**Jurnal Dialogica**
Volume I Issue 2 Tahun 2026

# Utbk Bocor: Gagal Sistem Atau Gagal Penegakan Hukum?

Marwati M Leo[1], Hambali Thalib[2], Muhammad Zulkifli Muhdar[3].

[123] Fakultas Hukum, Universitas Muslim Indonesia

*Email Koresponden*: marwahmleo44@gmail.com

**Abstrak**: Penelitian ini bertujuan untuk menganalisis bentuk pertanggungjawaban hukum serta faktor-faktor yang memengaruhi penerapan pertanggungjawaban terhadap pelaku peretasan sistem elektronik dalam pelaksanaan Ujian Tulis Berbasis Komputer Seleksi Nasional Berdasarkan Tes (UTBK-SNBT) di Universitas Hasanuddin tahun 2025. Kasus ini melibatkan keterlibatan joki dan peserta ujian dalam suatu skema peretasan sistem elektronik yang bertujuan memperoleh dan memanfaatkan informasi ujian secara tidak sah, sehingga berpotensi merusak integritas serta prinsip keadilan dalam sistem seleksi nasional berbasis komputer. Penelitian ini menggunakan metode penelitian hukum empiris dengan pendekatan kualitatif melalui wawancara dengan penyidik di Kepolisian Resor Kota Besar Makassar serta studi kepustakaan terhadap berbagai sumber hukum dan literatur yang relevan. Pembaharuan penelitian ini terletak pada analisis pertanggungjawaban hukum dalam kasus peretasan sistem elektronik yang terjadi dalam konteks pelaksanaan seleksi nasional pendidikan tinggi, dengan menyoroti keterlibatan beberapa pelaku dalam satu rangkaian perbuatan yang terorganisasi serta mengkaji faktor-faktor non-yuridis yang memengaruhi penerapan pertanggungjawaban hukum dalam praktik penegakan hukum. Hasil penelitian menunjukkan bahwa para pelaku peretasan sistem elektronik dikenakan pertanggungjawaban pidana berupa ancaman pidana penjara dan pidana denda. Selain itu, penerapan pertanggungjawaban hukum terhadap para pelaku dipengaruhi oleh beberapa faktor, antara lain usia serta kemampuan finansial pelaku yang menjadi pertimbangan dalam proses penegakan hukum. Kesimpulan penelitian ini menunjukkan bahwa praktik peretasan sistem elektronik dalam pelaksanaan UTBK-SNBT tidak hanya merupakan pelanggaran terhadap sistem teknologi informasi, tetapi juga berdampak pada kepercayaan publik terhadap sistem seleksi pendidikan tinggi. Rekomendasi dari Penelitian ini, antara lain diperlukan penguatan sistem keamanan teknologi informasi serta koordinasi yang lebih intensif antara penyelenggara ujian, institusi pendidikan tinggi, dan aparat penegak hukum guna mencegah terulangnya tindak pidana serupa di masa mendatang.

**Kata Kunci:** Peretasan Sistem Elektronik, Joki UTBK, Pertanggungjawaban Hukum.

***Abstract**: This study aims to analyze the forms of legal accountability and the factors influencing the application of legal responsibility toward perpetrators of electronic system hacking during the implementation of the Computer-Based Written Examination for the National Selection Based on Test (UTBK-SNBT) at Hasanuddin University in 2025. The case involves the participation of exam jockeys and actual test participants in an organized electronic system hacking scheme aimed at obtaining and utilizing examination information unlawfully, which potentially undermines the integrity and fairness of the national computer-based selection system. This research employs an empirical legal research method with a*

*qualitative approach through interviews with investigators at the Makassar City Police Resort as well as a literature study of various legal sources and relevant academic works. The novelty of this research lies in its analysis of legal accountability in electronic system hacking within the context of national higher education entrance examinations, highlighting the involvement of multiple actors in an organized series of actions and examining non-juridical factors that influence the implementation of legal accountability in law enforcement practices. The results of the study indicate that the perpetrators of electronic system hacking are subjected to criminal liability in the form of imprisonment and monetary fines. Furthermore, the application of legal accountability is influenced by several factors, including the perpetrators' age and financial capability, which are considered in the law enforcement process. This study concludes that electronic system hacking in the UTBK-SNBT examination not only constitutes a violation of information technology systems but also affects public trust in the higher education selection system. Therefore, strengthening information technology security systems and enhancing coordination among examination organizers, higher education institutions, and law enforcement agencies are necessary to prevent similar offenses from occurring in the future.*

***Keywords:*** *Electronic System Hacking, UTBK Jockey, Legal Accountability.*

## PENDAHULUAN

Meningkatnya ketergantungan terhadap sistem elektronik dalam proses ujian nasional telah secara signifikan meningkatkan efisiensi dan aksesibilitas, namun di sisi lain juga membuka peluang munculnya berbagai bentuk kejahatan siber [1]. Di Indonesia, penerapan ujian berbasis komputer, termasuk Ujian Tulis Berbasis Komputer (UTBK), merupakan bagian penting dari sistem seleksi masuk perguruan tinggi negeri [2]. Akan tetapi, perkembangan teknik peretasan sistem elektronik yang semakin canggih menimbulkan tantangan serius terhadap integritas, kredibilitas, dan prinsip keadilan dalam penyelenggaraan ujian tersebut.

UTBK dirancang untuk menjamin transparansi serta kesetaraan kesempatan bagi seluruh peserta dalam proses penerimaan mahasiswa baru. Namun demikian, terungkapnya sejumlah kasus peretasan sistem elektronik yang melibatkan joki ujian dan peserta terdaftar menunjukkan adanya kerentanan dalam sistem, khususnya pada aspek pengawasan, mekanisme autentikasi, serta infrastruktur keamanan digital[3]. Kejahatan siber terhadap sistem elektronik umumnya dilakukan secara sengaja dan terstruktur, sehingga memenuhi unsur perbuatan pidana dan kesalahan sebagaimana diatur dalam hukum pidana Indonesia [4].

Kajian-kajian sebelumnya mengenai kejahatan siber di Indonesia cenderung berfokus pada bentuk umum tindak pidana elektronik berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), seperti akses ilegal, manipulasi data, dan penipuan daring. Selain itu, penelitian mengenai peran alat bukti elektronik dan analisis forensik digital juga menekankan pentingnya kedua aspek tersebut dalam pembuktian dan penentuan pertanggungjawaban pidana dalam perkara kejahatan siber [5]. Namun, perhatian terhadap persoalan pertanggungjawaban hukum akibat peretasan sistem elektronik dalam konteks sistem ujian nasional masih relatif terbatas, terutama yang melibatkan banyak aktor dengan peran berbeda, seperti joki ujian dan peserta asli.[6]

Oleh karena itu, penelitian ini bertujuan untuk menganalisis bentuk pertanggungjawaban hukum terhadap pelaku tindak pidana peretasan sistem elektronik dalam pelaksanaan UTBK di Universitas Hasanuddin tahun 2025, serta mengidentifikasi faktor-faktor yang memengaruhi penjatuhan pertanggungjawaban tersebut. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan penegakan hukum pidana, sekaligus menjadi rekomendasi praktis dalam memperkuat mekanisme pengawasan dan keamanan pada sistem ujian berbasis komputer guna mencegah terulangnya tindak pidana serupa di masa mendatang.

## METODE PENELITIAN

Penelitian ini menggunakan metode pendekatan yuridis normatif yang dipadukan dengan pendekatan empiris untuk menelaah norma hukum yang berkaitan dengan tindak pidana peretasan sistem elektronik serta melihat penerapannya dalam praktik penegakan hukum. Pendekatan normatif dilakukan dengan mengkaji ketentuan hukum yang mengatur mengenai tindak pidana peretasan sistem elektronik dan pertanggungjawaban pidana, sedangkan pendekatan empiris dilakukan untuk melihat implementasi hukum dalam kasus peretasan sistem elektronik pada pelaksanaan Ujian Tulis Berbasis Komputer (UTBK) di Universitas Hasanuddin tahun 2025. Spesifikasi penelitian ini bersifat deskriptif-analitis, yaitu menggambarkan secara sistematis permasalahan hukum yang terjadi dalam kasus peretasan sistem elektronik serta menganalisis penerapan pertanggungjawaban hukum terhadap para pelaku. Jenis data yang digunakan dalam

penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara dengan penyidik Unit Siber atau Unit 3 Satuan Reserse Kriminal Kepolisian Resor Kota Besar Makassar yang menangani perkara tersebut. Sementara itu, data sekunder diperoleh dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang relevan dengan permasalahan penelitian, seperti peraturan perundang-undangan, buku, jurnal ilmiah, serta pemberitaan terkait. Teknik pengumpulan data dilakukan melalui wawancara dan studi kepustakaan terhadap berbagai dokumen hukum serta literatur yang berkaitan dengan tindak pidana peretasan sistem elektronik. Selanjutnya, data yang telah terkumpul dianalisis secara kualitatif dengan mengaitkan temuan empiris dengan norma hukum dan teori pertanggungjawaban pidana guna memperoleh pemahaman yang komprehensif mengenai bentuk pertanggungjawaban hukum serta faktor-faktor yang memengaruhi penerapannya dalam kasus peretasan sistem elektronik pada pelaksanaan UTBK di Universitas Hasanuddin tahun 2025.

## PEMBAHASAN

### 1. Bentuk Pertanggungjawaban Hukum Terhadap Para Pelaku Tindak Pidana Peretasan Sistem Elektronik Dalam Ujian Tulis Berbasis Komputer

Dalam kasus peretasan sistem elektronik pada ujian tulis berbasis komputer di Universitas Hasanuddin tahun 2025, para pelakunya dikualifikasikan menjadi 2 (dua). Pertama, joki (pelaku teknis) atau penerima jasa, yaitu pihak yang secara aktif melakukan tindakan peretasan sistem elektronik, memasang aplikasi remote, mengakses sistem komputer ujian secara tidak sah, serta membantu mengerjakan soal ujian. Kedua, peserta asli ujian atau pemberi jasa, yakni pihak yang secara sadar meminta, menyetujui, dan memfasilitasi penggunaan jasa joki dengan tujuan memperoleh keuntungan berupa kelulusan dalam seleksi Ujian Tulis Berbasis Komputer [7]. Adapun bentuk pertanggungjawaban hukum terhadap para pelaku berdasarkan hasil wawancara dengan penyidik Unit Siber 3 Satreskrim Polrestabes Makassar pada 20 Januari 2026, ialah:

1. Pidana Penjara

Yang dimaksud pidana penjara dalam penelitian ini adalah pidana penjara menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yakni:

a. Pasal 46 ayat (1)

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

Dikategorikannya pidana penjara ini pada pelaku jika ia memenuhi unsur-unsur dalam pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi:

(1) Pasal 30 menakut-nakuti yang ditujukan Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

b. Pasal 48 ayat (1)

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Dikategorikannya pidana penjara ini pada pelaku jika ia memenuhi unsur-unsur dalam pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi:

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

c. Pasal 48 ayat (2)

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

Dikategorikannya pidana penjara ini pada pelaku jika ia memenuhi unsur-unsur dalam pasal 32 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang berbunyi:

(2) setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

2. Pidana Denda

Selain pidana penjara, bentuk pertanggungjawaban hukum terhadap para pelaku tindak pidana peretasan sistem elektronik dalam pelaksanaan Ujian Tulis Berbasis Komputer (UTBK) Universitas Hasanuddin Tahun 2025 juga dapat dikenakan dalam bentuk pidana denda. Pidana denda dalam perkara ini merupakan sanksi pidana yang bersifat kumulatif maupun alternatif, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik [8]. Adapun pasal-pasal mengenai pinda denda tersebut, yakni:

a. Pidana denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah) berdasarkan Pasal 46 ayat (1)

Pasal 46 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menentukan bahwa selain pidana penjara paling lama 6 (enam) tahun, pelaku juga dapat dijatuhi pidana denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah). Pidana denda ini dikenakan apabila pelaku memenuhi unsur Pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu melakukan akses terhadap komputer dan/atau sistem elektronik milik orang lain secara sengaja dan tanpa hak.

b. Pidana denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah) berdasarkan Pasal 48 ayat (1)

Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, mengatur bahwa setiap orang yang memenuhi unsur Pasal 32 ayat (1) dapat dipidana dengan pidana denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah). Pidana denda ini dikenakan terhadap pelaku yang dengan sengaja dan tanpa hak mengubah, memindahkan, atau mentransmisikan informasi elektronik milik orang lain atau milik publik.

c. Pidana denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah) berdasarkan Pasal 48 ayat (2)

Pasal 48 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menentukan pidana denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah) bagi setiap orang yang memenuhi unsur Pasal 32 ayat (2), yaitu memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak.

Kasus peretasan sistem elektronik dalam pelaksanaan Ujian Tulis Berbasis Komputer (UTBK) di Universitas Hasanuddin tahun 2025 terungkap setelah pihak internal kampus menemukan aktivitas tidak wajar pada sejumlah komputer ujian dan melaporkannya kepada Polrestabes Makassar. Hasil penyelidikan melalui pemeriksaan sistem dan rekaman CCTV menunjukkan adanya pemasangan aplikasi remote access pada komputer ujian yang memungkinkan akses sistem dari luar ruang ujian tanpa izin penyelenggara. Dalam perkara ini, kepolisian menetapkan sembilan orang tersangka. AL berperan sebagai koordinator yang merekrut joki dan mengatur alur pengiriman soal dan jawaban. MYI yang merupakan staf IT bertugas memasang aplikasi remote access pada komputer ujian, ZR menyediakan aplikasi tersebut, MS mengoperasikan akses jarak jauh untuk menerima soal ujian dan meneruskannya kepada CAI, sedangkan I berperan sebagai penghubung antar pelaku.

CAI bertindak sebagai joki yang mengerjakan soal ujian dari luar ruang ujian setelah soal dikirim melalui sistem yang telah diretas. Dalam pengembangan perkara, tiga tersangka tambahan yaitu MT, I, dan HI yang merupakan staf IT dan admin sistem UTBK juga ditetapkan sebagai tersangka. Barang bukti yang diamankan antara lain rekaman CCTV, tangkapan layar soal ujian, perangkat elektronik seperti ponsel dan flash disk, serta akun media sosial yang digunakan untuk mengirimkan soal kepada pelaku joki. Para pelaku dijanjikan imbalan hingga Rp200.000.000 apabila peserta yang dibantu berhasil lolos seleksi. Perbuatan tersebut menunjukkan adanya kerja sama terorganisasi untuk melakukan akses tanpa hak ke sistem elektronik serta memindahkan data ujian kepada pihak lain [9].

Berdasarkan kronologi dan peran masing-masing pelaku sebagaimana diuraikan di atas, penulis melakukan analisis yuridis terhadap ketentuan hukum yang relevan guna menilai terpenuhinya unsur-unsur tindak pidana dalam perbuatan para pelaku, antara lain:

1. Pasal 30 ayat (1)

   Perbuatan para pelaku memenuhi unsur Pasal 30 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik karena secara sengaja dan tanpa hak mengakses sistem elektronik milik penyelenggara UTBK. Unsur "setiap orang" terpenuhi karena seluruh pelaku merupakan subjek hukum yang dapat dimintai pertanggungjawaban pidana. Unsur "dengan sengaja" terlihat dari adanya perencanaan dan pembagian peran, termasuk pemasangan aplikasi remote access sebelum pelaksanaan ujian. Sementara itu, unsur "tanpa hak atau melawan hukum" terpenuhi karena akses terhadap sistem UTBK dilakukan tanpa izin penyelenggara dan di luar kewenangan yang diberikan, meskipun sebagian pelaku merupakan staf IT. Adapun unsur "mengakses komputer dan/atau sistem elektronik" terpenuhi melalui penggunaan aplikasi remote access yang memungkinkan pengendalian komputer ujian dari luar ruang ujian. Dengan demikian, tindakan para pelaku yang memasuki dan mengendalikan sistem UTBK secara tidak sah telah memenuhi unsur tindak pidana akses ilegal sebagaimana dimaksud dalam Pasal 30 ayat (1).
2. Pasal 32 ayat (1) dan ayat (2)

   Para pelaku juga memenuhi unsur Pasal 32 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik karena memindahkan dan mentransfer informasi elektronik berupa soal ujian kepada pihak lain secara melawan hukum. Hal ini terlihat dari tindakan mengambil screenshot soal ujian serta mengirimkannya kepada joki yang berada di luar ruang ujian. Unsur kesengajaan tercermin dari adanya koordinasi dan mekanisme yang dirancang untuk mengambil dan mengirimkan soal dari sistem resmi UTBK kepada pihak luar. Unsur "tanpa hak atau melawan hukum" juga terpenuhi karena soal ujian merupakan informasi elektronik yang bersifat terbatas dan hanya dapat diakses oleh peserta yang sah sesuai prosedur yang ditentukan penyelenggara. Dengan demikian, perbuatan para pelaku tidak hanya berupa akses ilegal terhadap sistem elektronik, tetapi juga pemindahan dan distribusi informasi

elektronik secara melawan hukum yang mengakibatkan kebocoran soal ujian dan berpotensi merusak integritas sistem seleksi nasional.

3. Pasal 46 ayat (1)

   Dalam wawancara penulis dengan penyidik unit siber polrestabes, penyidik menyatakan lebih cenderung menerapkan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah) sebagaimana diatur dalam Pasal 46 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang merupakan ketentuan pidana atas pelanggaran Pasal 30 ayat (1). Hal ini karena unsur utama yang pertama kali terbukti secara jelas adalah adanya akses ilegal terhadap sistem elektronik. Unsur perbuatannya meliputi adanya subjek hukum (para pelaku), adanya perbuatan mengakses sistem elektronik, dilakukan tanpa hak, dan dilakukan dengan kesengajaan. Penyidik menilai bahwa pembuktian akses ilegal relatif lebih konkret melalui barang bukti digital seperti log sistem, rekaman CCTV, serta perangkat yang digunakan.

   Namun apabila dianalisis lebih lanjut, menurut penulis Pasal 48 ayat (1) dan ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan ancaman pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah) yang merupakan ketentuan pidana atas pelanggaran Pasal 32 ayat (1) dan ayat (2) juga memiliki relevansi kuat dalam perkara ini, karena telah terjadi pemindahan dan distribusi informasi elektronik secara melawan hukum.

   Apabila dicermati secara lebih mendalam, akses ilegal dalam perkara ini sesungguhnya bukan merupakan tujuan akhir dari perbuatan para pelaku, melainkan hanya sarana untuk melakukan kejahatan yang lebih substansial, yaitu penguasaan dan pendistribusian informasi elektronik berupa soal ujian. Dengan kata lain, perbuatan yang paling merugikan dan berdampak luas bukan semata-mata tindakan memasuki sistem, tetapi tindakan memindahkan dan membuat dapat diaksesnya informasi rahasia kepada pihak yang tidak berhak [10]. Oleh karena itu, apabila dianalisis dari sudut pandang tingkat bahaya perbuatan (*social harm*) dan akibat yang ditimbulkan, maka pelanggaran terhadap Pasal

32 ayat (1) dan ayat (2) jo. Pasal 48 (1) dan ayat (2) memiliki bobot yang lebih serius dibandingkan dengan pelanggaran Pasal 30 ayat (1) jo. Pasal 46 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Secara doktrinal, keadaan ini dapat dikualifikasikan sebagai perbarengan peraturan (*concursus idealis*), dimana satu rangkaian perbuatan memenuhi lebih dari satu ketentuan pidana. Akses ilegal menjadi pintu masuk terjadinya pemindahan informasi elektronik. Namun demikian, apabila harus ditentukan ketentuan mana yang lebih mencerminkan inti delik, maka Pasal 32 ayat (1) dan ayat (2) lebih tepat digunakan sebagai dasar utama karena menyangkut perlindungan terhadap integritas dan kerahasiaan informasi elektronik. Dalam konteks ini, kebocoran soal ujian bukan hanya pelanggaran teknis sistem, melainkan bentuk manipulasi informasi yang mengancam prinsip keadilan dan objektivitas seleksi nasional [11].

Selain itu, ancaman pidana yang lebih berat dalam Pasal 48 ayat (1) dan ayat (2) menunjukkan bahwa pembentuk undang-undang memandang perbuatan pemindahan atau distribusi informasi elektronik secara melawan hukum sebagai tindak pidana dengan tingkat keseriusan yang lebih tinggi. Dengan demikian, apabila dilihat dari asas proporsionalitas antara perbuatan dan ancaman pidana, penerapan Pasal 48 ayat (1) dan ayat (2) justru lebih mencerminkan derajat kesalahan (schuld) dan dampak yang ditimbulkan oleh para pelaku [12].

Walaupun pertimbangan penyidik yang menitikberatkan pada Pasal 46 ayat (1) dapat dipahami dari sudut strategi pembuktian, namun secara akademik penulis berpendapat bahwa penerapan Pasal 32 ayat (1) dan ayat (2) jo. Pasal 48 ayat (1) dan ayat (2) seharusnya menjadi dasar utama penjeratan pidana, sedangkan Pasal 30 ayat (1) jo. Pasal 46 ayat (1) dapat diposisikan sebagai delik yang menyertai atau bagian dari rangkaian perbuatan. Hal ini karena esensi kejahatan dalam perkara ini terletak pada kebocoran dan distribusi informasi elektronik yang bersifat rahasia dan strategis, bukan semata-mata pada tindakan akses tanpa hak.

Dengan demikian, secara normatif terdapat dasar penerapan baik Pasal 46 ayat (1) maupun Pasal 48 ayat (1) dan ayat (2). Namun dalam perspektif analisis hukum yang lebih komprehensif, penulis berpendapat bahwa Pasal 48 ayat (1) dan ayat (2) lebih tepat mencerminkan keseluruhan konstruksi tindak pidana yang dilakukan secara terorganisasi dan terstruktur dalam kasus peretasan sistem elektronik UTBK Universitas Hasanuddin tahun 2025. Pada akhirnya, berdasarkan keseluruhan penjelasan di atas, dapat disimpulkan bahwa penyidik telah menerapkan pasal-pasal yang relevan dengan fakta hukum yang terjadi dalam kasus peretasan sistem elektronik dalam Ujian Tulis Berbasis Komputer di Universitas Hasanuddin tahun 2025.

**2. Faktor-Faktor Yang Memengaruhi Pertanggungjawaban Hukum Terhadap Para Pelaku Tindak Pidana Peretasan Sistem Elektronik Dalam Ujian Tulis Berbasis Komputer**

Pertanggungjawaban hukum terhadap para pelaku tindak pidana peretasan sistem elektronik dalam pelaksanaan Ujian Tulis Berbasis Komputer di Universitas Hasanuddin tahun 2025, tidak ditetapkan secara seragam, melainkan dipengaruhi oleh berbagai faktor yang dianalisis secara teliti oleh penulis, yakni:

1. Faktor Umur

Dalam hukum pidana Indonesia, seseorang yang telah berusia 18 tahun atau lebih dikategorikan sebagai subjek hukum dewasa yang dapat dimintai pertanggungjawaban pidana secara penuh sebagaimana diatur dalam Pasal 1 angka 3 Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak. Dalam perkara ini, salah satu pelaku diketahui berusia 19 tahun dan berstatus sebagai mahasiswi, sehingga secara yuridis tidak terdapat alasan penghapus pertanggungjawaban pidana berdasarkan faktor usia. Berdasarkan hasil wawancara dengan penyidik, seluruh pelaku tetap ditetapkan sebagai tersangka tanpa pembedaan perlakuan dari segi usia karena seluruhnya telah memenuhi batas usia pertanggungjawaban pidana.

Meskipun pelaku telah berusia 19 (sembilan belas) tahun dan secara hukum dikategorikan sebagai orang dewasa, kondisi tersebut masih menunjukkan bahwa yang bersangkutan berada pada fase transisi perkembangan sosial dan pendidikan, sehingga

potensi untuk dilakukan rehabilitasi dan pembinaan masih terbuka. Pertimbangan demikian sejalan dengan ketentuan Pasal 8 ayat (2) Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman yang mewajibkan hakim dalam mempertimbangkan berat ringannya pidana untuk memperhatikan sifat yang baik dan jahat dari terdakwa, serta Pasal 54 ayat (1) huruf c Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana yang menegaskan bahwa dalam pemidanaan hakim wajib mempertimbangkan keadaan pribadi pelaku [13]. Dengan demikian, usia 19 tahun dapat dijadikan sebagai dasar pertimbangan yuridis dalam rangka menjatuhkan pidana yang berorientasi pada tujuan pemidanaan yang bersifat korektif dan rehabilitatif.

2. Faktor Kemampuan Finansial

Faktor kemampuan finansial yang dimaksudkan adalah kemampuan dari para pelaku untuk melakukan ganti kerugian terhadap pasal yang didakwakan oleh penyidik yaitu pasal 46 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dengan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp600.000.000,00 (enam ratus juta). Ancaman denda dalam jumlah besar tersebut menimbulkan relevansi terhadap latar belakang ekonomi para pelaku [14]. Dalam kasus ini, diketahui bahwa terdapat pelaku yang berstatus mahasiswi dan ada pula yang berstatus pegawai honorer. Dalam hal hakim menjatuhkan pidana denda dan terpidana tidak mampu membayarnya, sistem hukum pidana Indonesia mengatur adanya pidana pengganti berupa pidana kurungan. Ketentuan ini secara tegas diatur dalam Pasal 30 ayat (2) dan ayat (3) Kitab Undang-Undang Hukum Pidana (KUHP) lama, yang menyatakan bahwa apabila denda tidak dibayar, maka diganti dengan pidana kurungan, dengan lamanya kurungan pengganti ditentukan dalam putusan hakim. Sementara, dalam Kitab Undang-Undang Hukum Pidana (KUHP) 2023, Pasal 81 mengatur penyitaan dan pelelangan harta terpidana apabila denda tidak dibayar, Pasal 82 mengatur penggantian denda dengan pidana kerja sosial atau pidana pengawasan apabila harta tidak mencukupi, dan Pasal 83 mengatur pidana penjara sebagai alternatif terakhir apabila penggantian tersebut tidak dapat dilaksanakan. Dengan demikian, ketidakmampuan membayar denda tidak menghapus

pidana, melainkan berimplikasi pada pelaksanaan pidana pengganti sesuai ketentuan peraturan perundang-undangan [15]. Hal ini menunjukkan bahwa kemampuan finansial tidak memengaruhi eksistensi kesalahan, tetapi dapat memengaruhi bentuk pelaksanaan sanksi.

Dengan demikian, kemampuan finansial lebih relevan sebagai pertimbangan hakim dalam menentukan apakah pidana denda layak dijatuhkan secara maksimal atau tidak. Penjatuhan denda dalam jumlah besar terhadap pelaku yang secara ekonomi tidak mampu dapat berpotensi tidak efektif dan tidak proporsional [16]. Oleh karena itu, menurut penulis, faktor yang paling kuat dalam memengaruhi pertanggungjawaban hukum para pelaku tindak pidana peretasan sistem elektronik dalam Ujian Tulis Berbasis Komputer adalah faktor kemampuan finansial.

## KESIMPULAN

Penelitian ini menunjukkan bahwa peretasan sistem elektronik dalam pelaksanaan Ujian Tulis Berbasis Komputer (UTBK) di Universitas Hasanuddin tahun 2025 merupakan bentuk tindak pidana yang dilakukan secara terorganisasi melalui akses ilegal terhadap sistem elektronik serta pemindahan informasi elektronik berupa soal ujian kepada pihak yang tidak berhak. Analisis terhadap ketentuan hukum yang berlaku menunjukkan bahwa perbuatan tersebut menimbulkan pertanggungjawaban pidana bagi para pelaku karena telah memenuhi unsur akses tanpa hak dan distribusi informasi elektronik secara melawan hukum. Temuan penelitian juga memperlihatkan bahwa penerapan pertanggungjawaban hukum dalam perkara ini tidak terlepas dari pertimbangan faktor usia dan kemampuan finansial pelaku dalam proses penegakan hukum. Kondisi tersebut menunjukkan bahwa kejahatan siber dalam sistem seleksi pendidikan tinggi tidak hanya berkaitan dengan pelanggaran norma hukum, tetapi juga berimplikasi pada integritas dan keadilan sistem seleksi nasional. Oleh karena itu, penguatan tata kelola keamanan sistem elektronik, peningkatan pengawasan terhadap infrastruktur teknologi informasi, serta koordinasi yang lebih efektif antara penyelenggara ujian dan aparat penegak hukum menjadi langkah penting untuk mencegah terulangnya peretasan sistem elektronik dalam pelaksanaan UTBK di masa mendatang.

**REFERENSI**

[1] R. Siregar, "Cyber Crime and Legal Liability in Electronic Systems in Indonesia," *Journal of Law and Technology*, vol. 5, no. 2, pp. 112–130, 2021.

[2] F. Abdillah, "Peran Perguruan Tinggi dalam Meningkatkan Kualitas Sumber Daya Manusia di Indonesia," pp. 13–24. Website: https://j-educa.org/index.php/educazione

[3] M. Adam, A. Kamri, B. Hamza, "Upaya Kepolisian Dalam Penanggulangan Tindak Pidana Kejahatan Dunia Maya (Cyber Crime) Pada Kepolisian Daerah Sulawesi Selatan," *Journal of Lex Generalis* (JLS), vol. 2, no. 1, 2021. Website: http:pasca-umi.ac.id/indez.php/jlg

[4] T. Prasetyo, "Criminal Liability and Fault-Based Responsibility in Indonesian Criminal Law," *Indonesian Journal of Criminal Law*, vol. 3, no. 1, pp. 45–60, 2020.

[5] D. Rahmawati, "Electronic Evidence and Digital Forensics in Cybercrime Investigation," *Journal of Cyber Law Studies*, vol. 4, no. 3, pp. 201–220, 2022.

[6] N. Dzaky, "PENERAPAN SANKSI PIDANA PADA KASUS JOKI SELEKSI MASUK PERGURUAN TINGGI," *Jurnal Legisia*, vol. 15, no. 1, 2023. [Online]. Website: https://hot.liputan6.com/read/5053381/ltmpt-adalah-lembaga-tes-masuk-perguruan-tinggi-ketahui-fungsi-

[7] P. S. Vicky, V. Yati, "PERTANGGUNGJAWABAN MAHASISWA PENGGUNA JASA PENULISAN KARYA ILMIAH (SKRIPSI) DITINJAU DARI KITAB UNDANG-UNDANG HUKUM PIDANA," *Jurnal Duta Hukum*, vol. 1, no. 1, pp. 37–52, 2024.

[8] H. Djanggih, N. Qamar "Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)," *Pandecta*, vol. 13, no. 1, pp. 10–23, 2018. Website: http://journal.unnes.ac.id/nju/index.php/pandecta

[9] A. Fadlian, "PERTANGGUNGJAWABAN PIDANA DALAM SUATU KERANGKA TEORITIS," *Jurnal Hukum POSITUM*, vol. 5, no. 2, pp. 10–19, 2020.

[10] A. M. Zahra, M. Pawennai, and A. Tjolleng, "Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online di Media Sosial Elektronik," *Legal Dialogica*, vol. 1, no. 1, pp. 1–17.

[11] A. Putra, A. Perdana, "Penegakan Hukum Terhadap Eksistensi Jasa Joki Tugas Akhir Mahasiswa Perspektif Tanggung Jawab Hukum," *Jurnal Ilmu Hukum Prima*, vol. 7, no. 2, pp. 145–159, 2024.

[12] J. O. Said, M. Asbari, and H. I. Salsabila, "Seleksi Masuk Perguruan Tinggi Negeri : Langkah Menuju Pemerataan Akses Pendidikan Tinggi," *Literaksi : Jurnal Manajemen Pendidikan Transformasi*, vol. 02, no. 01, pp. 107–111, 2024.

[13] R. H. Mustafa and M. Pawennai, "Peretasan Terhadap Sistem Elektronik Pada Aplikasi Angkutan Umum," *Qawanin Jurnal Ilmu Hukum*, vol. 1, no. 1, pp. 59–71, 2020.

[14] Z. Musthofa, A. Rusilowati, Sulhadi, P. Marwoto, B. N. Mindiyarto "Analisis Perilaku Kecurangan Akademik Siswa dalam Pelaksanaan Ujian di Sekolah," *Jurnal Kependidikan*, vol. 7, no. 2, pp. 446–452, 2021. Website: https://e-journal.undikma.ac.id/index.php/jurnalkependidikan/index

[15] A. Sofyan, and N. Azisa, "Hukum Pidana" *Pustaka Pena Press*, 2016.

[16] A. Salong, "PERILAKU KECURANGAN AKADEMIK MAHASISWA DALAM PROSES PERKULIAHAN," *Jurnal Pedagogika dan Dinamika Pendidikan*, vol. 6, no. 2, 2018.