JURRISH: Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora
Volume. 4 Nomor. 3 Juli 2025
e-ISSN: 2828-7622; p-ISSN: 2828-7630, Hal. 858-867
DOI: https://doi.org/10.55606/jurrish.v4i3.6033
Available online at: https://prin.or.id/index.php/JURRISH

Tindak Pidana Penyebaran Aplikasi Malware Berbasis APK
(Studi terhadap Fenomena Modus Lowongan Kerja dan Paket Palsu)

Mhd. Raihan Rizqullah[1*], Rahmat Surkhalid Nasution[2], Sabda Abdillah Lubis[3], Muhammad Ichsan Parinduri[4], Limrogate Immanuel[5]
[1-4] Universitas Deztron Indonesia,Indonesia
[5] Universitas Nusa Cendana,indonesia
muhammadraihanrizqullah@udi.ac.id[1*], rahmatsurkhalidnst@udi.ac.id[2], sabdaabdillahlubis@udi.ac.id[3], muhammadichsanparinduri@udi.ac.id[4], limrogate.immanuel@staf.undana.ac.id[5]

Korespondensi Penulis: muhammadraihanrizqullah@udi.ac.id[*]

Abstract*. The development of digital technology has provided convenience in various aspects of life, but also presents new challenges in the form of cybercrime. One of the increasingly widespread modes in Indonesia is the spread of APK (Android Package Kit)-based malware via short messages offering fake job vacancies or fictitious package notifications. When the victim downloads and installs the application, the perpetrator gains access to personal data and banking accounts, which are then used for criminal acts. This phenomenon causes great financial and emotional losses for the community and tests the effectiveness of criminal law in dealing with technology-based cybercrime. This study uses a normative juridical approach with an analysis of laws and regulations, scientific literature, and actual case studies. The results of the study show that the perpetrators can be charged with Articles 30, 32, and 35 of the ITE Law, as well as provisions in the new Criminal Code. However, the implementation of law enforcement still faces challenges, such as digital evidence, limited investigator capacity, and minimal cross-country cooperation. Therefore, cyber law policy reform, increasing digital literacy in the community, and strengthening coordination between law enforcement agencies are needed.*

Keywords*: Criminal law; Cybercrime; Fake job vacancies; ITE Law; Malware APK*

Abstrak. Perkembangan teknologi digital telah memberikan kemudahan dalam berbagai aspek kehidupan, namun juga menghadirkan tantangan baru dalam bentuk kejahatan siber. Salah satu modus yang semakin marak di Indonesia adalah penyebaran malware berbasis APK (Android Package Kit) melalui pesan singkat yang menawarkan lowongan kerja palsu atau pemberitahuan paket fiktif. Saat korban mengunduh dan menginstal aplikasi tersebut, pelaku mendapatkan akses ke data pribadi hingga akun perbankan, yang kemudian digunakan untuk tindakan kriminal. Fenomena ini menimbulkan kerugian besar secara finansial dan emosional bagi masyarakat serta menguji efektivitas hukum pidana dalam menghadapi kejahatan siber berbasis teknologi. Penelitian ini menggunakan pendekatan yuridis normatif dengan analisis terhadap peraturan perundang-undangan, literatur ilmiah, dan studi kasus aktual. Hasil penelitian menunjukkan bahwa pelaku dapat dijerat dengan Pasal 30, 32, dan 35 UU ITE, serta ketentuan dalam KUHP baru. Namun, implementasi penegakan hukumnya masih menghadapi tantangan, seperti pembuktian digital, keterbatasan kapasitas penyidik, serta minimnya kerja sama lintas negara. Oleh karena itu, dibutuhkan reformasi kebijakan hukum siber, peningkatan literasi digital masyarakat, dan penguatan koordinasi antar lembaga penegak hukum.

Kata kunci: Cybercrime; Hukum pidana; Lowongan kerja palsu; Malware APK; UU ITE

1. PENDAHULUAN

Latar Belakang

Perkembangan teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, mulai dari komunikasi, transaksi ekonomi, hingga penyebaran informasi. Namun, bersamaan dengan kemajuan ini, muncul pula tantangan besar dalam bentuk kejahatan siber atau cybercrime yang terus mengalami evolusi dalam modus dan jangkauan. Salah satu bentuk cybercrime yang belakangan ini marak terjadi adalah penyebaran malware

Received: June 16, 2025; Revised: June 30, 2025; Accepted: Juli 01, 2025; Published : Juli 03, 2025

berbasis file APK (Android Package Kit), terutama dengan memanfaatkan media sosial dan aplikasi perpesanan seperti WhatsApp dan Telegram.

Modus kejahatan ini sangat mengkhawatirkan karena menyasar korban dari berbagai latar belakang usia dan pendidikan, termasuk pelajar, mahasiswa, pekerja, hingga ibu rumah tangga. Pelaku menyamar sebagai pihak yang memberikan tawaran pekerjaan, memberikan informasi paket, atau bahkan mengirimkan undangan wawancara kerja palsu. Tautan yang dikirim biasanya mengarah ke file APK yang jika diinstal, memungkinkan pelaku mengambil alih kendali atas perangkat korban, termasuk akses ke data pribadi, akun perbankan, dan dompet digital.

Fenomena ini menjadi sangat meresahkan karena sebagian besar masyarakat belum memiliki literasi digital yang memadai untuk memahami bahaya dari menginstal aplikasi di luar Google Play Store. Tidak sedikit korban yang mengalami kerugian finansial besar, kehilangan kontrol atas perangkatnya, hingga mengalami gangguan psikologis akibat data pribadinya disalahgunakan. Kejahatan ini memanfaatkan celah dalam kesadaran digital dan kelemahan sistem keamanan perangkat.

Dari sudut pandang hukum pidana, penyebaran malware melalui APK palsu ini tergolong sebagai tindak pidana serius karena melibatkan pelanggaran atas hak privasi, penipuan, peretasan, dan akses ilegal terhadap sistem elektronik. Pelaku dapat dijerat dengan berbagai pasal dalam UU ITE, serta ketentuan pidana umum dalam KUHP. Namun, implementasi penegakan hukum terhadap kejahatan ini masih menghadapi tantangan besar, baik dari sisi teknis, sumber daya, maupun kerjasama lintas negara.

Salah satu hambatan terbesar dalam pemberantasan kejahatan ini adalah sulitnya melacak pelaku karena mereka menggunakan teknologi canggih seperti virtual private network (VPN), akun palsu, dan nomor sekali pakai. Selain itu, banyak korban yang tidak melaporkan kejadian karena merasa malu atau tidak tahu prosedur hukum yang harus ditempuh. Ini menunjukkan perlunya pendekatan hukum yang tidak hanya represif, tetapi juga preventif dan edukatif.

Sejauh ini, respons pemerintah melalui Kemenkominfo dan BSSN masih bersifat reaktif, seperti pemblokiran tautan dan sosialisasi umum. Belum ada kerangka hukum yang secara spesifik menanggapi fenomena malware berbasis APK sebagai bentuk kejahatan siber dengan karakteristik tersendiri. Hal ini menimbulkan kekosongan hukum dalam perlindungan masyarakat yang menjadi korban.

Di sisi lain, kejahatan ini menunjukkan adanya pergeseran strategi pelaku yang tidak lagi mengandalkan teknik peretasan sistem, melainkan memanipulasi psikologis korban

melalui teknik social engineering. Dengan kata lain, pelaku menciptakan skenario yang membuat korban secara sukarela memberikan akses ke perangkatnya. Ini menuntut adanya pembaruan perspektif dalam memahami cybercrime, bukan hanya sebagai pelanggaran teknis, tetapi juga kejahatan berbasis manipulasi sosial.

Berdasarkan uraian di atas, penting bagi dunia akademik, aparat penegak hukum, dan pembuat kebijakan untuk mengkaji fenomena penyebaran malware berbasis APK secara mendalam. Kajian ini bertujuan untuk memahami bentuk kejahatannya, dampaknya terhadap korban, serta mencari solusi hukum yang tepat guna mencegah dan menindak pelaku secara efektif dan adil.

Rumusan Masalah

Penelitian ini bertujuan untuk menganalisis fenomena penyebaran aplikasi malware berbasis APK dalam konteks hukum pidana di Indonesia. Berdasarkan latar belakang yang telah dijelaskan, maka permasalahan utama dalam penelitian ini dirumuskan ke dalam beberapa pertanyaan penelitian sebagai berikut:

1. **Bagaimana mekanisme penyebaran malware berbasis APK yang dikemas dalam modus lowongan kerja dan pengiriman paket fiktif?**
   Penelitian akan mengkaji pola dan teknik yang digunakan pelaku untuk menipu korban agar menginstal file berbahaya ke dalam perangkatnya.
2. **Apa dampak hukum, sosial, dan ekonomi yang ditimbulkan terhadap korban kejahatan siber ini?**
   Penelitian ini mengidentifikasi kerugian yang dialami korban dari sudut pandang pidana, perlindungan data pribadi, dan aspek psikologis-sosial.
3. **Bagaimana ketentuan hukum pidana Indonesia mengatur dan menjerat pelaku penyebaran APK malware?**
   Pembahasan ini mencakup analisis terhadap pasal-pasal UU ITE, KUHP lama, serta KUHP baru yang mulai berlaku sejak 2023.
4. **Apa saja hambatan yang dihadapi aparat penegak hukum dalam memproses dan menindak pelaku kejahatan APK palsu ini?**
   Penelitian menyoroti aspek teknis dan kelembagaan yang menghambat penyidikan dan pembuktian kasus.

5. **Apa rekomendasi solusi hukum dan non-hukum yang dapat ditawarkan untuk mencegah dan mengatasi kejahatan ini secara efektif?**
   Poin ini menekankan pentingnya reformasi hukum, peningkatan kapasitas aparat, serta edukasi publik digital.

2. TINJAUAN PUSTAKA

Konsep Cybercrime dalam Perspektif Hukum Pidana

Cybercrime atau kejahatan siber didefinisikan sebagai setiap bentuk kejahatan yang dilakukan dengan menggunakan komputer atau jaringan komputer sebagai alat, sasaran, atau tempat kejahatan. Menurut David Wall, cybercrime terdiri dari tiga kategori: computer-assisted crime**,** computer-targeted crime**,** dan computer incidental. Dalam konteks penelitian ini, malware APK masuk ke dalam kategori kedua: perangkat digital menjadi sasaran kejahatan.

Hukum pidana Indonesia merespons fenomena cybercrime melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian diperbarui menjadi UU Nomor 19 Tahun 2016. Di dalamnya, diatur tindakan pidana seperti akses ilegal (Pasal 30), pengubahan data (Pasal 32), serta pemalsuan dokumen elektronik (Pasal 35). Ketiga pasal ini menjadi rujukan utama dalam menjerat pelaku penyebaran malware berbasis APK.

Namun, pengaturan dalam UU ITE belum sepenuhnya mampu menjangkau modus-modus baru dalam kejahatan digital, termasuk yang bersifat manipulatif atau berbasis teknik social engineering. Oleh karena itu, hukum pidana nasional, termasuk KUHP yang baru disahkan melalui UU Nomor 1 Tahun 2023, perlu diinterpretasikan lebih luas untuk merespons perkembangan teknologi informasi yang begitu pesat.

Malware dan Aplikasi Berbasis APK sebagai Alat Kejahatan

Malware adalah singkatan dari malicious software, yaitu perangkat lunak berbahaya yang dirancang untuk merusak, mencuri, atau mengakses sistem tanpa izin. Malware dapat berupa virus, trojan, spyware, ransomware, dan sebagainya. Dalam konteks Android, malware sering disisipkan dalam file APK yang dipasang di luar Play Store. Ketika diinstal, malware akan meminta izin akses, lalu mengendalikan perangkat pengguna secara diam-diam.

Laporan dari Kaspersky (2024) menunjukkan bahwa Indonesia mengalami peningkatan signifikan dalam penyebaran malware berbasis APK, terutama dengan modus lowongan kerja palsu. Banyak dari aplikasi ini meminta izin mengakses SMS, kontak, kamera, dan aplikasi

perbankan. Setelah memperoleh izin tersebut, pelaku dapat mencuri data, OTP, hingga mengosongkan saldo korban melalui e-wallet dan mobile banking.

APK palsu sangat efektif karena menyasar kelemahan psikologis korban, yaitu harapan mendapatkan pekerjaan, hadiah, atau status pengiriman paket. Maka dari itu, malware bukan lagi sekadar alat teknis, tetapi telah menjadi alat utama dalam manipulasi sosial untuk mengelabui masyarakat secara masif.

Social Engineering dan Kejahatan Siber Berbasis Psikologi

Salah satu aspek paling berbahaya dalam penyebaran malware APK adalah penggunaan teknik social engineering, yaitu cara memanipulasi psikologis korban agar secara sukarela memberikan akses. Ini mencakup pesan yang meyakinkan, berpura-pura sebagai institusi resmi, hingga menggunakan data pribadi korban yang telah bocor sebelumnya.

Berbeda dengan peretasan sistem melalui celah keamanan (hacking), social engineering mengandalkan ketidaktahuan, ketergesa-gesaan, atau harapan korban. Hal ini menjadikannya sulit untuk dicegah hanya dengan sistem keamanan teknis. Oleh karena itu, pendekatan hukum terhadap kejahatan ini tidak bisa hanya fokus pada aspek teknis, tetapi juga perlu menyentuh dimensi etika, perlindungan konsumen, dan regulasi platform digital.

Aspek ini juga menunjukkan pentingnya literasi digital sebagai bagian dari perlindungan hukum. Dalam banyak kasus, korban tidak sadar bahwa mereka sedang dimanipulasi, karena tidak memiliki kemampuan mengenali potensi bahaya dari file APK yang dikirim melalui media sosial.

3. METODE PENELITIAN

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode **yuridis normatif**, yaitu pendekatan yang memfokuskan kajian terhadap norma-norma hukum tertulis dalam peraturan perundang-undangan dan teori hukum yang relevan. Pendekatan ini dipilih karena penelitian lebih menitikberatkan pada interpretasi hukum yang berlaku terhadap fenomena penyebaran aplikasi malware berbasis APK.

Pendekatan yuridis normatif ini bertujuan untuk menganalisis bagaimana ketentuan hukum pidana, khususnya dalam UU ITE dan KUHP, mampu mengakomodasi dan menanggulangi modus kejahatan digital berbasis social engineering. Penelitian ini tidak melakukan survei lapangan, melainkan bersifat studi kepustakaan (library research).

Melalui pendekatan ini, penulis akan memaparkan ketentuan hukum yang relevan, menganalisisnya berdasarkan teori hukum pidana dan siber, serta mengaitkan dengan kondisi aktual yang terjadi di masyarakat melalui studi kasus. Dengan demikian, hasil penelitian ini diharapkan mampu memberikan pemahaman teoritis dan praktis secara bersamaan.

Sumber dan Teknik Pengumpulan Data

Data yang digunakan dalam penelitian ini bersifat sekunder, yang terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer mencakup peraturan perundang-undangan seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU Nomor 19 Tahun 2016 tentang Perubahannya, dan KUHP baru (UU No. 1 Tahun 2023). Sementara itu, bahan hukum sekunder meliputi buku-buku hukum pidana dan siber, jurnal ilmiah, laporan resmi dari instansi pemerintah seperti BSSN dan Kominfo, serta artikel berita terpercaya yang memuat informasi tentang kasus penyebaran APK palsu di Indonesia.

Teknik pengumpulan data dilakukan melalui studi dokumentasi terhadap regulasi, artikel ilmiah, dan sumber relevan lainnya. Penelusuran juga dilakukan melalui mesin pencari akademik dan portal hukum nasional.

Teknik Analisis Data

Data yang telah dikumpulkan dianalisis secara deskriptif-kualitatif. Analisis deskriptif dilakukan untuk menggambarkan fakta hukum, kerangka hukum yang berlaku, dan relevansi antara keduanya. Sementara itu, analisis kualitatif digunakan untuk menilai kecukupan dan efektivitas regulasi dalam menanggulangi kejahatan berbasis APK malware.

Penulis juga membandingkan antara norma hukum positif dengan praktik di lapangan melalui kasus-kasus yang diberitakan media dan dilaporkan ke pihak kepolisian. Dengan pendekatan ini, penulis dapat menunjukkan adanya kesenjangan antara aturan hukum dan pelaksanaannya.

4. HASIL DAN PEMBAHASAN

Modus penyebaran malware berbasis APK umumnya dilakukan melalui aplikasi pesan instan. Pelaku mengirimkan pesan yang menyatakan bahwa korban mendapat undangan kerja, informasi paket, atau tagihan, lengkap dengan tautan unduhan aplikasi. File yang dikirim bukan berasal dari platform resmi seperti Google Play Store, melainkan dari situs luar yang rawan malware.

Begitu korban mengunduh dan menginstal APK, aplikasi tersebut meminta izin untuk mengakses fitur penting seperti kamera, mikrofon, SMS, dan aplikasi keuangan. Jika izin diberikan, pelaku dapat mengakses informasi pribadi, kode OTP, bahkan melakukan transaksi atas nama korban.

Dalam beberapa kasus, pelaku juga menyertakan logo instansi resmi untuk memperkuat kredibilitasnya. Mereka menggunakan domain tiruan yang menyerupai domain asli, seperti .com.co atau .org.id. Hal ini menunjukkan bahwa kejahatan ini bukan dilakukan oleh individu acak, melainkan kelompok terorganisir.

Pelaku sering menyasar korban pada malam hari atau akhir pekan, saat layanan pelanggan bank dan institusi resmi tutup. Hal ini dimanfaatkan agar korban kesulitan mendapatkan bantuan segera, sehingga pelaku memiliki waktu yang cukup untuk mengeksploitasi sistem dan memindahkan dana. Strategi ini menunjukkan adanya perencanaan yang matang dan penguasaan terhadap kelemahan sistem pelayanan keuangan nasional.

Beberapa malware dirancang sedemikian rupa sehingga secara otomatis menyembunyikan ikon aplikasinya setelah diinstal. Hal ini membuat korban tidak menyadari bahwa aplikasi tersebut masih aktif di latar belakang dan terus mengakses data. Bahkan, ada malware yang dapat melakukan perekaman layar dan ketikan (keylogging), memungkinkan pelaku mencuri kata sandi dan data login.

APK jahat ini juga biasanya dilengkapi dengan fitur yang mencegah korban menerima SMS dari bank, sehingga notifikasi transaksi tidak muncul. Dalam kondisi ini, korban sering kali baru menyadari kejahatan terjadi setelah seluruh dana di rekening sudah terkuras. Pelaku memanfaatkan kelengahan dan ketidaktahuan korban mengenai keamanan digital.

Dalam banyak kasus, pelaku juga menggunakan sistem afiliasi untuk menyebarkan tautan APK palsu. Mereka merekrut orang-orang dengan imbalan komisi untuk menyebarkan link ke grup WhatsApp, Telegram, atau media sosial. Pola ini mempercepat penyebaran malware dan memperluas jangkauan korban, bahkan hingga ke pedesaan atau daerah terpencil. Ada pula pola penyebaran melalui iklan digital palsu di media sosial atau Google Ads yang mengarahkan ke situs berbahaya. Situs tersebut menyamar sebagai situs resmi perusahaan dan menawarkan file unduhan APK. Dengan meniru antarmuka asli, korban tidak menyadari bahwa mereka masuk ke dalam perangkap phishing dan malware sekaligus.

Polanya tidak hanya berkembang secara teknis, tapi juga adaptif terhadap tren sosial. Misalnya, saat banyak masyarakat mencari bantuan sosial digital, pelaku menyamar sebagai penyalur bansos dengan syarat mengunduh aplikasi. Pada saat lain, pelaku menyasar orang tua

dengan kedok aplikasi pelacak anak. Hal ini menunjukkan bahwa modus operandi malware APK bersifat fleksibel dan mengikuti perubahan psikologi masyarakat.

Kerugian dan Dampak terhadap Korban

Korban dari malware berbasis APK mengalami berbagai kerugian. Kerugian utama adalah kerugian finansial akibat dana di rekening atau dompet digital yang hilang secara misterius. Namun, kerugian tidak hanya bersifat materiil. Banyak korban juga mengalami tekanan psikologis dan gangguan mental akibat kehilangan kontrol atas perangkat dan data pribadi mereka.

> Dalam beberapa kasus, data korban seperti kontak, dokumen penting, hingga foto pribadi disalahgunakan. Ada juga korban yang menjadi sasaran doxing dan ancaman jika tidak membayar sejumlah uang sebagai tebusan. Hal ini membuat kejahatan ini berimplikasi ganda: pidana, privasi, dan mental.

Sayangnya, banyak korban tidak mengetahui bagaimana melaporkan kasusnya atau tidak percaya pada efektivitas proses hukum. Hal ini menunjukkan bahwa perlindungan hukum terhadap korban kejahatan siber masih belum optimal.

Penjeratan Hukum terhadap Pelaku APK Palsu

Secara hukum, pelaku penyebaran malware dapat dijerat melalui UU ITE Pasal 30 ayat (3) tentang akses ilegal terhadap sistem elektronik, Pasal 32 tentang perusakan atau pengubahan data, dan Pasal 35 tentang pemalsuan dokumen elektronik. Sanksi pidana yang diatur mencapai 12 tahun penjara dan denda hingga Rp12 miliar.

Selain itu, dalam KUHP baru Pasal 262–266 juga mengatur tindak pidana terhadap integritas sistem elektronik. Namun, implementasinya masih dalam tahap awal karena KUHP baru belum diadopsi sepenuhnya dalam praktik penyidikan.

Di lapangan, penyidik mengalami kendala dalam pembuktian, terutama dalam mengidentifikasi pelaku yang menggunakan server luar negeri, VPN, dan identitas palsu. Hal ini menunjukkan bahwa meskipun perangkat hukumnya ada, kemampuan penegak hukum masih perlu ditingkatkan.

Tantangan Penegakan Hukum

Beberapa tantangan besar dalam penegakan hukum terhadap kejahatan APK malware antara lain: kurangnya ahli forensik digital di daerah, keterbatasan alat bukti elektronik, belum

adanya standar prosedur tetap, serta minimnya kerja sama internasional dalam pelacakan dan ekstradisi pelaku.

Selain itu, regulasi yang bersifat umum dan tidak secara spesifik mengatur malware berbasis APK juga menjadi celah hukum yang dimanfaatkan pelaku. Hal ini membutuhkan pembaruan peraturan atau interpretasi hukum yang progresif agar aparat bisa bertindak cepat dan tepat.

Upaya Pencegahan dan Rekomendasi Kebijakan

Upaya pencegahan perlu dilakukan secara menyeluruh. Edukasi digital harus dimasukkan dalam kurikulum sekolah dan pelatihan masyarakat. Pemerintah melalui Kominfo perlu menggencarkan kampanye anti-modus APK palsu dengan menyasar pengguna aktif internet, khususnya di usia produktif.

Di sisi regulasi, pemerintah perlu merancang peraturan pelaksana atau peraturan turunan dari UU ITE yang secara tegas mengatur kejahatan siber berbasis manipulasi sosial. Industri teknologi juga didorong untuk memperketat izin instalasi aplikasi dan menyaring APK mencurigakan sebelum menyebar di platform.

KESIMPULAN

Penyebaran aplikasi malware berbasis APK melalui modus lowongan kerja dan paket palsu merupakan bentuk kejahatan siber yang berkembang pesat di Indonesia. Modus ini tidak hanya mengandalkan kemampuan teknis, tetapi juga manipulasi psikologis korban melalui teknik social engineering. Kejahatan ini menyebabkan kerugian besar baik secara materiil maupun imateriil.

Dari sisi hukum, pelaku dapat dijerat melalui UU ITE dan KUHP baru. Namun, tantangan dalam pembuktian, identifikasi pelaku, dan kerjasama internasional membuat penegakan hukum belum optimal. Perlindungan terhadap korban juga belum maksimal, mengingat kurangnya akses terhadap bantuan hukum dan pemulihan psikologis.

SARAN

Pemerintah perlu:

1. Meningkatkan kapasitas SDM penegak hukum dalam bidang forensik digital.
2. Menggencarkan literasi digital dan edukasi hukum siber kepada masyarakat luas.
3. Mempercepat kerja sama internasional dalam pelacakan dan ekstradisi pelaku lintas negara.

4. Menyusun regulasi khusus terkait penyebaran APK malware dan manipulasi sosial digital.
5. Mendorong kolaborasi dengan sektor teknologi untuk membatasi penyebaran file APK di luar sistem resmi.

DAFTAR PUSTAKA

Arief, B. N. (2015). Masalah penegakan hukum dan kebijakan hukum pidana. Prenada Media.

BSSN. (2024). Laporan tahunan keamanan siber nasional.

CNN Indonesia. (2024, [Tanggal Tidak Diketahui]). Polisi tangkap penyebar APK palsu, kerugian capai Rp3 Miliar.

Detik.com. (2024, [Tanggal Tidak Diketahui]). Modus penipuan pekerjaan lewat APK palsu marak di WhatsApp.

Kaspersky. (2024). Mobile malware report Q2.

Kominfo RI. (2023). Panduan pencegahan kejahatan siber.

Kompas.com. (2025, [Tanggal Tidak Diketahui]). Korban APK palsu bertambah, polisi imbau tidak sembarangan unduh aplikasi.

Mahfud MD. (2011). Politik hukum di Indonesia. LP3ES.

Prakoso, D. (2002). Tindak pidana dalam KUHP. Bina Aksara.

Setiadi, A. H. (2020). Hukum pidana Indonesia. Sinar Grafika.

Soekanto, S. (2013). Pengantar penelitian hukum. UI Press.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. (2023).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE. (2016).

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.