Jurnal Mitra Pengembangan Hukum

Vol. 1, No. 2, Juli 2025 E-ISSN: 3089-9494

Penegakan Hukum Tindak Pidana *Illegal Acces* Pada Seleksi Tes CPNS Tahun 2021 Di Kabupaten Pringsewu

Zaki Fauzan Al-Ghifari[1], Tri Andrisman[2], Dona Raisa Monica[3], Firganefi[4], Refi Meidiantama[5]

[1,2,3,4,5] Fakultas Hukum, Universitas Lampung

zakifauzzz@gmail.com[1], tri.andrisman@fh.unila.ac.id[2], dona.raisa.monica@fh.unila.ac.id[3], firganefi@fh.unila.ac.id[4], refi.meidiantama@fh.unila.ac.id[5]

Keywords:
CPNS Exam Implementation
Illegal Access Crime
Cybercrime

Kata Kunci:
Pelaksanaan Ujian CPNS
Kejahatan Akses Ilegal
Kejahatan Siber

Abstract

This study aims to analyze law enforcement efforts against the crime of illegal access during the 2021 Civil Servant Candidate (CPNS) selection process in Pringsewu Regency. The case emerged following the discovery of a cybercrime operation involving a syndicate of exam impersonators (jockeys) who used remote access applications and modified technological devices to unlawfully access the examination system. The research adopts both normative and empirical juridical approaches, utilizing data collection techniques through literature review and interviews with law enforcement officials and relevant stakeholders. The data were analyzed qualitatively using a descriptive-analytical method. The findings indicate that the primary factors contributing to illegal access crimes include weak information system security, inadequate technical training for system administrators, and low digital ethics awareness among test participants. The impacts of these crimes are significant, including financial losses to the state, a compromised integrity of the selection process, and a decline in public trust in the civil servant recruitment system. Law enforcement against the perpetrators is carried out based on the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions. While law enforcement authorities have taken action to create a deterrent effect, various technical and regulatory challenges remain obstacles in the process. In conclusion, addressing illegal access crimes in CPNS selection requires a comprehensive approach, including strengthening cybersecurity regulations, enhancing the capacity of system administrators, consistent law enforcement, and educating test takers on digital ethics. These efforts are crucial to safeguarding the integrity of the selection process and restoring public trust in civil servant recruitment in the digital era.

Abstrak

Penelitian ini bertujuan untuk menganalisis penegakan hukum terhadap tindak pidana illegal access dalam pelaksanaan seleksi Calon Pegawai Negeri Sipil (CPNS) Tahun 2021 di Kabupaten Pringsewu. Kasus ini mencuat setelah terungkapnya praktik kejahatan siber yang melibatkan sindikat joki menggunakan aplikasi remote access dan perangkat teknologi yang dimodifikasi untuk mengakses sistem ujian secara ilegal. Penelitian ini menggunakan metode pendekatan yuridis normatif dan yuridis empiris, dengan teknik pengumpulan data melalui studi kepustakaan dan wawancara terhadap aparat penegak hukum serta pihak terkait. Data dianalisis secara kualitatif dengan pendekatan deskriptif-analitis. Hasil penelitian menunjukkan bahwa faktor utama yang mendorong terjadinya kejahatan illegal access adalah lemahnya pengamanan sistem informasi, kurangnya pelatihan teknis bagi pengelola sistem, serta rendahnya kesadaran etika digital peserta ujian. Dampak dari tindak pidana ini meliputi kerugian negara, hilangnya integritas proses seleksi, serta turunnya kepercayaan masyarakat terhadap sistem rekrutmen ASN. Penegakan hukum terhadap pelaku dilakukan berdasarkan

ketentuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penanganan perkara ini menunjukkan adanya upaya aparat penegak hukum untuk memberikan efek jera, meskipun tantangan teknis dan regulasi masih menjadi hambatan. Kesimpulannya, penanggulangan kejahatan illegal access dalam seleksi CPNS membutuhkan pendekatan yang komprehensif melalui penguatan regulasi keamanan siber, peningkatan kapasitas pengelola sistem, penegakan hukum yang konsisten, serta edukasi etika digital bagi peserta tes. Langkah-langkah tersebut penting untuk memastikan integritas proses seleksi dan membangun kepercayaan publik terhadap rekrutmen aparatur sipil negara di era digital.

Corresponding Author:
Zaki Fauzan Al-Ghifari
Fakultas Hukum
Universitas Lampung
Email: zakifauzzz@gmail.com

1. PENDAHULUAN

Seleksi Calon Pegawai Negeri Sipil (CPNS) merupakan instrumen strategis dalam kerangka reformasi birokrasi nasional yang bertujuan untuk menjaring sumber daya manusia unggul guna mengisi jabatan di lingkungan instansi pemerintah (Kuswara & Mayasari, 2023). Proses seleksi ini dirancang untuk memastikan bahwa hanya individu yang memiliki kompetensi, integritas, dan kapabilitas sesuai standar kualifikasi yang ditetapkan yang dapat diangkat sebagai Aparatur Sipil Negara (ASN). Lebih dari sekadar mekanisme pengisian kebutuhan formasi, seleksi CPNS juga memainkan peran sentral dalam menciptakan pelayanan publik yang profesional, akuntabel, dan responsif terhadap tantangan pembangunan nasional (Hulu et al., 2024). Tahapan seleksi CPNS dilaksanakan secara berjenjang, mencakup seleksi administrasi, Seleksi Kompetensi Dasar (SKD), dan Seleksi Kompetensi Bidang (SKB), yang kesemuanya berbasis sistem komputerisasi guna menjamin transparansi dan akuntabilitas proses seleksi (Emilia Susanti & Eko Raharjo, 2018).

Namun, pelaksanaan seleksi CPNS tidak terlepas dari berbagai tantangan, khususnya dalam hal integritas dan keamanan sistem seleksi. Pada pelaksanaan seleksi CPNS Tahun 2021 di Kabupaten Pringsewu, terungkap praktik kejahatan *illegal access* yang dilakukan oleh sindikat joki dengan memanfaatkan aplikasi *remote access* serta perangkat khusus yang dimodifikasi. Tindakan ini termasuk dalam kategori kejahatan siber (*cybercrime*), yang menurut Rudiantoro terbagi atas kejahatan teknis seperti peretasan dan sabotase, serta kejahatan sosial seperti penipuan dan penyebaran informasi palsu. Kejahatan siber menimbulkan ancaman serius terhadap keamanan nasional dan privasi individu, sehingga membutuhkan regulasi yang komprehensif dan penegakan hukum yang tegas.

Menurut data Badan Kepegawaian Negara (BKN), pada penutupan pendaftaran seleksi CASN tahun 2021 tercatat sebanyak 4.030.090 pelamar terdaftar pada akun Sistem Seleksi Calon Aparatur Sipil Negara (SSCASN). Jumlah ini menunjukkan tingginya antusiasme masyarakat terhadap profesi ASN, yang dipandang memiliki jaminan keamanan kerja, pensiun, serta tunjangan kinerja. Per 30 Juni 2022, tercatat jumlah PNS aktif sebanyak 3.992.766 orang dan Pegawai Pemerintah dengan Perjanjian Kerja (PPPK) sebanyak 351.786 orang (Deni Achmad & Firganefi, 2016).

Meski demikian, praktik-praktik tidak etis dalam proses rekrutmen masih kerap terjadi, antara lain berupa nepotisme, percaloan, dan kolusi, yang mengarah pada rendahnya kualitas ASN. Kasus-kasus penyimpangan dalam seleksi CPNS hampir setiap tahun ditemukan, bahkan melibatkan pejabat pemerintah di pusat maupun daerah, serta panitia seleksi (Wahyuni, 2019). Tindakan *illegal access* merupakan pelanggaran terhadap Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (Handoyo et al., 2024). Pelanggaran ini mencakup akses tanpa hak terhadap sistem elektronik, manipulasi data, hingga sabotase sistem. Salah satu kasus yang menonjol yaitu Putusan No. 702/Pid.Sus/2022/PN Tjk, yang memutus tiga terdakwa (Indra Gunawan, Mohammad Rizki Alam, dan Muhammad Reza Akbar) bersalah atas pelanggaran Pasal 46 ayat (1) *jo*. Pasal 30 ayat (1) UU ITE *jo.* Pasal 55 ayat (1) ke-1 KUHP. Modus yang digunakan melibatkan kendali jarak jauh terhadap komputer peserta ujian sehingga para peserta dapat menerima jawaban dari lokasi lain, dengan tarif bervariasi antara Rp100 juta hingga Rp250 juta per peserta. Kejahatan serupa juga ditemukan di Sulawesi Tenggara, di mana sindikat mengakses sistem dari luar lokasi ujian melalui metode *remote desktop*.

Fenomena ini disebabkan oleh lemahnya sistem keamanan informasi, kurangnya pelatihan bagi pengelola sistem, serta rendahnya kesadaran etika digital di kalangan peserta. Dampaknya sangat signifikan, mencakup hilangnya integritas seleksi, rusaknya citra pemerintah, serta menurunnya kepercayaan masyarakat terhadap sistem rekrutmen ASN. Urgensi penelitian ini muncul dari meningkatnya ancaman kejahatan siber

(*cybercrime*) terhadap integritas proses seleksi CPNS, seperti kasus *illegal access* yang terjadi pada seleksi CPNS 2021 di Kabupaten Pringsewu. Dalam modus tersebut, sindikat joki menggunakan aplikasi remote access dan perangkat khusus yang dimodifikasi untuk mengakses sistem CAT secara ilegal dan terorganisir. Tindakan ini diperkarakan berdasarkan pasal 30 ayat (1) *jo.* pasal 46 ayat (1) UU ITE (Nomor 11 Tahun 2008 *jo*. 19 Tahun 2016), serta pasal 55 KUHP.

Meskipun berbagai penelitian telah mengulas tantangan dan dimensi normatif kejahatan siber, kesenjangan dalam kajian akademik masih terlihat signifikan, khususnya terkait praktik *illegal access* dalam konteks administrasi publik. Sebagian besar studi cenderung berfokus pada kejahatan siber yang bersifat komersial, lintas negara, atau berkaitan dengan sektor privat, sementara kajian terhadap ancaman siber terhadap sistem seleksi publik berbasis digital seperti seleksi Calon Pegawai Negeri Sipil (CPNS) masih sangat terbatas, terutama pada level pemerintahan daerah. Padahal, integritas proses seleksi CPNS merupakan pilar krusial dalam menjaga kualitas birokrasi dan membangun kepercayaan masyarakat terhadap sistem rekrutmen aparatur negara. Oleh karena itu, kebutuhan untuk mengkaji secara spesifik bentuk, modus, serta penegakan hukum terhadap tindak pidana *illegal access* dalam penyelenggaraan seleksi CPNS menjadi sangat relevan dan mendesak dalam kerangka penguatan tata kelola pemerintahan berbasis digital.

Kebaruan penelitian ini terletak pada kajian empiris dan normatif yang menggabungkan analisis hukum positif (UU ITE dan KUHP) dengan faktor sosial-teknis (modul teknologi, regulasi keamanan, dan budaya digital peserta tes). Studi ini juga menyertakan analisis kasus konkret (Pringsewu), sehingga menawarkan kontribusi baru dalam pengembangan ilmu hukum pidana siber yang lebih aplikatif dan lokal. Penelitian ini bertujuan untuk menganalisis penegakan hukum terhadap tindak pidana illegal access yang terjadi pada pelaksanaan tes Calon Pegawai Negeri Sipil (CPNS) Tahun 2021 di Kabupaten Pringsewu. Analisis ini mencakup aspek normatif dan empiris terhadap proses penyidikan, penuntutan, serta pertimbangan hukum dalam putusan pengadilan, dengan mengkaji efektivitas penerapan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta hambatan yang dihadapi dalam penegakan hukumnya.

Sejalan dengan kebaruan tersebut, penelitian ini bertujuan untuk menganalisis penegakan hukum terhadap tindak pidana *illegal access* yang terjadi dalam proses seleksi CPNS Tahun 2021 di Kabupaten Pringsewu. Analisis dilakukan secara normatif dan empiris, mencakup proses penyelidikan, penyidikan, penuntutan, serta pertimbangan hukum dalam putusan pengadilan. Penelitian ini juga mengevaluasi efektivitas penerapan ketentuan dalam UU ITE dan mengidentifikasi hambatan-hambatan yang dihadapi oleh aparat penegak hukum dalam menangani kasus tersebut. Dengan demikian, penelitian ini diharapkan dapat memperkuat fondasi penegakan hukum pidana siber yang lebih adaptif terhadap tantangan era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif dan yuridis empiris untuk memperoleh data yang objektif dan dapat dipertanggungjawabkan secara ilmiah. Pendekatan yuridis normatif dilakukan dengan menelaah hukum sebagai suatu kaidah atau norma melalui studi kepustakaan, yang mencakup analisis terhadap peraturan perundang-undangan, literatur hukum, dan dokumen-dokumen hukum yang relevan (Ketut Boby Suryawan, 2025). Sementara itu, pendekatan yuridis empiris dilakukan dengan mengkaji fakta dan realitas hukum yang terjadi di lapangan, melalui pengumpulan data primer yang diperoleh dari wawancara langsung dengan para narasumber yang kompeten, seperti aparat penegak hukum dan akademisi di bidang hukum (Sumarna & Kadriah, 2023).

Sumber data dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dengan pihak-pihak yang berwenang dan berkompeten, antara lain penyidik pada Direktorat Reserse Kriminal Khusus Polda Lampung dan dosen Fakultas Hukum Universitas Lampung. Adapun data sekunder diperoleh dari bahan-bahan hukum berupa peraturan perundang-undangan, buku teks, jurnal ilmiah, artikel hukum, dan sumber-sumber tertulis lainnya yang relevan dengan topik penelitian, yakni penegakan hukum terhadap tindak pidana *illegal access*.

Teknik pengumpulan data dilakukan melalui dua metode, yaitu studi kepustakaan untuk memperoleh dan mengkaji bahan hukum sekunder, serta studi lapangan berupa wawancara terstruktur dan mendalam guna memperoleh informasi empiris tentang praktik dan penerapan hukum dalam kasus *illegal access* pada pelaksanaan tes CPNS. Proses pengolahan dan analisis data dilakukan secara kualitatif melalui tiga tahapan utama: seleksi, klasifikasi, dan sistematisasi data. Seleksi data dilakukan untuk memastikan relevansi informasi dengan fokus penelitian, klasifikasi data digunakan untuk mengelompokkan data berdasarkan tema atau kategori tertentu agar lebih terorganisir, dan sistematisasi bertujuan menyusun data secara logis dan terpadu guna mempermudah proses analisis. Analisis dilakukan secara deskriptif-analitis, yaitu dengan menjelaskan dan menginterpretasikan data secara rinci untuk menjawab rumusan masalah dan mencapai tujuan penelitian secara utuh. Dengan demikian, hasil analisis ini diharapkan mampu memberikan gambaran yang akurat

mengenai kondisi aktual penegakan hukum serta upaya penanggulangan tindak pidana *illegal access* dalam konteks seleksi CPNS di Kabupaten Pringsewu.

3. PEMBAHASAN

3.1 Penegakan Hukum Tindak Pidana *Illegal Access* Pada Pelaksanaan Tes CPNS Tahun 2021 Di Kabupaten Pringsewu

Penegakan hukum membutuhkan motivasi dan dorongan yang kuat agar dapat berjalan secara efektif. Selain menerapkan hukum secara profesional dan konsisten, aparat penegak hukum juga dituntut untuk menindak individu maupun kelompok yang diduga terlibat dalam tindak kejahatan (Gilang Putra & Kayus Kayouwan Lewoleba, 2024). Kejahatan yang berkaitan dengan teknologi informasi sering kali digolongkan sebagai *white collar crime* karena umumnya dilakukan oleh individu dengan pemahaman yang mendalam mengenai aplikasi dan penggunaan teknologi internet. Karena sifatnya lintas batas, kejahatan siber juga termasuk dalam kategori kejahatan transnasional (Tabiu et al., 2023). Dalam konteks pelaksanaan seleksi Calon Pegawai Negeri Sipil (CPNS) Tahun 2021 di Kabupaten Pringsewu, penegakan hukum terhadap tindak pidana illegal access menunjukkan keseriusan aparat penegak hukum dalam menjaga integritas seleksi aparatur sipil negara. Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Lampung berhasil mengungkap praktik kecurangan dengan menggunakan aplikasi *remote access* dan perangkat teknologi khusus untuk mengendalikan komputer peserta tes dari jarak jauh. Empat orang tersangka utama berhasil ditetapkan, salah satunya merupakan oknum pegawai honorer pada Badan Kepegawaian Daerah (BKD) Provinsi Lampung yang memberikan informasi dan memfasilitasi akses ilegal tersebut.

Proses hukum telah berjalan melalui pemeriksaan dan pelimpahan berkas perkara ke kejaksaan, termasuk terhadap oknum pejabat tinggi di Kabupaten Pringsewu seperti Staf Ahli Bupati yang diduga turut memfasilitasi pengaturan kelulusan tes CPNS. Keterlibatan pejabat ini menunjukkan bahwa penegakan hukum tidak hanya menyasar pelaku teknis di lapangan, tetapi juga membongkar jaringan sistematis yang beroperasi secara terorganisasi. Kasus ini telah disidangkan di Pengadilan Negeri Tanjungkarang sebagai bentuk transparansi dan upaya menegakkan keadilan terhadap tindakan ilegal yang merusak integritas sistem rekrutmen ASN. Tujuan utama penegakan hukum terhadap tindak pidana *illegal access* ini adalah untuk memulihkan kepercayaan publik terhadap proses seleksi CPNS yang sempat tercoreng oleh kecurangan. Selain tindakan represif terhadap pelaku, pihak kepolisian dan aparat terkait juga melakukan upaya preventif dengan memperketat pengawasan pelaksanaan tes serta menerapkan teknologi keamanan yang lebih canggih agar kejadian serupa tidak terulang.

Kasubdit V Siber Ditreskrimsus Polda Lampung, Try Ramadona menyampaikan bahwa dalam kasus joki CPNS tahun 2021 tersebut, lima orang telah ditetapkan sebagai tersangka, termasuk Kepala BKPSDM Pringsewu dan oknum pegawai BKD Provinsi Lampung. Kasus ini ditangani dalam dua berkas perkara terpisah. Ia menambahkan bahwa faktor utama terjadinya tindak pidana ini adalah kolaborasi antara oknum internal dan lemahnya sistem keamanan. Salah satu tersangka merupakan pegawai honorer yang membocorkan informasi penting kepada peserta. Sistem keamanan yang tidak ketat memungkinkan akses jarak jauh tanpa terdeteksi terhadap komputer peserta. Menurut Hartono Suta, rendahnya kesadaran masyarakat terhadap penggunaan internet dan teknologi, disertai minimnya sosialisasi dan literasi digital, menjadi penyebab masih maraknya kejahatan *cyber crime*. Dalam konteks ini, pelaku justru merupakan individu yang sangat memahami celah hukum di dunia digital. Oleh karena itu, diperlukan penyuluhan dan edukasi dari pemerintah terkait dampak serta sanksi hukum terhadap penyalahgunaan teknologi informasi.

Temuan di atas menunjukkan bahwa pelaksanaan penegakan hukum terhadap tindak pidana *illegal access* belum sepenuhnya mampu memberikan efek jera (*deterrent effect*) yang maksimal. Hukuman pidana yang dijatuhkan masih relatif ringan dibanding dampak kejahatan terhadap integritas seleksi ASN. Selain itu, belum adanya koordinasi yang optimal antara BKN, BKPSDM daerah, dan aparat penegak hukum membuat sistem pengawasan terhadap penyalahgunaan teknologi dalam seleksi CPNS menjadi lemah. Kejahatan ini tidak hanya merugikan sistem elektronik, tetapi juga mencederai asas meritokrasi dalam rekrutmen aparatur sipil negara. Dalam konteks hukum pidana, perbuatan ini termasuk kejahatan terhadap kepercayaan publik (*public trust crime*), karena menimbulkan persepsi negatif terhadap netralitas dan transparansi proses seleksi CPNS.

Ditinjau dari perspektif teori *routine activity* yang dikemukakan oleh Cohen dan Felson (Hikmatulloh & Nurmiati, 2020), tindak pidana *illegal access* terjadi karena adanya pelaku yang termotivasi, target yang rentan (komputer tes), dan tidak adanya pengawasan yang memadai. Kasus di Pringsewu mengafirmasi teori ini karena pelaku memiliki motivasi untuk lolos seleksi, sistem komputer tidak diawasi secara ketat, dan celah keamanan tidak segera diperbaiki oleh penyelenggara. Penelitian oleh Holt dan Bossler Tahun 2014 juga menegaskan bahwa *cyber offender* tidak selalu termotivasi oleh ancaman hukuman, melainkan oleh kesempatan dan pengetahuan teknis untuk mengeksploitasi sistem (Budiyanto, 2025). Hal ini sesuai dengan kondisi di lapangan, di mana pelaku *illegal access* menggunakan celah teknis dan kelemahan internal dalam

sistem seleksi. Selain itu, studi Jansen dan Leukfeldt Tahun 2018 menyoroti pentingnya *insider threat* dalam kejahatan siber, yaitu keterlibatan pihak internal dalam memfasilitasi akses illegal (Budiyanto, 2025). Ini relevan dengan kasus di Pringsewu, karena terungkap adanya peran oknum panitia seleksi yang membantu pemasangan aplikasi jarak jauh di komputer peserta.

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa penegakan hukum terhadap tindak pidana *illegal access* harus ditempatkan dalam kerangka hukum pidana yang adaptif terhadap perkembangan teknologi digital. Model penegakan hukum yang hanya menitikberatkan pada aspek represif belum memadai untuk menghadapi kejahatan siber berbasis sistem rekrutmen ASN. Diperlukan modifikasi pendekatan dengan membangun sistem *cyber justice enforcement* yang melibatkan integrasi antara penegakan hukum, penguatan tata kelola digital instansi, dan reformasi dalam pelatihan penyidik siber. Pendekatan ini menekankan pentingnya preventive measures, seperti audit sistem elektronik, peningkatan *digital literacy* panitia seleksi, serta penyusunan SOP keamanan digital dalam seleksi CPNS. Penelitian ini juga berkontribusi dalam pengembangan pendekatan law and technology, dengan menekankan bahwa reformasi hukum pidana siber harus berjalan beriringan dengan peningkatan kapasitas kelembagaan dalam menghadapi kejahatan digital yang semakin kompleks dan terspesialisasi.

3.2 Faktor Penghambat Penegakan Hukum Tindak Pidana Illegal Access pada Pelaksanaan Tes CPNS Tahun 2021 di Kabupaten Pringsewu

Penegakan hukum terhadap tindak pidana *illegal access* tidak terlepas dari berbagai kendala yang bersifat struktural maupun teknis. Menurut Khotimah Lubis, suatu perbuatan dapat dijadikan sebagai tindak pidana apabila memenuhi sejumlah unsur, seperti: (a) merugikan masyarakat, (b) dilakukan berulang kali, (c) menimbulkan reaksi sosial, dan (d) adanya unsur bukti. Namun dalam praktiknya, penegakan hukum terhadap kejahatan siber menghadapi hambatan yang kompleks. Salah satu faktor utama adalah lemahnya regulasi serta prosedur keamanan dalam pelaksanaan seleksi CPNS. Sistem pengawasan dan perlindungan data yang belum optimal membuka peluang bagi pelaku untuk melakukan manipulasi dan akses ilegal terhadap perangkat komputer peserta. Hal ini mencerminkan bahwa kesiapan teknologi informasi belum mampu mengantisipasi ancaman siber secara menyeluruh.

Keterbatasan sumber daya manusia yang kompeten di bidang teknologi informasi dan forensik digital turut memperlambat proses penegakan hukum (Andarek, 2025). Banyak aparat penegak hukum maupun panitia pelaksana seleksi belum memiliki keahlian yang cukup untuk mengidentifikasi dan menindak kejahatan siber yang kompleks dan cepat berkembang. Akibatnya, proses penyidikan menjadi lambat dan tidak efektif dalam mengungkap jaringan kejahatan (Anwar, 2023). Faktor internal birokrasi, seperti kurangnya koordinasi antarlembaga dan keterlibatan oknum pegawai, turut memperumit penanganan kasus ini. Adanya kolusi dan nepotisme dalam institusi pemerintah melemahkan integritas sistem dan menimbulkan keraguan publik terhadap komitmen pemerintah dalam pemberantasan *cyber crime*. Dari sisi teknologi, keterbatasan perangkat pendukung seperti *monitoring tools, security software*, dan teknologi enkripsi menyebabkan kelemahan dalam sistem deteksi dini dan respon terhadap serangan siber. Proses hukum yang panjang dan birokratis juga menurunkan efektivitas penindakan hukum, sementara peraturan perundang-undangan yang ada belum sepenuhnya mengakomodasi kompleksitas kejahatan siber. Hambatan lainnya meliputi minimnya koordinasi dan sinergi antara lembaga penegak hukum dan instansi teknis terkait, lemahnya pengawasan internal, serta resistensi sosial dan budaya terhadap upaya pelaporan kejahatan. Budaya melindungi kelompok atau oknum tertentu, serta rasa takut terhadap konsekuensi sosial, membuat banyak pihak enggan bersikap tegas terhadap pelanggaran.

Lebih lanjut, penegakan hukum terhadap tindak pidana *illegal access* di Kabupaten Pringsewu menemui sejumlah hambatan yang bersifat struktural, instrumental, dan kultural. Berdasarkan hasil wawancara dengan aparat penegak hukum, telaah dokumen, serta studi perbandingan, ditemukan lima faktor utama yang menjadi penghambat:

a. Keterbatasan kapasitas teknologi dan SDM aparat penegak hukum

Salah satu hambatan utama adalah kurangnya kemampuan teknis aparat penegak hukum, khususnya penyidik kepolisian dan kejaksaan, dalam menangani bukti elektronik secara forensik. Penanganan kasus siber membutuhkan keahlian khusus dalam digital *evidence preservation, data recovery*, dan *cyber forensic analysis*, yang belum menjadi kompetensi umum penyidik di daerah. Banyak kasus cybercrime yang tidak bisa dilanjutkan ke proses peradilan karena tidak terpenuhinya chain of custody bukti digital yang sah menurut hukum acara pidana. Ini menunjukkan belum optimalnya infrastruktur dan pelatihan aparat penegak hukum di daerah dalam mengadopsi pendekatan cyber law enforcement yang profesional.

b. Tidak adanya standar pengamanan sistem seleksi CPNS secara nasional

Kejahatan *illegal access* dalam seleksi CPNS memanfaatkan kelemahan sistem teknologi informasi, seperti buruknya *endpoint security*, tidak adanya *firewall log*, serta lemahnya pengawasan fisik perangkat ujian.

Ketiadaan standar pengamanan sistem seleksi CPNS yang seragam secara nasional (baik dari BKN maupun KemenPAN-RB) menyebabkan sistem rentan disusupi oleh pihak luar maupun dalam. Hal ini sejalan dengan temuan dari Badan Siber dan Sandi Negara (BSSN), yang menyebutkan bahwa sektor administrasi publik menjadi salah satu target utama serangan siber karena lemahnya infrastruktur keamanan data (BSSN, 2022).

c. Keterlibatan oknum internal (*insider threat*)

Berdasarkan hasil penelusuran kasus di Pringsewu, ditemukan bahwa pelaku dibantu oleh oknum internal penyelenggara seleksi dalam hal akses fisik dan teknis terhadap komputer yang digunakan. Model ancaman seperti ini dikenal sebagai insider threat, yang menurut Jansen dan Leukfeldt (2018) justru menjadi celah paling sulit dideteksi dalam kejahatan siber. Keterlibatan panitia seleksi menjadi penghambat karena memperumit pembuktian dan menurunkan kepercayaan publik terhadap objektivitas proses rekrutmen ASN. Ancaman dari dalam inilah yang sering kali luput dari pengawasan dan belum mendapatkan perhatian serius dalam desain sistem seleksi.

d. Rendahnya kesadaran digital (*digital literacy*) penyelenggara tes

Penyelenggara seleksi di tingkat daerah (BKPSDM) umumnya tidak memiliki latar belakang teknologi informasi yang memadai. Hal ini menyebabkan rendahnya kewaspadaan terhadap risiko siber, seperti pemasangan aplikasi pengendali jarak jauh (*remote access trojan*) yang tidak terdeteksi sebelum ujian berlangsung. Ketidaksiapan sumber daya manusia ini menciptakan celah krusial dalam sistem keamanan digital. Menurut penelitian Nasution et al. (2021), *low institutional digital literacy* pada sektor publik merupakan penyebab utama kebocoran data dan manipulasi sistem di instansi pemerintahan Indonesia.

e. Tidak adanya regulasi teknis terkait penegakan hukum siber di daerah

UU ITE dan KUHP memang mengatur pidana terhadap pelaku *illegal access*, namun dalam tataran implementasi, belum tersedia regulasi teknis atau peraturan pelaksana (turunan) yang dapat dioperasionalkan oleh instansi daerah. Akibatnya, aparat penegak hukum di daerah sering menghadapi kebingungan dalam mengidentifikasi tindak pidana siber dan prosedur pembuktiannya. Absennya *lex specialis* untuk mekanisme penegakan hukum digital di sektor seleksi ASN menyebabkan ruang hukum yang terlalu luas, sehingga sulit dijangkau oleh hukum acara pidana konvensional. Hal ini menjadi bukti bahwa hukum pidana belum bertransformasi mengikuti logika digital.

Guna mengatasi berbagai hambatan tersebut, diperlukan peningkatan kapasitas aparat penegak hukum, penguatan regulasi perlindungan data, serta modernisasi teknologi keamanan informasi. Edukasi dan literasi digital kepada masyarakat serta penguatan sistem kontrol internal dalam pelaksanaan tes CPNS menjadi langkah strategis untuk mewujudkan proses seleksi yang adil, transparan, dan bebas dari intervensi *cyber crime*. Faktor-faktor penghambat di atas menunjukkan bahwa kejahatan illegal access tidak dapat diberantas hanya melalui pendekatan penegakan hukum represif. Diperlukan reformasi regulasi dan kelembagaan, antara lain:

a. Penyusunan SOP nasional sistem keamanan digital seleksi CPNS oleh BKN dan BSSN, termasuk pedoman *cyber incident response plan*.
b. Peningkatan kapasitas penyidik digital forensik di tingkat Polda dan Kejaksaan Tinggi melalui kerja sama dengan lembaga pelatihan TI internasional.
c. Pemberian mandat hukum bagi BSSN untuk melakukan audit sistem seleksi CPNS secara periodik, guna mendeteksi kelemahan sistem sebelum dimanfaatkan oleh pelaku kejahatan.
d. Penerbitan Peraturan Presiden atau Peraturan Menteri PAN-RB yang mengatur perlindungan data, pengawasan sistem seleksi, dan mekanisme pelaporan kejahatan digital dalam seleksi ASN.

4. KESIMPULAN DAN SARAN/REKOMENDASI

4.1 Kesimpulan

Kejahatan *illegal access* merupakan bentuk kejahatan yang lahir dari interaksi antara individu, lingkungan sosial, dan perkembangan sistem teknologi informasi. Kejahatan ini termasuk dalam kategori *cybercrime*, yaitu tindak pidana yang muncul sebagai konsekuensi dari kemajuan teknologi informasi dan komunikasi yang pesat, terutama di era globalisasi. Kemampuan individu dalam melakukan tindak pidana juga mengalami transformasi seiring dengan kemudahan akses terhadap perangkat digital dan informasi teknis. Penanggulangan kejahatan illegal access tidak dapat dibebankan semata-mata kepada pemerintah atau aparat penegak hukum. Perlu adanya partisipasi aktif dari seluruh elemen masyarakat, termasuk mahasiswa dan sektor privat. Peningkatan literasi digital, edukasi keamanan siber, pengembangan teknologi pelindung sistem informasi, serta pengawasan sosial dan kolaborasi lintas sektor menjadi langkah penting untuk menciptakan ekosistem digital yang aman dan terpercaya. Dengan cara tersebut, kemajuan teknologi dapat dimanfaatkan secara optimal tanpa terhambat oleh ancaman kejahatan siber.

4.2 Saran/Rekomendasi

Pemerintah perlu meningkatkan pengamanan sistem informasi, khususnya dalam pelaksanaan seleksi Calon Pegawai Negeri Sipil (CPNS). Upaya tersebut dapat dilakukan melalui penerapan teknologi enkripsi yang kuat, sistem autentikasi ganda, serta peningkatan pengawasan internal dan eksternal secara berkelanjutan. Sistem informasi pada proses seleksi CPNS harus memiliki standar keamanan siber nasional yang ketat untuk mencegah potensi akses ilegal dan manipulasi data. Selain itu, aparat penegak hukum perlu melakukan penegakan hukum yang tegas terhadap pelaku tindak pidana illegal access. Penegakan ini harus didukung oleh kapasitas forensik digital yang mumpuni serta penerapan sanksi pidana yang jelas, terukur, dan menimbulkan efek jera. Dengan demikian, akan terbentuk individu-individu yang lebih taat hukum dan sistem rekrutmen ASN yang lebih kredibel, transparan, dan akuntabel.

REFERENSI

Andarek, R. R. (2025). Penerapan Forensic Science Dalam Proses Penyidikan Kasus Pembunuhan Vina Dan Risky: Antara Bukti Ilmiah Dan Keadilan Substantif. *Jurnal Sosial Teknologi*, *5*(5), 1568–1589. https://doi.org/10.59188/jurnalsostech.v5i5.32152

Anwar, M. (2023). The Urgency of Reforming Regulations for Money Laundering in the Digital Era. *East Asian Journal of Multidisciplinary Research*, *2*(7), 2895–2906. https://doi.org/10.55927/eajmr.v2i7.5009

Budiyanto. (2025). *Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia*. Sada Kurnia Pustaka.

Deni Achmad, & Firganefi. (2016). *Pengantar Kriminologi dan Viktimologi*. Justice Publisher.

Emilia Susanti, & Eko Raharjo. (2018). *Buku Ajar Hukum dan Kriminologi*. CV. Anugrah Utama Rahardja.

Gilang Putra, & Kayus Kayouwan Lewoleba. (2024). Menyingkapi Penurunan Kepercayaan Masyarakat Terhadap Aparat Penegak Hukum Di Indonesia. *Birokrasi: JURNAL ILMU HUKUM DAN TATA NEGARA*, *2*(3), 306–315. https://doi.org/10.55606/birokrasi.v2i3.1342

Handoyo, B., MZ, H., Rahma, I., & Asy'ari. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah Dan Hukum*, 40–55. https://doi.org/10.47498/maqasidi.v4i1.2966

Hikmatulloh, R., & Nurmiati, E. (2020). Analisis Strategi Pencegahan Cybercrime Berdasarkan UU ITE Di Indonesia (Studi Kasus: Penipuan Pelanggan Gojek). *Kosmik Hukum*, *20*(2), 121. https://doi.org/10.30595/kosmikhukum.v20i2.6449

Hulu, A. R., Ndraha, A. B., Lase, D., & Halawa, O. (2024). Analisis Perencanaan Sumber Daya Manusia Perspektif Pengadaan Pegawai Negeri Sipil di Badan Kepegawaian dan Pengembangan Sumber Daya Manusia Kota Gunungsitoli. *Arus Jurnal Sosial Dan Humaniora*, *4*(3), 1543–1552. https://doi.org/10.57250/ajsh.v4i3.725

Ketut Boby Suryawan. (2025). Memahami Fungsi dan Tujuan Hukum dalam Pengantar Ilmu Hukum. *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *2*(3), 226–236.

Kuswara, D., & Mayasari, I. (2023). Implementasi Manajemen PNS Berbasis Sistem Merit Dalam Penempatan Jabatan Struktural Pegawai di Pemerintah Provinsi DKI Jakarta. *Cakrawala Repositori IMWI*, *6*(1), 336–351. https://doi.org/10.52851/cakrawala.v6i1.241

Sumarna, D., & Kadriah, A. (2023). Penelitian Kualitatif Terhadap Hukum Empiris. *JURNAL PENELITIAN SERAMBI HUKUM*, *16*(02), 101–113. https://doi.org/10.59582/sh.v16i02.730

Tabiu, R., Heryanti, Intan, N., & Safiuddin, S. (2023). Globalisasi dan Kejahatan Transnasional Terorganisasi. *Halu Oleo Law Review*, *7*(1), 99–110. https://doi.org/10.33561/holrev.v7i1.11

Wahyuni, W. (2019). Aspek Hukum Terhadap Seleksi Penerimaan Cpns Tahun 2018. *Bilancia: Jurnal Studi Ilmu Syariah Dan Hukum*, *13*(1), 1–18. https://doi.org/10.24239/blc.v13i1.449