Tindak Pidana Pencurian Data Melalui *WiFi* Perspektif Pasal 30 Ayat (3) UU Nomor 11 Tahun 2008 dan Hukum Pidana Islam

Dikri Abdul Jabar Ahmad¹, Muhamad Kholid², Didi Sumardi³

^{1,2,3}Universitas Islam Negeri Sunan Gunung Djati Bandung

¹dikriabduljabarahmad@gmail.com, ²muhamadkholid@uinsgd.ac.id,

³didisumardi@uinsgd.ac.id

ABSTRACT

The advancement of digital technology has transformed data into a crucial asset, while significantly increasing the threat of cybercrime, including the growing phenomenon of personal data asset theft through public Wi-Fi networks. This research examines this criminal act from two legal perspectives: Indonesian positive law through Article 30 Paragraph (3) of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) as amended by Law Number 1 of 2024, and Islamic criminal law (fiqh jinayah). This study aims to analyze the juridical qualifications, elements of the offense, evidentiary challenges, and compare the philosophy of punishment between the two legal systems. The research method employed is normative juridical with statutory, conceptual, comparative, and jurisprudential case study approaches. The results indicate that data that via Wi-Fi can be qualified as the crime of illegal access based on the elements in Article 30 paragraph (3) of the ITE Law, which constitutes a formal delict. Jurisprudence analysis reveals how judges interpret the element of "breaching a security system" in various modus operandi. From the perspective of Islamic criminal law, this act does not meet the requirements of sariqah (hudud theft) but is classified as jarimah ta'zir as it violates the principle of property protection (hifz al-mal) within the maqashid al-syariah. Data, as an intangible asset with economic value (Maliyah), receives legal protection based on contemporary ijihad. A comparison of sanctions highlights that the ITE Law is retributive-deterrent with rigid criminal threats, whereas ta'zir in Islamic law is flexible, educative, and restorative, focusing on substantive justice and public interest. It is concluded that there is an urgent need to reform the national cyber law policy by integrating the values of flexibility and substantive justice from the philosophy of ta'zir to address the evolving dynamics of cybercrime.

Keywords: Data Theft, Wi-Fi, ITE Law, Islamic Criminal Law, Cybercrime

ABSTRAK

Kemajuan teknologi digital telah mentransformasi data menjadi aset krusial, sekaligus meningkatkan secara signifikan ancaman kejahatan siber, termasuk fenomena pencurian aset data pribadi melalui jaringan *Wi-Fi public* yang semakin marak. Penelitian ini mengkaji tindak pidana tersebut dari dua perspektif hukum: hukum positif Indonesia melalui Pasal 30 ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 1 Tahun 2024, dan hukum pidana Islam (*fiqh jinayah*). Penelitian ini bertujuan untuk menganalisis kualifikasi yuridis, unsur-unsur delik, tantangan pembuktian, serta membandingkan filosofi pembedaan antara kedua sistem hukum tersebut. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, komparatif, dan studi kasus jurisprudensi. Hasil penelitian menunjukkan bahwa pencurian data melalui *Wi-Fi* dapat

dikualifikasikan sebagai tindak pidana akses ilegal berdasarkan unsur-unsur dalam Pasal 30 ayat (3) UU ITE, yang merupakan delik formil. Analisis yurisprudensi memperlihatkan bagaimana hakim menafsirkan unsur “menjebol sistem pengamanan” dalam berbagai modus operandi. Dalam perspektif hukum pidana Islam, perbuatan ini tidak memenuhi syarat *sariqah* (pencurian hudud), namun diklasifikasikan sebagai *jarimah ta'zir* karena melanggar prinsip perlindungan harta (*hifz al-mal*) dalam *maqashid al-syariah*. Data, sebagai aset tidak berwujud (*intangible asset*) yang memiliki nilai ekonomi (*Maliyah*), mendapat perlindungan hukum berdasarkan ijtihad kontemporer. Perbandingan sanksi menyoroti bahwa UU ITE bersifat retributive-deterren dengan ancaman pidana yang kaku, sedangkan *ta'zir* dalam hukum Islam bersifat fleksibel, edukatif, dan *restorative*, dengan fokus pada keadilan substantif dan kemaslahatan umum. Disimpulkan bahwa terdapat kebutuhan mendesak untuk mereformasi kebijakan hukum siber nasional dengan mengintegrasikan nilai-nilai fleksibilitas dan keadilan substantif dari filosofi *ta'zir* untuk menjawab dinamika kejahatan siber yang terus berkembang.

Kata Kunci: Pencurian Data, *Wifi*, UU ITE, Hukum Pidana Islam, Kejahatan Siber

PENDAHULUAN

Perkembangan pesat teknologi digital telah menjadi pedang bermata dua. Di satu sisi, ia menawarkan kemudahan konektivitas dan efisiensi yang belum pernah terbayangkan sebelumnya, namun di sisi lain, ia membuka gerbang bagi bentuk-bentuk kejahatan baru yang semakin canggih dan merasakan (Hapsari & Pambayun, 2023). Dalam ekosistem digital ini, data telah berevolusi dari sekedar informasi menjadi kelas aset baru yang sangat berharga (*valuable asset class*). Data pribadi, data keuangan, dan data korporasi kini menjadi komoditas utama dalam ekonomi digital, yang mendorong inovasi sekaligus menjadi target utama para pelaku kejahatan siber (*cybercrime*) (Habibi & Liviani, 2020; Citranu et al., 2024).

Salah satu modus kejahatan yang paling dekat dengan kehidupan sehari-hari dan seringkali tidak disadari oleh masyarakat luas adalah pencurian aset data melalui jaringan *Wireless Fidelity (Wi-Fi)* publik. Jaringan *Wi-Fi* yang tersedia di ruang-ruang publik seperti kafe, bandara, kampus, dan pusat perbelanjaan menawarkan kenyamanan akses internet gratis, namun sekaligus menjadi celah keamanan yang sangat berbahaya. Pengguna sering kali tidak menyadari bahwa data yang mereka transmisikan melalui jaringan ini rentan terhadap penyadapan dan intersepsi oleh pihak yang tidak berwenang (Europol, 2020)

Modus operandi pelaku umumnya melibatkan teknik-teknik canggih namun semakin mudah diakses. Salah satu metode yang paling umum adalah serangan *Man-in-the-Middle (MITM)*, di masa pelaku secara diam-diam menempatkan dirinya di antara pengguna dan titik akses (*router*) jaringan, sehingga dapat mencegat, membaca, bahkan memodifikasi seluruh lalu lintas data yang lewat (Haryadi & S, 2022). Teknik lain yang juga marak digunakan adalah pembuatan titik akses palsu (*rogue access point*) atau yang dikenal dengan istilah “*evil twin*”. Pelaku membuat jaringan *Wi-Fi* dengan nama yang sangat mirip dengan jaringan sah (misalnya, “Kafe_Gratis_WiFi” sebagai tiruan dari “Kafe_WiFi_Resmi”). Ketika korban terkecoh dan terhubung ke jaringan palsu ini, pelaku memiliki kendali penuh atas koneksi

internet korban dan dapat mencuri informasi sensitif seperti kata sandi email, kredensial media sosial, data perbankan, dan informasi pribadi lainnya dengan mudah (Europol, 2020). Dampak dari kejahatan ini melampaui sekedar kerugian finansial; ia mencakup pencurian identitas, kerusakan reputasi, dan yang lebih fundamental, erosi kepercayaan publik terhadap infrastruktur digital yang menjadi tulang punggung masyarakat modern (Habibi & Liviani, 2020).

Pemerintah Indonesia menyadari betul skala ancaman siber yang terus meningkat dan telah mengambil Langkah-langkah strategis untuk membangun arsitektur pertahanan siber nasional. Badan Siber dan Sandi Negara (BSSN) diposisikan sebagai garda terdepan dalam mengkoordinasikan upaya mitigasi dan respons terhadap insiden siber di seluruh negeri (antaranews.com, 2023). Sebagai manifestasi dari keseriusan ini, pemerintah mengesahkan Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Regulasi ini menjadi landasan kebijakan makro yang kemudian diturunkan ke dalam peraturan teknis oleh BSSN, yaitu Peraturan BSSN Nomor 1 Tahun 2024 Tentang Manajemen Insiden Siber dan Peraturan BSSN Nomor 2 Tahun 2024 Tentang Manajemen Krisis Siber (SSEK, 2024).

Regulasi-regulasi ini mengamankan pendekatan yang lebih terstruktur dan prosedural dalam penanganan insiden, seperti kewajiban bagi semua Penyelenggara Sistem Elektronik (PSE) untuk membentuk *Cyber Incident Response Team* (CIRT) dan melaporkan insiden dalam waktu 24 jam (SSEK, 2024). Pendekatan ini menunjukkan upaya negara untuk menciptakan sebuah ekosistem yang responsif dan terkoordinasi. Namun, fokus pada kepatuhan prosedural ini belum tentu diimbangi dengan evolusi filosofi penegakan hukum pidananya.

Di ranah penegakan hukum pidana, instrumen utama yang digunakan untuk menjerat pelaku kejahatan siber adalah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang ini telah mengalami dua kali perubahan, pertama melalui Undang-Undang Nomor 19 Tahun 2016, dan yang terbaru melalui Undang-Undang Nomor 1 Tahun 2024 (Undang-Undang Nomor 1 Tahun 2024, 2024; Primadhany et al., 2025). UU ITE menjadi landasan hukum siber di Indonesia (*cyber law*) yang mengkriminalisasi berbagai perbuatan terlarang di ruang digital, mulai dari penyebaran konten ilegal hingga kejahatan yang lebih teknis. Dalam konteks pencurian data melalui *Wi-Fi*, delik yang paling relevan adalah akses ilegal (*illegal access*), yang secara spesifik diatur dalam Pasal 30 ayat (3) UU ITE (Chazawi, 2022; OXSANA PUTRI FERADOVA, 2025). Pasal inilah yang menjadi payung hukum utama bagi penegakan hukum untuk menindak perbuatan mengakses sistem elektronik milik orang lain secara tanpa hak dan melawan hukum dengan cara menjebol sistem pengamanan.

Analisis terhadap suatu kejahatan tidak akan lengkap jika hanya berhenti pada kerangka hukum positif. Hukum Pidana Islam (*fiqh jinayah*) menawarkan perspektif etis-filosofis yang mendalam dan universal untuk memahami serta menanggulangi kejahatan dalam berbagai bentuknya, termasuk yang lahir dari Rahim teknologi modern (Siregar dkk., 2024). Meskipun kejahatan siber seperti pencurian

data merupakan fenomena kontemporer yang tidak dikenal pada masa kodifikasi hukum Islam klasik, substansi perbuatannya yakni perampasan hak milik, pelanggaran privasi, dan menimbulkan kerugian (*dharar*) secara fundamental bertentangan dengan prinsip-prinsip universal yang dilindungi oleh syariat Islam (Suharyadi dkk., 2020).

Fondasi filosofis dari larangan ini berakar pada tujuan utama syariat (*maqashid al-syariah*), yaitu perlindungan terhadap lima kebutuhan pokok manusia (*al-dharuriyyat al-khamsah*). Salah satu dari lima pilar ini adalah perlindungan terhadap harta (*hifz al-mal*) (Suharyadi dkk., 2020; Al-Ghazali, 2023). Di era informasi, data telah menjadi aset tidak berwujud (*intangible asset*) yang memiliki nilai ekonomi, strategis, dan personal yang sangat signifikan. Oleh karena itu, perlindungan terhadap aset data dapat dianalogikan (*qiyas*) dengan perlindungan terhadap harta benda fisik. Perampasan data secara tidak sah merupakan bentuk kezaliman (*zulm*) yang merusak tatanan sosial dan ekonomi, sehingga menuntut adanya respons hukum yang adil dan efektif.

Kajian mengenai kejahatan siber dari perspektif UU ITE telah banyak dilakukan, demikian pula studi mengenai konsep pencurian (*sariqah*) dalam hukum pidana Islam klasik (ANGGRIAWAN, 2018). Namun, terdapat kesenjangan riset yang signifikan dalam menganalisis tindak pidana pencurian data melalui *Wi-Fi* secara spesifik, mendalam, dan integratif, terutama pasca amandemen terbaru UU ITE pada tahun 2024. Hukum positif di Indonesia, termasuk UU ITE, sering kali menghadapi tantangan dalam menangani kejahatan siber secara efektif, seperti kesulitan pembuktian digital, anonimitas pelaku, yurisdiksi lintas negara, dan kerangka hukum yang cenderung reaktif dan kaku (Habibi & Liviani, 2020; Sitanggang dkk., 2024).

Di sisi lain, hukum pidana Islam melalui konsep *jarimah ta'zir* (delik yang sanksinya diserahkan pada kebijakan hakim) menawarkan pendekatan yang lebih adaptif, berorientasi pada keadilan restoratif, dan didasari oleh bimbingan moral yang kuat. Terdapat sebuah dialektika yang menarik antara pendekatan negara yang semakin prosedural dan terstruktur, sebagaimana tercermin dalam regulasi BSSN, dengan kebutuhan akan kerangka hukum pidana yang fleksibel untuk menghadapi ancaman siber yang dinamis (SSEK, 2024; Wahyudi, 2023).

Kebaruan (*novelty*) penelitian ini terletak pada upaya menjembatani kesenjangan tersebut melalui beberapa kontribusi utama: 1) Menganalisis kualifikasi yuridis pencurian data *Wi-Fi* berdasarkan kerangka UU ITE yang telah diperbarui dengan UU Nomor 1 Tahun 2024, termasuk menelaah implikasi perubahan pada pasal-pasal terkait penegakan hukum (Undang-Undang Nomor 1 Tahun 2024, 2024). 2) Melakukan analisis yurisprudensi yang mendalam terhadap putusan-putusan Mahkamah Agung terkait Pasal 30 UU ITE untuk membedah bagaimana hakim menginterpretasikan unsur-unsur delik dalam praktik peradilan (Mahkamah Agung Republik Indonesia, 2021, 2022, 2023). 3) Membangun argumentasi fikih kontemporer yang kokoh mengenai status data sebagai harta (*mal*) yang dilindungi, dengan merujuk pada pandangan ulama modern dan ijtihad Lembaga fatwa di Indonesia seperti DSN-MUI (Mahafzah, Q. A., & Melhem, B. M., 2009; Dewan Syariah

Nasional Majelis Ulama Indonesia, 2021). 4) Merumuskan sebuah proposal integrasi antara kepastian hukum dalam UU ITE dengan fleksibilitas dan filosofi keadilan substantif dari *jarimah ta'zir*.

Penelitian ini tidak hanya bertujuan untuk mendeskripsikan dan membandingkan dua sistem hukum, tetapi juga untuk menawarkan sebuah proposal preskriptif. Di saat legislasi positif menunjukkan kelembaman dalam merevisi substansi Pasal 30 UU ITE, sementara yurisprudensi Islam secara dinamis melakukan *ijtihad* untuk merespons isu aset digital, penelitian ini berargumen bahwa dialog antara kedua sistem dapat menghasilkan model penegakan hukum siber yang lebih adaptif dan berkeadilan. Berdasarkan latar belakang tersebut, penelitian ini akan mengkaji secara komprehensif "Tindak Pidana Pencurian Aset Data Melalui Jaringan Wi-Fi: Analisis Komparatif Pasal 30 Ayat (3) UU ITE dan *Fiqh Jinayah*" (Haryadi & S, 2022).

METODE PENELITIAN

Penelitian ini diklasifikasikan sebagai penelitian hukum normatif atau yuridis normatif. Fokus utama dari penelitian normatif adalah analisis terhadap bahan hukum primer dan sekunder untuk menemukan kebenaran koherensi dengan mengkaji norma, asas, dan doktrin hukum yang relevan. Untuk menjawab rumusan masalah, digunakan beberapa pendekatan.

Pertama, pendekatan perundang-undangan (*statute approach*) yang dilakukan dengan menelaah semua peraturan perundang-undangan yang bersangkutan paut dengan isu hukum yang ditangani, khususnya UU ITE (Amin dkk., 2020). *Kedua*, pendekatan konseptual (*conceptual approach*) yang beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam ilmu hukum untuk memahami konsep hukum pidana Islam terkait pencurian dan *ta'zir*.

Ketiga, pendekatan perbandingan hukum (*comparative law approach*) yang digunakan untuk membandingkan sistem hukum positif Indonesia dengan sistem hukum pidana Islam guna menemukan persamaan, perbedaan, serta kelebihan dan kekurangan masing-masing sistem (Rochman dkk., 2021).

Sumber data yang digunakan dalam penelitian ini terdiri dari tiga jenis bahan hukum yang saling melengkapi.

1. Bahan Hukum Primer, yaitu bahan hukum yang bersifat otoritatif dan mengikat. Sumber ini meliputi perundang-undangan, terutama Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik beserta perubahannya. Selain itu, putusan-putusan pengadilan yang telah berkekuatan hukum tetap (*inkracht van gewijsde*) yang berkaitan dengan kasus akses ilegal juga digunakan sebagai yurisprudensi, yang dihimpun dari direktori putusan Mahkamah Agung Republik Indonesia.
2. Bahan Hukum Sekunder, yaitu bahan yang memberikan penjelasan mengenai bahan hukum primer. Sumber ini mencakup literatur ilmiah seperti buku teks mengenai hukum siber dan *fiqh jinayah*, artikel dalam jurnal ilmiah nasional

dan internasional yang terindeks (Hapsari & Pambayun, 2023; Haryadi & S, 2022), serta hasil penelitian dalam bentuk skripsi dan tesis.

3. Bahan Hukum Tersier, yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus hukum, ensiklopedia, dan artikel dari sumber daring terpercaya.

Pengumpulan bahan hukum dilakukan melalui teknik studi keperpustakaan (*library research*) dan penelusuran dokumen secara daring dari sumber-sumber yang kredibel. Seluruh bahan hukum yang terkumpul kemudian dianalisis secara kualitatif dengan menggunakan teknik deskriptif-analitis. Proses analisis dimulai dengan identifikasi dan klasifikasi bahan hukum sesuai dengan relevansinya terhadap norma-norma dalam UU ITE dan konsep-konsep dalam hukum pidana Islam. Melalui pendekatan perbandingan, kedua sistem hukum tersebut dianalisis untuk menyoroti perbedaan filosofis, bentuk sanksi, dan tujuan pemidanaan. Sintesis dari hasil analisis tersebut kemudian digunakan untuk menarik kesimpulan yang menjawab permasalahan penelitian secara komprehensif (ANGGRIAWAN, 2018; Rochman dkk., 2021).

HASIL DAN PEMBAHASAN

KUALIFIKASI YURIDIS PENCURIAN DATA DALAM HUKUM POSITIF INDONESIA

Analisis Doktrinal Pasal 30 Ayat (3) UU ITE: Delik Formil Akses Ilegal

Kerangka hukum pidana utama yang menjadi untuk menindak perbuatan pencurian data melalui jaringan *Wi-Fi* dalam sistem hukum positif Indonesia adalah Pasal 30 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Meskipun UU ITE telah mengalami perubahan melalui UU Nomor 19 Tahun 2016 dan terakhir UU Nomor 1 Tahun 2024, substansi dari pasal mengenai akses ilegal ini tetap dipertahankan (Undang-Undang Nomor 1 Tahun 2024, 2024). Pasal 30 ayat (3) UU ITE secara tegas menyatakan:

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.” (Undang-Undang Nomor 11 Tahun 2008, 2008).

Penjelasan resmi dari pasal ini memberikan definisi bahwa yang dimaksud dengan “sistem pengamanan” adalah suatu sistem yang berfungsi membatasi atau melarang akses ke dalam Komputer atau Sistem Elektronik berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang telah ditentukan (Chazawi, 2022).

Secara doktrinal, pasal ini merupakan delik formil (*formeel delict*). Ini adalah sebuah kualifikasi hukum yang sangat penting, karena implikasinya adalah tindak pidana dianggap telah selesai dan sempurna (*voltooid*) pada saat perbuatan yang dilarang yaitu mengakses sistem elektronik secara ilegal dengan cara-cara yang disebutkan telah dilakukan oleh pelaku (Chazawi, 2022). Dengan cara lain, fokus

pembuktian Jaksa Penuntut Umum adalah pada perbuatan pelaku (*actus reus*) yang aktif menembus sistem keamanan, bukan pada akibat yang ditimbulkannya. Tidak menjadi syarat apakah pelaku berhasil mencuri data, memodifikasi data, atau menimbulkan kerugian finansial pada korban. Selama perbuatan “melanggar, menerobos, melampaui, atau menjebol” sistem pengamanan telah terjadi, maka delik ini telah terpenuhi. Hal ini membedakannya secara fundamental dari delik materiel (*materieel delict*), yang mensyaratkan adanya suatu akibat tertentu (misalnya, kerugian atau kematian) sebagai unsur selesainya tindak pidana (Utrecht, 1966).

Pembuktian Unsur-Unsur Delik dalam Praktik Peradilan

Untuk dapat menjerat seorang pelaku berdasarkan Pasal 30 ayat (3) UU ITE, seluruh unsur yang terkandung di dalamnya harus dapat dibuktikan secara sah dan meyakinkan di muka persidangan. Berdasarkan analisis para ahli hukum dan praktik peradilan, unsur-unsur tersebut dapat diuraikan sebagai berikut (Chazawi, 2022):

1. *Actus Reus*: Menafsirkan “Menjebol Sistem Pengamanan” pada Jaringan Wi-Fi

Unsur ini merupakan inti dari perbuatan (*actus reus*) yang dilarang. “mengakses” diartikan sebagai setiap bentuk interaksi dengan sistem elektronik, dan cara mengaksesnya dirumuskan secara alternatif namun limitatif, atau menjebol sistem pengamanan”. Istilah-istilah ini menunjukkan adanya upaya aktif dari pelaku untuk melewati suatu bentuk proteksi digital yang telah dipasang oleh pemilik sistem yang sah (Chazawi, 2022).

Dalam konteks pencurian data melalui *Wi-Fi*, penafsiran unsur ini menjadi sangat teknis. “Sistem pengamanan” dapat berupa berbagai lapisan proteksi, seperti:

- a. Enkripsi Jaringan: Kata sandi yang melindungi akses ke jaringan *Wi-Fi* (misalnya, WPA2 atau WPA3). “Menjebol” sistem ini bisa berarti melakukan *brute-force attack* untuk menebak kata sandi.
- b. Firewall Router: Perangkat lunak yang membatasi lalu lintas data yang masuk dan keluar dari jaringan. “Menerobos” *firewall* bisa melibatkan eksploitasi kerentanan pada perangkat lunak *router*.
- c. Kepercayaan Pengguna: Dalam serangan *evil twin*, pelaku tidak menjebol enkripsi secara teknis, melainkan “melampaui” sistem pengamanan sosial dengan mengelabui pengguna agar terhubung ke jaringan palsu yang dikendalikan (Europol, 2020).

Praktik peradilan telah menunjukkan bagaimana unsur ini ditafsirkan dalam berbagai modus. Dalam kasus *skimming* ATM, penggunaan alat *skimmer* fisik yang dipasang di mesin ATM dan *router* yang terhubung ke laptop untuk menyalin data nasabah dianggap sebagai perbuatan “menerobos” dan “menjebol” sistem keamanan perbankan (Mahkamah Agung Republik Indonesia, 2022). Demikian pula, dalam kasus peretasan situs web, Tindakan mengunggah skrip berbahaya (seperti *file* PHP) untuk mendapatkan akses ke *file manager* server dan mencuri basis data secara eksplisit dipandang sebagai pemenuhan

unsur “menjebol sistem pengamanan” (Mahkamah Agung Republik Indonesia, 2021).

2. *Mens Rea*: Tantangan Pembuktian Niat Jahat (*Dolus Malus*) di Ruang Siber

Unsur “dengan sengaja” (*opzet*) merujuk pada sikap batin atau niat jahat (*mens rea*) dari pelaku. Dalam teori hukum pidana, kesenjangan ini harus dibuktikan bahwa pelaku menghendaki (*willens*) perbuatannya dan mengetahui (*wettens*) bahwa perbuatannya tersebut dilarang (Utrecht, 1966). Pelaku harus sadar bahwa ia sedang melakukan akses ilegal terhadap sistem elektronik yang bukan miliknya.

Pembuktian *mens rea* dalam kejahatan siber merupakan salah satu tantangan terbesar bagi penegakan hukum (Sitanggang dkk., 2024). Sifat ruang siber yang anonim, yurisdiksi yang tak terbatas, dan sering kali ketiadaan interaksi fisik antara pelaku dan korban memuat pembuktian niat menjadi sangat kompleks. Penuntut umum harus mampu menunjukkan, melalui bukti-bukti digital seperti log aktivitas, Riwayat penelusuran, atau percakapan, bahwa tindakan pelaku bukanlah suatu kealpaan (*culpa*) atau ketidaksengajaan. Misalnya, dalam kasus pencurian data melalui *Wi-Fi*, jaksa harus membuktikan bahwa pelaku secara sadar memasang perangkat lunak penyadap atau membuat jaringan *evil twin* dengan tujuan untuk mencuri data, bukan karena ketidaktahuan teknis.

Unsur lainnya adalah “setiap orang” yang merujuk pada subjek hukum (Orang perseorangan atau korporasi), dan “tanpa hak atau melawan hukum” yang bersifat alternatif. “Tanpa hak” berarti pelaku tidak memiliki izin atau kewenangan dari pemilik sah, sedangkan “melawan hukum” (*wederrechtelijk*) berarti perbuatan tersebut secara formal dilarang oleh undang-undang (Chazawi, 2022). Dalam hampir semua kasus pencurian data, kedua unsur ini terpenuhi karena pelaku jelas tidak memiliki otorisasi untuk mengakses data korban.

Analisis Yurisprudensi: Studi Kasus Akses Ilegal dari Putusan Mahkamah Agung

Meskipun putusan pengadilan yang secara spesifik menangani pencurian data melalui *Wi-Fi* public masih jarang ditemukan dalam direktori Mahkamah Agung, prinsip penegakan hukumnya dapat dianalisis secara mendalam melalui yurisprudensi kasus-kasus akses ilegal lainnya yang dijerat dengan Pasal 30 UU ITE. Analisis terhadap putusan-putusan ini memberikan gambaran konkret tentang bagaimana hakim menafsirkan dan menerapkan pasal tersebut dalam berbagai skenario teknis (Mahkamah Agung Republik Indonesia, 2020, 2020).

Kasus 1: Hacking dan Penjualan Data Kependudukan (Putusan PN Jakarta Selatan, Terdakwa Chandra Kirana)

Dalam kasus ini, terdakwa berhasil mengakses dan mengunduh 2,3 juta data kependudukan dari server Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) Kabupaten Bekasi, yang kemudian ia tawarkan untuk dijual di sebuah forum daring (Mahkamah Agung Republik Indonesia, 2021). Pertimbangan hukum (*ratio decidendi*) hakim sangat relevan untuk memahami penerapan Pasal 30.

Pembuktian *Actus Reus*: Hakim menemukan bahwa unsur “mengakses... dengan cara menjebol sistem pengamanan” terbukti melalui Tindakan terdakwa yang mengunggah sebuah file skrip PHP berbahaya ke dalam sistem melalui celah pada fitur unggah KTP. Skrip ini memberinya akses ke *file manager* server, yang memungkinkannya untuk menavigasi sistem dan mengunduh seluruh basis data. Tindakan ini secara jelas dipandang sebagai upaya aktif untuk “menjebol” proteksi sistem (Mahkamah Agung Republik Indonesia, 2021).

Pembuktian *Mens Rea*: Niat jahat terdakwa terbukti dari rangkaian perbuatannya. Ia terinspirasi oleh berita penjualan data di forum gelap, secara aktif mencari kerentanan sistem, mengunduh data dalam jumlah massif, dan kemudian secara eksplisit menawarkannya untuk dijual seharga USD 300 dengan tujuan agar data tersebut dapat digunakan untuk kejahatan lain seperti registrasi SIM palsu atau pinjaman *online* ilegal. Rangkaian Tindakan ini menunjukkan adanya kehendak (*willens*) dan pengetahuan (*wettens*) yang jelas (Mahkamah Agung Republik Indonesia, 2021).

Kasus 2: Skimming ATM Menggunakan Router dan Alat Skimmer (Putusan PN Malang)

Kasus ini melibatkan sindikat kejahatan yang memasang alat *skimmer* pada mesin ATM untuk menyalin data strip magnetic kartu dan sebuah *router* yang terhubung dengan laptop untuk mencegat data transaksi (Mahkamah Agung Republik Indonesia, 2022).

Pembuktian *Actus Reus*: Hakim dalam putusannya menyatakan bahwa perbuatan para pelaku telah memenuhi unsur “melanggar, menerobos, melampaui, atau menjebol sistem pengamanan”. Pengguna alat *skimmer* dan *router* eksternal untuk menyadap komunikasi antara kartu ATM dan sistem bank secara fisik dan elektronik merupakan bentuk “penerobosan” terhadap sistem keamanan perbankan yang seharusnya tertutup dan terenkripsi (Mahkamah Agung Republik Indonesia, 2022).

Kasus 3: Perbuatan dan Distribusi Aplikasi Penipuan (APK) (Putusan PN Pinrang)

Dalam kasus ini, terdakwa tidak secara langsung meretas korban, melainkan membuat dan mendistribusikan file aplikasi (*apk*) yang dirancang untuk melakukan akses illegal. Ketika diinstal oleh korban, aplikasi tersebut dapat mencuri data sensitive seperti SMS (termasuk kode OTP perbankan) dari perangkat korban (Mahkamah Agung Republik Indonesia, 2023).

Pembuktian *Actus Reus dan Mens Rea*: Ahli dalam persidangan menjelaskan bahwa perbuatan terdakwa dapat dikategorikan sebagai “memfasilitasi untuk mengakses illegal”. Meskipun ia bukan pengguna akhir, dengan merancang dan menyediakan alat secara khusus ditujukan untuk melakukan kejahatan berdasarkan Pasal 30, ia dianggap turut serta dalam kejahatan tersebut. Niat jahatnya terbukti dari peruntukan aplikasi yang ia buat, yaitu untuk memungkinkan pembelinya melakukan

penipuan. Ini menunjukkan perluasan interpretasi hukum, dimana penyedia alat kejahatan siber juga dapat dijerat (Mahkamah Agung Republik Indonesia, 2023).

Kasus 4: Manipulasi Sistem untuk Order Fiktif Transportasi Online (Putusan PN Medan)

Kasus ini menunjukkan penerapan Pasal 30 ayat (3) pada modus yang tidak melibatkan “peretasan” dalam arti tradisional. Terdakwa, seorang pengemudi ojek *online*, menggunakan aplikasi “pemacu” (*mock location*) untuk memanipulasi sistem GPS dan membuat pesanan fiktif untuk mendapatkan bonus dari perusahaan (ANGGRIAWAN, 2018).

Pembuktian *Actus Reus*: Majelis hakim berpendapat bahwa Tindakan memanipulasi sistem elektronik milik perusahaan transformasi online untuk mendapatkan keuntungan yang tidak sah telah memenuhi unsur “mengakses sistem elektronik dengan cara apa pun dengan melanggar sistem pengamanan”. Sistem pengamanan di sini diartikan lebih luas, tidak hanya *firewall* atau enkripsi, tetapi juga logika bisnis dan mekanisme kontrol yang dirancang oleh perusahaan untuk memastikan operasional yang adil dan sah (ANGGRIAWAN, 2018).

Implikasi UU Nomor 1 Tahun 2024: Penegasan Sanksi dan Kewenangan Penegakan Hukum

Revisi kedua UU ITE melalui UU Nomor 1 Tahun 2024 tidak mengubah rumusan Pasal 30 tentang akses ilegal (Undang-Undang Nomor 1 Tahun 2024, 2024). Hal ini menunjukkan bahwa secara legislatif, norma yang ada dianggap masih relevan. Namun, perubahan signifikan terjadi pada pasal-pasal lain yang memiliki implikasi penting terhadap penegakan hukum kasus akses ilegal.

Salah satu perubahan yang paling krusial adalah pada Pasal 36. Rumusan baru Pasal ini berbunyi: “*Setiap Orang dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 34 yang mengakibatkan kerugian material bagi orang lain.*” (Undang-Undang Nomor 1 Tahun 2024, 2024). Pasal ini kemudian diikuti dengan sanksi pidana yang diatur dalam pasal lain. Perubahan ini memiliki dampak filosofis yang signifikan. Jika sebelumnya Pasal 30 ayat (3) adalah delik formil murni yang hanya melihat pada perbuatan, Pasal 36 yang baru kini secara eksplisit mengaitkan perbuatan dalam Pasal 30 dengan timbulnya “kerugian materiil” sebagai faktor yang memberatkan atau menjadi dasar penjatuhan sanksi.

Perubahan ini secara tidak langsung menciptakan jembatan konseptual antara hukum positif Indonesia dan filosofi hukum pidana Islam. Dalam hukum Islam, khususnya dalam penentuan sanksi *ta'zir*, tingkat kerugian atau kemudaratan (*dharar*) yang nyata menjadi salah satu pertimbangan utama hakim (Siregar dkk., 2024; Wahyudi, 2023). Dengan adanya penekanan pada “kerugian materiil” dalam Pasal 36, sistem hukum positif Indonesia mulai bergerak dari pendekatan yang murni procedural-formalistik menuju pendekatan yang lebih substantif, di mana dampak nyata dari kejahatan menjadi relevan dalam proses pemidanaan. Meskipun Pasal 30

ayat (3) tetap sebagai delik formil, konsekuensi dari perbuatan tersebut kini memiliki landasan hukum yang lebih kuat untuk dipertimbangkan dalam penjatuhan sanksi, sebuah perkembangan yang mendekatkan UU ITE pada prinsip keadilan yang berbasis dampak (*harm-based justice*).

Selain itu, UU Nomor 1 Tahun 2024 juga memperkuat kewenangan pemerintah dan penyidik, misalnya melalui Pasal 40 dan 43, untuk melakukan pemutusan akses dan bekerja sama secara internasional dalam pengungkapan tindak pidana siber, yang diharapkan dapat mengatasi Sebagian tantangan penegakan hukum yang ada (Undang-Undang Nomor 1 Tahun 2024, 2024).

PERSPEKTIF FIQH JINAYAH TERHADAP PENCURIAN ASET DIGITAL

Status Data sebagai Harta (*mal*) yang Dilindungi dalam Fiqh Kontemporer

Langkah pertama dan paling fundamental dalam menganalisis pencurian data dari perspektif *fiqh jinayah* adalah menetapkan status hukum dari "data" itu sendiri. Hukum Islam klasik secara ekstensif membahas perlindungan terhadap harta (*mal*), namun konsep harta pada saat itu didominasi oleh objek-objek yang berwujud fisik (*a'yan*). Pertanyaannya adalah, apakah data digital yang bersifat tidak berwujud (*intangible*) dapat diklasifikasikan sebagai *mal* yang dilindungi oleh syariat? (Europol, 2020).

Para ulama kontemporer secara luas telah menjawab pertanyaan ini secara afirmatif melalui proses ijtihad. Mereka berargumen bahwa esensi dari *mal* bukanlah pada wujud fisiknya, melainkan pada nilai (*Maliyah*) dan manfaat (*manfa'at*) yang dimilikinya serta dapat dikuasai (*hiazah*) dan diperjualbelikan. Mufti Taqi Usmani, seorang ulama terkemuka dari Pakistan, berpendapat bahwa tidak ada dalil eksplisit dalam Al-Quran maupun Hadis yang membatasi kepemilikan (*malkiyyah*) hanya pada objek-objek berwujud. Oleh karena itu, hak cipta, paten, dan merek dagang dan secara analogis, data adalah klaim kepemilikan yang sah yang memberikan hak kepada pemiliknya untuk mengambil keuntungan darinya (Mahafzah, Q. A., & Melhem, B. M., 2009).

Pandangan ini didukung oleh prinsip-prinsip umum. Dalam syariat. Hadis Nabi Muhammad SAW yang menyatakan, "*Barangsiapa terbunuh karena melindungi hartanya, makai ia seorang syahid*" (HR. Bukhari & Muslim), menggunakan kata "harta" secara umum, yang dapat ditafsirkan mencakup segala sesuatu yang berharga bagi seseorang, baik berwujud maupun tidak (Khan, I. A., 2017). Demikian pula, Al-Quran dalam Surat Al-Baqarah ayat 188 melarang memakan harta sesame dengan cara yang batil, sebuah larangan yang bersifat universal.

Dalam fiqh, sesuatu dapat dianggap *mal* jika memenuhi dua syarat utama:

1. Memiliki Manfaat (*Muntafa' bih*): data jelas memiliki manfaat yang luar biasa, baik untuk individu (privasi, komunikasi) maupun entitas bisnis (analisis pasar, aset strategis)
2. Dapat Dikuasai (*Muhraz*): Data dapat disimpan, dikontrol, diakses, dan ditransfer, yang menunjukkan adanya untuk penguasaan, meskipun secara digital (Europol, 2020).

Oleh karena itu, mayoritas ulama modern, termasuk Lembaga-lembaga fatwa, mengakui bahwa kekayaan intelektual dan aset digital seperti data adalah bentuk baru dari *mal* atau setidaknya hak yang melekat pada *mal* (*haqq al-mall*) yang wajib dilindungi (Mahafzah, Q. A., & Melhem, B. M., 2009). Mengambilnya tanpa izin adalah sebuah pelanggaran terhadap hak milik yang dijamin oleh syariat.

Analisis Komparatif dengan *Sariqah*: Mengapa Pencurian Data Bukan Delik *Hudud*

Setelah menciptakan data sebagai harta yang dilindungi, kualifikasi tindak pidana pencuriannya perlu ditentukan. Dalam *fiqh jinayah*, pencurian yang paling berat adalah *sariqah*, yang diancam dengan hukuman *hudud* (potong tangan) sebagaimana disebutkan dalam AlQuran Surat Al-Ma'idah ayat 38. Namun, penerapan sanksi *hudud* yang bersifat tetap dan berat ini mensyaratkan pemenuhan rukun dan syarat yang sangat ketat dan bersifat limitative (*tawqifi*), tanpa ruang untuk interpretasi luas (Irfan, 2022; Munajat, 2009).

Pencurian data melalui *Wi-Fi* tidak memenuhi syarat-syarat formal *sariqah* karena beberapa alasan fundamental:

1. Syarat Objek Pencurian (*Al-Masruq*): Objek yang dicuri dalam *sariqah* haruslah harta berwujud (*mal mutaqqawwim*) yang dapat dipindahkan secara fisik. Data, sebagai aset tidak berwujud, tidak memenuhi kriteria ini dalam pandangan jumhur (mayoritas) ulama klasik (ANGGRIAWAN, 2018).
2. Syarat Tempat Penyimpanan (*Hirs*): *Sariqah* mensyaratkan bahwa harta tersebut diambil dari tempat penyimpanannya yang layak dan terkunci (*hirs*). Konsep *hirs* secara tradisional merujuk pada tempat fisik seperti rumah, lemari, atau brankas. Meskipun beberapa ulama kontemporer mencoba menganalogikan (*qiyas*) sistem keamanan digital seperti *firewall*, enkripsi, atau kata sandi dengan *hirs*, analogi ini masih menjadi subjek perdebatan (*ikhtilaf*). Karena adanya keraguan (adanya keraguan (*Syubhat*) dalam pemenuhan syarat ini, dan berdasarkan kaidah fiqh bahwa hukuman *hudud* gugur karena adanya keraguan (*idra'u al-hudud bi al-syubhat*), maka sanksi *sariqah* tidak dapat diterapkan (Irfan, 2022)
3. Syarat Pengambilan Secara Sembunyi-sembunyi (*Khafyah*): *Sariqah* adalah pengambilan harta secara diam-diam. Dalam pencurian data, pelaku seringkali hanya menyalin (*copy*) data tanpa menghilangkan data aslinya dari server korban. Hal ini berbeda dengan pencurian fisik dimana barang yang dicuri hilang dari pemiliknya (ANGGRIAWAN, 2018)

Karena syarat-syarat yang ketat ini tidak terpenuhi, maka perbuatan pencurian data tidak dapat dikualifikasikan sebagai *jarimah hudud* (Hasibuan| dkk., 2023).

Kualifikasi sebagai *Jarimah Ta'zir*: Fleksibel Hukum Islam Menghadapi Kejahatan Baru

Ketika suatu perbuatan jahat tidak memenuhi kriteria *hudud* atau *qisas*, ia tidak lantas menjadi perbuatan yang dibiarkan tanpa sanksi, Hukum Pidana Islam menyediakan kategori ketiga yang sangat luas dan dinamis, yaitu *jarimah ta'zir*. *Ta'zir* adalah tindak pidana yang bentuk dan kadar sanksinya tidak ditentukan secara spesifik oleh nas Al-Quran dan Hadis, melainkan diserahkan sepenuhnya kepada ijtihad dan kebijaksanaan hakim (*qadi*) atau penguasa (*ulim amri*) (Siregar dkk., 2024; Wahyudi, 2023).

Kualifikasi pencurian data sebagai *jarimah ta'zir* adalah kesimpulan yang paling tepat dan diterima secara luas oleh para ahli hukum Islam kontemporer (Suharyadi dkk., 2020). Keistimewaan *ta'zir* terletak pada fleksibilitasnya sangat luar biasa. Ia dirancang untuk merespons segala bentuk kemaksiatan dan pelanggaran hukum yang belum diatur secara eksplisit, termasuk bentuk-bentuk kejahatan baru yang muncul seiring dengan perkembangan zaman dan teknologi, seperti kejahatan siber (Siregar dkk., 2024). Dengan mengategorikan pencurian data sebagai delik *ta'zir*, sistem hukum Islam menunjukkan kemampuannya untuk beradaptasi (*murunah*) dan tetap relevan dalam menjaga ketertiban dan keadilan di era digital.

Landasan Filosofis: Perlindungan Harta (*Hifz al-Mal*) dan Kaidah Pencegahan Mudarat (*La Dharara wa la Dhillara*)

Larangan dan sanksi terhadap pencurian data dalam hukum Islam tidak muncul dari ruang hampa, melainkan berakar kuat pada tujuan-tujuan luhur syariat (*maqashid al-syariah*). Prinsip utama yang dilanggar oleh perbuatan ini adalah perlindungan terhadap harta (*hifz al-mal*), yang merupakan salah satu dari lima tujuan esensial syariat (Al-Ghazali, 2023). Sebagaimana telah diuraikan, data di era digital adalah aset berharga yang memiliki nilai ekonomi, privasi, dan keamanan. Melindungi data sama pentingnya dengan melindungi harta benda fisik, dan perampasannya secara tidak sah adalah bentuk kezaliman yang dilarang.

Selain itu, landasan normatifnya dapat ditemukan dalam kaidah fikih fundamental (kaidah *kulliyah*) yang disepakati oleh seluruh ulama: *لَا ضَرَرَ وَلَا ضِرَارَ* (*La dharara wa la dhillara*), yang berarti "tidak boleh menimbulkan bahaya/kerugian bagi diri sendiri dan tidak boleh pula membahayakan *dharar* (kerugian) yang besar bagi korban, yang dapat bersifat:

1. Kerugian Materiil: Kerugian finansial langsung akibat penipuan, pembobolan rekening, atau biaya pemulihan kecemasan.
2. Kerugian Immateriil: Pelanggaran privasi, kerusakan reputasi, tekanan psikologis, dan kecemasan.

Berdasarkan kaidah turunan *الضَّرَرُ يُزَالُ* (*al-dharar yuzal*) atau "kemudaratan harus dihilangkan", maka negara (melalui sistem peradilan) memiliki kewajiban syar'i untuk bertindak. Negara harus menciptakan regulasi, melakukan penegakan hukum, dan menjatuhkan sanksi yang adil untuk mencegah dan menanggulangi

perbuatan yang merugikan tersebut, demi terwujudnya kemaslahatan umum (*masalah 'ammah*) (Asifae dkk., 2024).

Ijtihad Kontemporer di Indonesia: Refleksi dari Fatwa DSN-MUI tentang Aset Digital

Argumentasi fiqh yang bersifat teoritis ini mendapatkan penguatan kontekstual dari praktik ijtihad di Indonesia. Dewan Syariah Nasional-Majelis Ulama Indonesia (DSN-MUI), sebagai Lembaga otoritatif dalam penetapan hukum Islam di bidang ekonomi dan keuangan, telah beberapa kali mengeluarkan fatwa terkait aset digital, khususnya *cryptocurrency* (Dewan Syariah Nasional Majelis Ulama Indonesia, 2021, 2024).

Meskipun fatwa-fatwa ini berfokus pada hukum kehalalan *cryptocurrency* sebagai mata uang atau komoditas investasi, analisis terhadap dasar pertimbangan (*illah*) di balik fatwa tersebut sangat relevan. Dalam fatwanya, DSN-MUI secara implisit mengakui bahwa aset digital yang tidak berwujud adalah subjek yang sah bagi analisis hukum Islam. Mereka membahas apakah aset digital memiliki nilai (*Maliyah*), apakah memenuhi syarat sebagai komoditas (*si'ah*), dan apakah mengandung unsur-unsur terlarang seperti ketidakpastian (*gharar*), spekulasi (*maisir*), dan kerugian (*dharar*) (Dewan Syariah Nasional Majelis Ulama Indonesia, 2021).

Dengan terlibat aktif dalam perdebatan ini, DSN MUI telah menegaskan bahwa konstruksi digital yang tidak berwujud namun memiliki nilai ekonomi adalah objek yang berada dalam cakupan hukum Islam. Berdasarkan prinsip analogi (*qiyas*), dapat ditarik sebuah argumen yang kuat: jika Lembaga fiqh tertinggi di Indonesia mengakui substansi hukum dan ekonomi dari satu jenis aset digital (*cryptocurrency*), maka prinsip perlindungan nilai dan pencegahan kerugian yang sama harus berlaku pula untuk jenis aset digital berharga lainnya, yaitu data pribadi dan korporasi. Pengakuan ini memberikan landasan yuridis Islami yang kokoh dari konteks keindonesiaan untuk mengkriminalisasi pencurian data sebagai sebuah pelanggaran serius terhadap prinsip *hifz al-mal* (Dewan Syariah Nasional Majelis Ulama Indonesia, 2024).

ANALISIS KOMPARATIF FILOSOFI DAN SISTEM SANKSI

Sanksi dalam UU ITE: Orientasi Retributif dan Deterensi

Pelanggaran terhadap Pasal 30 ayat (3) UU ITE diancam dengan sanksi pidana yang tercantum dalam Pasal 46 ayat (3) UU ITE. Pasal ini menetapkan bahwa pelaku dapat dipidanakan dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (Undang-Undang Nomor 11 Tahun 2008, 2008). Sistem sanksi ini mencerminkan filosofi pidanaan modern yang dominan dalam hukum pidana positif, yang berorientasi pada dua tujuan utama: retribusi dan deterensi (Suharyadi dkk., 2020).

Filosofi Retributif (Pembalasan), yang berakar dari pemikiran para filsuf seperti Immanuel Kant dan Hegel, memandang pidana sebagai pembalasan yang

setimpal atas kesalahan yang telah dilakukan pelaku. Fokusnya adalah pada perbuatan di masa lalu (*backward looking*). Pidana dijatuhkan bukan untuk mencapai tujuan praktis di masa depan, melainkan karena kejahatan itu sendiri menuntut adanya balasan agar keadilan dapat ditegakkan (Suharyadi dkk., 2020). Dalam konteks pencurian data, ancaman penjara dan denda yang berat dilihat sebagai balasan yang adil atas pelanggaran terhadap hak privasi dan keamanan sistem elektronik milik orang lain.

Filosofi Deterensi (Pencegahan) bertujuan untuk mencegah terjadinya kejahatan di masa depan. Ini terbagi menjadi dua, yaitu deterensi khusus (*special deterrence*), yang ditujukan agar pelaku jera dan tidak mengulangi perbuatannya, dan deterensi umum (*general deterrence*), yang ditujukan untuk memberikan contoh kepada masyarakat luas agar tidak melakukan kejahatan serupa (Suharyadi dkk., 2020). Ancaman sanksi yang berat dalam Pasal 46 ayat (3) diharapkan dapat menimbulkan efek gentar bagi calon pelaku kejahatan siber.

Karakteristik utama dari sistem sanksi dalam UU ITE adalah sifatnya yang relatif kaku dan formalistik. Meskipun hakim memiliki diskresi untuk menentukan beratnya hukuman dalam rentang maksimal yang telah ditetapkan, kerangka sanksinya telah ditentukan secara pasti oleh legislator. Paradoksnya, ketegasan ancaman hukuman ini sering kali tidak diimbangi dengan kemudahan dalam penegakannya. Kekakuan dalam pembuktian unsur-unsur delik, terutama *mens rea* di ruang siber yang anonim, serta tantangan teknis dalam forensik digital, dapat menjadikan Pasal yang tampak tegas di atas kertas menjadi tumpul dalam implementasinya (Sitanggang dkk., 2024).

Sanksi *Ta'zir*: Orientasi Edukatif, Restoratif, dan proporsionalitas

Berbeda secara fundamental, sanksi *ta'zir* dalam hukum pidana Islam tidak dirancang untuk menjadi kaku atau semata-mata bersifat membalas. Filosofi utamanya adalah multifaset dan berorientasi ke depan (*forward looking*), yang mencakup (Wahyudi, 2023).

1. Pendidikan (*ta'dib*): sanksi bertujuan untuk mendidik dan memperbaiki karakter pelaku agar ia menyadari kesalahannya dan menjadi individu yang lebih baik.
2. Perbaikan/Pemulihan (*islah*): sanksi harus mampu memulihkan kerusakan yang terjadi, baik pada korban maupun pada tatanan sosial. Ini membuka ruang bagi pendekatan keadilan restoratif.
3. Pencegahan (*radd* atau *zajr*): Sanksi juga berfungsi untuk mencegah pelaku dan orang lain melakukan kejahatan serupa, namun pencegahan ini dicapai melalui keadilan yang dirasakan, bukan semata-mata melalui ketakutan.

Bentuk sanksi *ta'zir* sangat beragam dan diserahkan pada diskresi (*ijtihad*) hakim atau penguasa (*ulil amri*). Sanksi ini dapat berkisar dari yang paling ringan seperti teguran (*tawbikh*) atau nasihat, hingga hukuman yang lebih berat seperti denda finansial (*ghuramah*), hukuman cambuk (*jjlid*), pengasingan, dan pidana

penjara (*habs*) (Siregar dkk., 2024). Untuk kejahatan yang sangat berat dan mengancam keamanan publik, seperti spionase atau terorisme, sanksi *ta'zir* bahkan bisa mencapai hukuman mati.

Kekuatan utama *ta'zir* adalah kemampuannya untuk beradaptasi dengan kompleksitas setiap kasus dan perkembangan zaman. Dalam menentukan hukuman, seorang hakim tidak terikat pada satu jenis sanksi, melainkan dapat mempertimbangkan berbagai faktor secara holistik, seperti:

1. Tingkat kerugian (*dharar*) yang ditimbulkan, baik materiil maupun immaterial.
2. Modus operandi dan tingkat kecanggihan kejahatan.
3. Motif, kondisi psikologis, dan latar belakang pelaku.
4. Apakah pelaku merupakan residivis atau baru pertama kali melakukan kejahatan.
5. Dampak sosial yang lebih luas dan kemaslahatan umum (*masalahah 'ammah*) (Al-Ghazali, 2023).

Fleksibilitas ini memberikan tingkat penegakan (*enforceability*) yang lebih tinggi dalam menghadapi kejahatan yang dinamis seperti pencurian data. Hakim dapat memfokuskan penilaiannya pada substansi kerugian yang nyata, bahkan jika pembuktian niat jahat secara formalistic menghadapi kendala teknis yang rumit (Wahyudi, 2023). Efektivitas hukum dalam perspektif ini tidak diukur dari beratnya ancaman sanksi, melainkan dari kemampuannya untuk diterapkan secara adil dan kemampuannya untuk memperbaiki pelaku serta melindungi masyarakat.

SINTESIS DAN PROYEKSI REFORMASI HUKUM SIBER INDONESIA

Dialektika antara Kekuatan Prosedural dan Kebutuhan Keadilan Substantif

Sintesis dari analisis komparatif di atas menyingkap sebuah dialektika fundamental dalam penegakan hukum siber di Indonesia. Di satu sisi, UU ITE dengan kerangka hukum positifnya menawarkan pilar penting berupa kepastian hukum (*rechtssicherheit*). Rumusan delik yang jelas dalam Pasal 30 ayat (3) dan ancaman sanksi yang tegas dalam Pasal 46 ayat (3) memberikan landasan procedural yang kokoh bagi penegak hukum (Chazawi, 2022). Namun, kekakuan procedural ini seringkali berbenturan dengan realitas kejahatan siber yang sangat dinamis, cair, dan terus berevolusi (Hapsari & Pambayun, 2023).

Tantangan dalam pembuktian *mens rea*, kompleksitas forensic digital, dan keterbatasan sumber daya penegak hukum menunjukkan adanya jurang antara hukum di atas kertas (*law in books*) dan hukum dalam praktik (*law in action*) (Sitanggang dkk., 2024). Akibatnya, hukum yang tampak keras bisa jadi sulit untuk diterapkan secara efektif, dan Ketika diterapkan, fokusnya yang retributive kurang mengakomodasi upaya pemulihan kerugian korban dan perbaikan pelaku. Sistem ini, dengan segala kekuatannya dalam memberikan kepastian, berisiko gagal mencapai keadilan substantif yaitu keadilan yang dirasakan secara nyata oleh korban dan masyarakat.

Di sisi lain, hukum pidana Islam melalui konsep *ta'zir* menawarkan sebuah antithesis. Fleksibilitasnya yang inhera, fokusnya pada substansi kerugian (*dharar*), dan tujuannya yang berorientasi pada perbaikan (*islah*) dan Pendidikan (*ta'dib*) menyediakan kerangka yang secara filosofis lebih siap menghadapi kejahatan-kejahatan baru yang tidak terbayangkan oleh para legislator di masa lalu (Siregar dkk., 2024). Namun, pendekatan ini juga memiliki tantangan dalam konteks negara modern, yaitu potensi inkonsistensi dan kurangnya kepastian hukum jika tidak dibarengi dengan pedoman yang jelas bagi para hakim.

Proposal Integrasi Nilai-Nilai *Ta'zir* dalam Kebijakan Pidana Siber

Jalan keluar dari dialektika ini bukanlah dengan mengganti satu sistem dengan yang lain, melainkan dengan melakukan sintesis yang cerdas. Kebijakan hukum siber Indonesia di masa depan dapat diperkaya dengan mengintegrasikan *nilai-nilai* dan *filosofi* keadilan substantif yang diilhami oleh *ta'zir* ke dalam kerangka hukum positif yang sudah ada. Integritas ini tidak berarti mengadopsi hukum Islam secara formal, melainkan menyerap prinsip-prinsip universalnya untuk menciptakan sistem yang lebih adil, adaptif, dan efektif. Beberapa Langkah konkret yang dapat dipertimbangkan adalah:

1. Pengembangan Pedoman Pidana (*Sentencing Guidelines*): Mahkamah Agung, bekerja sama dengan para ahli hukum, teknologi, dan akademisi, dapat merumuskan pedoman pidana khusus untuk kejahatan siber. Pedoman ini dapat memberikan arahan kepada hakim untuk mempertimbangkan faktor-faktor yang selama ini menjadi inti dari penjatuhan sanksi *ta'zir*, seperti:
 - a. Tingkat dan sifat kerugian yang diderita korban (baik materiil maupun immaterial).
 - b. Motif dan tingkat kesenjangan pelaku.
 - c. Peran pelaku dalam sindikat kejahatan (apakah pelaku utama, fasilitator, atau sekedar coba-coba).
 - d. Upaya pelaku untuk memulihkan kerugian atau menunjukkan penyesalan.
 - e. Dampak kejahatan terhadap kepentingan publik atau keamanan nasional.
2. Penguatan Mekanisme Keadilan Restoratif (*Islah*): Untuk banyak kasus kejahatan siber, terutama yang kerugiannya bersifat finansial, pendekatan punitive semata sering kali tidak memulihkan penderitaan korban. Perlu ada penguatan mekanisme keadilan restoratif, seperti mediasi penal, di mana pelaku diberi kesempatan bertanggung jawab langsung kepada korban, misalnya melalui ganti rugi (*diyat* atau *arsy* dalam terminology fikih) atau pemulihan data. Ini sejalan dengan tujuan *islah* dalam *ta'zir* dan dapat menjadi alternatif atau pelengkap dari sanksi pidana penjara (Amin dkk., 2020)
3. Implementasi Sanksi Edukatif (*Ta'dib*): Tidak semua pelaku kejahatan siber adalah penjahat kambuhan. Beberapa diantaranya mungkin adalah peretas

muda atau individu yang kurang memiliki pemahaman etika digital. Untuk pelaku tingkat rendah, sanksi alternatif yang edukatif dapat lebih efektif daripada pemenjaraan. Sanksi ini bisa berupa kewajiban mengikuti program pelatihan keamanan siber, melakukan kerja sosial dengan mengedukasi masyarakat tentang literasi digital, atau pembinaan moral dan etika.

Fleksibilitas *ta'zir* memberikan *enforceability* yang lebih tinggi dalam menghadapi kejahatan yang dinamis seperti pencurian data, karena hakim dapat memfokuskan penilaiannya pada substansi kerugian (*dharar*) yang nyata, bahkan jika pembuktian niat jahat secara formalistic menghadapi kendala.

KESIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat ditarik beberapa kesimpulan. *Pertama*, tindak pidana pencurian data melalui *Wi-Fi* secara yuridis positif dapat dikualifikasikan sebagai kejahatan akses ilegal yang memenuhi seluruh unsur delik dalam Pasal 30 ayat (3) UU ITE. *Kedua*, dari perspektif hukum pidana Islam, perbuatan ini merupakan sebuah *jarimah* (tindak pidana) yang secara fundamental bertentangan *maqashid al-syariah*, khususnya prinsip perlindungan harta (*hifz al-mal*). Karena tidak memenuhi syarat-syarat formal *sariqah*, kejahatan ini diklasifikasikan sebagai *jarimah ta'zir*, yang sanksinya bersifat fleksibel dan diserahkan kepada ijtihad hakim. *Ketiga*, terdapat perbedaan filosofis yang mendasar antara kedua sistem hukum: hukum positif Indonesia (UU ITE) cenderung bersifat kaku, formalistic, dan retributive, sedangkan hukum pidana Islam (melalui konsep *ta'zir*) menawarkan pendekatan yang fleksibel, substantif, dan berorientasi pada Pendidikan serta perbaikan.

SARAN

Sebagai tindak lanjut dari kesimpulan di atas, beberapa saran dapat dirumuskan untuk kebijakan hukum dan praktik di masa depan.

1. Saran Kebijakan (Legislatif dan Yudikatif): diperlukan adanya reformasi dalam kebijakan hukum siber di Indonesia. Reformasi ini tidak seharusnya hanya berfokus pada penambahan atau pemberatan sanksi pidana dalam UU ITE, tetapi lebih kepada integrasi nilai-nilai keadilan substantif yang diilhami oleh filosofi *ta'zir*. Hal ini dapat diwujudkan dengan memberikan ruang diskresi yang lebih luas dan terukur bagi hakim untuk mempertimbangan dampak kerugian nyata (*dharar*), motif pelaku, dan kemaslahatan umum dalam penjatuhan sanksi. Selain itu, perlu dipertimbangkan penguatan mekanisme keadilan restoratif dalam penyelesaian perkara siber untuk memulihkan kerugian korban secara lebih efektif.
2. Saran Praktis (Penegak Hukum dan Masyarakat): Upaya penanggulangan kejahatan siber tidak dapat hanya mengandalkan pendekatan punitif. Diperlukan strategi preventif yang komprehensif, yang mencakup peningkatan literasi digital dan kesadaran keamanan siber di seluruh lapisan masyarakat. Penguatan sanksi moral melalui edukasi berbasis nilai-nilai etika

As-Syar'i: Jurnal Bimbingan & Konseling Keluarga

Volume 7 Nomor 3 (2025) 404 - 425 E-ISSN 2656-8152 P-ISSN 2656-4807

DOI: 10.47476/assyari.v7i3.9220

dan agama dapat menjadi benteng pertahanan utama untuk mencegah individu terjerumus dalam kejahatan digital. Kolaborasi sinergis antara pemerintah, Lembaga penegak hukum, institusi Pendidikan, tokoh agama, dan masyarakat sipil menjadi kunci untuk menciptakan ekosistem digital yang aman dan beradab.

DAFTAR PUSTAKA

- Al-Ghazali, A. H. (2023). *Al-Mustasfa min 'Ilm al-Usul*. Terjemahan. Penerbit Pustaka Islamika.
- Amin, R., Al Aziz, M. F., & Manalu, I. (2020). Penerapan Keadilan Restoratif Dalam Penyelesaian Perkara Kecelakaan Lalu Lintas Berat Di Kepolisian Resort Metro Jakarta Pusat. *KRTHA BHAYANGKARA*, 14(1), 1-26. <https://doi.org/10.31599/krtha.v14i1.35>
- ANGGRIAWAN, M. A. (2018). *STUDI KOMPARATIF TINDAK PIDANA PENCURIAN DALAM HUKUM ISLAM DAN HUKUM PIDANA INDONESIA* [Skripsi, Universitas Mataram]. <https://eprints.unram.ac.id/10140/>
- Antaranews.com. (2023, Oktober 25). *BSSN team to tackle cyberattacks during 2024 elections*. Antara News. <https://en.antaranews.com/news/297030/bssn-team-to-tackle-cyberattacks-during-2024-elections>
- Asifae, U., Amaniar, T. R., & Anastasya, J. (2024). *Penerapan Kaidah Fiqhiyyah terhadap Kejahatan Siber dalam Hukum Jinayah*. 2(1).
- Chazawi, D. H. A. C., S. H; Ardi Ferdian, S. H. (2022). *Tindak Pidana Informasi Dan Transaksi Elektronik Ed. Revisi*. Media Nusa Creative (MNC Publishing).
- Citrano, C., Rahmawati, R., Watkat, F. X., Siburian, H. K., Mulyadi, D., Abas, M., & Dwirainaningsih, Y. (2024). *Hukum Siber*. Get Press Indonesia.
- Dewan Syariah Nasional Majelis Ulama Indonesia. (2021). *Fatwa No. 123/DSN-MUI/III/2021 tentang Cryptocurrency dalam Perspektif Syariah*. Jakarta: MUI.
- Dewan Syariah Nasional Majelis Ulama Indonesia. (2024). *Fatwa No. 157/DSN-MUI/III/2024 tentang Penerapan Prinsip Syariah dalam Pelindungan Aset Investor Pasar Modal*. Jakarta: MUI.
- Europol. (2020). *Risks of using public Wi-Fi*. Europol. <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/risks-of-using-public-wi-fi>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), Article 2. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, 5(1), 1-17. <https://doi.org/10.33701/jk.v5i1.3208>
- Haryadi, T., & S, H. (2022). Pencurian Wifi Dalam Perspektif Hukum Pidana Nasional. *Lex Librum*, 8(2), 269-282. <https://doi.org/10.46839/lljih.v8i2.650>
- Hasibuan, N., Panjaitan, B. S., & Sativa, A. (2023). Tinjauan Hukum Pidana Islam terhadap Tindak Pidana Penipuan. *Hukum dan Demokrasi (HD)*, 23(1), 1-19. <https://doi.org/10.61234/hd.v23i1.11>
- Irfan, N. (2022). *Hukum Pidana Islam*. Amzah.

As-Syar'i: Jurnal Bimbingan & Konseling Keluarga

Volume 7 Nomor 3 (2025) 404 - 425 E-ISSN 2656-8152 P-ISSN 2656-4807

DOI: 10.47476/assyari.v7i3.9220

- Khan, I. A., (2017). *Intellectual Property Rights in Islam: A Perspective*. *Journal of Islamic Thought and Civilization*. - Penelusuran Google. https://www.researchgate.net/publication/273449547_Intellectual_Property_Rights_in_Islam_A_Perspective
- Mahafzah, Q. A., & Melhem, B. M. (2009). *The Perspective of Moral and Financial Rights of Intellectual Property in Islam*. *Arab Law Quarterly*, 23(4), 457-468. - Penelusuran Google. https://www.researchgate.net/publication/274499644_The_Perspective_of_Moral_and_Financial_Rights_of_Intellectual_Property_in_Islam
- Mahkamah Agung Republik Indonesia. (2020). *Putusan Nomor 1470 K/Pid.Sus/2020*. Direktori Putusan Mahkamah Agung.
- Mahkamah Agung Republik Indonesia. (2021). *Putusan Pengadilan Negeri Jakarta Selatan Nomor 796/Pid.Sus/2021/PN JKT.SEL tentang Tindak Pidana Akses Ilegal*.
- Mahkamah Agung Republik Indonesia. (2022). *Putusan Nomor 4898 K/Pid.Sus/2022*. Direktori Putusan Mahkamah Agung.
- Mahkamah Agung Republik Indonesia. (2023). *Putusan Pengadilan Negeri Pinrang Nomor 77/Pid.Sus/2023/PN Pin tentang Tindak Pidana Memfasilitasi Akses Ilegal*.
- Munajat, M. (2009). *Hukum Pidana Islam di Indonesia*. Teras.
- Nasution, C. P. (2020). *Fiqh Kontemporer Dalam Ragam Aspek Hukum*. Perdana Publishing.
- OXSANA PUTRI FERADOVA. (2025). *TINJAUAN YURIDIS PENERAPAN PASAL 30 UNDANG-UNDANG No.01 TAHUN 2024 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (ITE) DALAM MENGATASI PENIPUAN IDENTITAS DIDUNIA MAYA* [Skripsi, UNIVERSITAS MUHAMMADIYAH PALEMBANG]. <https://repository.um-palembang.ac.id/id/eprint/31573/>
- Primadhany, E. F., et al. (2025). *Pengantar Hukum Siber Indonesia*. Sada Kurnia Pustaka.
- Rochman, S., Akmal, H., & Andriansyah, Y. (2021). *PENCEMARAN NAMA BAIK MELALUI MEDIA SOSIAL: PERBANDINGAN HUKUM PIDANA POSITIF DAN PIDANA ISLAM*. *DIKTUM: Jurnal Syariah dan Hukum*, 19, 32-42. <https://doi.org/10.35905/diktum.v19i1.2080>
- Siregar, F. A., Harahap, R. B., Fauziah, Y., Julu, T., & Munawar, S. A. (2024). *Fikih jinayah kontemporer: Telaah historis, perkembangan dan penerapan qanun*. Semesta Aksara. <https://repo.uinsyahada.ac.id/1536/>
- Sitanggang, A., Darmawan, F., & Saputra, D. (2024). *Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber*. *Jurnal Pendidikan dan Teknologi Indonesia*, 4, 79-83. <https://doi.org/10.52436/1.jpti.409>
- SSEK. (2024, Mei 20). *Fortifying Indonesia's Cyber Defenses: New Regulations for National Security and Crisis Management*. *SSEK Law Firm*.

As-Syar'i: Jurnal Bimbingan & Konseling Keluarga

Volume 7 Nomor 3 (2025) 404 - 425 E-ISSN 2656-8152 P-ISSN 2656-4807

DOI: 10.47476/assyari.v7i3.9220

<https://ssek.com/blog/fortifying-indonesias-cyber-defenses-new-regulations-for-national-security-and-crisis-management/?lang=id>

Suharyadi, S., Sampara, S., & Ahmad, K. (2020). Kejahatan Dunia Maya (Cyber Crime) Dalam Prespektif Hukum Islam. *Journal of Lex Generalis (JLG)*, 1(5), Article 5. <https://doi.org/10.52103/jlg.v1i5.199>

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2024). Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). JDIH Kementerian Komunikasi dan Digital.

Utrecht, E. (1966). *Pengantar dalam hukum Indonesia*. Universitas Indonesia Library; Ichtiar. <https://lib.ui.ac.id>

Wahyudi, W. (2023). *Analisis Jarimah Ta'zir Terhadap Tindak Pidana Penyebaran Berita Bohong Dalam Transaksi Elektronik* [Undergraduate, IAIN Parepare]. <https://repository.iainpare.ac.id/id/eprint/6568/>