

The Role Of Criminal Law In Combating Hacking Crimes And Protecting User Accounts: Analysis Of Articles 31 And 32 Of The Ite Law

Aditiarman

Ilmu Hukum, Fakultas Hukum, Universitas Jambi

e-mail: aditiarmankrc@gmail.com

ABSTRACT

The advancement of information and communication technology has ushered in a new era in human life, particularly in the digital realm. Despite its convenience and benefits, the digital era also exposes vulnerabilities to various cybercrimes, one of which is hacking. Hacking can lead to significant losses for individuals, organizations, and even nations. Cybercrime, especially hacking and threats to user account security, poses a serious challenge in the digital age. Criminal law, specifically Articles 31 and 32 of the Information and Electronic Transactions Act (ITE Act) in Indonesia, plays a crucial role in combating these crimes. This article examines the role of criminal law in protecting computer systems and electronic networks, and analyzes the effectiveness of Articles 31 and 32 of the ITE Act in this context.

Keywords: *cybercrime, hacking, account security, Criminal Law, Article 31 ITE Act, Article 32 ITE Act.*

Article submission: 24 Jul 24

Article revision: 27 Jul 24

Article acceptance: 29 Jul 24

I. INTRODUCTION

Perkembangan pesat dalam teknologi informasi dan komunikasi telah mengubah lanskap kehidupan manusia di era digital. Manfaatnya yang besar dalam mempermudah akses informasi dan memfasilitasi komunikasi global juga diimbangi dengan tantangan keamanan yang semakin kompleks. Salah satu

ancaman utama dalam dunia digital adalah kejahatan hacking, yang tidak hanya dapat mengakibatkan kerugian finansial yang signifikan tetapi juga mengancam privasi dan keamanan data pengguna. Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 31 dan 32, memainkan peran sentral dalam menanggulangi kejahatan semacam ini.

Penelitian terkini menyoroti kesenjangan antara kondisi ideal dan realitas yang dihadapi dalam penerapan hukum pidana terhadap kejahatan hacking. Meskipun kerangka hukum telah ditetapkan, implementasi yang efektif dan penegakan yang konsisten masih menjadi tantangan. Studi oleh Wahyuni (2022) menunjukkan bahwa meskipun Indonesia memiliki kerangka hukum seperti UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penegakan hukum terhadap kejahatan hacking masih belum efektif. Hal ini disebabkan oleh kompleksitas dan transnasionalitas kejahatan hacking, yang sulit untuk diatur oleh hukum nasional. Dalam konteks ini, perlindungan akun pengguna menjadi krusial, dengan Habibi dan Liviani (2020) menemukan bahwa Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah "cybercrime".

Namun demikian, upaya hukum dalam melindungi sistem komputer dan jaringan elektronik dari serangan cyber masih perlu diperkuat. Oleh karena itu, penelitian ini bertujuan untuk menganalisis peran konkret dari Pasal 31 dan 32 UU ITE dalam konteks perlindungan terhadap kejahatan hacking dan mempertimbangkan inovasi dalam penerapan hukum pidana untuk meningkatkan efektivitasnya.

Dengan mengintegrasikan perspektif teori dan hasil penelitian terkini, pendahuluan ini menguraikan pentingnya mengevaluasi dan memperkuat kerangka hukum yang ada dalam menanggapi tantangan keamanan yang berkembang di era digital saat ini. Analisis mendalam terhadap Pasal 31 dan 32 UU ITE diharapkan akan memberikan kontribusi yang signifikan dalam memperbaiki kerangka hukum

yang ada dan menyediakan landasan yang lebih kokoh untuk perlindungan terhadap kejahatan siber di masa mendatang.

II. LITERATURE REVIEW

Deskripsi Pasal 31 dan 32 UU ITE

Pasal 31 UU ITE mengatur larangan terhadap akses ilegal terhadap sistem komputer atau jaringan elektronik. Penelitian ini menemukan bahwa Pasal 31 memberikan dasar hukum yang kuat untuk melindungi infrastruktur digital dari akses yang tidak sah dan serangan hacking yang mengancam keamanan sistem komputer.

Pasal 32 UU ITE, di sisi lain, mengatur tentang larangan terhadap penyalahgunaan informasi dalam sistem elektronik dengan tujuan memperoleh keuntungan secara tidak sah atau merugikan pihak lain. Analisis menunjukkan bahwa Pasal 32 memberikan landasan hukum yang penting untuk menghukum pelaku kejahatan yang menggunakan teknik hacking untuk tujuan ekonomi atau merugikan pihak lain.

III. METHODS

Penelitian ini menggunakan pendekatan analisis hukum normatif untuk mengkaji peran Pasal 31 dan 32 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam melawan kejahatan hacking dan perlindungan akun pengguna di Indonesia. Rancangan penelitian berfokus pada analisis teks hukum dan interpretasi pasal-pasal yang relevan dalam konteks kejahatan siber.

Populasi dan Sampel

Populasi penelitian ini adalah seluruh regulasi dan putusan hukum terkait kejahatan hacking serta perlindungan akun pengguna yang berada dalam lingkup UU ITE. Sampel yang digunakan adalah Pasal 31 dan 32 UU ITE beserta penafsiran dan aplikasinya dalam kasus-kasus konkret.

Teknik Pengumpulan Data

Data dikumpulkan melalui studi pustaka terhadap literatur hukum, regulasi resmi, putusan pengadilan, dan panduan interpretatif terkait hukum cyber di Indonesia.

Informasi juga diperoleh dari laporan kasus yang berkaitan dengan kejahatan hacking dan pelanggaran akun pengguna yang dipublikasikan oleh lembaga terkait.

Teknik Analisis Data

Analisis data dilakukan dengan pendekatan deskriptif kualitatif, yang melibatkan proses pengumpulan data primer berupa teks hukum dan interpretasi resmi. Data dianalisis secara tematis dan kontekstual untuk mengeksplorasi implementasi Pasal 31 dan 32 UU ITE dalam penegakan hukum terhadap kejahatan siber.

Prosedur penelitian yang lengkap dapat dilihat dalam diagram alir yang menyajikan langkah-langkah analisis teks hukum dan aplikasi interpretatif secara sistematis tanpa penomoran subjudul yang panjang.

IV. RESULTS

Hasil penelitian ini berfokus pada analisis terhadap peran Pasal 31 dan 32 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam melawan kejahatan hacking dan perlindungan akun pengguna di Indonesia. Berikut adalah temuan utama dari penelitian ini:

1. Implementasi dan Penegakan Hukum

Meskipun kerangka hukum yang kuat telah ditetapkan melalui Pasal 31 dan 32 UU ITE, implementasi dan penegakan hukum yang konsisten masih menjadi tantangan. Data dari studi kasus menunjukkan bahwa ada kesenjangan dalam implementasi hukum antara kasus yang dilaporkan dan tindakan hukum yang sesungguhnya diambil terhadap pelaku kejahatan cyber.

Menurut Ishak, S., Malik, F., & Suwarti, S. (2023), hukuman penjara bagi pelaku kejahatan cyber bertujuan untuk menghukum, melindungi masyarakat, dan menciptakan efek jera, sesuai dengan prinsip-prinsip filosofi hukum pidana.

2. Tantangan dan Solusi

Pembahasan dari hasil penelitian ini menyoroti beberapa tantangan utama dalam melawan kejahatan hacking, termasuk kebutuhan akan peningkatan kapasitas penyidikan digital, kerjasama lintas sektoral antara pemerintah dan sektor swasta, serta kesadaran masyarakat tentang keamanan cyber. Solusi yang diajukan

termasuk pendekatan holistik dalam penegakan hukum dan peningkatan investasi dalam keamanan teknologi informasi.

Pembahasan dari hasil penelitian ini menggarisbawahi pentingnya peran hukum pidana, khususnya Pasal 31 dan 32 UU ITE, dalam melindungi infrastruktur digital dari ancaman hacking dan penyalahgunaan data. Meskipun Pasal-pasal ini memberikan dasar hukum yang kuat, tantangan utama tetap terletak pada implementasi yang efektif dan penegakan hukum yang konsisten.

Hukum pidana memiliki peran yang sangat penting dalam upaya melawan kejahatan hacking dan melindungi akun pengguna. Di Indonesia, terdapat Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur mengenai tindak pidana terkait dengan hacking.

Pasal 31 UU ITE mengatur mengenai tindak pidana akses tanpa izin terhadap komputer dan/atau sistem elektronik milik orang lain. Sementara itu, Pasal 32 UU ITE mengatur mengenai tindak pidana perubahan, penambahan, pengurangan, transmisi, kerusakan, penghapusan, pemindahan, atau penyembunyian informasi elektronik dan/atau dokumen elektronik milik orang lain atau publik tanpa izin. Kedua pasal ini merupakan landasan hukum yang digunakan untuk menangkap pelaku kejahatan hacking. Ketentuan dalam UU ITE memberikan wewenang kepada aparat penegak hukum untuk melakukan penyelidikan, penyidikan, dan penuntutan terhadap pelaku hacking. Dengan demikian, hukum pidana dalam UU ITE memiliki peran strategis dalam menegakkan keadilan dan menjamin perlindungan terhadap korban kejahatan hacking di Indonesia.

Analisis mendalam terhadap studi kasus dan data statistik menunjukkan bahwa masih ada ruang untuk perbaikan dalam kapasitas penyidikan cyber dan koordinasi antara lembaga penegak hukum. Perbaikan ini dapat mencakup peningkatan pelatihan bagi petugas penegak hukum dalam teknik investigasi digital serta penguatan kerjasama internasional dalam penanganan kejahatan cyber lintas batas.

Pengembangan kebijakan yang lebih proaktif untuk meningkatkan kesadaran masyarakat tentang keamanan cyber dianggap sangat penting dalam menghadapi tantangan kejahatan siber, terutama hacking, yang bisa terjadi di masa depan.

Keamanan cyber semakin penting seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi yang telah menjangkau hampir semua bidang kehidupan modern. Dalam konteks ini, usaha untuk meningkatkan pemahaman masyarakat tentang risiko dan tindakan pencegahan terhadap ancaman keamanan cyber menjadi sangat diperlukan. Oleh karena itu, upaya untuk menghadapi dan mencegah kejahatan siber tidak hanya menjadi tanggung jawab pemerintah, tetapi juga memerlukan partisipasi aktif dari semua pihak, termasuk sektor swasta, akademisi, dan masyarakat umum. Dengan demikian, penelitian ini memberikan kontribusi penting dalam mempertimbangkan inovasi dalam penerapan hukum pidana untuk memastikan efektivitas dalam melawan kejahatan siber yang semakin kompleks.

Kejahatan hacking, yang sering melibatkan penetrasi sistem komputer atau jaringan dengan tujuan merusak, mencuri data sensitif, atau mengganggu operasi organisasi atau pemerintahan, telah menunjukkan pola yang semakin canggih dan berpotensi merugikan. Serangan cyber dapat mengakibatkan kerugian finansial yang signifikan, melanggar privasi individu atau perusahaan, serta mengganggu stabilitas sosial dan politik.

Menurut Kirana, P., & Khalisah, A. M. (2022). Kejahatan dunia maya merujuk pada tindakan kriminal yang terkait dengan teknologi atau dunia maya yang dapat merugikan kepentingan umum atau pribadi. Undang-Undang Nomor 11 Tahun 2009 tentang Informasi dan Transaksi Elektronik yang telah mengalami perubahan dalam Undang-Undang Nomor 19 Tahun 2019 (disingkat sebagai UU ITE) mengatur berbagai bentuk kejahatan dunia maya dalam 9 pasal utama, di antaranya termasuk kejahatan peretasan. Norma hukum Indonesia yang mengatur kejahatan dunia maya masih terbatas pada UU ITE. Meskipun aksesibilitas internet di Indonesia semakin meningkat, koordinasi dengan penegakan hukum belum optimal, dan masyarakat menghadapi permasalahan serius.

Dalam penelitian yang di lakukan oleh Saputra, PY, Yuniato, DR, & Arissandy, SS (2019). Selaku negeri hukum, Indonesia mempunyai peraturan-peraturan yang mengendalikan ikatan antar warga, salah satunya merupakan peraturan tentang data serta transaksi elektronik. Peraturan tersebut tertulis pada

UU Nomor 19 tahun 2016 tentang pergantian atas undang- undang no 11 tahun 2008 UU ITE. UU ITE terbuat disebabkan pada era digital ini gempar terjalin permasalahan kriminal lebih- lebih pada bidang data serta transaksi elektronik(CyberCrime) semacam, penipuan online, perjudian online, pemakaian informasi yang ilegal, serta kabar palsu(hoax). Kasus- kasus tersebut meyakinkan bahwa UU ITE belum tersosialisasi dengan baik kepada warga, sehingga perlunya suatu sistem pencarian data(Information Retrieval) bersumber pada permasalahan tentang undang- undang ini supaya mempermudah dalam memahaminya. Pada riset ini, information retrieval ataupun sistem temu kembali informasi digunakan buat mencari pasal- pasal di UU ITE yang relevan pada sesuatu permasalahan bersumber pada deskripsi permasalahan tersebut. Pada pencarian pasal tersebut digunakan tata cara Latent Semantic Indexing(LSI). Metode dalam LSI mengadopsi proses matematis reduksi ukuran Singular Value Decomposition(SVD). Tata cara cosine kesamaan digunakan buat menghitung kesamaan ataupun keakraban dokumen pasal dengan query. Sistem ini memakai 21 pasal syarat beserta 21 pasal pidananya serta 10 query permasalahan ataupun deskripsi kejahatan selaku informasi uji. Sistem menghitung serta memastikan pasal yang terpaut bersumber pada query ataupun deskripsi permasalahan kejahatan yang dimasukkan. Tingkatan keberhasilan dari tata cara ini buat menciptakan hasil pencarian yang relevan bisa dilihat lewat besarnya 83. 33% untuk recall, 50% untuk precission serta 62. 5% untuk f-measure. Kata kunci-pengambilan informasi, pengindeksan semantik laten, dekomposisi nilai singular, kesamaan kosinus, penambahan teks, UU ITE.

Hasil dari penelitian Azizah, N. (2023). diuraikan dalam ketentuan Pasal 40 UU No. 36 Tahun 1999 tentang Telekomunikasi, Pasal 31 UU No. 11 Tahun 2008 tentang ITE, dan Pasal 322 ayat 1-3 UU No. 1 Tahun 2023 tentang KUHP yang dengan tegas menyatakan bahwa penyadapan yang dilakukan dalam bentuk apapun merupakan suatu perbuatan pidana yang berakibat penjatuhan sanksi pidana, dengan kriteria penyadapan itu dilakukan dengan sengaja secara melawan hukum untuk memperoleh informasi/dokumen elektronik milik orang lain. Meskipun penyadapan merupakan suatu perbuatan yang dilarang, namun didalam beberapa peraturan perundang-undangan, penyadapan ini dapat dimungkinkan

untuk dilakukan oleh aparat penegak hukum guna mengungkap suatu tindak pidana tertentu berdasarkan undang-undang yang berlaku.

Kecanduan gadget di kalangan remaja dieratkan dengan rendahnya pengendalian diri, kesepian, dan perilaku mencari sensasi, dan peran sentral orang tua, guru, pemerintah, dan masyarakat memainkan peran penting dalam mencegahnya. Menurut DM, M., & Hardianto, R. (2022), Sosialisasi UU ITE sangat signifikan untuk mengantisipasi penyalahgunaan dan menghindari potensi jatuhnya korban, khususnya di kalangan masyarakat kelas bawah dan pengguna media sosial.

Pasal 31 UU ITE mengatur tentang unsur-unsur tindak pidana “tanpa hak” mengakses komputer dan/atau sistem elektronik milik orang lain, yaitu : Melakukan perbuatan (Pelaku melakukan suatu tindakan), tanpa hak (Pelaku tidak memiliki hak untuk mengakses komputer dan/atau sistem elektronik milik orang lain), mengakses (Pelaku memasuki atau menembus sistem komputer dan/atau sistem elektronik milik orang lain), Komputer dan/atau sistem elektronik (Sasaran tindakan adalah komputer dan/atau sistem elektronik); Milik orang lain (Komputer dan/atau sistem elektronik tersebut dimiliki oleh orang lain).

Pasal 32 UU ITE mengatur tentang unsur-unsur tindak pidana “tanpa hak” mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik, yaitu : Melakukan perbuatan (Pelaku melakukan suatu tindakan), tanpa hak (Pelaku tidak memiliki hak untuk mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan Informasi Elektronik dan/atau Dokumen Elektronik), mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan (Pelaku melakukan tindakan terhadap Informasi Elektronik dan/atau Dokumen Elektronik), informasi Elektronik dan/atau Dokumen Elektronik (Sasaran tindakan adalah Informasi Elektronik dan/atau Dokumen Elektronik), milik orang lain atau milik publik (Informasi Elektronik dan/atau Dokumen Elektronik tersebut dimiliki oleh orang lain atau milik publik).

Selain penegakan hukum pidana, penting juga untuk melakukan upaya pencegahan dan perlindungan akun pengguna dari kejahatan hacking. Beberapa langkah yang dapat dilakukan untuk melindungi akun pengguna, antara lain : Membuat password yang kuat dan unik untuk setiap akun, mengaktifkan autentikasi dua faktor (2FA), menginstal perangkat lunak antivirus dan anti-malware yang terbaru; berhati-hati saat mengklik tautan atau membuka lampiran.

V. CONCLUSION AND SUGGESTION

dan/atau Dokumen Elektronik), informasi Elektronik dan/atau Dokumen Elektronik (Sasaran tindakan adalah Informasi Elektronik dan/atau Dokumen Elektronik), milik orang lain atau milik publik (Informasi Elektronik dan/atau Dokumen Elektronik tersebut dimiliki oleh orang lain atau milik publik).

Selain penegakan hukum pidana, penting juga untuk melakukan upaya pencegahan dan perlindungan akun pengguna dari kejahatan hacking. Beberapa langkah yang dapat dilakukan untuk melindungi akun pengguna, antara lain : Membuat password yang kuat dan unik untuk setiap akun, mengaktifkan autentikasi dua faktor (2FA), menginstal perangkat lunak antivirus dan anti-malware yang terbaru; berhati-hati saat mengklik tautan atau membuka lampiran.

VI. BIBLIOGRAPHY

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime). *Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 401.

Wahyuni, S., Murni, I., & Yarni, N. (2023). Kecanduan Gadget Oleh Remaja Dalam Perspektif Sosiologi. *Pendas: Jurnal Ilmiah Pendidikan Dasar*. <https://doi.org/10.23969/jp.v8i1.7588>.

DM, M., & Hardianto, R. (2022). Sosialisasi UU ITE di Tengah Maraknya Penggunaan Media Sosial. *Jurnal Riset Keterlibatan Masyarakat untuk Keberlanjutan*. <https://doi.org/10.31258/cers.2.1.12-19>.

Kirana, P., & Khalisah, A. M. (2022). Implementasi Norma Hukum Terhadap Tindak Pidana Peretasan (Hacking) di Indonesia. *Jurist-Diction*, 5(6).

Azizah, N. (2023). Tindak Pidana Penyadapan (Cyber Espionage) Menurut Hukum Positif Di Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, 9(13), 475-486.

Ishak, S., Malik, F., & Suwarti, S. (2023). Analisis Pelaksanaan Pidana Penjara terhadap Pelaku Kejahatan Dunia Maya. *Jurnal Ilmu Sosial*. <https://doi.org/10.46799/jss.v4i2.538>.

Saputra, PY, Yuniarto, DR, & Arissandy, SS (2019). Pencarian Pasal Pada UU ITE Berdasarkan Kasus Cyber Crime Dengan Metode Latent Semantic Indexing (LSI).

UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008

Undang-Undang Nomor 11 Tahun 2009

Undang-Undang Nomor 19 Tahun 2019

Pasal 40 UU No. 36 Tahun 1999 tentang Telekomunikasi

Wahyuni, W. (2022, September 12). Jerat Hukum Peretasan oleh Hacker. Retrieved Juli 23, 2024, from hukumonline: <https://www.hukumonline.com/berita/a/jerat-hukum-peretasan-oleh-hacker-lt631ec0ed9e52c>

Pasal 322 ayat 1-3 UU No. 1 Tahun 2023