di Indonesia. Ini bisa memperlambat laju pertumbuhan ekonomi, khususnya dalam sektor teknologi dan industri yang berbasis data. Selain mencuri data finansial, *cracking* juga sering kali melibatkan pencurian kekayaan intelektual. Di sektor bisnis, pelaku *cracking* dapat meretas sistem perusahaan untuk mencuri ide, paten, atau teknologi yang sedang dikembangkan. Ini merugikan perusahaan dari segi inovasi dan bisa melemahkan daya saing perusahaan Indonesia di pasar global.

Perusahaan rintisan (*startup*) dan Usaha Mikro, Kecil, dan Menengah (UMKM) juga rentan terhadap serangan *cracking*. Kebanyakan dari mereka tidak memiliki sistem keamanan siber yang canggih, sehingga mudah menjadi sasaran. Serangan terhadap mereka dapat menyebabkan kebangkrutan, terutama jika data penting mereka dicuri atau jika serangan tersebut menghancurkan reputasi mereka di pasar. *Cracking* juga memperburuk kesenjangan digital di Indonesia. Negara-negara dengan infrastruktur teknologi yang lebih kuat mampu melindungi diri dari serangan siber lebih baik dibanding negara-negara berkembang. Di Indonesia, kesenjangan ini bisa

[9] Rio Christiawan, *Aspek Hukum Startup* (Sinar Grafika, 2022). Hlm 43

semakin lebar antara perusahaan-perusahaan yang mampu berinvestasi dalam keamanan siber dan yang tidak.

Menyadari bahaya yang ditimbulkan oleh *Cracker*, pemerintah telah mengesahkan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang ini dirancang untuk menangani kejahatan dunia maya, termasuk *cracking*. Pasal 30 secara khusus mengatur tentang akses ilegal, di mana *cracking* dikategorikan sebagai tindakan ilegal untuk meretas sistem elektronik milik orang lain dengan tujuan memperoleh keuntungan dari tindakan tersebut. *Cracking* tidak hanya dianggap sebagai pelanggaran akses tetapi juga berhubungan dengan pencurian, karena pelaku berusaha mengakses dan mengambil konten dari sistem elektronik yang diretas.[10]

Fenomena *Cracker* dan aktivitas *cracking* telah menjadi perhatian yang meningkat dalam beberapa tahun terakhir, dalam rentang waktu tahun 2020 hingga tahun 2024, Indonesia mengalami beberapa kasus *cracking* yang signifikan, mencerminkan tantangan serius dalam keamanan siber nasional. Meski Indonesia terbilang lambat dalam mengadopsi teknologi informasi, negara ini juga telah menjadi korban dari kejahatan *cracking*. Contoh kasus *cracking* di Indonesia kasus serangan siber pada Pusat Data Nasional, pada bulan juni tahun 2024, Pusat Data Nasional Indonesia menjadi target serangan siber yang mempengaruhi lebih dari 200 lembaga pemerintah, kelompok peretas menuntut tebusan sebesar Rp131 miliar (sekitar $8 juta). Serangan ini menunjukkan ancaman serius terhadap infrastruktur digital pemerintah dan kebutuhan mendesak untuk meningkatkan keamanan siber nasional. Kemudian pencurian data nasabah dari peretasan data Bank Jago pada tahun 2023 dimana ribuan data nasabah Bank Jago bocor dan diperjualbelikan di dark web kemudian pelaku *cracking* menggunakan teknik *SQL Injection* untuk mengakses data tanpa izin yang mengakibatkan, nasabah mengalami kebocoran data pribadi, kehilangan akses ke akun

[10] Tomi Wicaksono Putra and Abdurrachman Hamidah, *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking* (NEM, 2023). Hlm 59

perbankan, dan kerugian finansial. Selain itu, serangan *ransomware* pada Rumah Sakit Dharmais dan Rumah Sakit Harapan Kita pada tahun 2022 terjadi karena sistem komputer rumah sakit lumpuh karena serangan *cracking* menggunakan *ransomware* mengakibatkan data medis pasien terkunci dan hanya bisa dibuka dengan tebusan puluhan juta rupiah namun, pelaku tidak berhasil diidentifikasi karena menggunakan IP Address luar negeri dan sistem enkripsi canggih sehingga dari kasus Kasus ini menunjukkan kesulitan dalam pembuktian tindak pidana *cracking*, karena bukti digital mudah dihapus atau disamarkan. Pada bulan mei tahun 2021, situs resmi Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan diretas, mengakibatkan kebocoran data 279 juta penduduk Indonesia. Data yang bocor mencakup NIK, nomor ponsel, email, alamat, hingga gaji, dan dijual di forum online oleh pelaku dengan nama samaran "Kotz" seharga 0,15 Bitcoin (sekitar Rp84,4 juta saat itu). Kasus ini menyoroti kerentanan data sensitif di lembaga pemerintah.

Data nasional yang dipaparkan sebelumnya, baik dari Badan Siber dan Sandi Negara (BSSN) maupun Kominfo, telah secara gamblang menunjukkan bahwa Indonesia berada dalam status darurat keamanan siber . Insiden-insiden berskala besar seperti lumpuhnya Pusat Data Nasional (PDN) pada tahun 2024 dan kebocoran data masif BPJS Kesehatan pada tahun 2021 mengonfirmasi bahwa cracking bukan lagi ancaman teoritis. Ia telah menjadi realitas destruktif yang mengancam infrastruktur vital negara dan kedaulatan data kependudukan.

Eskalasi ancaman pada level makro (nasional) tersebut secara logis terefleksi pada level mikro di berbagai yurisdiksi kepolisian daerah. Sebagai negara dengan tingkat urbanisasi dan penetrasi internet yang sangat tinggi, provinsi-provinsi besar di Indonesia secara otomatis menjadi episentrum dari aktivitas kejahatan siber, sekaligus menjadi medan pertempuran utama bagi aparat penegak hukum di lapangan. Dalam konteks ini, Provinsi Jawa Barat menjadi sangat relevan untuk dikaji. Sebagai provinsi dengan jumlah penduduk terbanyak di Indonesia dan salah satu motor penggerak ekonomi digital serta industri nasional, Jawa Barat menghadirkan lanskap yang sangat rentan. Tingginya volume transaksi elektronik, aktivitas media sosial, dan penggunaan

layanan digital di wilayah ini berbanding lurus dengan peningkatan risiko dan insiden kejahatan siber.

Kondisi ini menempatkan Kepolisian Daerah (Polda) Jawa Barat sebagai salah satu unit kepolisian yang berada di garis depan dalam menghadapi ancaman cracking. Fenomena inilah yang menjadi fokus utama penelitian. Berdasarkan studi pendahuluan, ditemukan bahwa wilayah hukum Polda Jawa Barat telah menangani berbagai modus operandi tindak pidana cracking yang kompleks dan terus berevolusi, yang menunjukkan urgensi untuk memahami bagaimana aparat merespons tantangan ini secara praktis.

Sebagai contoh nyata, pada tahun 2020, Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Jabar berhasil mengungkap sindikat kejahatan siber transnasional dengan modus pembobolan kartu kredit (*carding*) . Kasus ini mengonfirmasi bahwa cracking dengan motif ekonomi yang terorganisir telah beroperasi di wilayah ini, menyasar kerugian finansial yang signifikan dan menunjukkan kompleksitas jaringan pelaku yang dihadapi penyidik. Ancaman tidak hanya datang dari motif finansial. Pada tahun yang sama, layanan publik vital di Jawa Barat juga menjadi sasaran ketika situs resmi Penerimaan Peserta Didik Baru (PPDB) mengalami peretasan (*deface*) . Insiden ini membuktikan bahwa cracking juga digunakan untuk mengganggu stabilitas layanan pemerintah dan menciptakan kerugian imateriel yang besar, yaitu rusaknya kepercayaan publik terhadap sistem digital pemerintah dan lebih jauh lagi, dampak *cracking* telah meresap hingga ke level individu dan sosial. Hal ini terbukti dari pengungkapan kasus pengambilalihan akun media sosial dan WhatsApp untuk modus penipuan di wilayah Cirebon pada tahun 2022 . Kasus ini mengilustrasikan bagaimana *cracking* (akses ilegal) dieksploitasi sebagai "pintu masuk" untuk melakukan kejahatan konvensional seperti penipuan, dengan memanfaatkan celah kepercayaan dalam jejaring sosial korban.

Tantangan terbesar dalam menangani tindak pidana *cracking* adalah anonimitas pelaku. *Cracker* biasanya menggunakan jaringan pribadi virtual (VPN) atau teknologi lain yang membuat identitas mereka sulit dilacak, hal ini menyulitkan aparat penegak

hukum dalam mengidentifikasi pelaku dan menegakkan hukum yang berlaku.[11] Meskipun teknologi forensik siber terus berkembang, kemampuan untuk mendeteksi bukti *cracking* masih sering tertinggal dibandingkan dengan teknik *cracking* yang semakin canggih. Pelaku sering kali menghapus jejak atau menggunakan metode yang sangat terorganisir, sehingga investigasi menjadi sulit dilakukan. Bukti tindak pidana *cracking* biasanya berupa data digital yang sangat mudah dimanipulasi, dihapus, atau disembunyikan.[12] Ketika *cracker* berhasil mengakses sistem, mereka sering kali meninggalkan sangat sedikit jejak yang bisa dianalisis secara forensik. Bukti digital ini memerlukan alat-alat khusus untuk diakses dan dianalisis, yang tidak selalu tersedia di setiap institusi penegak hukum di Indonesia.

Hukum siber di Indonesia relatif masih baru, dan penegak hukum serta pengadilan sering kali menghadapi kesulitan dalam menafsirkan undang-undang yang terkait dengan tindak pidana *cracking*. Ini termasuk menentukan jenis bukti yang sah di pengadilan dan memahami cara membedakan antara *cracking* dengan tindak pidana siber lainnya. *Cracking* sering kali melibatkan pelaku yang beroperasi di luar negeri, ini menambah lapisan kompleksitas karena aparat penegak hukum Indonesia harus bekerja sama dengan lembaga internasional untuk melacak pelaku. Proses ini bisa memakan waktu lama dan sering kali terhambat oleh kendala yuridiksi serta perbedaan hukum antarnegara. *Cracker* sering menggunakan alat enkripsi dan teknik pengelabuan lain untuk menyembunyikan aktivitas mereka, membuat proses investigasi menjadi lebih sulit karena data yang diakses atau dicuri oleh *cracker* mungkin dienkripsi sehingga membutuhkan waktu dan sumber daya yang besar untuk mendekripsinya.[13] Dalam beberapa kasus, *cracker* melakukan serangan berulang pada sistem yang sama. Ini membuat upaya untuk menentukan bukti semakin rumit karena penegak hukum

[11] Miftahul Huda, *Keamanan Informasi* (Nulisbuku, 2020). Hlm 51
[12] M. Qahar Awaka, "Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police.," *Jurnal Hukum Sehasen 9, No. 2* , 2023, 455–77.
[13] Budi Gunawan, *KUASA SIBER: Sebuah Refleksi Kritis* (PT. Rayyana Komunikasindo, 2022). Hlm 29

harus membedakan serangan yang satu dengan serangan lainnya, serta memisahkan jejak yang relevan dari yang tidak relevan.

Perkembangan pemikiran yang berperan dalam teknologi informasi dan telekomunikasi, berbagai alat bukti baru sebagai unsur mulai muncul dalam praktik, sebagaimana kita sebut alat bukti elektronik, contohnya termasuk email, pemeriksaan saksi melalui *video conference* (*teleconference*), sistem aplikasi pesan singkat (*WhatsApp*), hasil rekaman kamera tersembunyi (*Closed-Circuit Television*), informasi elektronik, tiket elektronik, data atau dokumen elektronik, dan sarana elektronik lainnya sebagai media penyimpan data. Menurut Williams dan Sawyer, Teknologi *Interconnected Network* atau Internet Teknologi Informasi (*Information Technology*) adalah teknologi yang menggabungkan komputasi dengan jalur komunikasi berkecepatan tinggi yang membawa data, suara, dan video.[14] Salah satu perubahan besar yang diakibatkan oleh perkembangan teknologi informasi adalah dalam aspek pembuktian.

Pernyataan di atas sejalan dengan pandangan Abdul Wahid dan Muhammad Labib, yang menambahkan bahwa masyarakat saat ini sangat mementingkan peran teknologi, sampai-sampai masyarakat tampak sangat bergantung pada teknologi, baik untuk tujuan positif maupun negatif.[15] Pendapat Abdul Wahid dan Muhammad Labib, jika diterapkan dalam konteks hukum, mengindikasikan bahwa perkembangan teknologi menuntut adanya seperangkat aturan untuk mengatur dan mengantisipasi kemungkinan pelanggaran yang belum diatur.[16] Aturan tersebut harus bersifat kompleks dan bermanfaat bagi masyarakat, mencakup masalah yurisdiksi, alat bukti, dan berbagai aspek esensial lainnya terkait tindakan tersebut.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah menyediakan dasar hukum untuk menangani kejahatan siber, termasuk

---

[14] Duma Megaria Elisabeth, "Kajian Terhadap Peranan Teknologi Informasi Dalam Perkembangan Audit Komputerisasi (Studi Kajian Teoritis).," *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi 3, No. 1* , 2019, 40–53.
[15] Nur. Ahmad, "Tantangan Dakwah Di Era Teknologi Dan Informasi," *Addin 8, No. 2* , 2014, 319–44.
[16] Sigar P Berutu, *DIGITAL SECURITY.* (PUBLISH BUKU UNPRI PRESS, 2024). Hlm 54

tindak pidana *cracking*. Namun, dalam praktiknya, penerapan undang-undang ini menghadapi berbagai tantangan, terutama terkait dengan pengumpulan dan penggunaan bukti elektronik di pengadilan. Salah satu kesulitannya adalah interpretasi yang beragam mengenai jenis bukti elektronik yang dapat diterima, serta bagaimana bukti tersebut harus diautentikasi. Meskipun Undang-Undang ITE menyediakan regulasi dasar untuk menindak *cracking*, kerangka hukum ini masih relatif baru dan belum seoptimal undang-undang yang lebih mapan di negara-negara lain. Peraturan yang ada sering kali belum mengantisipasi perkembangan teknologi terbaru yang digunakan oleh para pelaku *cracking*, sehingga menyulitkan aparat penegak hukum dalam menyesuaikan pendekatan mereka terhadap pembuktian elektronik. Ketidakjelasan dalam mendefinisikan bukti elektronik yang diterima oleh pengadilan dapat menimbulkan masalah, misalnya, ada perbedaan pandangan mengenai apakah data yang dikumpulkan dari *log server* atau rekaman aktivitas jaringan bisa diterima sebagai bukti. Ketidakjelasan ini menghambat kelancaran proses pembuktian. Salah satu kesulitan utama dalam pembuktian elektronik adalah autentikasi. Untuk diterima di pengadilan, bukti elektronik harus dapat diverifikasi keasliannya, bahwa data tersebut tidak diubah atau dimanipulasi. Dalam praktik lapangan, hal ini sulit dilakukan karena *cracker* sering kali menggunakan teknik yang canggih untuk menyembunyikan atau menghapus jejak digital mereka, atau bahkan memalsukan bukti elektronik.

Penanganan tindak pidana *cracking* memerlukan teknik forensik digital yang handal. Namun, forensik digital di Indonesia masih kurang berkembang jika dibandingkan dengan negara-negara lain. Kekurangan tenaga ahli forensik yang memiliki pengetahuan dan keterampilan dalam menganalisis data digital menjadi tantangan besar dalam proses pengumpulan dan verifikasi bukti. Dalam praktik lapangan, aparat penegak hukum di Indonesia sering kali menghadapi keterbatasan dalam hal peralatan dan infrastruktur teknis untuk melakukan investigasi digital.[17]

[17] Nurul Aini and Fauziah Lubis, "TANTANGAN PEMBUKTIAN DALAM KASUS KEJAHATAN SIBER.," *Judge: Jurnal Hukum 5, No. 02* , 2024, 55–63.

Peralatan yang digunakan untuk mengumpulkan dan menganalisis bukti elektronik membutuhkan teknologi canggih dan investasi besar, yang mungkin tidak dimiliki oleh banyak lembaga penegak hukum di tingkat daerah. Sering kali terjadi kesenjangan pemahaman antara aparat penegak hukum yang memproses kasus *cracking* dengan para ahli teknologi yang terlibat dalam investigasi teknis. Aparat hukum mungkin tidak memahami sepenuhnya kompleksitas teknis di balik *cracking* dan cara mengumpulkan bukti elektronik secara efektif, sementara ahli teknologi tidak selalu memahami prosedur hukum yang diperlukan untuk memastikan bukti tersebut diterima di pengadilan.

Inkonsistensi pengadilan dalam menerima bukti elektronik di Indonesia, terdapat inkonsistensi dalam bagaimana pengadilan menerima bukti elektronik dalam kasus tindak pidana *cracking*. Beberapa pengadilan mungkin lebih menerima bukti elektronik dengan lebih terbuka, sementara yang lain mungkin lebih skeptis dan memerlukan bukti tambahan untuk memastikan keabsahan data tersebut. Inkonsistensi ini menghambat penegakan hukum yang efektif. *Cracking* sering kali dilakukan oleh pelaku yang berada di luar negeri, sehingga pengumpulan bukti elektronik lintas batas menjadi masalah. Indonesia memiliki keterbatasan dalam hal kewenangan yuridiksi untuk mengakses data atau bukti yang berada di luar negeri. Tanpa kerjasama internasional yang memadai, proses pengumpulan bukti menjadi sangat sulit, terutama jika negara asal pelaku tidak memiliki perjanjian kerjasama hukum dengan Indonesia.

Cracker sering menggunakan teknologi enkripsi untuk menyembunyikan jejak mereka dan membuat bukti elektronik sulit diakses. Data yang telah dienkripsi membutuhkan waktu dan sumber daya yang signifikan untuk didekripsi, yang bisa memperlambat proses investigasi dan pembuktian.[18] Ini menjadi salah satu tantangan terbesar dalam pengungkapan kejahatan *cracking* di Indonesia. Bukti elektronik sangat rentan terhadap manipulasi, baik oleh pelaku *cracking* itu sendiri maupun oleh pihak

[18] Zen Munawar, *KEAMANAN SISTEM INFORMASI: Prinsip Dasar, Teori, Dan Rekayasa Penerapan Konsep* (Kaizen Media Publishing, 2023). Hlm 66

ketiga. *Cracker* sering kali memiliki kemampuan untuk mengubah *log*, menghapus bukti, atau menanamkan bukti palsu untuk mengalihkan penyelidikan, ini mempersulit proses pembuktian karena aparat penegak hukum harus memastikan keaslian setiap bukti yang diperoleh.[19] Sistem peradilan di Indonesia masih belum sepenuhnya siap untuk menangani kejahatan siber, termasuk *cracking*. Banyak hakim dan jaksa yang belum memiliki pengetahuan teknis yang memadai tentang bukti elektronik dan bagaimana cara menanganinya. Kurangnya pelatihan khusus untuk menangani kasus-kasus ini membuat proses peradilan menjadi lambat dan kurang efektif, Indonesia belum memiliki standar nasional yang seragam untuk pengumpulan dan verifikasi bukti elektronik. Di beberapa negara maju, standar-standar ini sudah jelas dan diterapkan secara konsisten. Namun, di Indonesia, belum ada keseragaman dalam praktik di lapangan, yang membuat proses pembuktian bisa bervariasi antara satu kasus dengan kasus lainnya.

Lembaga-lembaga penegak hukum di Indonesia, seperti Kepolisian dan Kominfo, sering kali memiliki pendekatan yang berbeda dalam menangani bukti elektronik.[20] Perbedaan prosedur dan kurangnya koordinasi ini menyebabkan hambatan dalam pengumpulan dan pemrosesan bukti yang komprehensif dan konsisten, yang pada akhirnya mempengaruhi hasil investigasi. Banyak institusi di Indonesia yang masih belum memiliki kesadaran yang tinggi tentang pentingnya keamanan data. Hal ini membuat mereka tidak siap ketika serangan *cracking* terjadi, sehingga proses pengumpulan bukti menjadi lebih sulit. Tanpa sistem keamanan yang baik, bukti sering kali rusak atau dihapus sebelum sempat dikumpulkan oleh penegak hukum. Dalam kasus *cracking*, bukti elektronik sering kali bersifat sementara. Data seperti log akses atau rekaman aktivitas jaringan mungkin hanya tersedia untuk waktu yang terbatas sebelum dihapus secara otomatis oleh sistem. Jika bukti ini tidak segera

[19] Chamdan Mashuri and Permadi Ginanjar Setyo, *Buku Ajar Literasi Digital*, 2022. Hlm 43
[20] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum 2, No. 1* , 2024, 8–16.

dikumpulkan, ada risiko bahwa bukti tersebut akan hilang selamanya, yang membuat proses pembuktian menjadi sangat sulit.

Indonesia menghadapi keterbatasan dalam hal tenaga ahli di bidang keamanan siber dan forensik digital. Jumlah ahli yang mampu menganalisis bukti elektronik secara menyeluruh dan tepat waktu masih sangat terbatas, yang memperlambat proses investigasi dan pembuktian. Teknologi di dunia siber berkembang sangat cepat, termasuk alat-alat yang digunakan oleh *cracker*. Aparat penegak hukum sering kali kesulitan mengikuti perkembangan ini, sehingga metode pembuktian yang mereka gunakan mungkin sudah usang atau tidak memadai untuk menangani serangan terbaru yang lebih canggih. Indonesia masih menghadapi tantangan regulasi dalam menangani *cracking* yang bersifat lintas negara. Meskipun Indonesia telah menandatangani beberapa perjanjian internasional terkait kejahatan siber, implementasinya masih belum optimal. Regulasi yang ada sering kali tidak cukup spesifik untuk menangani kejahatan yang melibatkan lebih dari satu negara, terutama dalam hal pengumpulan bukti elektronik lintas yurisdiksi.

Bukti elektronik dalam praktiknya dianggap sebagai tantangan baru akibat pesatnya perkembangan teknologi informasi, terutama melalui internet.[21] Perubahan ini telah mengalihkan berbagai aktivitas yang sebelumnya dilakukan secara fisik menjadi aktivitas di dunia maya. Jika terjadi kasus kejahatan siber, bukti yang digunakan adalah bukti elektronik. Menurut Paton dalam bukunya "*A Textbook Jurisprudence*", alat bukti bisa bersifat oral, yakni kata-kata yang diucapkan oleh seseorang di persidangan sebagai kesaksian mengenai suatu peristiwa.[22] Surat adalah alat bukti dokumenter, sedangkan alat bukti material merupakan bukti fisik yang terlihat dan tidak bersifat dokumenter, tetapi merupakan bukti demonstratif. Di Indonesia, bukti elektronik memiliki kedudukan yang sangat penting. Informasi dan/atau dokumen elektronik beserta hasil cetaknya diakui sebagai alat bukti yang sah.

---

[21] Lydyana Trisnaeni Martin and Nasyira Ania, "KEDUDUKAN ALAT BUKTI ELEKTRONIK PADA CYBERCRIME," *Jurnal Kritis Studi Hukum 9, No. 6* , n.d. Hlm 77

[22] George Whitecross Paton, *A Textbook of Jurisprudence*, 1946. Hlm 223

Ini menunjukkan adanya perluasan jenis alat bukti dalam Hukum Acara yang berlaku di Indonesia, dengan syarat bahwa informasi dan/atau dokumen elektronik tersebut menggunakan sistem elektronik yang sesuai dengan ketentuan yang berlaku.

Locus delicti dari kejahatan siber berada di dunia maya atau ruang siber, sehingga hal ini berbeda dengan tindak pidana konvensional yang diatur dalam KUHP, di mana tempat terjadinya tindak pidana biasanya adalah di dunia nyata. Oleh karena itu, cara pembuktiannya juga berbeda. Kejahatan siber, yang terjadi di ranah digital atau elektronik, meninggalkan jejak digital berupa dokumen elektronik yang dapat digunakan sebagai alat bukti. Dalam proses pembuktian tindak pidana siber, dokumen elektronik ini bisa dicetak dan dijadikan alat bukti. Meskipun kegiatan siber bersifat virtual, kegiatan tersebut dianggap sebagai tindakan hukum yang nyata. Secara yuridis, ruang siber tidak lagi cocok untuk dikategorikan menggunakan ukuran dan kualifikasi konvensional untuk dijadikan objek dan perbuatan. Penggunaan cara konvensional akan menimbulkan banyak kesulitan dan celah hukum. Kegiatan siber adalah aktivitas virtual yang berdampak nyata meskipun alat buktinya bersifat elektronik. Oleh karena itu, pelaku kejahatan siber harus dianggap telah melakukan perbuatan hukum yang nyata. Perkembangan terbaru dalam hukum pidana, terutama hukum acara pidana, telah berupaya mengakomodasi perkembangan teknologi informasi ini.[23]

Namun, tidak semua informasi elektronik atau dokumen elektronik dapat dijadikan alat bukti yang sah. Berdasarkan Undang-Undang ITE, informasi atau dokumen elektronik hanya sah sebagai alat bukti jika menggunakan sistem elektronik yang sesuai dengan ketentuan dalam undang-undang tersebut. Pasal 6 Undang-Undang ITE menetapkan bahwa informasi dan/atau dokumen elektronik dianggap sah jika informasi di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Selain itu, ada ketentuan khusus terkait penyelenggaraan sertifikasi elektronik, sistem elektronik, dan

[23] Muhammad Anthony Aldriano and Agus Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana," *Jurnal Kewarganegaraan 6, No. 1* , 2022, 2169–75.

transaksi elektronik yang harus dipatuhi. Meskipun *hacker* dan *cracker* memiliki kesamaan dalam melakukan aktivitas *hacking*, mereka berbeda dalam hal motivasi dan tujuan *hacking. Cracker* hanya melakukan *hacking* yang merusak, sementara *hacker* sejati memiliki semangat profesional untuk membantu menyelesaikan masalah pada sistem komputer.[24]

Untuk menghindari ketidakadilan bagi korban, aparat penegak hukum perlu memiliki kemampuan dan keberanian untuk melakukan penemuan hukum. Ini bisa dilakukan dengan menerapkan metode interpretasi hukum sebelum ada payung hukum yang memadai. Dengan demikian, diharapkan tidak akan terjadi kekosongan hukum dalam menuntut dan mengadili pelaku kejahatan siber di Indonesia. Meskipun Undang-Undang ITE telah mengatur tindak pidana *cracking*, proses pembuktiannya masih menghadapi banyak kendala. Tidak adanya standar baku untuk autentikasi bukti elektronik membuat banyak kasus *cracking* sulit diproses di pengadilan selain itu, minimnya tenaga ahli digital forensik dan sulitnya melacak pelaku yang menggunakan jaringan anonim menjadi tantangan besar dalam sistem peradilan pidana. Oleh karena itu, penelitian ini bertujuan untuk menganalisis validitas dan tantangan penggunaan alat bukti elektronik dalam pembuktian kejahatan *cracking* dalam sistem peradilan pidana di Indonesia serta mengevaluasi penerapan sanksi pidana terhadap pelaku *cracking*. Dengan latar belakang ini, penulis tertarik untuk mendalami dan mengkaji kasus tersebut, yang dituangkan dalam sebuah karya tulis berjudul "Analisis Pembuktian Tindak Pidana *Cracking* Dalam Sistem Peradilan Pidana Di Indonesia".

[24] Richard Stallman, *Free Software, Free Society: Selected Essays of Richard M. Stallman*, 2022. Hlm 81

B. Rumusan Masalah

Agar penelitian tetap fokus dan mendalam, diperlukan batasan masalah. Hal ini membutuhkan penyusunan masalah secara sistematis dan teratur. Oleh karena itu, rumusan masalah yang disusun adalah sebagai berikut:

1. Bagaimana pembuktian tindak pidana *cracking* dalam sistem peradilan pidana di Indonesia?
2. Bagaimana cara menjaga keabsahan barang bukti elektronik dalam proses pembuktian tindak pidana *cracking* di wilayah hukum Polda Jawa Barat?
3. Bagaimana validitas alat bukti elektronik dalam pembuktian tindak pidana *cracking* di Polda Jawa Barat?

C. Tujuan Penelitian

1. Untuk menganalisis pembuktian tindak pidana *cracking* dalam sistem peradilan pidana di Indonesia
2. Untuk menganalisis cara menjaga keabsahan barang bukti elektronik dalam proses pembuktian tindak pidana *cracking* di wilayah hukum Polda Jawa Barat
3. Untuk menganalisis validitas alat bukti elektronik dalam pembuktian tindak pidana *cracking* di Polda Jawa Barat

D. Manfaat Hasil Penelitian

Berdasarkan dengan tujuan penelitian di atas untuk memperjelas dan mempertegas manfaat dari penelitian ini mengarah kepada dua hal, yaitu sebagai berikut:

1. Manfaat Teoritis

   Hasil penelitian ini diharapkan dapat memberikan kontribusi dan menambah wawasan dalam literatur akademis bagi para akademisi. Secara teoritis, penelitian ini bertujuan untuk memberikan pemahaman mengenai pembuktian pidana dalam sistem hukum positif di Indonesia, khususnya terkait tindak pidana *cracking*, serta kontribusi hukum *cybercrime* dalam Undang-Undang Informasi dan Transaksi

Elektronik terhadap pelaku tersebut. Diharapkan, penelitian ini dapat menjadi referensi tambahan bagi penelitian lain terkait tindak pidana *cybercrime*.

2. Manfaat Praktis

Secara praktis, hasil penelitian ini diharapkan dapat menjadi referensi bagi praktisi hukum dan masyarakat dalam menyelesaikan masalah pembuktian tindak pidana siber, terutama dalam kasus tindak pidana *cracking*, dengan mengacu pada sumber hukum yang berlaku sesuai dengan konstitusi Indonesia.

E. Kerangka Berpikir

Menurut Sugiyono, kerangka pemikiran yang menjelaskan fenomena secara teoritis dianggap sebagai kerangka yang baik dalam sebuah penelitian. Kerangka pemikiran ini merupakan konsep yang menjelaskan isi dari kajian teoritis dalam suatu karya tulis, terkait dengan faktor-faktor yang telah diidentifikasi sebagai rumusan masalah penting. Dalam penelitian hukum, kerangka teori dapat dibagi menjadi *Grand Theory, Middle Theory*, dan *Applied Theory*. Teori-teori yang digunakan untuk menjawab rumusan masalah dalam penelitian ini mencakup beberapa teori berikut:

1. *Grand Theory*

Grand Theory adalah teori yang mendasari teori-teori *middle* dan *applied* yang akan digunakan dalam penelitian. Dalam penelitian ini, *Grand Theory* yang digunakan adalah teori Teori Tujuan Hukum. Teori ini menyatakan bahwa pembentukan dan penegakan hukum pada hakikatnya harus mengabdi pada tiga nilai dasar: keadilan (*gerechtigkeit*), kemanfaatan (*zweckmäßigkeit*), dan kepastian hukum (*rechtssicherheit*). Dalam konteks tindak pidana *cracking*, ketiga tujuan ini menjadi standar ideal (*das Sollen*) yang ingin dicapai oleh sistem peradilan pidana Indonesia.[25] Keadilan, hukum harus mampu memberikan keadilan bagi para korban *cracking* yang menderita kerugian materiil maupun imateriel, serta menindak pelaku

[25] Laia and Sri Wahyuni, "Urgensi Landasan Filosofis, Sosiologis, Dan Yuridis Dalam Pembentukan Undang-Undang Yang Bersifat Demokratis Di Indonesia," *Urnal Education and Development 10, No. 1*, 2022, 545–52.

sesuai dengan perbuatannya. Kemanfaatan, penegakan hukum terhadap *cracking* harus memberikan manfaat bagi masyarakat luas, seperti melindungi stabilitas ekonomi digital, menjaga kepercayaan publik terhadap sistem elektronik, dan mencegah kejahatan serupa di masa depan. Kepastian Hukum, harus ada aturan yang jelas, prosedur yang terstandar, dan penegakan yang konsisten dalam menangani pembuktian tindak pidana *cracking*, sehingga setiap kasus dapat diselesaikan dengan cara yang dapat diprediksi dan tidak arbitrer.

Penelitian ini berangkat dari asumsi bahwa telah terjadi ketegangan antara ketiga tujuan hukum tersebut dengan realitas di lapangan (*das Sein*). Sulitnya membuktikan kejahatan *cracking* telah mengganggu rasa keadilan bagi korban, mengurangi kemanfaatan hukum dalam melindungi ekonomi digital, dan menggerus kepastian hukum karena proses yang seringkali tidak efektif.

Dalam konteks pembuktian tindak pidana *cracking*, teori tujuan hukum sangat relevan karena sistem peradilan pidana di Indonesia berlandaskan pada hukum tertulis. Teori Tujuan Hukum menyediakan landasan filosofis paling dasar untuk mengevaluasi keseluruhan sistem peradilan pidana. Teori ini mempostulatkan bahwa hukum yang ideal harus mengabdi dan menyeimbangkan tiga nilai dasar: Keadilan (*Gerechtigkeit*), Kemanfaatan (*Zweckmäßigkeit*), dan Kepastian Hukum (*Rechtssicherheit*). Penelitian ini menggunakan ketiga pilar tersebut sebagai standar ideal (*das Sollen*) untuk mengukur bagaimana sistem peradilan pidana kita merespons tindak pidana cracking dalam praktiknya (*das Sein*).[26] Oleh karena itu, pembuktian suatu tindak pidana, termasuk *cracking*, harus merujuk pada aturan yang telah diatur dalam peraturan perundang-undangan yang berlaku. Aturan-aturan hukum yang menjadi dasar pembuktian dalam tindak pidana *cracking* di Indonesia meliputi Kitab Undang-Undang Hukum Acara Pidana (Kitab Undang-Undang Hukum Acara Pidana) yang mengatur sistem pembuktian dan alat bukti yang sah,

[26] Firdaus and Arikatul, "POSITIVISME HUKUM DALAM PROSEDUR LEGISLASI DI INDONESIA," *Urnal Multidisiplin Ilmu Akademik 2, No. 1*, 2025, 192–201.

serta Undang-Undang Informasi dan Transaksi Elektronik, khususnya Pasal 30-32 yang secara eksplisit mengatur tentang kejahatan siber, termasuk *cracking*. Selain itu, terdapat Peraturan Pemerintah dan Peraturan Mahkamah Agung tentang alat bukti elektronik, yang memberikan landasan hukum bagi penggunaan bukti digital dalam proses peradilan.

Dari perspektif tujuan hukum, relevansi utama teori ini terletak pada ketegangan yang timbul antara ketiga nilai tersebut akibat sifat unik dari tindak pidana *cracking*. Kesulitan dalam pembuktian *cracking* yang bersifat *borderless*, anonim, dan teknis telah secara nyata mengganggu keseimbangan ideal tersebut. Tesis ini pada hakikatnya adalah analisis tentang bagaimana ketegangan tersebut bermanifestasi dalam sistem peradilan pidana, khususnya di wilayah hukum Polda Jawa Barat.[27]

2. *Middle Theory*

Middle theory adalah teori yang digunakan untuk memfokuskan dan mendetailkan pembahasan atas suatu *grand theory*. Dalam penelitian ini, teori yang digunakan adalah teori Tindak Pidana Siber, merupakan sebuah kerangka analisis konseptual yang bersifat interdisipliner, yang memadukan perspektif dari ilmu hukum, kriminologi, sosiologi, dan ilmu komputer. Teori ini lahir sebagai respons akademis terhadap evolusi kejahatan yang melampaui batas-batas fisik dan bermanifestasi dalam ranah virtual. Fokus utama teori ini adalah untuk mengidentifikasi, mengklasifikasikan, dan menganalisis sifat serta karakteristik unik dari perbuatan pidana yang dimediasi oleh jaringan komputer dan internet.[28]

Landasan fundamental dari teori ini adalah pengakuan bahwa "ruang siber" (*cyberspace*) telah membentuk sebuah locus delicti (tempat kejadian perkara) baru yang berbeda secara diametral dari locus delicti dalam kejahatan konvensional . Ruang siber sebagai sebuah konstruksi sosial-teknis yang bersifat virtual, artifisial, dan terdesentralisasi, melahirkan bentuk-bentuk perbuatan (*actus reus*) dan niat

[27] Nurwati, *Hukum Teknologi Informasi & Komunikasi* (KBM Indonesia, 2024). Hlm 31
[28] Eddy Army, *Bukti Elektronik Dalam Praktik Peradilan* (Sinar Grafika, 2020). Hlm 44

jahat (*mens rea*) yang khas, serta modus operandi yang tidak dikenal sebelumnya dalam hukum pidana tradisional.

Teori Tindak Pidana Siber mengidentifikasi beberapa karakteristik inheren dari kejahatan di ranah virtual. Karakteristik utama adalah sifatnya yang transnasional atau tanpa batas (*borderless*). Seorang pelaku di satu yurisdiksi negara dapat melakukan serangan terhadap sistem elektronik di yurisdiksi negara lain, seringkali melalui infrastruktur yang berlokasi di yurisdiksi ketiga. Karakteristik ini secara langsung menantang pilar-pilar kedaulatan hukum nasional dan menciptakan kompleksitas yuridis dalam hal penentuan yurisdiksi, investigasi, dan ekstradisi.[29]

Karakteristik krusial kedua adalah anonimitas (*anonymity*) pelaku. Teknologi digital memungkinkan pelaku untuk menyembunyikan identitas aslinya melalui berbagai teknik pelapisan (*layering*), seperti penggunaan *Virtual Private Network* (VPN), proxy server, jaringan Tor, maupun penggunaan identitas palsu. Anonimitas ini menjadi tantangan terbesar dalam proses pembuktian, di mana proses atribusi yakni menghubungkan jejak digital dengan individu pelaku di dunia nyata menjadi tugas penyidikan yang paling sulit..[30] Karakteristik ketiga berkaitan dengan sifat objek dan dampak kejahatan. Objek yang menjadi sasaran dalam tindak pidana siber seringkali bersifat tidak berwujud (*intangible*), seperti data, informasi, reputasi, dan kekayaan intelektual. Dampak yang ditimbulkan dapat terjadi dalam skala masif dan kecepatan instan. Satu perbuatan pidana, seperti dalam kasus *cracking* terhadap sebuah basis data, dapat merugikan jutaan korban secara simultan hanya dalam hitungan menit.[31] Secara akademis, Teori Tindak Pidana Siber menyediakan tipologi

[29] M. C Amiruddin and Syamsuddin R, "Analisis Yuridis Pertimbangan Tentang Keyakinan Hakim Dalam Memutus Perkara Dengan Berdasarkan Circumstantial Evidence Atau Bukti Tidak Langsung (Studi Putusan No. 777/Pid. B/2016/Pn. Jkt. Pst Kasus Jessica Kumala Wongso)," *Alauddin Law Development Journal, 3(3)*, 2021, 531–34.
[30] P. D. P. A WATANSOPPENG, *PENERAPAN TEORI TEORI PEMBUKTIAN MENURUT HUKUM ACARA*, 2018. Hlm 33
[31] M. S Hartono, "Penggunaan Bukti Elektronik Dalam Peradilan Pidana," *Jurnal Komunikasi Hukum (JKH), 6(1)*, n.d.

kejahatan untuk mempermudah klasifikasi. Secara umum, kejahatan siber dapat dikategorikan menjadi dua tipologi utama:

a. Kejahatan di mana komputer sebagai target (*computer as a target*), di mana sistem elektronik itu sendiri yang diserang, contoh utamanya adalah cracking, hacking ilegal, penyebaran malware (virus, ransomware), dan serangan Denial-of-Service (DDoS).
b. Kejahatan di mana komputer sebagai alat (*computer as a tool*), di mana sistem elektronik digunakan sebagai sarana untuk melakukan kejahatan konvensional, seperti penipuan daring (*phishing*), pencurian data kartu kredit (*carding*), penyebaran konten ilegal, dan pencucian uang

Dari perspektif kriminologi, teori ini juga mengkaji etiologi atau penyebab kejahatan. Teori-teori kriminologi tradisional diadaptasi ke dalam konteks digital. Sebagai contoh, Teori Aktivitas Rutin (*Routine Activity Theory*) menjelaskan bahwa seseorang menjadi korban kejahatan siber karena "rutinitas digital" mereka (misalnya, penggunaan Wi-Fi publik tanpa proteksi, kata sandi yang lemah) mempertemukan mereka secara virtual dengan pelaku yang termotivasi (motivated offender) dalam lingkungan yang minim pengawasan (*absence of capable guardianship*).[32]

Pada akhirnya, Teori Tindak Pidana Siber memberikan justifikasi teoretis atas urgensi reformasi hukum. Teori ini menegaskan bahwa sifat kejahatan yang fundamental berbeda menuntut adanya instrumen hukum materiil yang baru (seperti Undang-Undang ITE) dan hukum acara yang juga baru. Ia menegaskan bahwa kejahatan virtual yang hanya menyisakan jejak digital, secara logis hanya dapat dibuktikan melalui metode pembuktian yang berorientasi digital, yang dalam hal ini adalah forensik digital.[33]

---

[32] M. Y Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, Dan Putusan Pengadilan* (Sinar Grafika, 2017). Hlm 29
[33] Eddy Army, *Bukti Elektronik Dalam Praktik Peradilan* (Sinar Grafika, 2020). Hlm 15

Relevansi Teori Tindak Pidana Siber bersifat langsung dan fundamental terhadap judul penelitian ini. Judul tesis secara spesifik mengangkat "Tindak Pidana *Cracking*" sebagai objek kajian utama. Teori Tindak Pidana Siber merupakan kerangka konseptual yang menyediakan definisi, klasifikasi, dan pemahaman mendalam mengenai cracking itu sendiri. Teori ini membantu membedah *cracking* sebagai salah satu bentuk kejahatan di mana komputer menjadi target (*computer as a target*), yakni perbuatan mengakses sistem elektronik milik orang lain secara tanpa hak atau melawan hukum, sebagaimana diatur dalam Pasal 30 Undang-Undang ITE. Tanpa teori ini, *cracking* berisiko dianalisis secara keliru menggunakan kacamata tindak pidana konvensional, padahal sifat perbuatan (*virtual*) dan objeknya (data) bersifat fundamental berbeda.[34] Pada akhirnya, Teori Tindak Pidana Siber berfungsi sebagai jembatan teoretis yang logis menuju *applied theory* (Teori Pembuktian dan Teori Forensik Digital). Karena teori ini menegaskan bahwa tindak pidana *cracking* adalah kejahatan virtual yang hanya menyisakan jejak bukti digital, maka ia secara otomatis menuntut adanya metode pembuktian yang juga bersifat digital. Dengan demikian, teori ini memberikan justifikasi teoretis yang kuat mengapa "Analisis Pembuktian" dalam judul tesis ini tidak dapat dipisahkan dari analisis validitas alat bukti elektronik dan penerapan disiplin ilmu forensik digital, yang merupakan satu-satunya cara ilmiah untuk mengungkap kejahatan siber.

3. *Applied Theory*

Teori aplikasi (*applied theory*) akan menjelaskan bagaimana prinsip-prinsip hukum tertentu dapat digunakan untuk menjawab permasalahan yang diteliti. Menurut Utrecht, asas hukum (*recht beginsel*) adalah dasar dari peraturan-peraturan hukum yang mengkualifikasikan beberapa peraturan hukum, sehingga peraturan-peraturan tersebut secara bersama-sama membentuk suatu lembaga hukum.[35]

---

[34] Rionov Oktana, "ANALISIS HUKUM TERHADAP MEDIA SOSIAL DALAM PEMBUKTIAN TINDAK PIDANA INFORMASI DAN TRANSAKSI ELEKTRONIK= Legal Analysis of Social Media in Proof of Information and Electronic Transaction Crimes." (2023). Hlm 37

[35] P. A. F Lamintang, *Dasar-Dasar Hukum Pidana Di Indonesia* (Sinar Grafika, 2022). Hlm 44

Dalam penelitian ini, *applied theory* yang digunakan adalah teori Forensik Digital. Teori forensik digital merupakan cabang ilmu forensik yang berfokus pada pengumpulan, analisis, interpretasi, dan presentasi bukti digital dalam proses hukum. Forensik digital bertujuan untuk menemukan, melacak, dan memvalidasi bukti elektronik yang dapat digunakan dalam penyelidikan dan persidangan kasus kejahatan siber, termasuk *cracking*.

Menurut Eoghan Casey dalam bukunya *Digital Evidence and Computer Crime*, forensik digital harus memenuhi tiga prinsip utama agar dapat diterima sebagai alat bukti yang sah dalam persidangan:[36]

a. *Authenticity* (Keaslian).

   Bukti digital harus dapat diverifikasi keasliannya dan tidak mengalami manipulasi.

b. *Integrity* (Integritas).

   Data harus tetap utuh dan tidak mengalami perubahan selama proses investigasi.

c. *Reliability* (Keandalan).

   Bukti harus dikumpulkan melalui prosedur yang sah dan dapat dipertanggungjawabkan di pengadilan.

Proses forensik digital mencakup beberapa tahapan, mulai dari identifikasi, pengumpulan, analisis, hingga pelaporan hasil investigasi. Dalam konteks pembuktian *cracking*, teknik forensik digital sering digunakan untuk mengidentifikasi pelaku, melacak jejak digital, dan memverifikasi keabsahan alat bukti elektronik.[37]

Forensik digital memiliki peran yang sangat penting dalam pembuktian tindak pidana *cracking*, karena kejahatan ini dilakukan dalam dunia maya dan tidak meninggalkan bukti fisik seperti kejahatan konvensional. Sebagai kejahatan

[36] Eoghan Casey, *Digital Evidence and Computer Crime* (British Library Cataloguing-in-Publication Data, 2011). Hlm 66
[37] Casey.

berbasis teknologi, *cracking* umumnya hanya meninggalkan jejak digital, seperti alamat IP, log aktivitas pengguna, serta file yang telah dimodifikasi atau dihapus oleh pelaku. Oleh karena itu, pendekatan forensik digital diperlukan untuk mengidentifikasi, mengumpulkan, dan memverifikasi alat bukti elektronik yang dapat digunakan dalam proses penyelidikan dan persidangan. Sistem peradilan pidana di Indonesia telah mengakui informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah dalam persidangan, sebagaimana diatur dalam Pasal 5 Ayat (1) dan (2) Undang-Undang ITE. Namun, bukti digital harus memenuhi standar keabsahan dan autentikasi agar dapat diterima oleh hakim. Dalam konteks sistem pembuktian negatif (*Negatief Wettelijke Bewijs Theorie*), hakim tidak hanya harus memastikan bahwa alat bukti elektronik sah menurut undang-undang, tetapi juga harus yakin bahwa bukti tersebut benar-benar dapat membuktikan keterlibatan terdakwa dalam tindak pidana *cracking*. Di sinilah peran forensik digital menjadi sangat penting dalam menjamin keandalan dan integritas alat bukti elektronik.

Forensik digital juga berperan dalam pelacakan dan identifikasi pelaku tindak pidana *cracking*. Cracker sering menggunakan berbagai teknik untuk menyembunyikan identitas mereka, seperti VPN, proxy server, jaringan Tor, serta teknik enkripsi tingkat tinggi. Dengan menerapkan metode analisis *log server*, identifikasi alamat IP, dan *digital forensics imaging*, penyidik dapat melacak aktivitas peretasan, mengidentifikasi perangkat yang digunakan, serta menemukan jejak digital yang ditinggalkan oleh pelaku. Selain itu, teknik *live forensics* memungkinkan penyidik untuk memperoleh data dari sistem yang masih aktif sebelum bukti tersebut dihapus atau dienkripsi oleh pelaku. Selain membantu dalam identifikasi pelaku, forensik digital juga diperlukan dalam menguji keabsahan dan integritas bukti elektronik yang diajukan dalam persidangan. Bukti digital dapat dimanipulasi, dipalsukan, atau disisipi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, dalam proses investigasi, diperlukan metode verifikasi seperti *hashing* (MD5, SHA-256) untuk memastikan bahwa bukti yang diajukan adalah asli dan tidak mengalami perubahan sejak pertama kali ditemukan. Teknik ini

memberikan jaminan integritas data, sehingga hakim dapat lebih yakin dalam mempertimbangkan alat bukti elektronik sebagai dasar pengambilan keputusan. Dengan demikian, penerapan forensik digital dalam pembuktian tindak pidana *cracking* menjadi semakin krusial, mengingat kejahatan siber terus berkembang dengan teknologi yang semakin canggih. Dalam sistem peradilan pidana di Indonesia, forensik digital dapat membantu memastikan bahwa bukti elektronik yang diajukan telah dikumpulkan dan dianalisis secara sah, sehingga dapat digunakan secara efektif dalam proses pembuktian di pengadilan.[38] Namun, tantangan utama dalam penerapan forensik digital di Indonesia adalah kurangnya standar baku serta keterbatasan tenaga ahli digital forensik, yang dapat mempengaruhi efektivitas pembuktian tindak pidana *cracking* dalam sistem hukum yang berlaku.

F. Penelitian Terdahulu

Kejahatan siber telah menjadi topik hangat dalam ranah hukum Indonesia dan menarik perhatian banyak pihak, termasuk akademisi. Banyak karya tulis yang membahas mengenai hal ini, seperti yang dapat ditemukan melalui berbagai penelitian. Setelah meneliti dan mengkaji literatur dari beberapa situs, termasuk digilib.uinsgd.ac.id, *Google Scholar*, dan lainnya, terdapat beberapa penelitian yang menyoroti pembuktian tindak pidana atas kejahatan *cracking* di Indonesia, di antaranya:

1. Penelitian yang dilakukan oleh Dheny Wahyudi yang berjudul "*Perlindungan Hukum terhadap Korban Kejahatan Cybercrime di Indonesia*".[39] Jurnal, tahun 2013. membahas bahwa pemerintah telah mengeluarkan Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) untuk memberikan

[38] Eugenia and Felicia, "Tantangan Praktis Dalam Proses Pembuktian Perkara Pidana: Kredibilitas Saksi Dan Validitas Bukti Elektronik.," *Iuris Studia: Jurnal Kajian Hukum 5, No. 2*, 2024, 492–503.
[39] Dheny Wahyudi, "Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia," *Jurnal Ilmu Hukum Jambi 4, No. 1* , 2013. Hlm 29

perlindungan terhadap korban *cybercrime*. Undang-Undang ini mengatur ancaman hukuman bagi tindak kejahatan melalui internet. Perlindungan hukum terhadap korban *cybercrime* secara mendasar dilakukan melalui dua model pendekatan, yaitu model hak-hak prosedural dan model pelayanan.

2. Penelitian yang dilakukan oleh Beni Setiawan yang berjudul "Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (*Hacking*) Dan Menimbulkan Kerusakan (*Cracking*) Dalam Kejahatan Dunia Maya (*Cybercrime*) Menurut Perspektif Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik".[40] Tesis, Universitas Batanghari, tahun 2019. *Hacking* dan *cracking* pada intinya adalah tindak pidana di mana seseorang secara sengaja dan tanpa izin atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dengan tujuan mendapatkan informasi atau dokumen elektronik, dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Tindakan *hacking* sering kali menjadi langkah awal bagi pelaku kejahatan siber untuk melakukan kejahatan lain di dunia maya
3. Penelitian yang dilakukan oleh Mustika Indah Jelita Sinaga yang berjudul "*Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum Di Indonesia*".[41] Tesis, 2021, Universitas Kristen Indonesia. Kejahatan dunia maya transnasional sering didefinisikan sebagai kejahatan di internet yang melibatkan lebih dari satu negara dan dilakukan secara terorganisir, termasuk persiapan, perencanaan, pengarahan, atau pengendalian yang dilakukan di negara lain, serta memberikan dampak pada korban di berbagai negara. Karena melibatkan banyak negara, penanggulangan *cybercrime* ini sering

[40] Beni Setiawan, "Penegakan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) Dan Menimbulkan Kerusakan (Cracking) Dalam Kejahatan Dunia Maya (Cybercrime) Menurut Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik" (Universitas Batanghari, 2019). HLm88

[41] Mustika Indah Jelita Sinaga, "Penetapan Tersangka Dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum Di Indonesia" (2021). Hlm 78

menghadapi masalah terkait yurisdiksi. Yurisdiksi pada dasarnya adalah kompetensi hukum suatu negara terhadap orang, benda, atau peristiwa hukum, atau kekuasaan yang dimiliki oleh negara tersebut.

4. Penelitian yang dilakukan oleh Fadli M yang berjudul "Penegakan hukum terhadap pelaku *Phising* dalam *E-commerce* menurut Undang-Undang ITE No 19 tahun 2016 tentang informasi dan transaksi elektronik : Studi di wilayah hukum kepolisian daerah Jawa".[42] Tesis, Program Studi Ilmu Hukum, Pascasarjana, Universitas Islam Negeri Sunan Gunung Djati Bandung tahun 2022. Adapun pokok pembahasannya meliputi Modus operandi kejahatan *phishing* melibatkan penggunaan email, website palsu, *spyware*, dan berbagai media lainnya dengan mengirimkan tautan yang dapat diakses oleh pelanggan *e-commerce*. Ketika pelanggan *e-commerce* mengakses tautan tersebut, peretas atau *hacker* dapat mencuri data, mulai dari password media sosial hingga membobol rekening. Penegakan hukum terhadap tindak pidana phishing pada dasarnya sama dengan penipuan konvensional, namun perbedaannya terletak pada alat bukti atau sarana perbuatannya, yaitu menggunakan sistem elektronik seperti komputer, internet, dan perangkat telekomunikasi. Penegakan hukum pidana terhadap pelaku phishing dalam *e-commerce* dilakukan sesuai dengan aturan hukum pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Karena kasus ini mengandung unsur penipuan, maka dikenakan Pasal 378 KUHP. Namun, karena ancaman pidana dalam Pasal 378 KUHP dianggap terlalu ringan, aparat kepolisian juga menggunakan Pasal 28 ayat (1) dan Pasal 45A ayat (1) Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
5. Penelitian yang dilakukan oleh Addy Bima Satria Dandy Putra yang berjudul "*Analisis Tindak Pidana Cracker dalam Kerangka Undang-Undang Informasi dan*

[42] Fadli M, "Penegakan Hukum Terhadap Pelaku Phising Datam E-Commerce Menurut Undang-Undang ITE No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik : Studi Di Wilayah Hukum Kepolisian Daerah Jawa Barat" (Universitas Islam Negeri Sunan Gunung Djati Bandung, 2022). Hlm 88

Transaksi Elektronik".[43] Jurnal, tahun 2023. Membahas tentang memahami metodologi yang digunakan oleh *Cracker*, seperti *footprinting*, *scanning*, dan penciptaan *backdoors*, penelitian ini menyoroti kesenjangan dalam respon hukum saat ini. Pentingnya peningkatan keamanan siber dan strategi pencegahan menjadi jelas, terutama dalam melindungi infrastruktur kritis. Tinjauan terhadap teori hukum, termasuk teori absolut, relatif, dan gabungan, menunjukkan bahwa pemberian sanksi pidana harus mempertimbangkan aspek pembalasan dan rehabilitasi. Ini menekankan pentingnya pendekatan multidisiplin dalam penanganan kejahatan siber, yang tidak hanya berfokus pada hukuman tetapi juga pada reformasi pelaku.

[43] Addy Bima Satria Dandy Putra, "Analisis Tindak Pidana Cracker Dalam Kerangka Undang-Undang Informasi Dan Transaksi Elektronik," *Sekolah Tinggi Ilmu Hukum IBLAM*, 2023. Hlm 41