**Pengaturan Keamanan Jaringan dan Kejahatan Siber dalam Hukum ITE**

**Dery Ardianto**

**Sekolah Tinggi Ilmu Hukum IBLAM**

1. **Abstrak**

Dalam era globalisasi teknologi informasi, perkembangan pesat dalam teknologi internet telah mengubah lanskap sosial, ekonomi, dan politik. Namun, bersamaan dengan kemajuan ini, kejahatan siber semakin mengintensif dan memerlukan kerangka hukum yang komprehensif.

Penelitian ini menggunakan pendekatan kualitatif dengan fokus pada analisis hukum normatif dan studi kepustakaan. Data diperoleh melalui wawancara dan pengamatan terhadap perilaku serta pendekatan peraturan perundang-undangan.

Hasil penelitian menunjukkan bahwa Indonesia perlu segera membentuk Rancangan Undang-Undang Ketahanan dan Keamanan Siber (KKS) yang komprehensif untuk mengatasi ancaman kejahatan siber yang semakin kompleks. RUU KKS harus dirancang secara transparan melibatkan berbagai pihak, mencakup ketentuan sanksi tegas terhadap pelanggaran kedaulatan digital, dan memperkuat kerangka hukum dalam menghadapi perkembangan teknologi yang terus berlanjut.

Keyword: Kejahatan Siber, Ketahanan Siber, Undang-Undang Ketahanan dan Keamanan Siber (KKS), Hukum Informasi Transaksi Elektronik, Kebebasan Internet.

*In the era of globalization of information technology, rapid developments in internet technology have changed the social, economic, and political landscape. However, along with these advances, cybercrimes are intensifying and require a comprehensive legal framework.*

*This study uses a qualitative approach with a focus on normative legal analysis and literature studies. Data were obtained through interviews, observations of behavior, and a law and regulation approach.*

*The research results show that Indonesia needs to immediately form a comprehensive Cyber Resilience and Security (KKS) Bill to overcome the increasingly complex threat of cybercrime. The KKS Bill must be drafted in a transparent manner involving various parties, include provisions for strict sanctions against violations of digital sovereignty, and strengthen the legal framework in the face of continuing technological developments.*

***Keywords****: Cybercrime, Cyber Resilience, Cyber Resilience and Security Law (KKS), Electronic Transaction Information Law, Internet Freedom.*

1. **Pendahuluan**

Semakin majunya perkembangan teknologi dan fenomena globalisasi saat ini turut mendorong pesatnya pertumbuhan teknologi informasi. Fenomena ini tidak terbatas pada negara-negara maju saja, tetapi juga telah merambah hingga ke negara-negara berkembang seperti Indonesia. Dalam konteks ini, teknologi informasi memegang peranan yang sangat penting dalam kemajuan suatu negara (Rahmad, 2019)

Perkembangan teknologi yang saat ini mempengaruhi kehidupan masyarakat global adalah teknologi informasi berupa internet. Pada awalnya, internet hanya dikembangkan untuk keperluan militer, riset, dan pendidikan, namun kemudian berkembang hingga merasuki berbagai aspek kehidupan manusia di seluruh dunia. Saat ini, internet telah menjadi faktor pembentuk masyarakat dengan budaya yang baru, di mana pembatasan wilayah antar negara menjadi lebih fleksibel. Namun, di balik kilau gemerlapnya, internet juga membawa berbagai tantangan baru, termasuk meningkatnya kompleksitas kejahatan siber yang semakin canggih (Kaimuddin Haris et al., 2023)

Cybercrime atau yang dikenal juga sebagai kejahatan dunia maya adalah istilah yang merujuk pada tindakan kejahatan yang menggunakan komputer atau jaringan komputer sebagai alat, target, atau tempat terjadinya tindakan kejahatan. Dalam Kongres Perserikatan Bangsa-Bangsa (PBB) ke-10 yang diselenggarakan di Wina, Austria, pada tanggal 10-17 April 2000, istilah cybercrime dibagi menjadi dua kategori, yaitu cybercrime dalam pengertian sempit (kejahatan komputer) dan cybercrime dalam pengertian luas (kejahatan terkait komputer) (Akbar & Putra, 2014) dengan definisi yang lebih rinci sebagai berikut:

1. Kejahatan komputer (cybercrime dalam arti sempit): Merupakan setiap perilaku hukum yang dilakukan melalui operasi elektronik yang bertujuan untuk mengancam keamanan sistem komputer dan data yang diolah olehnya.
2. Kejahatan terkait komputer (cybercrime dalam arti luas): Merupakan segala tindakan ilegal yang dilakukan melalui sistem atau jaringan komputer, termasuk tindakan kejahatan seperti kepemilikan ilegal, penawaran, atau distribusi informasi melalui sistem atau jaringan komputer (Akbar & Putra, 2014)

Selain itu, perkembangan teknologi yang terus berkembang telah membawa berbagai implikasi yang perlu diantisipasi dan diwaspadai. Upaya untuk mengatasi dampak dari perkembangan ini telah menghasilkan produk hukum dalam bentuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik (UU ITE). Namun, meskipun UU ITE telah ada, belum semua aspek permasalahan terkait ITE dapat diatasi. Salah satu permasalahan utamanya adalah bahwa tidak semua orang yang menggunakan teknologi informasi dan praktisi hukum mengenal UU ini (Winarni, 2016)

Dalam praktiknya, masih banyak peraturan yang berkaitan dengan tindakan kriminal atau tindakan yang dapat dikenai hukuman yang belum termasuk dalam cakupan Undang-Undang ITE, seperti aspek-aspek yang dijelaskan dalam buku 1 KUHP yang tidak diakomodasi dalam Undang-Undang ITE (Winarni, 2016) Di Indonesia, walaupun telah ada peraturan untuk melawan kejahatan komputer, masih terdapat kendala dalam upaya penanggulangan dan pemberantasannya. Penanganan kasus cybercrime sering mengalami hambatan, terutama dalam hal penangkapan tersangka dan penyitaan barang bukti. Saat melakukan penangkapan tersangka, sering kali sulit untuk mengidentifikasi dengan pasti siapa pelakunya karena tindakan kejahatan tersebut dapat dilakukan melalui komputer dari mana saja tanpa adanya saksi yang dapat menyaksikannya secara langsung. Hasil pelacakan sering kali hanya dapat mencapai IP Address dari pelaku dan komputer yang digunakan. Kesulitan semakin meningkat jika pelaku menggunakan warnet (warung internet), karena saat ini jarang sekali warnet yang mewajibkan registrasi terhadap pengguna layanan mereka, sehingga sulit untuk mengetahui siapa yang menggunakan komputer tersebut ketika tindak pidana terjadi (Pahajow, 2016)

Menurut Widodo, cybercrime dapat diartikan sebagai kegiatan individu, kelompok, atau badan hukum yang menggunakan komputer sebagai alat untuk melakukan kejahatan, baik sebagai pelaku maupun sasaran dari kejahatan tersebut. Beberapa jenis kejahatan yang sering terjadi di Internet meliputi:

1. Illegal access/unauthorized access to computer system and service

Ini adalah bentuk kejahatan yang terjadi ketika seseorang meretas atau masuk ke dalam suatu sistem jaringan komputer tanpa izin dari pemilik sistem tersebut.

1. Illegal contents

Kejahatan ini terkait dengan penyebaran data atau informasi yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum di internet.

1. Data forgery

Kejahatan ini melibatkan pemalsuan data atau dokumen penting yang disimpan dalam format digital melalui internet. Biasanya, penjahat mencoba memanipulasi data e-commerce untuk menguntungkan diri mereka sendiri, seperti mendapatkan data pribadi dan nomor kartu kredit korban.

1. Cyber espionage

Ini adalah bentuk kejahatan yang melibatkan penyusupan ke sistem jaringan komputer pihak lain untuk tujuan mata-mata.

1. Cyber sabotage and extortion (sabotase dan pemerasan dunia maya)

Jenis kejahatan ini melibatkan gangguan, kerusakan, atau penghancuran data, program komputer, atau sistem jaringan komputer melalui internet. Biasanya dilakukan dengan memasukkan virus komputer, logic bomb, atau program berbahaya lainnya.

1. Offense against intellectual property (pelanggaran terhadap Hak atas Kekayaan Intelektual)

Kejahatan ini menargetkan hak kekayaan intelektual milik pihak lain di Internet, seperti meniru tampilan website orang lain secara ilegal.

1. Infringements of privacy

Jenis kejahatan ini biasanya mengincar informasi pribadi yang disimpan dalam format digital, seperti data pribadi yang tersimpan dalam formulir. Pengetahuan orang lain terhadap informasi ini dapat menyebabkan kerugian bagi korban baik secara materiil maupun immaterial, seperti kebocoran nomor PIN ATM dan lainnya (Rokhman & Liviani, 2020)

Undang-undang tentang Informasi dan Transaksi Elektronik, yang sering disingkat sebagai UU ITE, awalnya diberlakukan melalui Undang-undang nomor 11 tahun 2008. Namun, kemudian mengalami revisi dengan UU No. 19 Tahun 2016. UU ITE mengatur berbagai aspek terkait informasi, transaksi elektronik, dan teknologi informasi secara umum. Undang-undang ini disahkan oleh Presiden Susilo Bambang Yudhoyono dan DPR RI, dan resmi berlaku pada tanggal 21 April 2008. Artinya, UU ini memiliki cakupan yang berlaku bagi individu yang terlibat dalam aktivitas hukum sebagaimana dijelaskan dalam Undang-Undang ini, baik berada di dalam wilayah hukum Indonesia maupun di luar wilayahnya. Undang-undang ini berlaku jika perbuatan tersebut memiliki dampak hukum di dalam dan di luar wilayah hukum Indonesia serta berpotensi merugikan kepentingan Indonesia (Arief, 2022)

1. **Metode**

Penelitian ini menerapkan pendekatan kualitatif, khususnya mengadopsi pendekatan penelitian hukum normatif sebagai kerangka dasarnya (Robbani & Yuliana, 2022) Data yang dihasilkan dari penelitian ini bersifat deskriptif, meliputi informasi tertulis maupun lisan yang diperoleh melalui wawancara dengan individu serta pengamatan perilaku.

Selain itu, penelitian ini juga menggabungkan pendekatan penelitian hukum normatif, dengan fokus pada eksplorasi hukum positif, prinsip-prinsip hukum, struktur hukum, serta sejauh mana keselarasan vertikal dan horizontal dapat dicapai (Putranto & Harvelian, 2023)

Metode studi kepustakaan juga menjadi komponen penting dalam penelitian ini, dipilih karena sumber literatur yang digunakan melibatkan berbagai referensi, seperti buku, jurnal ilmiah, dan tulisan lainnya. Pendekatan peraturan perundang-undangan (statute approach) digunakan untuk mengumpulkan semua undang-undang dan regulasi yang relevan dengan isu hukum yang sedang diteliti, terutama dalam konteks regulasi keamanan siber di Indonesia (Dames Lewansorna et al., 2022)

Dalam proses penelitian ini, sumber hukum dibagi menjadi dua kategori, yaitu sumber utama dan sumber sekunder. Sumber utama mencakup semua dokumen hukum yang dikeluarkan oleh lembaga pemerintahan yang memiliki kewenangan dalam merumuskan peraturan hukum, serta dokumen yang memiliki keterkaitan hukum dengan pihak-pihak yang terlibat dalam proses pembuatannya dan memiliki kekuatan mengikat (Irawan, 2020). Di sisi lain, sumber sekunder merujuk pada materi hukum yang memiliki pengaruh yang kurang signifikan secara hukum, tetapi memiliki nilai persuasif dan digunakan sebagai referensi dan dukungan bagi sumber utama (Irawan, 2020) Dalam upaya mencari materi hukum, pendekatan studi kepustakaan digunakan, dan analisis kualitatif diterapkan untuk mengevaluasi temuan (Lewansorna et al., 2022)

1. **Hasil dan Pembahasan**

**Hasil**

Sistem perundang-undangan di Indonesia tidak secara eksplisit mengatur tentang hukum siber, namun sejumlah undang-undang telah digunakan untuk mengendalikan kejahatan siber. Contohnya, Undang-undang No. 36 tahun 1999 tentang Telekomunikasi, Undang-undang No. 19 tahun 2002 tentang Hak Cipta, Undang-undang No. 15 tahun 2003 tentang Pemberantasan Terorisme, dan Undang-undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Melalui undang-undang dan peraturan ini, jenis kejahatan di dunia maya (cybercrime) telah dianggap sebagai tindakan ilegal, dengan ancaman hukuman bagi pelanggarnya (Rokhman & Liviani, 2020)

Di samping itu, kebijakan kriminalisasi yang terkait dengan kejahatan siber juga telah diuraikan dalam Rancangan Kitab Undang-Undang Hukum Pidana (RKUHP) yang dapat ditemukan di Buku Kedua (Bab VIII): Tindak Pidana yang Membahayakan Keamanan Umum bagi Orang, Barang, Lingkungan Hidup. Bagian ini, khususnya Pasal 373-379, mengatur berbagai tindak pidana seperti illegal access, illegal interception, data interference dan system interference, penyalahgunaan nama domain, dan pornografi anak (Rokhman & Liviani, 2020)

Jika terjadi tindak kejahatan yang melibatkan situasi tersebut, konsekuensinya adalah penerapan Pasal 50 yang berbunyi,“Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah) (Kaimuddin Haris et al., 2023)

Dalam menghadapi perkembangan hukum pidana di masa depan, penanganan dan pencegahan kejahatan siber harus diiringi dengan peningkatan dan pengembangan keseluruhan kerangka hukum pidana, termasuk pembangunan struktur, budaya, serta substansi hukum pidana (Liviani, 2020). Di Indonesia, meskipun peraturan untuk melawan kejahatan komputer telah ada, masih terdapat sejumlah kendala dalam upaya penanggulangan dan pemberantasan kejahatan tersebut. Penanganan kasus cybercrime sering menghadapi kesulitan, terutama dalam hal penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka, sering kali sulit untuk mengidentifikasi pelaku dengan pasti karena pelanggaran tersebut dapat dilakukan melalui komputer di lokasi yang berbeda tanpa adanya saksi langsung. Hasil pelacakan terkadang hanya dapat mencapai IP Address pelaku dan komputer yang digunakan. Kendala semakin meningkat jika pelaku menggunakan warnet (warung internet), karena saat ini jarang ada warnet yang mewajibkan pengguna jasanya melakukan registrasi, sehingga sulit untuk mengetahui siapa yang menggunakan komputer tersebut ketika terjadi tindak pidana (Pahajow, 2016)

**Pembahasan**

Undang-undang tentang Informasi dan Transaksi Elektronik, yang sering disingkat sebagai UU ITE, awalnya diberlakukan melalui Undang-undang nomor 11 tahun 2008. Namun, kemudian mengalami revisi dengan UU No. 19 Tahun 2016. UU ITE mengatur berbagai aspek terkait informasi, transaksi elektronik, dan teknologi informasi secara umum. Undang-undang ini disahkan oleh Presiden Susilo Bambang Yudhoyono dan DPR RI, dan resmi berlaku pada tanggal 21 April 2008. Artinya, UU ini memiliki cakupan yang berlaku bagi individu yang terlibat dalam aktivitas hukum sebagaimana dijelaskan dalam Undang-Undang ini, baik berada di dalam wilayah hukum Indonesia maupun di luar wilayahnya. Undang-undang ini berlaku jika perbuatan tersebut memiliki dampak hukum di dalam dan di luar wilayah hukum Indonesia serta berpotensi merugikan kepentingan Indonesia (Arief, 2022)

Undang-Undang yang sedang berlaku dalam mengatur tentang kejahatan cybercrime saat ini adalah Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hal ini dikarenakan dengan pesatnya perkembangan teknologi informasi, ada kebutuhan untuk memperhatikan upaya penyempurnaan dan perbaikan Kitab Undang-Undang Hukum Pidana Nasional. Dengan semakin banyaknya kejahatan yang muncul sebagai hasil dari kemajuan teknologi informasi, terutama dalam bentuk cybercrime, penting untuk mengadaptasi alat bukti sesuai dengan perkembangan ilmu pengetahuan dan teknologi (IPTEK), termasuk penggunaan alat bukti berbasis teknologi seperti surat elektronik (electronic mail) dan rekaman elektronik (Kaimuddin Haris et al., 2023)

Salah satu karakteristik dari kejahatan cybercrime adalah pemanfaatan jaringan telematika global, yang mencakup telekomunikasi, media, dan informatika. Aspek global ini menciptakan situasi di mana dunia terasa tanpa batas (borderless), yang berarti bahwa pelaku, korban, dan lokasi tindak pidana (locus delicti) dapat berada di berbagai negara yang berbeda (Herman, 2023; Singgi, 2020)

Menyusun dan menetapkan tindakan-tindakan yang dapat dikenakan sanksi pidana dalam konteks lingkungan yang relatif baru dan dinamis bukanlah tugas yang sederhana. Oleh karena itu, untuk menangani pelaku kejahatan di dunia maya (cybercrime), lembaga penafsiran hukum (interpretasi) dapat digunakan sebagai sarana untuk menghindari terjadinya kekosongan hukum (Kaimuddin Haris et al., 2023)

Meskipun masih ada masalah terkait kurang memadainya infrastruktur digital yang mendukung ketahanan siber, serta tantangan dalam pengalokasian investasi yang sesuai, penting bagi Indonesia untuk memiliki kerangka hukum yang mengatur ketahanan siber. Terdapat empat fokus utama yang harus diperhatikan dalam pembentukan regulasi ketahanan siber ini. Pertama, harus ada perhatian terhadap keamanan data digital yang dapat menjamin bahwa tidak ada pihak yang dapat mengakses atau menggunakan data tanpa izin atau hak yang sah dari negara. Kedua, regulasi tersebut juga perlu mencakup aspek manfaat digital, termasuk pengembangan infrastruktur digital dan regulasi persaingan dalam konteks bisnis digital. Ketiga, penting untuk meningkatkan kerjasama siber dalam upaya menegakkan kedaulatan digital mengingat sifat global dunia digital. Keempat, regulasi harus mencakup ketentuan sanksi yang tegas terhadap pelanggaran kedaulatan digital untuk memastikan perlindungan tersebut efektif (Arief, 2022)

Pentingnya mengembangkan Rancangan Undang-Undang (RUU) Ketahanan dan Keamanan Siber (KKS) untuk segera disahkan mengemuka atas dasar tiga pertimbangan utama (Arief, 2022). Pertama, hukum siber memiliki lingkup yang luas, karena mencakup perlindungan terhadap penggunaan teknologi internet, yang tidak hanya melibatkan negara sebagai pengguna, tetapi juga individu warga negara biasa dan sektor bisnis. Hukum siber berperan dalam menjaga kepentingan seluruh individu yang terkoneksi melalui internet. Kedua, sebagai negara yang mendukung komitmen internasional, Indonesia perlu mengikuti kesepakatan global dalam upaya mempromosikan internet yang terbuka, aman, dan damai. Sulit untuk mencapai tujuan tersebut jika pembahasan RUU KKS dilakukan secara tertutup. Ketiga, perumusan hukum siber yang tertutup akan merusak reputasi Indonesia sebagai negara demokratis yang seharusnya mendorong kebebasan media dan menghargai kebebasan berekspresi. Terlebih lagi, sejarah Indonesia menunjukkan bahwa pembatasan internet telah terjadi dalam beberapa situasi, seperti saat pengumuman hasil Pemilu 2019 dan dalam kasus kerusuhan di Papua. Tanpa keterbukaan informasi mengenai perumusan RUU KKS kepada publik, sulit bagi masyarakat sipil untuk memantau apakah pembatasan internet di masa depan akan didasarkan pada alasan yang jelas, parameter situasi darurat, dan upaya mitigasi dampak yang transparan. Dua kasus pembatasan internet sebelumnya telah berdampak negatif pada perekonomian masyarakat (Arief, 2022)

1. **Kesimpulan**

Dalam era globalisasi teknologi informasi yang sedang berlangsung, perkembangan pesat dalam bidang ini telah mengubah tatanan dunia secara signifikan. Teknologi informasi dan internet telah menjadi bagian integral dari kehidupan sehari-hari, merambah ke berbagai aspek kehidupan masyarakat global. Namun, bersamaan dengan kemajuan ini, kejahatan siber telah menjadi ancaman yang semakin kompleks dan serius.

Kajian ini mencermati pentingnya pembentukan Rancangan Undang-Undang Ketahanan dan Keamanan Siber (KKS) dalam konteks Indonesia. Meskipun telah ada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik (UU ITE) yang mengatur sebagian masalah terkait kejahatan siber, masih banyak aspek yang belum tercakup dalam kerangka hukum ini. Kejahatan siber mencakup berbagai tindakan ilegal, mulai dari peretasan hingga penyebaran informasi palsu, dan penanganannya memerlukan perhatian khusus.

Penelitian ini menggarisbawahi pentingnya RUU KKS yang berfokus pada ketahanan dan keamanan siber. RUU ini harus dirancang secara transparan dan melibatkan berbagai pihak, termasuk masyarakat sipil, untuk memastikan bahwa pembatasan internet dan kebijakan terkait teknologi informasi didasarkan pada alasan yang jelas dan dapat dipertanggungjawabkan. Selain itu, RUU KKS harus mencakup ketentuan sanksi yang tegas terhadap pelanggaran kedaulatan digital.

Dalam menghadapi perkembangan teknologi yang terus berlanjut, Indonesia harus memperkuat kerangka hukumnya untuk mengatasi ancaman kejahatan siber. Dengan adanya RUU KKS yang kuat dan komprehensif, diharapkan bahwa negara dan masyarakat dapat lebih baik melindungi diri dari berbagai ancaman di dunia maya dan memastikan ketahanan siber yang lebih baik untuk masa depan.

**Daftar Pustaka**

Akbar, O. :, & Putra, K. (2014). HARMONISASI KONVENSI CYBER CRIME DALAM HUKUM NASIONAL. *Jurnal Ilmu Hukum*. http://id.wikipedia.org/wiki/Kejahatan\_dunia\_maya,

Arief, M. (2022). Urgensi Regulasi Ketahanan dan Keamanan Siber dalam Undang-Undang ITE. *JULIA : Jurnal Litigasi Amsir*, *9*(4). https://id.wikipedia.org/wiki/UndangUndang\_Infor

Dames Lewansorna, Rina, E., Toule, M., & Sopacua, M. (2022). *Pertanggungjawaban Pidana Aparat Kepolisian Yang Melakukan Kekerasan Terhadap Demonstran* (Vol. 2, Issue 1).

Irawan, V. (2020). ANALISIS YURIDIS TERHADAP PELANGGARAN HAK CIPTA PERMAINAN VIDEO (VIDEO GAMES) BERUPA PEMBAJAKAN SECARA ONLINE. In *Journal of Intellectual Property* (Vol. 3, Issue 2). www.journal.uii.ac.id/JIPRO

Kaimuddin Haris, O., Hidayat, S., & Dwitasari, R. (2023). Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia Carding Crime as a Form of Cyber Crime in Indonesian Criminal Law. In *Halu Oleo Legal Research |* (Vol. 5, Issue 2). https://www.hukumonline.com/klinik/a/tindak-pidana-cyber-crime-cl2824/.

Pahajow, A. A. J. (2016). PEMBUKTIAN TERHADAP KEJAHATAN DUNIA MAYA DAN UPAYA MENGATASINYA MENURUT HUKUM POSITIF DI INDONESIA. *Lex Crimen*, *5*(2). https://balianzahab.wordpress.com/artikel/penyidikan-

Putranto, R. D., & Harvelian, A. (2023). Tanggung Jawab Pelaku Usaha dalam Transaksi Elektronik melalui Situs Internet di Tinjau dari Perspektif Hukum Perlindungan Konsumen. *FOCUS*, *4*(1), 36–41. https://doi.org/10.37010/fcs.v4i1.1153

Rahmad, N. (2019). Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online. *JHES-Jurnal Hukum Ekonomi Syariah*, *3*(2).

Robbani, H., & Yuliana, N. (2022). Analysis of Factors Affecting Learning Difficulties during the Covid 19 Pandemic. *FOCUS*, *3*(1), 55–58. https://doi.org/10.37010/fcs.v3i1.537

Rokhman, M., & Liviani, H.-I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qānūn: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2).

Winarni, R. R. (2016). EFEKTIVITAS PENERAPAN UNDANG – UNDANG ITE DALAM TINDAK PIDANA CYBER CRIME. *Hukum Dan Dinamika Masyarakat*, *14*(1).