PUSKAPSI Law Review
Volume 5 Issue 1 (2025), pp 247-262
Tersedia Secara *Online* Juni, 2025

Formulasi Tindak Pidana Siber Menggunakan *Malware* Menurut Hukum Pidana Islam

Adnin Yusuf
Universitas Islam Negeri Sumatera Utara
adnin0205193140@uinsu.ac.id

Mari'e Mahfudz Harahap
Universitas Islam Negeri Sumatera Utara

ABSTRAK

Kemajuan teknologi yang pesat telah meningkatkan prevalensi kejahatan siber, termasuk penggunaan malware, yang menimbulkan tantangan signifikan bagi kerangka hukum. Penelitian ini mengkaji pengaturan tindak pidana siber yang melibatkan malware dari perspektif hukum positif dan hukum pidana Islam. Penelitian ini menggunakan pendekatan normatif dengan menganalisis sumber hukum primer, seperti Al-Qur'an, Hadis, teks fikih klasik dan kontemporer, serta peraturan perundang-undangan seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Hasil penelitian menunjukkan bahwa hukum positif menyediakan kerangka umum untuk memerangi kejahatan siber, tetapi kurang adaptif terhadap sifat tindak pidana yang melibatkan malware yang terus berkembang. Sebaliknya, hukum pidana Islam menawarkan prinsip-prinsip keadilan dan pencegahan kerugian (dharar), dengan penekanan pada perlindungan kepentingan individu dan publik (maqashid syariah). Penelitian ini mengidentifikasi potensi integrasi kedua sistem untuk secara efektif menghadapi tantangan saat ini dan di masa mendatang. Sebuah kerangka hukum futuristik diusulkan, yang mengintegrasikan kemajuan teknologi seperti kecerdasan buatan untuk pencegahan kejahatan siber dan kolaborasi global dalam menghadapi tindak pidana lintas batas. Kesimpulan penelitian menekankan perlunya regulasi yang adaptif dan berorientasi pada keadilan, yang mengharmonisasikan prinsip-prinsip hukum Islam dengan praktik hukum kontemporer, guna memastikan perlindungan menyeluruh terhadap kejahatan siber dengan tetap menjaga nilai-nilai etika dan moral.

KATA KUNCI: Hukum Pidana Islam, Kejahatan Siber, Malware, Tindak Pidana

I. PENDAHULUAN

Kejahatan siber merupakan tindak kejahatan yang muncul karna akibat dari perkembangan teknologi informasi yang telah berevolusi. Kejahatan siber dikategorikan sebagai tindak kejahatan yang mempunyai korelasi dengan dunia maya dan komputer sebagai medianya. Kemajuan teknologi digital tidak hanya membawa manfaat, tetapi juga membuka ruang baru bagi berbagai bentuk tindak kejahatan. Salah satu wujudnya adalah tindak pidana siber dengan menggunakan *malware* (malicious software), yaitu perangkat lunak berbahaya yang dirancang untuk mengganggu, merusak, mencuri, atau mendapatkan akses tidak sah ke sistem computer.[1]

Dikutip dari website resmi CNN Indoneisa, pada tahun 2023 Indonesia mencatat lebih dari 411.000 *malware* baru muncul setiap harinya, menunjukkan betapa cepatnya perkembangan ancaman ini. Ransomware berfungsi dengan cara mengenkripsi data korban dan meminta tebusan untuk mengembalikannya. Menurut data dari Kaspersky, pada tahun 2023 terdapat 97.226 insiden ransomware yang terdeteksi di Indonesia.[2]

Dalam hukum Islam, segala bentuk tindakan yang merugikan orang lain, termasuk melalui media digital, dikategorikan sebagai bentuk kezaliman yang dilarang. Kejahatan siber menggunakan *malware* dapat diqiyaskan dengan tindak pidana pencurian (sariqah) dan perusakan (ifsād fī al-arḍ), karena melibatkan pengambilan data atau perusakan sistem secara tidak sah. Al-Qur'an secara tegas melarang memakan harta orang lain dengan cara yang batil (QS. Al-Baqarah: 188), yang dalam konteks digital dapat mencakup pencurian informasi, peretasan, atau sabotase sistem. Dalam prinsip ta'zir, negara berwenang menetapkan sanksi terhadap pelanggaran yang tidak disebutkan secara eksplisit dalam nash, termasuk tindak pidana siber, demi menjaga maqashid al-shariah, khususnya perlindungan terhadap harta dan keamanan masyarakat.[3]

Padahal, pada dasarnya penggunaan teknologi termasuk internet justru untuk mempermudah dan membuat penggunanya dapat menjangkau dunia lebih luas. Banyak hal yang dapat dimanfaatkan, seperti internet memungkinkan interaksi sosial yang lebih luas, di mana orang dapat berkomunikasi secara global melalui media sosial dan platform online, mengubah cara mereka berhubungan satu sama lain. Selain itu, akses informasi menjadi sangat mudah, pengguna dapat mencari dan mendapatkan data tentang berbagai topik, yang mendukung pembelajaran mandiri.

Perdagangan elektronik juga mengalami perkembangan pesat, memudahkan transaksi jual beli secara daring melalui platform seperti Shopee dan Tokopedia. Di sisi lain, banyak individu kini berperan sebagai konten kreator di platform seperti

---

[1] H. Hasibuan, *Keamanan Siber Dan Perlindungan Data Pribadi Di Era Digital* (Yogyakarta: Deepublish, 2022).

[2] Kaspersky, "Https://Www.Cnnindonesia.Com/Teknologi/20240522130109-185-1100872/Serangan-Siber-Menggila-411-Ribu-*Malware*-Baru-Muncul-Tiap-Hari-Di-Ri#:~:Text=Serangan%20ransomware%20atau%20peretasan%20dengan%20modus%20pemerasan%20terlacak,Pembobol%20sistem%20yang%20baru."

[3] A.H.M. Al-Ghazali, *Al-Mustashfa Min 'Ilm Al-Usul* (Beirut: Dar Al-Kutub Al-'Ilmiyyah, 1993).

TikTok dan Instagram, menciptakan peluang baru untuk ekspresi diri dan monetisasi.[4]

Kekurangan dalam penelitian tentang tindak pidana siber yang menggunakan *malware* di Indonesia mencakup beberapa aspek.[5] Pertama, keterbatasan data dan metodologi sering kali menghambat pengumpulan informasi yang lengkap, terutama karena bank dan lembaga terkait tidak selalu memberikan data yang diperlukan untuk investigasi. Kedua, fokus penelitian yang terlalu sempit pada jenis kejahatan tertentu[6], seperti cyberbullying, mengabaikan kejahatan yang lebih kompleks seperti ransomware, sehingga tidak mencerminkan keseluruhan spektrum masalah.[7]

Selain itu, banyak penelitian menggunakan pendekatan yuridis normatif tanpa mempertimbangkan aspek teknologi dan psikologis dari kejahatan siber. Hal ini mengakibatkan pemahaman yang tidak komprehensif. Regulasi yang ada, seperti UU ITE, juga menunjukkan kelemahan dalam pengaturan unsur-unsur tindak pidana, membuat penegakan hukum menjadi sulit dan sering kali multitafsir.

Penelitian terdahulu mengenai tindak pidana siber yang menggunakan *malware* di Indonesia mencakup beberapa studi yang penting.[8] Salah satunya adalah penelitian oleh Zainuddin Kasim yang membahas kebijakan hukum pidana untuk penanggulangan *Cybercrime*.[9] Penelitian ini menekankan perlunya reformasi hukum yang lebih adaptif dan komprehensif untuk menghadapi ancaman kejahatan siber yang semakin canggih, serta mengusulkan peningkatan kerjasama internasional dan kesadaran masyarakat tentang keamanan digital.

Studi lain oleh Nabillah Kamila Affandi dan Ayu Nrangwesti fokus pada respons sistem peradilan pidana terhadap peretasan,[10] termasuk serangan ransomware yang menargetkan Bank Syariah Indonesia. Penelitian ini menunjukkan bahwa kejahatan siber, terutama yang melibatkan *malware*, memerlukan pendekatan penegakan hukum yang lebih kuat dan kesadaran publik untuk mencegah dan melaporkan aktivitas ilegal.[11]

Selain itu, tesis oleh Wendi Asmoro mengkaji tindak pidana pengiriman aplikasi (APK) yang mengandung *malware* di wilayah Polda Jawa Tengah. Penelitian ini mengeksplorasi hambatan dalam penerapan hukum terhadap pengiriman file

---

[4] O Wijaya, "E-Commerce: Perkembangan, Tren, Dan Peraturan Perundang-Undangan," *Jurnal Ilmiah Ekonomi Dan Bisnis* 16, no. 1 (2023): 41–47.

[5] S. A. N. Wahdini and F. F. B Irfansyah, "Analisis Keselarasan Pengaturan Yurisdiksi Cybercrime Dengan Implementasinya Di Kehidupan Nyata," *Indonesian Journal Of Law And Justice* 1, no. 3 (2024): 1–11.

[6] N. A. Agustin and R. M. Firdos, "Agustin, N. A., & Firdos, R. M. (2024). Studi Literatur: Ancaman Cybercrime Di Indonesia Dan Pentingnya Pemahaman Akan Fenomena Kejahatan Digital.," *Jurnal Mahasiswa Teknik Informatika* 3, no. 126–131 (2024).

[7] S. Widhaningroem, "Analisis Yuridis Penyidikan Kejahatan E-Commerce Di Indonesia (Kajian Kejahatan Penipuan Dan Pencurian Identitas)," *Doctoral Dissertation, Universitas Muhammadiyah Yogyakarta*, 2024.

[8] R. Putri, E. H. A. D., Kasim and L. D. Nurmala, "Analisis Yuridis Terhadap Penegakan Dan Pengaturan Hukum Kejahatan Dunia Maya (Cybercrime) Di Indonesia," *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 3 (2024): 102–11.

[9] Z. Kasim, "Kebijakan Hukum Pidana Untuk Penanggulangan Cybercrime Di Indonesia.," *Indragiri Law Review* 2, no. 1 (2024): 18–24.

[10] N. K. Affandi and A. Nrangwesti, "Penegakan Hukum Perampokan Bersenjata Di Selat Malaka Berdasarkan Hukum Laut Internasional," *Reformasi Hukum Trisakti* 5, no. 1 (2023): 82–93.

[11] R. P. Wijanarko, "Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia.," *In Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 2023.

berbahaya dan langkah-langkah pencegahan yang perlu diambil oleh aparat kepolisian.[12]

Perkembangan teknologi yang cepat membuat banyak penelitian menjadi usang jika tidak diperbarui secara berkala. Kekurangan-kekurangan ini menunjukkan perlunya penelitian lebih lanjut yang lebih komprehensif dan multidisipliner untuk menangani tindak pidana siber secara efektif di Indonesia. Secara keseluruhan, penelitian-penelitian ini menunjukkan kompleksitas dan tantangan dalam penanganan kejahatan siber di Indonesia, serta perlunya pendekatan yang lebih terintegrasi dalam kebijakan hukum dan penegakan hukum.

Dalam konteks hukum pidana, pengaturan terhadap tindak pidana ini menjadi penting untuk mencegah dan menanggulangi dampak yang ditimbulkannya. Oleh karena itu, diperlukan kajian mengenai bagaimana hukum pidana saat ini mengatur tindak pidana siber yang melibatkan penggunaan *malware*, baik dari segi definisi, unsur-unsur delik, hingga sanksi yang diatur. Selain itu, menarik untuk melihat bagaimana hukum pidana Islam, sebagai sistem hukum yang bersumber dari syariat, memberikan pandangan atau pengaturan terkait kejahatan siber, termasuk penggunaan *malware* yang merugikan individu maupun masyarakat.

Melihat perkembangan teknologi yang terus berlanjut, diperlukan pula konsep pengaturan hukum pidana di masa depan yang lebih responsif terhadap ancaman tindak pidana siber menggunakan *malware*. Pengaturan ini harus mampu menyeimbangkan perlindungan terhadap kepentingan masyarakat dengan hak-hak individu, serta memberikan dasar hukum yang jelas untuk menindak pelaku kejahatan siber. Dengan demikian, pembahasan ini menjadi relevan dalam rangka merumuskan kebijakan hukum pidana yang adaptif dan efektif di era digital.

Hasil penelitian ini dirumuskan untuk memberikan solusi atas permasalahan regulasi, termasuk pengembangan kerangka hukum di masa depan yang lebih adaptif terhadap perkembangan teknologi. Rekomendasi yang diberikan mencakup integrasi teknologi canggih seperti kecerdasan buatan dan peningkatan kerja sama internasional untuk menanggulangi kejahatan siber yang bersifat lintas negara. Hal ini bertujuan menciptakan regulasi yang lebih efektif, berkeadilan, dan selaras dengan nilai-nilai etika serta moral.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan normatif dengan metode analisis kualitatif-deskriptif untuk menelaah pengaturan tindak pidana siber yang menggunakan *malware* dalam hukum positif dan hukum pidana Islam. Sumber data yang digunakan meliputi sumber hukum primer, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang terdapat dalam pasal 30 Undang-undang No.1 Tahun 2024 terkait perubahan atas Undang-undang No.11 Tahun 2008 tentang UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP), serta Al-Qur'an dan Hadis sebagai landasan hukum Islam. Sumber hukum sekunder mencakup literatur hukum pidana, penelitian terdahulu, dan pandangan ulama serta ahli fikih kontemporer yang relevan dengan fenomena kejahatan siber. Sumber hukum tersier diperoleh dari kamus

[12] Wendi Asmoro, "Analisis Terhadap Tindak Pidana Pengiriman File Aplikasi (Apk) Yang Berisi *Malware* Dan Upaya Pencegahannya Di Wilayah Hukum Polda Jawa Tengah," *Doctoral Dissertation, UPT. Perpustakaan Undaris*, 2024.

hukum, ensiklopedia, serta data statistik yang mendukung, seperti laporan dari media dan website yang kredibel.[13]

Teknik pengumpulan data dilakukan melalui studi kepustakaan terhadap dokumen hukum, artikel ilmiah, dan data statistik terkait kejahatan siber. Analisis data dilakukan secara kualitatif dengan mengkaji regulasi yang ada, seperti UU ITE, untuk mengidentifikasi kekurangan dan potensinya dalam menghadapi ancaman *malware* yang terus berkembang. Prinsip keadilan dan perlindungan dalam *maqashid syariah* juga dianalisis sebagai pendekatan hukum pidana Islam terhadap kejahatan ini.

III. KERANGKA TEORITIS

Tindak pidana siber, termasuk penggunaan *malware*, dapat dianalisis berdasarkan teori hukum pidana klasik dan modern. Moeljatno mendefinisikan tindak pidana sebagai suatu perbuatan yang oleh aturan hukum dilarang dan diancam dengan pidana bagi yang melanggarnya[14]. Dalam hal ini, penggunaan *malware* yang mengakibatkan pelanggaran terhadap sistem elektronik memenuhi unsur perbuatan pidana karena bersifat melawan hukum dan telah ditentukan sanksinya dalam peraturan perundang-undangan.

Sudarto menegaskan bahwa hukum pidana memiliki fungsi untuk melindungi kepentingan hukum masyarakat dari perbuatan yang merugikan dan membahayakan.[15] Dalam konteks digital, perlindungan tersebut meluas pada data pribadi, keamanan siber, dan hak atas privasi. Oleh karena itu, tindak pidana yang menyerang sistem elektronik, seperti serangan *malware*, wajib mendapat perhatian dari sistem hukum pidana yang bersifat preventif maupun represif.

Dalam perspektif global, Clough menjelaskan bahwa kejahatan siber bersifat lintas batas, sulit dilacak, dan sering dilakukan secara anonim.[16] Hal ini menuntut pengembangan perangkat hukum yang adaptif terhadap teknologi, serta kolaborasi lintas negara untuk penegakan hukum yang efektif.

Lebih lanjut, Hadjon menambahkan bahwa perlindungan hukum merupakan upaya untuk menjaga hak-hak individu dari tindakan sewenang-wenang melalui perangkat hukum yang tersedia, baik secara preventif maupun kuratif.[17] Dalam kerangka ini, hukum pidana harus mampu mengantisipasi perkembangan modus kejahatan digital, termasuk yang dilakukan melalui *malware*, demi menjamin rasa aman dan keadilan bagi masyarakat.

Berdasarkan uraian teoritis, dapat disimpulkan bahwa tindak pidana siber menggunakan *malware* merupakan bentuk kejahatan modern yang tetap relevan dianalisis melalui teori hukum pidana klasik dan prinsip hukum kontemporer. Moeljatno dan Sudarto menegaskan bahwa unsur melawan hukum dan perlindungan terhadap kepentingan masyarakat tetap menjadi dasar dalam penegakan hukum pidana, termasuk dalam ranah digital. Di sisi lain, pendekatan modern sebagaimana dikemukakan Jonathan Clough menunjukkan perlunya adaptasi hukum terhadap

---

[13] M. Benuf, K., & Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (2020): 20–33.

[14] Moeljatno, *Asas-Asas Hukum Pidana* (Jakarta: Renika Cipta, 2000).

[15] Sudarto, *Hukum Dan Hukum Pidana* (Bandung: Alumni, 1986).

[16] J. Clough, *Principles Of Cybercrime (2nd Ed.)* (Cambridge: Cambridge University Press, 2015).

[17] P. M. Hadjon, *Perlindungan Hukum Bagi Rakyat Di Indonesia* (Surabaya: Bina Ilmu, n.d.).

karakteristik khas kejahatan siber yang lintas batas, anonim, dan bersifat kompleks. Prinsip perlindungan hukum dari Hadjon memperkuat urgensi kehadiran regulasi yang mampu memberikan jaminan rasa aman terhadap pelanggaran hak digital masyarakat. Oleh karena itu, perpaduan teori hukum pidana konvensional dan pendekatan hukum siber modern menjadi fondasi konseptual dalam merumuskan kebijakan hukum yang efektif terhadap kejahatan digital berbasis *malware*.

IV. HASIL PENELITIAN

A. Pengaturan Terkait Tindak Pidana Siber Menggunakan *Malware*

1. Definisi dan Karakteristik *Malware*

Malware, singkatan dari "malicious software," adalah perangkat lunak berbahaya yang dirancang untuk mengganggu, merusak, atau mengakses sistem komputer tanpa izin. *Malware* mencakup berbagai jenis, seperti virus, worm, trojan, ransomware, spyware, dan adware. Setiap jenis *malware* memiliki karakteristik unik dalam modus operandi dan dampaknya, tetapi secara umum, *malware* bertujuan untuk mencuri data, merusak perangkat, mengganggu sistem, atau memeras korban.

Karakteristik utama *malware* adalah sifatnya yang ilegal dan merugikan. Malware biasanya disebarkan melalui email phishing, unduhan tidak resmi, atau kerentanan sistem. Dampak dari penggunaan malware sangat luas, mulai dari kerugian finansial, pencurian identitas, hingga gangguan terhadap infrastruktur penting seperti sistem perbankan dan layanan kesehatan. Dalam konteks tindak pidana siber, *malware* sering kali digunakan oleh pelaku untuk mencuri informasi, mengancam keamanan data, atau mendapatkan keuntungan dengan cara melanggar hukum.

Dalam konteks hukum, tindak pidana yang melibatkan *malware* menjadi perhatian penting karena sifatnya yang lintas batas negara dan terus berkembang seiring kemajuan teknologi. Hal ini menimbulkan tantangan dalam pengaturan hukum, terutama untuk memastikan bahwa regulasi yang ada mampu menghadapi ancaman dan dampak dari tindak pidana ini. *Malware* menjadi salah satu bentuk kejahatan digital yang membutuhkan pengawasan ketat serta penegakan hukum yang efektif, baik dari perspektif hukum positif maupun dalam sudut pandang hukum Islam.

2. Landasan Hukum dalam Hukum Positif Terkait Tindak Pidana Siber Menggunakan *Malware*

Undang-Undang Nomor 1 Tahun 2024 sebagai perubahan kedua atas UU ITE memuat sejumlah ketentuan yang relevan dalam menanggulangi kejahatan siber berbasis *malware*. Pasal 30 misalnya, mengatur larangan terhadap akses ilegal ke sistem elektronik milik orang lain. Pelaku yang menggunakan *malware* untuk masuk ke dalam sistem tanpa hak atau melawan hukum dapat dijerat berdasarkan ketentuan ini, karena *malware* berfungsi sebagai alat untuk membuka jalur masuk ke sistem, baik untuk membaca, mengambil, maupun merusak data elektronik. Pasal 33 memperluas perlindungan hukum dengan melarang intersepsi atau penyadapan atas informasi elektronik. Jenis *malware* seperti *keylogger*, *spyware*, atau *trojan horse* biasa digunakan

untuk mencatat aktivitas pengguna dan menyadap komunikasi rahasia, sehingga sangat sesuai dijerat melalui pasal ini. Sementara itu, Pasal 34 memberikan landasan hukum untuk menindak pembuatan, distribusi, dan penyediaan perangkat lunak berbahaya, termasuk *malware*, meskipun pelaku tidak menggunakannya secara langsung, ia tetap dapat dikenai pertanggungjawaban pidana berdasarkan pasal ini.[18] Ketentuan ini penting untuk mencegah penyebaran alat-alat kejahatan digital yang dapat dimanfaatkan oleh pihak lain. Selanjutnya, Pasal 46 memberikan sanksi pidana terhadap pelanggaran-pelanggaran tersebut, dengan ancaman hukuman penjara hingga delapan tahun dan denda maksimal delapan ratus juta rupiah. Ini menunjukkan keseriusan negara dalam memberikan efek jera terhadap pelaku kejahatan digital.[19]

Selain pengaturan dalam UU ITE, KUHP baru melalui Undang-Undang Nomor 1 Tahun 2023 juga telah merespons perkembangan kejahatan *siber*, termasuk penggunaan *malware*. Pasal 322 ayat (1) mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak mengakses komputer atau sistem elektronik milik orang lain dapat dikenakan pidana penjara paling lama enam tahun atau denda kategori V. Ketentuan ini mengakomodasi realitas di mana *malware* menjadi alat utama untuk memperoleh akses tanpa izin ke sistem target. Apabila akses ilegal tersebut dilakukan untuk memperoleh informasi elektronik atau dokumen elektronik, sebagaimana diatur dalam ayat (2) pasal yang sama, maka ancaman pidana meningkat menjadi tujuh tahun. Bahkan, jika tindakan tersebut dilakukan dengan menjebol sistem pengamanan, pelaku dapat dikenai pidana delapan tahun sesuai ayat (3). Tidak hanya melindungi kepentingan individu, KUHP baru juga memberikan perlindungan terhadap kepentingan negara. Pasal 333 mengatur bahwa pelaku yang secara tanpa hak mengakses sistem informasi yang memuat informasi pertahanan atau keamanan nasional, dan mengubah, merusak, atau menghilangkan data tersebut, dapat dipidana paling lama tujuh tahun atau dikenai denda kategori VI. Dengan demikian, kejahatan siber yang menargetkan sistem negara juga dapat dijerat secara tegas oleh hukum pidana nasional.[20]

Kehadiran ketentuan-ketentuan ini memperlihatkan bahwa sistem hukum nasional Indonesia telah semakin responsif terhadap dinamika kejahatan di era digital. Baik melalui UU ITE maupun KUHP baru, negara memberikan kerangka hukum yang komprehensif untuk mencegah, menindak, dan mengadili pelaku kejahatan siber yang menggunakan *malware*. Hal ini menunjukkan adanya komitmen untuk menjaga ruang digital tetap aman dan terlindungi dari ancaman yang bersifat destruktif dan melanggar hukum. Tindak pidana siber menggunakan *malware* merupakan kejahatan modern yang memerlukan penanganan hukum yang tegas dan komprehensif. Undang-Undang Nomor 1 Tahun 2024 telah memberikan kerangka hukum yang cukup kuat melalui pengaturan terhadap akses ilegal, penyadapan, penyebaran perangkat berbahaya, serta pemberian sanksi pidana. Dengan demikian, penegakan hukum terhadap pelaku kejahatan siber dapat dilakukan secara lebih efektif,

[18] S. Afrianie, *Hukum Kejahatan Siber Di Indonesia: Antara Tantangan Dan Solusi* (Jakarta: Prenadamedia Group, 2020).
[19] E. Setiadi, *Pengantar Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2019).
[20] Republik Indonesia, "Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana" (2023).

sekaligus memberikan perlindungan terhadap hak privasi dan keamanan digital masyarakat Indonesia.[21]

Namun, meskipun UU ITE telah mengatur secara umum tentang kejahatan siber, terdapat beberapa kelemahan dalam implementasinya. Salah satunya adalah tidak adanya pengaturan khusus yang secara eksplisit mendefinisikan *malware* atau bentuk-bentuk kejahatan siber tertentu lainnya. Akibatnya, penegakan hukum sering kali harus mengandalkan interpretasi luas dari pasal-pasal yang ada, yang dapat menimbulkan ketidakpastian hukum. Selain itu, kecepatan perkembangan teknologi sering kali melampaui kemampuan regulasi yang ada untuk mengantisipasi modus-modus baru kejahatan siber, termasuk serangan *malware* yang semakin kompleks.

Selain UU ITE, regulasi tambahan seperti Kitab Undang-Undang Hukum Pidana (KUHP) dan peraturan teknis terkait keamanan siber juga berperan dalam melengkapi pengaturan hukum. Namun, integrasi dan harmonisasi antara UU ITE dengan peraturan lainnya masih menjadi tantangan. Hal ini menunjukkan perlunya pengembangan kerangka hukum yang lebih komprehensif, responsif, dan adaptif terhadap tantangan kejahatan siber yang terus berkembang.

3. Contoh Kasus di Indonesia atau Internasional Terkait Tindak Pidana Siber Menggunakan *Malware*

Untuk memberikan ilustrasi yang konkret tentang penerapan hukum terkait tindak pidana siber menggunakan *malware*, beberapa kasus dapat dijadikan acuan. Salah satu contoh yang cukup terkenal di Indonesia adalah kasus peretasan sistem jaringan bank menggunakan *malware*. Dalam kasus ini, pelaku menggunakan *malware* untuk mencuri data nasabah dan melakukan transaksi ilegal, yang mengakibatkan kerugian finansial besar bagi pihak bank dan nasabah. Peraturan yang digunakan untuk menjerat pelaku adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 30 dan Pasal 31 yang mengatur tentang akses ilegal dan penyadapan sistem elektronik.

Di tingkat internasional, kasus "*WannaCry Ransomware Attack*" pada tahun 2017 menjadi salah satu insiden paling signifikan dalam sejarah kejahatan siber. *WannaCry*, sebuah *malware* yang mengenkripsi data komputer korban, digunakan untuk meminta tebusan dalam bentuk *cryptocurrency*. Serangan ini berdampak pada berbagai negara, termasuk rumah sakit di Inggris, perusahaan besar, dan institusi pemerintah. Meskipun tidak secara langsung terkait dengan hukum Indonesia, kasus ini memberikan gambaran tentang betapa seriusnya ancaman *malware* dan pentingnya regulasi hukum siber yang efektif.

Kedua contoh tersebut menunjukkan kompleksitas tindak pidana siber menggunakan *malware*, yang tidak hanya berdampak secara lokal tetapi juga lintas negara. Hal ini menekankan kebutuhan akan pengaturan hukum yang lebih spesifik dan kuat dalam menangani kejahatan siber, baik di Indonesia maupun di tingkat global.

---

[21] Wahyudi Ajad, Umar Mahdi, and M Agmar Media, "Analisis Yuridis Terhadap Tindak Pidana Penipuan Siber Dengan Modus Operandi Busuness Email," *Jurnal Hukum Dan Teknologi* 4, no. 2 (2024): 229–51.

B. Pengaturan Hukum Pidana Islam Terkait Tindak Pidana Siber Menggunakan *Malware*

1. Konsep Kejahatan dalam Hukum Pidana Islam

Dalam hukum pidana Islam, kejahatan atau tindak pidana dikenal sebagai jinayah, yang mencakup segala bentuk perbuatan yang dilarang oleh syariah karena melanggar hak Allah atau hak manusia. Jinayah tidak hanya terbatas pada tindakan fisik, tetapi juga mencakup tindakan yang bersifat non-fisik, seperti penipuan atau pencurian data, yang merugikan pihak lain. Tindak pidana siber menggunakan *malware* dapat dikategorikan sebagai bentuk jinayah karena secara langsung bertentangan dengan prinsip-prinsip Islam, seperti larangan dharar (merugikan orang lain) dan ifsad (merusak).

Prinsip dharar didasarkan pada kaidah fikih yang berbunyi, "Laa dharara wa laa dhirara" (Tidak boleh ada bahaya dan tidak boleh membahayakan orang lain). *Malware* yang dirancang untuk mencuri, merusak, atau mengganggu sistem informasi merupakan bentuk pelanggaran terhadap kaidah ini, karena menyebabkan kerugian material maupun non-material kepada korban. Selain itu, tindakan tersebut juga melanggar prinsip ifsad, yang dilarang dalam Al-Qur'an, seperti dalam Surah Al-Baqarah (2:205) yang menyebutkan bahwa Allah tidak menyukai orang-orang yang membuat kerusakan di muka bumi.

Dengan demikian, kejahatan siber menggunakan *malware* dapat dipahami sebagai bentuk pelanggaran serius dalam hukum pidana Islam. Islam memandang bahwa setiap tindakan yang merugikan individu atau masyarakat secara keseluruhan harus diatasi dengan mekanisme hukum yang tegas untuk menjaga keadilan dan kemaslahatan umum (maslahat al-ammah). Dalam konteks ini, tindak pidana siber menggunakan *malware* dapat digolongkan sebagai tindakan kriminal modern yang memerlukan adaptasi prinsip-prinsip hukum Islam untuk menghadapinya secara efektif.

2. Analisis Dalil Syariah Terkait Tindak Pidana Siber Menggunakan *Malware*

Dalam perspektif hukum Islam, tindak pidana siber menggunakan *malware* dapat dianalisis melalui dalil-dalil syariah yang melarang tindakan merugikan, mencuri, atau merusak milik orang lain. Beberapa dalil Al-Qur'an dan Hadis yang relevan meliputi:

a. Larangan Melakukan Kerusakan (Ifsad)
   Al-Qur'an menyatakan dengan tegas larangan berbuat kerusakan di muka bumi, sebagaimana dalam Surah Al-Baqarah ayat 205: "Dan apabila ia berpaling (dari kamu), ia berusaha di bumi untuk mengadakan kerusakan padanya dan merusak tanaman-tanaman dan binatang ternak, dan Allah tidak menyukai kerusakan."
   Tindak pidana siber menggunakan *malware* yang merusak data, sistem, atau infrastruktur digital, sejalan dengan pengertian ifsad ini.

b. Larangan Mencuri dan Melakukan Kecurangan
   Larangan mengambil sesuatu yang bukan miliknya (mencuri) juga berlaku dalam konteks digital. Dalam Al-Qur'an Surah Al-Maidah ayat 38 disebutkan:
   "Laki-laki yang mencuri dan perempuan yang mencuri, potonglah tangan keduanya sebagai pembalasan terhadap apa yang mereka kerjakan."
   Dalam konteks modern, penggunaan *malware* untuk mencuri data atau informasi pribadi dapat dianalogikan sebagai bentuk pencurian, meskipun hukumannya disesuaikan berdasarkan ta'zir karena sifatnya tidak langsung merampas harta fisik.
c. Larangan Menzalimi Orang Lain
   Islam melarang segala bentuk kezaliman, termasuk tindakan yang membahayakan hak atau harta orang lain. Rasulullah SAW bersabda:
   "Tidak boleh membahayakan diri sendiri ataupun orang lain." (HR. Ahmad dan Ibnu Majah).
   Malware yang digunakan untuk mengakses data tanpa izin, merusak perangkat, atau bahkan melakukan pemerasan melalui ransomware, termasuk tindakan zalim yang bertentangan dengan syariat.
d. Relevansi dengan Konsep Amanah
   Islam memandang keamanan informasi sebagai amanah yang harus dijaga. Dalam Surah Al-Anfal ayat 27, Allah SWT berfirman:
   "Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul-Nya, dan juga janganlah kamu mengkhianati amanah-amanah yang dipercayakan kepadamu, sedang kamu mengetahui."
   Malware yang dirancang untuk mengkhianati kepercayaan pengguna atau sistem digital merupakan pelanggaran terhadap prinsip amanah ini.

3. Penafsiran Ulama dan Relevansi dengan Kejahatan Siber

Para ulama kontemporer memandang bahwa kejahatan modern, termasuk tindak pidana siber, dapat dikenakan sanksi ta'zir karena tidak secara langsung disebutkan dalam nash. *Ta'zir* memberikan otoritas kepada pemerintah atau hakim untuk menetapkan hukuman yang adil, dengan tujuan melindungi masyarakat dan mencegah kejahatan serupa di masa depan. Hal ini didasarkan pada prinsip kemaslahatan (*maqashid syariah*), yaitu menjaga agama, jiwa, akal, keturunan, dan harta.

Analisis dalil ini menegaskan bahwa tindak pidana siber menggunakan *malware* bertentangan dengan nilai-nilai syariah, baik dari aspek larangan berbuat kerusakan, mencuri, maupun menzalimi orang lain. Oleh karena itu, hukum pidana Islam dapat memberikan kerangka normatif untuk menangani kejahatan ini secara adil dan preventif.

4. **Jenis Hukuman dalam Hukum Pidana Islam untuk Tindak Pidana Siber Menggunakan *Malware***

Dalam hukum pidana Islam, jenis hukuman untuk tindak pidana siber menggunakan *malware* dapat diklasifikasikan ke dalam tiga kategori utama: *hudud*, *qishash*, dan *ta'zir*,

tergantung pada sifat dan dampak kejahatan yang dilakukan. Karena tindak pidana siber menggunakan *malware* tidak secara langsung disebutkan dalam nash (teks Al-Qur'an atau Hadis), hukuman yang relevan cenderung dikelompokkan ke dalam kategori ta'zir, yaitu hukuman yang ditentukan oleh hakim atau pemerintah untuk menjaga ketertiban dan mencegah kejahatan.

a. *Hudud* dan Relevansinya

Tindak pidana siber menggunakan *malware* tidak memenuhi syarat untuk dikategorikan sebagai hudud karena hudud hanya mencakup kejahatan yang sudah ditentukan secara spesifik oleh syariah, seperti pencurian (sariqah), perampokan (hirabah), atau perzinaan (zina). Namun, dalam kasus tertentu, penggunaan *malware* yang menyebabkan pencurian data atau harta benda secara ilegal dapat dianggap menyerupai tindakan sariqah jika memenuhi unsur-unsur pencurian, seperti niat mencuri, adanya harta yang dilindungi, dan pengambilan tanpa izin.

b. *Qishash* dan *Diyat*

Jika penggunaan *malware* secara langsung atau tidak langsung menyebabkan kerugian fisik, seperti mengganggu sistem yang mengancam keselamatan jiwa (misalnya, meretas sistem rumah sakit yang mengakibatkan kegagalan operasi medis), maka kejahatan ini dapat dikaitkan dengan kategori qishash atau diyat. Dalam kasus seperti ini, pelaku bertanggung jawab atas dampak yang ditimbulkan sesuai prinsip hukum Islam, yaitu menuntut balasan setimpal atau memberikan kompensasi kepada korban.

c. *Ta'zir* sebagai Pendekatan Utama

Sebagian besar kasus tindak pidana siber menggunakan *malware* cenderung masuk ke dalam kategori *ta'zir*. Dalam konteks ini, pemerintah atau otoritas memiliki kewenangan untuk menentukan jenis dan berat hukuman berdasarkan prinsip kemaslahatan (*maslahat*) dan pencegahan (*zawajir*). Hukuman dapat berupa denda (*gharamah*), penjara, atau tindakan lain yang dianggap sesuai untuk memberikan efek jera kepada pelaku. Pendekatan ini memberikan fleksibilitas kepada hakim untuk menyesuaikan hukuman dengan perkembangan zaman dan teknologi.

Dengan menempatkan tindak pidana siber dalam kategori *ta'zir*, hukum pidana Islam menunjukkan kapasitasnya untuk adaptif terhadap kejahatan modern seperti penggunaan *malware*. Pendekatan ini juga memungkinkan penerapan sanksi yang berkeadilan dan bertujuan untuk melindungi masyarakat dari dampak negatif kejahatan siber.

C. Konsep Pengaturan Tindak Pidana Siber Menggunakan *Malware* di Masa Depan Kelemahan Pengaturan Hukum Positif Saat Ini

Dalam konteks tindak pidana siber menggunakan *malware*, pengaturan hukum positif di Indonesia, terutama melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya, memiliki sejumlah kelemahan. Salah satu kelemahan utama adalah ketidakjelasan definisi *malware* dalam regulasi tersebut. UU ITE lebih banyak memberikan pengaturan umum mengenai akses ilegal, manipulasi data, atau perusakan sistem elektronik tanpa secara spesifik mengatur tentang *malware* sebagai alat kejahatan. Hal ini mengakibatkan interpretasi

yang berbeda-beda dalam penerapan hukum, terutama dalam menentukan bentuk dan jenis *malware* yang termasuk tindak pidana.[22]

Selain itu, pendekatan hukum positif saat ini cenderung bersifat reaktif, lebih fokus pada penindakan setelah kejahatan terjadi daripada memberikan perlindungan preventif. Ketiadaan regulasi yang memadai untuk mencegah penyebaran *malware* atau memberikan mekanisme perlindungan terhadap individu dan institusi yang rentan menjadi korban menunjukkan kurangnya responsifitas hukum terhadap sifat dinamis tindak pidana siber. Sebagai contoh, peraturan tentang kewajiban pelaporan insiden keamanan siber atau perlindungan data korban masih sangat minim dan belum terintegrasi dengan baik dalam sistem hukum siber di Indonesia.

Tantangan lainnya adalah kesenjangan antara kemampuan penegak hukum dan kompleksitas tindak pidana siber. Kasus-kasus *malware* sering kali melibatkan teknologi yang terus berkembang, jaringan internasional, dan aktor yang sulit dilacak, sehingga mempersulit proses penegakan hukum. Kelemahan ini menunjukkan perlunya pembaruan regulasi yang lebih komprehensif dan adaptif, termasuk penguatan kapasitas institusi penegak hukum untuk memahami dan menangani tindak pidana siber secara efektif.

Integrasi Hukum Islam dan Hukum Positif

Pendekatan integrasi antara hukum pidana Islam dan hukum positif dapat menjadi solusi yang efektif untuk menangani tindak pidana siber menggunakan *malware*. Prinsip-prinsip dasar dalam hukum pidana Islam, seperti keadilan, perlindungan harta, dan larangan perusakan, memiliki relevansi yang kuat dalam mengatasi kejahatan modern. Dalam hal ini, hukum pidana Islam dapat memberikan landasan etis dan moral yang lebih universal, sementara hukum positif dapat menawarkan kerangka regulasi yang konkret dan spesifik.

Integrasi ini dapat dilakukan melalui harmonisasi nilai-nilai *maqashid syariah* dengan hukum positif. Sebagai contoh, *maqashid syariah* yang bertujuan melindungi lima hal utama—agama, jiwa, akal, keturunan, dan harta—dapat dijadikan pijakan dalam penyusunan regulasi terkait tindak pidana siber. Kejahatan siber yang merugikan harta dan melanggar privasi, misalnya, dapat didekati dengan prinsip larangan mencuri (*sariqah*) dalam Islam, yang juga diatur secara spesifik dalam hukum positif melalui UU ITE.

Dalam implementasinya, integrasi ini juga membutuhkan pemahaman yang mendalam tentang konteks sosial dan teknologi yang berkembang. Penyesuaian hukum Islam dengan realitas kejahatan siber tidak hanya memperkuat legitimasi hukum, tetapi juga memperkaya sistem hukum positif dengan nilai-nilai keadilan berbasis syariah. Hal ini berpotensi menciptakan pengaturan hukum yang lebih komprehensif dan berorientasi pada perlindungan maslahat masyarakat luas.

[22] Republik Indonesia., "Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik" (2024).

Konsep Pengaturan Tindak Pidana Siber Menggunakan *Malware* di Masa Depan

Perkembangan teknologi yang semakin pesat memunculkan berbagai tantangan baru dalam mengatur tindak pidana siber, termasuk penggunaan *malware*. Salah satu kelemahan utama pengaturan hukum positif saat ini adalah kurangnya adaptasi terhadap dinamika teknologi yang terus berubah. Peraturan seperti UU ITE seringkali bersifat reaktif dan belum mencakup detail teknis tentang modus operandi terbaru kejahatan siber. Selain itu, implementasi hukum di lapangan masih terkendala oleh keterbatasan sumber daya manusia yang memahami kompleksitas teknologi, sehingga perlindungan bagi korban tindak pidana siber belum optimal.

Dalam menghadapi tantangan tersebut, diperlukan integrasi antara hukum positif dan hukum Islam sebagai landasan untuk menciptakan pengaturan yang lebih responsif. Prinsip-prinsip dalam hukum pidana Islam, seperti larangan merugikan (dharar) dan perlindungan terhadap harta benda, dapat dijadikan dasar untuk membangun kerangka hukum yang berorientasi pada kemaslahatan umum (*maqashid syariah*). Penggunaan *maqashid syariah* ini memungkinkan pengaturan hukum yang tidak hanya mengedepankan keadilan, tetapi juga pencegahan dan perlindungan terhadap kerugian yang diakibatkan oleh tindak pidana siber. Dengan mengintegrasikan nilai-nilai syariah ke dalam regulasi modern, hukum dapat lebih relevan dalam menangani kasus-kasus baru yang kompleks.

Konsep hukum futuristik yang direkomendasikan melibatkan pengembangan regulasi berbasis teknologi. Misalnya, menciptakan mekanisme pencegahan berbasis artificial intelligence (AI) untuk mendeteksi aktivitas *malware* sebelum merugikan pihak lain. Selain itu, regulasi masa depan perlu mengatur kerjasama internasional untuk melacak dan menghukum pelaku kejahatan siber lintas negara. Dalam konteks ini, pendekatan hukum Islam yang bersifat universal dapat menjadi nilai tambah, karena hukum Islam menekankan keadilan yang berlaku bagi seluruh umat manusia. Dengan demikian, hukum masa depan tidak hanya adaptif terhadap perkembangan teknologi, tetapi juga mencerminkan nilai-nilai moral dan kemanusiaan yang mendalam.

V. KESIMPULAN

Penelitian ini mengungkapkan bahwa tindak pidana siber menggunakan *malware* merupakan salah satu bentuk kejahatan yang terus berkembang seiring kemajuan teknologi. Dalam hukum positif, pengaturan tindak pidana ini diatur terutama melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun masih terdapat berbagai kelemahan dalam cakupan pengaturannya, terutama dalam menghadapi modus operandi kejahatan yang semakin kompleks. Regulasi yang ada cenderung reaktif dan memerlukan pembaruan untuk menyesuaikan dengan perkembangan teknologi yang dinamis.

Dalam perspektif hukum pidana Islam, tindak pidana siber menggunakan *malware* dapat digolongkan sebagai tindakan yang melanggar prinsip keadilan, larangan perusakan (*ifsad*), dan larangan mencuri (*sariqah*). Dalil-dalil syariah dari Al-Qur'an dan Hadis memberikan landasan yang kuat untuk mengkategorikan kejahatan ini sebagai bentuk jinayah yang merugikan individu maupun masyarakat. Hukum

pidana Islam mengutamakan prinsip kemaslahatan umum (*maqashid syariah*), sehingga memberikan peluang untuk mengintegrasikan nilai-nilainya ke dalam pengaturan hukum modern.
Saran dari penulis, pengaturan tindak pidana siber menggunakan *malware* di masa depan perlu mengadopsi pendekatan yang lebih futuristik dan adaptif. Hal ini dapat dilakukan dengan mengintegrasikan nilai-nilai hukum Islam ke dalam regulasi modern, membangun mekanisme pencegahan berbasis teknologi, dan meningkatkan kerjasama internasional untuk menanggulangi kejahatan lintas negara. Dengan landasan *maqashid syariah*, regulasi dapat dirancang untuk melindungi masyarakat secara holistik, tidak hanya melalui penegakan hukum yang tegas, tetapi juga dengan menciptakan lingkungan digital yang aman, adil, dan bermartabat.

REFERENSI

Buku

Afrianie, S. *Hukum Kejahatan Siber Di Indonesia: Antara Tantangan Dan Solusi*. Jakarta: Prenadamedia Group, 2020.

Al-Ghazali, A.H.M. *Al-Mustashfa Min 'Ilm Al-Usul*. Beirut: Dar Al-Kutub Al-'Ilmiyyah, 1993.

Clough, J. *Principles Of Cybercrime (2nd Ed.)*. Cambridge: Cambridge University Press, 2015.

Hadjon, P. M. *Perlindungan Hukum Bagi Rakyat Di Indonesia*. Surabaya: Bina Ilmu, n.d.

Hasibuan, H. *Keamanan Siber Dan Perlindungan Data Pribadi Di Era Digital*. Yogyakarta: Deepublish, 2022.

Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Renika Cipta, 2000.

Setiadi, E. *Pengantar Hukum Teknologi Informasi*. Bandung: Refika Aditama, 2019.

Sudarto. *Hukum Dan Hukum Pidana*. Bandung: Alumni, 1986.

Artikel/Jurnal

Affandi, N. K., and A. Nrangwesti. "Penegakan Hukum Perampokan Bersenjata Di Selat Malaka Berdasarkan Hukum Laut Internasional." *Reformasi Hukum Trisakti* 5, no. 1 (2023): 82–93.

Agustin, N. A., and R. M. Firdos. "Agustin, N. A., & Firdos, R. M. (2024). Studi Literatur: Ancaman Cybercrime Di Indonesia Dan Pentingnya Pemahaman Akan Fenomena Kejahatan Digital." *Jurnal Mahasiswa Teknik Informatika* 3, no.

126–131 (2024).

Ajad, Wahyudi, Umar Mahdi, and M Agmar Media. "Analisis Yuridis Terhadap Tindak Pidana Penipuan Siber Dengan Modus Operandi Busuness Email." *Jurnal Hukum Dan Teknologi* 4, no. 2 (2024): 229–51.

Asmoro, Wendi. "Analisis Terhadap Tindak Pidana Pengiriman File Aplikasi (Apk) Yang Berisi *Malware* Dan Upaya Pencegahannya Di Wilayah Hukum Polda Jawa Tengah." *Doctoral Dissertation, UPT. Perpustakaan Undaris*, 2024.

Benuf, K., & Azhar, M. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33.

Kasim, Z. "Kebijakan Hukum Pidana Untuk Penanggulangan Cybercrime Di Indonesia." *Indragiri Law Review* 2, no. 1 (2024): 18–24.

Putri, E. H. A. D., Kasim, R., and L. D. Nurmala. "Analisis Yuridis Terhadap Penegakan Dan Pengaturan Hukum Kejahatan Dunia Maya (Cybercrime) Di Indonesia." *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora* 2, no. 3 (2024): 102–11.

Wahdini, S. A. N., and F. F. B Irfansyah. "Analisis Keselarasan Pengaturan Yurisdiksi Cybercrime Dengan Implementasinya Di Kehidupan Nyata." *Indonesian Journal Of Law And Justice* 1, no. 3 (2024): 1–11.

Widhaningroem, S. "Analisis Yuridis Penyidikan Kejahatan E-Commerce Di Indonesia (Kajian Kejahatan Penipuan Dan Pencurian Identitas)." *Doctoral Dissertation, Universitas Muhammadiyah Yogyakarta*, 2024.

Wijanarko, R. P. "Analisis Dan Simulasi Serangan Ransomware Terhadap Database Bank Syariah Indonesia." *In Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, 2023.

Wijaya, O. "E-Commerce: Perkembangan, Tren, Dan Peraturan Perundang-Undangan." *Jurnal Ilmiah Ekonomi Dan Bisnis* 16, no. 1 (2023): 41–47.

Peraturan Perundang-Undangan

Indonesia., Republik. Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (2024).

Indonesia, Republik. Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana (2023).

Internet

Kaspersky."Https://Www.Cnnindonesia.Com/Teknologi/20240522130109-185 1100872 /Serangan-Siber-Menggila-411-Ribu-*Malware*-Baru-Muncul-Tiap-Hari-DiRi#:~:Tex t=Serangan%20ransomware%20atau%20peretasan%20dengan%20modus%20 pemerasan%20terlacak,Pembobol%20sistem%20yang%20baru." 2024.