**Analysis of Cracker Crimes within the Framework of the Information and Electronic Transactions Law**

**Analisis Tindak Pidana Cracker dalam Kerangka Undang-Undang Informasi dan Transaksi Elektronik**

**Addy Bima Satria Dandy Putra**

***Abstract***

*In the era of rapidly developing information technology, cybercrime such as cracking is a serious threat. This research focuses on the analysis of cracker crimes in the context of the Information and Electronic Transactions Law (UU ITE) in Indonesia. We investigate how cracking, which involves illegal access to electronic systems with the aim of gaining profit or accessing information, is regulated and punished under the ITE Law. This study also discusses the social and economic impacts of cracking, as well as challenges in implementing the law. We analyze specific cases in Indonesia to understand the legal and law enforcement implications related to cracker actions. Finally, this research explores the effectiveness of current regulations in tackling cybercrime and provides recommendations for policy improvements.*

*The method used in this research is qualitative, with a normative legal approach. We examined relevant laws, regulations, and court decisions, as well as academic literature. Data is collected through primary and secondary sources to gain comprehensive insight into legal issues and law enforcement practices.*

*The research results show that the ITE Law provides a legal framework to overcome the crime of cracking, but there are still gaps and challenges in its enforcement. Related articles in the ITE Law, such as Articles 30 and 32, specifically target illegal access and theft of information. We find that criminal sanctions are often disproportionate to the harm caused by crackers, requiring a more comprehensive legal approach. Case analysis shows that crackers usually use systematic and sophisticated methods, which makes law enforcement difficult. This research also identifies the need for a multidisciplinary approach in dealing with cybercrime, including increasing cyber security and public awareness. Finally, we recommend changes in law enforcement policies and practices to address weaknesses in the current legal system.*

***Keywords****: Cracking, Information and Electronic Transactions Law, Cyber Crime, Law Enforcement, Cyber Security.*

**Abstrak**

Dalam era teknologi informasi yang berkembang pesat, kejahatan siber seperti cracking menjadi ancaman serius. Penelitian ini berfokus pada analisis tindak pidana cracker dalam konteks Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Kami menyelidiki bagaimana tindakan cracking, yang melibatkan akses ilegal ke sistem elektronik dengan tujuan meraih keuntungan atau akses informasi, diatur dan dihukum menurut UU ITE. Studi ini juga membahas dampak sosial dan ekonomi cracking, serta tantangan dalam penerapan hukum. Kami menganalisis kasus-kasus spesifik di Indonesia untuk memahami implikasi hukum dan penegakan hukum terkait tindakan cracker. Terakhir, penelitian ini mengeksplorasi keefektifan regulasi saat ini dalam menanggulangi kejahatan siber dan memberikan rekomendasi untuk perbaikan kebijakan.

Metode yang digunakan dalam penelitian ini adalah kualitatif, dengan pendekatan hukum normatif. Kami memeriksa undang-undang, regulasi, dan putusan pengadilan terkait, serta literatur akademis. Data dikumpulkan melalui sumber primer dan sekunder untuk mendapatkan wawasan menyeluruh tentang isu hukum dan praktik penegakan hukum.

Hasil penelitian menunjukkan bahwa UU ITE menyediakan kerangka hukum untuk mengatasi tindak pidana cracking, namun masih terdapat celah dan tantangan dalam penegakannya. Pasal-pasal terkait dalam UU ITE, seperti Pasal 30 dan 32, secara spesifik menargetkan akses ilegal dan pencurian informasi. Kami menemukan bahwa sanksi pidana sering tidak sebanding dengan kerugian yang ditimbulkan oleh cracker, memerlukan pendekatan hukum yang lebih komprehensif. Analisis kasus menunjukkan bahwa cracker biasanya menggunakan metode sistematis dan canggih, yang mempersulit penegakan hukum. Penelitian ini juga mengidentifikasi kebutuhan akan pendekatan multidisiplin dalam penanganan kejahatan siber, termasuk peningkatan keamanan siber dan kesadaran publik. Terakhir, kami merekomendasikan perubahan dalam kebijakan dan praktik penegakan hukum untuk mengatasi kelemahan dalam sistem hukum saat ini.

**Kata kunci**: Cracking, Undang-Undang Informasi dan Transaksi Elektronik, Kejahatan Siber, Penegakan Hukum, Keamanan Siber.

### PENDAHULUAN

Teknologi informasi saat ini dan di masa depan memiliki peran krusial di seluruh dunia. Kredibilitasnya sebagai katalisator utama bagi kemajuan global terutama dalam ekonomi, didukung oleh dua aspek utama. Pertama, teknologi informasi meningkatkan permintaan untuk perangkat dan solusi teknologinya sendiri, seperti modem dan infrastruktur jaringan internet. Kedua, teknologi ini memudahkan pelaksanaan transaksi bisnis, khususnya dalam sektor keuangan dan bidang komersial lainnya (Azis & Rumlus, 2021)

Penerapan teknologi informasi sangat vital dalam perdagangan dan pertumbuhan ekonomi nasional, membantu meningkatkan kesejahteraan masyarakat. Pemerintah harus berperan aktif mendukung teknologi ini, termasuk penyediaan infrastruktur hukum dan regulasi yang memastikan penggunaannya secara efektif dan aman, serta meminimalisir penyalahgunaan yang bertentangan dengan nilai-nilai agama dan budaya masyarakat Indonesia (Azis & Rumlus, 2021)

Era globalisasi membawa perubahan besar dalam teknologi informasi, yang 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 (Tacino, 2020)

Di Indonesia, isu cybercrime atau kejahatan siber diatur secara khusus dalam Undang-Undang. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diperbaharui oleh Undang-Undang Nomor 19 Tahun 2016, mencakup berbagai bentuk kejahatan siber termasuk cracking. Cracking, yang bertujuan merusak sistem untuk kepentingan pribadi dengan cara ilegal, dianggap sebagai salah satu bentuk kejahatan yang diatur dalam undang-undang tersebut. Pelaku cracking sering kali merusak sistem pengamanan untuk mencapai tujuan mereka, yang bisa meliputi pencarian keuntungan pribadi (Febriliani et al., 2019)

Para pelaku 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 menimbulkan kerugian finansial dan non-finansial yang signifikan. 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 (Abdurrahman et al., 2023)

Mengingat bahaya yang ditimbulkan oleh cracker, pemerintah telah mengesahkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang ini bertujuan untuk mengatasi kejahatan dunia maya, termasuk cracking. Pasal 30 Undang-Undang ini secara spesifik mengatur tentang akses ilegal, di mana cracking dianggap sebagai kegiatan ilegal meretas sistem elektronik orang lain dengan tujuan mendapatkan manfaat dari tindakan tersebut. Cracking tidak hanya dianggap sebagai pelanggaran akses tetapi juga berkaitan dengan pencurian, karena pelaku berusaha mengakses dan mengambil konten dari sistem elektronik yang diretas (Satria, 2016)

Fenomena cracker dan aktivitas cracking telah menjadi kekhawatiran yang meningkat dalam beberapa tahun terakhir. Sejarah cracking dimulai dengan insiden pada tanggal 12 Juni dan 12 Agustus 1995 terhadap The Spot dan Cracker Movie Page. Di Indonesia, serangan cracker pertama kali tercatat pada tahun 1997 dengan lima insiden terpisah. Situs internasional seperti NASA, Partai Konservatif Inggris, dan Spice Girls juga mengalami serangan cracker pada tahun yang sama (Sa’diyah, 2012)

Sejak serangan awal tersebut, jumlah korban serangan cracker terus meningkat, meskipun banyak yang tidak terdokumentasi dengan baik. Meski Indonesia terbilang lambat dalam mengadopsi teknologi informasi, negara ini juga telah menjadi korban dari kejahatan cracking (Sa’diyah, 2012)

### METODE PENELITIAN

Studi ini menggunakan metodologi kualitatif, berlandaskan pada kerangka hukum normatif sebagai dasar teoretisnya (Hamzah, 2022). Dengan menggunakan pendekatan hukum normatif, tujuan utamanya adalah untuk mengeksplorasi dan menganalisis struktur hukum yang ada saat ini, meliputi prinsip-prinsip dasarnya, regulasi yang relevan, serta bagaimana hukum ini diterapkan dalam kehidupan sehari-hari (Putranto & Harvelin, 2023)

Dalam kajian literatur, literasi hukum sangat krusial. Pemilihan bahan literatur dilakukan dengan mempertimbangkan keberagaman sumber, termasuk buku-buku, artikel jurnal, dan materi lain yang relevan, untuk mendapatkan pemahaman yang komprehensif tentang norma hukum yang terkait dengan subjek penelitian (Lewansorna et al., 2022)

Mengenai pengumpulan data, penelitian ini mengutamakan dua jenis sumber data, yakni data primer dan sekunder. Data primer diperoleh dari dokumen resmi pemerintah dan dokumen lain yang memiliki validitas yang terverifikasi (Irawan, 2020). Meskipun data sekunder mungkin tidak seotentik data primer dalam konteks hukum, keduanya berkontribusi secara komplementer dalam proses pengumpulan data. Penelitian ini berfokus pada ulasan literatur, dengan menggunakan analisis kualitatif sebagai metodologi utama dalam menyimpulkan hasil berdasarkan temuan yang diperoleh (Lewansorna et al., 2022)

### PEMBAHASAN I

1. **Hasil**

Cracking adalah bentuk serangan siber yang melibatkan peretasan sistem elektronik tanpa izin, seringkali dengan tujuan untuk memperoleh keuntungan atau akses ilegal ke informasi. Tindakan ini dianggap sebagai pelanggaran serius dalam hukum, dengan sanksi yang jelas dan ditetapkan. Selain dikenal sebagai pelanggaran akses, cracking seringkali dihubungkan dengan pencurian, karena pelaku bertujuan untuk tidak hanya memasuki sistem elektronik milik orang lain tetapi juga untuk mengambil konten yang ada di dalamnya. Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) khusus menangani akses ilegal, sementara Pasal 32 ayat (2) UU ITE secara spesifik mengatur cracking sebagai bentuk pencurian (Azis & Rumlus, 2021)

Selanjutnya, Pasal 362 dari Kitab Undang-Undang Hukum Pidana (KUHP) menyatakan bahwa pencurian adalah pengambilan barang milik orang lain dengan niat untuk memiliki secara ilegal. Hukumannya termasuk pidana penjara dan denda. Pasal 167 ayat (1) KUHP juga relevan, mengatur tentang pelanggaran hukum yang terjadi saat seseorang memasuki atau tinggal di dalam properti orang lain tanpa izin, menegaskan hukuman penjara dan denda bagi pelaku (Azis & Rumlus, 2021)

Cracker umumnya mengikuti serangkaian langkah metodis dalam proses penyusupan mereka. Tahapan ini meliputi:

1. Footprinting dan/atau Pencarian Data: Tahap awal di mana cracker mencari sistem yang rentan untuk disusupi. Mereka mengumpulkan data tentang target, termasuk jaringan dan ruang lingkup serangan potensial.
2. Scanning atau Pemilihan Sasaran: Tahap ini lebih aktif, di mana cracker mencari kelemahan dalam sistem target. Alat scanning seperti nmap digunakan untuk mengidentifikasi celah keamanan.
3. Enumerasi: Tahap intrusif yang melibatkan pencarian informasi sensitif seperti nama pengguna dan kata sandi. Alat seperti SMB Scanner digunakan untuk mengeksploitasi sumber daya yang dibagi dalam jaringan.
4. Gaining Access: Upaya mendapatkan akses sebagai pengguna biasa, seringkali melalui tebakan kata sandi.
5. Escalating Privilege: Setelah mendapatkan akses, cracker berusaha meningkatkan hak akses menjadi admin atau root, seringkali dengan mencuri file password yang tersimpan dalam sistem.
6. Pilfering: Mengumpulkan informasi lebih lanjut tentang sistem dan mencari akses ke sistem yang lebih terpercaya.
7. Covering Tracks: Menyembunyikan aktivitas ilegal, termasuk membersihkan log jaringan dan menggunakan alat seperti rootkit.
8. Creating Backdoors: Membuat pintu belakang dalam sistem untuk memudahkan akses di masa depan.
9. Denial of Service: Jika gagal menembus pertahanan, serangan Denial of Service dapat dilakukan untuk melumpuhkan sistem.

Tahapan-tahapan ini menunjukkan proses yang kompleks dan canggih yang digunakan oleh cracker untuk menembus dan mengendalikan sistem elektronik. Mereka menggunakan serangkaian alat dan teknik untuk mengidentifikasi dan mengeksploitasi kelemahan, serta untuk mempertahankan akses dan menyembunyikan jejak mereka. Proses ini tidak hanya menunjukkan keterampilan teknis tinggi tetapi juga perencanaan yang matang dan pemahaman mendalam tentang sistem yang mereka targetkan.

Pentingnya keamanan siber menjadi sangat jelas dalam konteks cracking. Organisasi dan individu harus sadar akan ancaman ini dan mengambil langkah-langkah pencegahan yang sesuai, termasuk mengimplementasikan keamanan yang kuat dan memastikan pembaruan sistem secara teratur untuk menangkal serangan cracker. Kesadaran dan pendidikan tentang keamanan siber adalah kunci dalam melindungi data dan sistem dari serangan semacam ini, yang bisa memiliki konsekuensi yang merusak dan jangka panjang bagi korban.

1. **Pembahasan**

Keberadaan tindak pidana memberikan alasan bagi negara untuk menggunakan haknya dalam penerapan hukum pidana melalui lembaga seperti kepolisian, kejaksaan, dan pengadilan. Hak negara ini meliputi hak untuk menuntut, mengadili, dan menjatuhkan hukuman kepada individu yang diduga melakukan tindak pidana, baik itu tindakan aktif (melakukan sesuatu) atau pasif (tidak melakukan sesuatu). Dengan kata lain, sebuah perbuatan hanya dapat dipandang sebagai tindak pidana jika memenuhi semua unsur-unsur yang diperlukan. Jika salah satu unsur tidak terpenuhi, maka tidak dapat dianggap sebagai tindak pidana karena arti dan maksudnya berbeda (Satria, 2016)

Sebuah perbuatan dapat diklasifikasikan sebagai tindak pidana jika memenuhi lima unsur berikut: 1) Harus ada suatu tindakan; 2) Tindakan tersebut harus sesuai dengan deskripsi dalam undang-undang; 3) Tindakan itu dilakukan tanpa hak (melawan hukum); 4) Tindakan tersebut harus dapat dipertanggungjawabkan kepada pelaku; 5) Tindakan tersebut diancam dengan hukuman (Satria, 2016)

Pemberian sanksi pidana merupakan salah satu cara untuk mencapai tujuan hukum pidana. Ada tiga teori utama tentang pembenaran dan syarat pemidanaan: 1) Teori Absolut atau Teori Pembalasan, yang menekankan pada hukuman yang setara dengan kejahatan yang dilakukan; 2) Teori Relatif, yang bertujuan untuk mencapai manfaat dari pemidanaan, termasuk mencegah kejahatan dan memperbaiki pelaku; 3) Teori Gabungan, yang menggabungkan aspek pembalasan dan tujuan pemidanaan (Satria, 2016)

Dalam konteks penanganan kejahatan cracking terhadap sistem elektronik pemerintah, penggunaan hukum pidana dan sanksi memiliki tujuan tertentu. Berdasarkan teori absolut, tujuan pemidanaan adalah sebagai pembalasan atas tindakan pelaku di dunia siber. Menurut teori relatif, tujuannya adalah untuk memelihara ketertiban masyarakat, memperbaiki kerugian akibat kejahatan, memperbaiki perilaku pelaku, dan mencegah kejahatan. Sementara teori gabungan menggabungkan kedua aspek tersebut, bukan hanya bertujuan untuk pembalasan dan memberikan rasa aman, tetapi juga mencari alternatif non-pidana dalam rehabilitasi pelaku (Abdurrahman et al., 2023)

Untuk cracker yang melakukan cracking terhadap sistem elektronik pemerintah, upaya penal dapat diterapkan melalui UU ITE. Untuk kepastian hukum dan manfaat dari aturan yang ditetapkan, penuntut umum dapat merujuk pada Pasal 52 ayat (2) UU ITE yang menyatakan sistem elektronik dan informasi elektronik milik pemerintah yang digunakan untuk layanan publik dapat dipidana. UU ITE mengklasifikasikan dua jenis sistem elektronik milik pemerintah, yaitu sistem untuk layanan publik dan badan strategis. Penentuan jumlah atau lamanya sanksi pidana harus sesuai dengan modus dan kehendak terdakwa (Abdurrahman et al., 2023)

Lebih jauh lagi, dalam penegakan hukum pidana, penegak hukum juga sebaiknya menggunakan Pasal 52 ayat (3) UU ITE, yang menambah dua pertiga dari ancaman pidana pokok untuk tindakan terhadap komputer dan/atau sistem elektronik milik pemerintah dan badan strategis. Ini termasuk lembaga seperti bank sentral, keuangan, dan lembaga internasional. Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga menyediakan panduan untuk melindungi institusi dengan data elektronik strategis (Abdurrahman et al., 2023)

1. **PENUTUP**
2. **Kesimpulan**

Pentingnya Teknologi Informasi dan Tantangan Kejahatan Siber: Studi ini menggarisbawahi pentingnya teknologi informasi dalam perkembangan ekonomi dan sosial global. Namun, dengan kemajuan ini, muncul tantangan kejahatan siber seperti cracking, yang tidak hanya merugikan secara finansial tetapi juga mengancam kepercayaan publik terhadap teknologi.

Regulasi Undang-Undang ITE dan Penanganan Cracking: Analisis menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia memberikan kerangka hukum untuk mengatasi cracking. Namun, penelitian ini menemukan bahwa ada kebutuhan untuk penegakan hukum yang lebih efektif dan penyesuaian regulasi untuk menangani bentuk kejahatan siber yang terus berkembang.

Metodologi Cracker dan Respon Hukum: Dengan memahami metodologi yang digunakan oleh cracker, termasuk 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.

Pengaruh Teori Hukum pada Cracking: 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.

1. **Saran**

Perbaikan Regulasi dan Penegakan Hukum: Diperlukan revisi dan peningkatan dalam regulasi UU ITE untuk lebih efektif menangani kejahatan siber. Ini termasuk penyesuaian pasal-pasal tertentu untuk mengakomodasi perubahan teknologi dan praktik cracking.

Peningkatan Keamanan Siber dan Kesadaran Publik: Penelitian ini menyarankan peningkatan infrastruktur keamanan siber dan peningkatan kesadaran publik tentang risiko kejahatan siber. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat umum perlu ditingkatkan untuk membangun pertahanan yang lebih kuat terhadap serangan siber.

Pendekatan Multidisiplin dalam Penanganan Kejahatan Siber: Terakhir, penelitian ini merekomendasikan pendekatan multidisiplin dalam penanganan kejahatan siber. Ini termasuk menggabungkan aspek hukum, teknologi, psikologi, dan sosial untuk tidak hanya menghukum tetapi juga merehabilitasi pelaku, sehingga mengurangi insiden kejahatan siber di masa depan.

1. **DAFTAR PUSTAKA**

Irawan, V. (2020). ANALISIS YURIDIS TERHADAP PELANGGARAN HAK CIPTA PERMAINAN VIDEO (VIDEO GAMES) BERUPA PEMBAJAKAN SECARA ONLINE. *In Journal of Intellectual Property (Vol. 3, Issue 2). www.journal.uii.ac.id/JIPRO*

Lewansorna, D., Rina, E., Toule, M., & Sopacua, M. (2022). Pertanggungjawaban Pidana Aparat Kepolisian Yang Melakukan Kekerasan Terhadap Demonstran *(Vol. 2, Issue 1)*

Putranto, R. D., & Harvelian, A. (2023). Tanggung Jawab Pelaku Usaha dalam Transaksi Elektronik melalui Situs Internet di Tinjau dari Perspektif Hukum Perlindungan Konsumen. *FOCUS, 4(1), 36–41. https://doi.org/10.37010/fcs.v4i1.1153*

Robbani, H., & Yuliana, N. (2022). Analysis of Factors Affecting Learning Difficulties during the Covid 19 Pandemic. *FOCUS, 3(1), 55–58.* <https://doi.org/10.37010/fcs.v3i1.537>

Satria, Banu Rachman (2016) *Cracking Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Hukum Pidana Islam.* Yogyakarta : Universitas Islam Negeri Sunan Kalijaga.

Tacino, M. Jefri Maruli (2020) Perlindungan Hukum Terhadap Hak Pribadi Seseorang Di Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Dinamika, Jurnal Ilmiah Ilmu Hukum, Volume 26, Nomor 2.*

Febriliani, C., Ismunarno & Lukitasari, Diana (2019) Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta. *Recidive Volume 8 No. 3.*

Abdurrahman, Wulandari, Widati & Putri, Nella Sumika (2023) Model Penegakan Hukum Pidana Terhadap Cracker Pada Sistem Elektronik Milik Pemerintah Dikaitkan Dengan Undang-Undang Informasi Transaksi Elektronik. *Eksekusi: Journal Of Law Vol. 5 No. 1.*

Sa’diyah, Nur Khalimatus (2012) Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik. *PERSPEKTIF Volume 17. No. 2.*

Azis, Mariya & Rumlus, Muhammad Hasan (2021) Perlindungan Hukum Pada Masyarakat Dari Tindakan Cracking Perspektif Uu Informasi Dan Transaksi Elektronik Dan Hukum Pidana Islam. *Equality Before The Law, Vol 1 No 1.*