JURNAL HUKUM SASANA, Volume 10, Iss. 2 (2024), pp. 105 - 123
ISSN 2461-0453 (print) | ISSN 2722-3779 (online)
Available online at: http://ejurnal.ubharajaya.ac.id/index.php/SASANA

Globalisasi Digital Dan *Cybercrime*: Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas

Clara Ignatia Tobing[1], Tiofanny Marylin Surya[2], Liris Roesa Selvias[3], Stepania Rehulina Girsang[4], Putri Berliana Azzahra[5], Lustri Yolanda Purba[6], Mahezha Agnia Putera[7], Nurrahman Rusmana[8]
[1,2,3]Universitas Bhayangkara Jakarta Raya
Email: clara.tobing@ubharajaya.co.id, tiofannymarylin@yahoo.com, lirisselvias@gmail.com, stepania3057@gmail.com, putriberlianaazzahra@gmail.com, lustriyolanda@gmail.com, mahezhap16@gmail.com, anunnurrahman@gmail.com

DOI : https://doi.org/10.31599/sasana.v10i2.3170

Received:
04-11-2024

Revised:
09-12-2024

Accepted:
27-12-2024

Abstract: *As the digital era advances, the threat of cybercrime has become an increasingly pressing issue in Indonesia. Although various laws have been implemented to address cybercrime, including the Electronic Information and Transactions Law (UU ITE), challenges persist, particularly in handling cross-border cybercrime. Legal gaps and regulatory differences between countries complicate effective international cooperation. This study examines the impact of digital globalization on the rise of cybercrime in Indonesia and highlights the legal challenges in enforcing justice against foreign cybercrime offenders. Using a normative-juridical approach, this research analyzes existing policies and emphasizes the importance of enhancing international collaboration to strengthen law enforcement against cross-border cybercrime.*

Keywords: *Cybercrime, Digital Globalization, Law Enforcement.*

Abstrak
Seiring berkembangnya era digital, ancaman kejahatan siber menjadi isu yang semakin marak di Indonesia. Meskipun berbagai undang-undang telah diimplementasikan untuk menangani kejahatan siber, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), tantangan tetap muncul, terutama dalam penanganan kejahatan siber lintas negara. Kekosongan hukum dan perbedaan regulasi antarnegara memperumit kerja sama internasional yang efektif. Studi ini membahas dampak globalisasi digital terhadap peningkatan kejahatan siber di Indonesia, serta menyoroti berbagai tantangan hukum dalam menegakkan keadilan terhadap pelaku kejahatan siber dari luar negeri. Dengan pendekatan yuridis-normatif, penelitian ini menganalisis kebijakan yang ada dan pentingnya peningkatan kolaborasi internasional untuk memperkuat penegakan hukum terhadap kejahatan siber lintas batas.

Kata Kunci: Kejahatan Siber, Globalisasi Digital, Penegakan Hukum.

PENDAHULUAN

Dunia modern saat ini ditandai dengan meningkatnya interaksi global yang semakin luas dan intensif di berbagai bidang, seperti politik, ekonomi, sosial, budaya, dan telekomunikasi. Perkembangan teknologi di bidang transportasi, telekomunikasi, internet, serta teknologi komputer dan digital telah mempercepat interaksi ini. Abad ke-21 menjadi periode penting di mana hubungan antarnegara terjadi dalam skala besar, didorong oleh kemajuan teknologi dalam transportasi, telekomunikasi, internet, serta teknologi komputer dan digital.[1]

Perubahan ini menghasilkan fenomena yang disebut globalisasi, yang telah mengubah dunia dari batas-batas wilayah yang kaku menjadi lebih fleksibel dan terbuka.[2] Globalisasi telah menjadi isu penting yang terus diperbincangkan hingga saat ini, meskipun waktu dan tempat pastinya masih menjadi perdebatan. Fase globalisasi modern diperkirakan dimulai setelah tahun 1960-an, didorong oleh kemajuan pesat dalam transportasi darat, laut, dan udara, serta perkembangan komunikasi dan teknologi informasi yang semakin meluas di seluruh dunia.[3]

Globalisasi telah memperkuat saling ketergantungan (interdependence) antarnegara, ditandai oleh peningkatan besar-besaran dalam perdagangan global, arus modal, akses yang lebih mudah terhadap teknologi asing, serta penggunaan sumber daya internasional untuk pembangunan, termasuk bantuan internasional. Ekspansi ini turut juga menciptakan peluang baru bagi negara-negara untuk memanfaatkan sumber daya yang sebelumnya tidak tersedia bagi mereka dalam upaya pembangunan nasional.[4]

Salah satu ciri dari globalisasi adalah perkembangan teknologi[5] yang kemudian menjadi cikal bakal timbulnya globalisasi digital. Globalisasi digital mengacu pada proses dimana teknologi digital, terutama internet dan perangkat komunikasi, mempercepat dan memperluas interaksi dan integrasi antara individu, perusahaan, dan negara di seluruh dunia. Dalam era globalisasi digital, batas-batas geografis menjadi semakin tidak relevan karena

---

[1] Ariesani Hermawanto dan Melaty Anggraini Globalisasi, *Revolusi Digital dan Lokalitas: Dinamika Internasional dan Domestik di Era Borderless World*, Yogyakarta: LPPM Press. 2020, hlm.1.
[2] *Ibid*, hlm.2.
[3] A,G Hopkins, "Globalisation and Decolonisation", *The Journal of Imperial and Commonwealth History,* Vol. 45, No.5, 2017.
[4] Ernest Aryeetey and Natalia Dinello (eds), *Testing Global Interdependence Issues on Trade, Aid, Migration and Development*, Massachusetts: Edward Elgar Publishing, Inc.,2007, hlm. 14.
[5] Tranggono, et.al, "Pengaruh Perkembangan Teknologi di Era Globalisasi dan Peran Pendidikan Terhadap Degradasi Moral Pada Remaja", *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance,* Vol. 3 No. 2, 2023.

teknologi memungkinkan pertukaran informasi, layanan, dan produk secara instan dan lintas batas.[6]

Teknologi digital yang berkembang dalam globalisasi ini tidak hanya mempermudah pertukaran barang dan jasa melalui platform e-commerce global, tetapi juga mempercepat arus modal dan investasi antar negara. Dengan kemudahan akses terhadap informasi pasar global, perusahaan dapat menganalisis tren konsumen dan menyesuaikan strategi pemasaran mereka secara real-time berkat kemampuan analitik yang ditawarkan oleh teknologi digital. Namun, tantangan dalam memanfaatkan potensi teknologi digital tidak boleh diabaikan. Perlindungan data pribadi dan keamanan siber menjadi isu utama yang perlu diatasi di tengah era digitalisasi ini.[7]

Cybercrime atau kejahatan siber diartikan sebagai tindak criminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Kejahatan ini memanfaatkan perkembangan teknologi komputer khususnya internet.[8] *Cybercrime* adalah tindak pidana yang memiliki beberapa karakteristik. Kejahatan ini mencakup akses tanpa izin yang bertujuan untuk memfasilitasi kejahatan. Selain itu, tindakan ini juga meliputi perubahan atau penghancuran data tanpa izin, serta mengganggu atau merusak operasi komputer. Tak kalah penting, *cybercrime* juga dapat mencakup tindakan yang mencegah atau menghambat akses ke komputer. Karakteristik-karakteristik ini menunjukkan betapa kompleks dan beragamnya bentuk kejahatan siber yang ada saat ini.[9]

Kejahatan siber termasuk dalam kategori kejahatan transnasional karena sifatnya yang melibatkan tindakan kriminal yang melampaui batas-batas negara. Kejahatan ini sering kali dilakukan oleh pelaku yang berada di satu negara tetapi menargetkan korban di negara lain, seperti seorang *hacker* di negara A yang dapat meretas sistem komputer di negara B tanpa harus berada di lokasi fisik tersebut. Perkembangan teknologi informasi dan komunikasi telah menciptakan ruang siber yang tidak terikat oleh batas-batas fisik, membuat pelaku dapat menggunakan internet untuk berkomunikasi, melakukan transaksi, dan menyembunyikan identitas mereka, sehingga menyulitkan penegakan hukum. Selain itu, banyak kejahatan siber melibatkan jaringan pelaku yang berkolaborasi secara internasional, berbagi informasi, alat, dan teknik untuk melakukan serangan, yang semakin memperkuat sifat transnasional

[6] Agus Wibowo, *Globalisasi Digital,* Semarang:Yayasan Prima Agus Teknik, 2023, hlm. 12.
[7] *Ibid,* hlm.4.
[8] Lita Sari Marita, "Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia", *Cakrawala:Jurnal Humaniora Unievrsitas Bina Sarana Informatika*, Vol.15 no.2, 2015.
[9] *Ibid.*

kejahatan ini.[10]

Variasi hukum mengenai kejahatan siber antara negara-negara juga menambah kesulitan dalam penanganan jenis kejahatan ini karena sering kali tidak ada kesepakatan internasional yang kuat mengenai cara menangani kejahatan ini, menciptakan kekosongan hukum yang dimanfaatkan oleh pelaku. Kejahatan siber dapat memiliki dampak luas dan merusak bagi ekonomi global, keamanan nasional, dan hubungan internasional. Misalnya, serangan *ransomware* dapat mempengaruhi operasi perusahaan di berbagai negara dan mengganggu rantai ekonomi internasional.[11]

Berdasarkan laporan data anomali trafik dari BSSN di tahun 2021, Indonesia mengalami serangan siber sebanyak 495,3 juta kali sepanjang tahun 2020. Melalui laporan tersebut, Indonesia menjadi salah satu negara dengan jumlah serangan kejahatan siber tertinggi. Laporan ini juga mencatat adanya 2.549 kasus phishing melalui email, dengan peningkatan yang signifikan antara Maret hingga Mei 2020. Selain itu, terjadi 79.439 insiden pelanggaran data dan 9.749 kasus perusakan situs web (*web defacement*), di mana sektor akademik mengalami jumlah kasus terbanyak sepanjang tahun tersebut.[12]

Salah satu serangan kejahatan siber ini misalnya terjadi di tahun 2017, saat terjadi insiden virus komputer di Indonesia *Malware Ransomware Wannacry* yang menginfeksi sistem di Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta. Data-data di komputer yang terinfeksi terenkripsi karena adanya *Ransomware Wannacry*. Seragan ini mengakibatkan lumpuhnya sistem antrian Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais karena serangan tersebut mengunci semua data dan mengganggu sistem teknologi informasi yang menyimpan seluruh data kesehatan pasien juga catatan pembayaran rumah sakit.[13] Serangan ransomware *WannaCry* pada Mei 2017 tidak hanya berdampak pada Indonesia, tetapi juga melanda banyak negara di seluruh dunia. Di Inggris, Prancis, Spanyol, Jerman dan Brasil juga menjadi korban dari serangan ini. Pemerintah Amerika Serikat mencurigai bahwa sekelompok teroris digital dari Korea Utara adalah dalang dari serangan-serangan tersebut.[14]

---

[10] Gianpiero Greco, Nicola Montinaro, "The Phenomenon Of Cybercrime: From The Transnational Connotation To The Need For Globalization Of Justice", *European Journal of Social Sciences Studies,* Vol.6 ,No. 1, 2021.

[11] *Ibid.*

[12] Ratna Christianingrum dan Ade Nurul Aida, Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan Nasional , diakses dari https://berkas.dpr.go.id/pa3kn/analisis-apbn/public-file/analisis-apbn-public-65.pdf pada 9 Oktober 2024 pukul 20.35 WIB.

[13] Gilang Ramadhan, "Perlidungan Hukum Bagi Korban Ransomware Wannacry: Tindak Pidana Ransomware", *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat,* Vol.1 No.2, 2023.

[14] Radosław Fordoński, Wojciech Kasprzak, "WannaCry Ransomware Cyberattack As Violation Of International Law", *Studia Prawnoustrojowe Journal*, No.44, 2019.

Kemudian, beberapa *e-commerce* di Indonesia juga telah mengalami peretasan sejak tahun 2019. Peretasan ini diawali oleh Gnosticplayers yang mengklaim mencuri sekitar 13 juta data pengguna Bukalapak. Kumpulan data pengguna itu dihargai US$ 5.000 atau Rp 74,5 juta dengan kurs Rp 14.900/US$. Awal Mei 2020 Tokopedia pun mengalami kebocoran data. Terdapat 91 juta data pengguna dan lebih dari tujuh juta data *merchant* berhasil diperdagangkan dengan US$ 5.000 atau Rp 74,5 juta. Jenis data yang diambil berupa nama, e-mail, dan kata sandi pengguna. ShinyHunters, sebuah kelompok hacker internasional kemudian diketahui sebagai dalang kelompok peretas yang menyerang Tokopedia.[15] Kemudian, pada tahun 2021 juga terjadi kebocoran data yang diduga berasal dari BPJS Kesehatan, yang mencakup data aparatur sipil negara (ASN). 279 juta data penduduk Indonesia, termasuk ASN, TNI, dan Polri yang berisi nama, nomor telepon, alamat, gaji, dan data kependudukan dijual di beberapa forum internet. Kejadian ini diduga dilakukan oleh kelompok *hacker* internasional Lockbit.[16]

Sebagai negara hukum, Indonesia memiliki kewajiban melindungi warganya dari ancaman yang merugikan, termasuk kejahatan siber. Meskipun belum ada undang-undang khusus mengenai kejahatan siber, beberapa peraturan seperti Undang-undang Telekomunikasi No. 36 Tahun 1999, UU Hak Cipta No. 19 Tahun 2002, Undang-undang Pemberantasan Terorisme No. 15 Tahun 2003, dan Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah mengatur pencegahan dan penindakan kejahatan siber. Kejahatan siber melibatkan segala tindakan kriminal yang menggunakan sistem elektronik, seperti terorisme, perdagangan manusia, dan pencucian uang. Undang-undang ITE mengatur lebih spesifik tentang kejahatan siber, termasuk akses ilegal, penyebaran konten ilegal seperti pornografi dan fitnah, serta ancaman siber lainnya.

Namun, perlu diingat bahwa permasalahan kejahatan siber lintas negara adalah salah satu tantangan terbesar dalam dunia digital saat ini. Kejahatan ini melibatkan pelaku dari berbagai negara yang melakukan serangan terhadap sistem elektronik atau data yang berada di negara lain. Kejahatan siber lintas negara bisa berupa serangan hacking, pencurian identitas, penyebaran malware, atau pembobolan data pribadi. Tantangan utamanya adalah bahwa pelaku kejahatan sering berada di yurisdiksi yang berbeda, sehingga sulit bagi negara

[15] Sendi Eka Nanda, Winda Widyaningsih, "Pengaruh Terpaan Berita Peretasan Tokopedia Terhadap Reputasi Perusahaan", *Broadcasting Communication Journal,* Vol.3 No.1, 2021.
[16] Muhammad Izzar Damargara, Muhammad Alhidayah, Muhammad Raihan Faiqy, Jatnika Maulana, "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi", *Padjadjaran Law Review,* Vol.10 No.1, 2022.

korban untuk menegakkan hukum terhadap pelaku tersebut.

Di Indonesia, meskipun sudah ada beberapa undang-undang yang mengatur kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), belum ada aturan hukum khusus yang secara eksplisit mengatur kejahatan siber lintas negara. Hal ini menyebabkan adanya kekosongan hukum dalam penegakan terhadap kejahatan yang dilakukan oleh pelaku dari luar negeri. Proses hukum untuk menangani kejahatan siber lintas negara menjadi kompleks karena melibatkan kerja sama antar negara, yang membutuhkan perjanjian ekstradisi dan koordinasi antara penegak hukum internasional. Permasalahan ini semakin diperumit oleh perbedaan regulasi di setiap negara. Setiap negara memiliki standar hukum siber yang berbeda-beda, yang dapat menghambat penegakan hukum lintas batas. Untuk mengatasi ini, diperlukan kerjasama internasional yang lebih kuat serta pembentukan regulasi yang dapat mengikat pelaku kejahatan siber lintas negara secara efektif.

METODE PENELITIAN

Penelitian ini merupakan kajian hukum yuridis-normatif, yang berfokus pada analisis ketentuan peraturan perundang-undangan yang berlaku sebagai hukum positif di Indonesia. Data sekunder untuk penelitian ini dikumpulkan melalui studi kepustakaan yang terkait dengan isu hukum atau permasalahan yang diangkat. Data sekunder kemudian dianalisis secara kualitatif dengan pendekatan sistematis untuk menghasilkan kesimpulan yang sesuai dengan permasalahan yang dikaji. Data penelitian disajikan dalam kalimat yang jelas, efektif, teratur, logis, dan runtut, sehingga memudahkan analisis dan pembahasan terhadap permasalahan penelitian.

PEMBAHASAN

Tinjauan Umum Kejahatan Siber

Cybercrime atau kejahatan siber diartikan sebagai tindak criminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Kejahatan ini memanfaatkan perkembangan teknologi komputer khususnya internet.[17] *Cybercrime* adalah tindak pidana yang memiliki empat elemen utama, yaitu: lokasi pelaku terkait dengan tempat kejadian, korban, pelaku dan upaya yang dilakukan untuk mengatasi ancaman tersebut.[18]

[17] Lita Sari Marita, *Op Cit.*
[18] David L. Speer, "Redefining Borders: The Challenges Of Cybercrime", *Crime, Law & Social Change Journal,* No. 34, 2000.

a. Lokasi

Lokasi pelaku kejahatan terkait dengan tempat kejadian merupakan karakteristik kejahatan siber yang paling membedakannya dari jenis kejahatan lainnya. Dalam ancaman tradisional, pelaku biasanya hadir secara fisik di lokasi kejahatan, sehingga aparat penegak hukum dapat menangkap dan membawa mereka ke pengadilan. Namun, dalam kasus kejahatan siber, pelaku seringkali tidak berada di lokasi kejadian, sehingga penangkapan menjadi sulit. Banyak pelaku justru berada di negara atau wilayah lain, sehingga kerjasama antar aparat penegak hukum dari berbagai negara menjadi sangat penting.

b. Korban

Selain tantangan kerjasama dan yurisdiksi, terdapat pula masalah dalam menangani berbagai macam korban kejahatan siber. Korban utama adalah pemerintah dan berbagai agensinya, perusahaan, dan organisasi, masing-masing memiliki tujuan yang seringkali bertentangan satu sama lain, yang menghambat upaya bersama untuk mengeliminasi kejahatan siber. Selain itu, banyak kejahatan siber juga terjadi terhadap individu, namun perhatian terhadap korban individu seringkali terbatas karena mereka memiliki pengaruh yang minim terhadap pemerintah.

c. Legislasi mengenai kejahatan siber juga terhambat oleh tuntutan yang bersaing dari lobi-lobi korban. Sebagai contoh, pemerintah Amerika Serikat telah membentuk Jaringan Deteksi Intrusi Federal (FIDNET), yang bertujuan untuk memantau komputer pemerintah dari pelanggaran keamanan. Namun, upaya untuk memusatkan FIDNET di bawah *Federal Bureau of Investigation* (FBI) mendapatkan tentangan dari organisasi, perusahaan, dan individu karena dianggap sebagai pelanggaran privasi dan berpotensi disalahgunakan. Ketidakpuasan terhadap kontrol ini menciptakan ketegangan antara pihak-pihak yang khawatir akan privasi mereka dan kebutuhan untuk melindungi dari kejahatan siber.

d. Pelaku

Aspek lain dari ancaman ini adalah pelaku dan motif serta niat mereka. Di satu sisi, pelaku bisa saja pelakunya adalah remaja yang mencoba mengakses komputer orang lain untuk bersenang-senang atau membuktikan kemampuan di depan teman-teman mereka. Di sisi lain, pelaku bisa juga adalah individu dewasa yang ingin merusak sistem komputer atau mencuri informasi sensitive. Namun, banyak pelanggaran yang terjadi di area abu-abu di mana individu atau kelompok mungkin tidak menyadari bahwa tindakan mereka

adalah kejahatan atau tidak memahami konsekuensi dari tindakan tersebut. Misalnya, tindakan membajak perangkat lunak dari teman dapat dianggap sebagai kejahatan tanpa disadari oleh pelakunya, terutama di kalangan orang-orang yang baru mengenal dunia komputer. Hal ini membuat pengawasan terhadap individu dengan potensi melakukan kejahatan siber menjadi sulit.

Kejahatan siber ini sering menyasar baik individu maupun perusahaan besar. Penyerang umumnya mengarahkan perhatian mereka pada organisasi dengan tujuan mendapatkan keuntungan finansial secara langsung atau merintangi serta merusak operasi mereka. Selain itu, mereka juga berusaha menipu individu dengan skala besar atau merusak perangkat teknologi untuk digunakan sebagai basis pelaksanaan aktivitas kejahatan mereka. Kejahatan siber sendiri dibagi menjadi 2 kategori, yakni Kejahatan siber dalam pengertian sempit dan dalam pengertian luas. Kejahatan siber dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan Kejahatan siber dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer. [19] Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*) yang digagas oleh Uni Eropa kemudian membahas ini lebih lanjut dan mengelompokkan jenis tindak pidana siber yang dikelompokan dalam empat kategori tindak kejahatan atau pidana, yaitu:[20]

a. Kelompok pertama: tindak pidana terhadap kerahasiaan *(confidentiality),* integritas *(integrity),* dan ketersediaan data *(availability)* data dan sistem komputer terdiri dari : *illegal access, illegal interception, data interference, system interference,* dan *misuse of device.*
b. Kelompok kedua: tindak pidana yang berkaitan dengan komputer, terdiri dari pemalsuan yang berkaitan dengan komputer *(computer related forgery,* dan penipuan yang berkaitan dengan komputer *(computer related fraud).*
c. Kelompok ketiga: tindak pidana yang berkaitan dengan konten yang berisi ketentuan tentang tindak pidana yang berkaitan dengan pornografi anak *(offense related to child pornography).*
d. Kelompok keempat: tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait.

Kejahatan Dunia Maya sendiri termasuk kedalam tindak pidana. Pengertian tindak pidana yang dimuat di dalam Kitab Undang-Undang Hukum Pidana (KUHP) oleh pembentuk undang-undang sering disebut dengan *strafbaarfeit*. Para pembentuk undang-undang tersebut tidak memberikan penjelasan lebih lanjut mengenai strafbaarfeit itu, maka

[19] Muhammad Anthony Aldriano, Mas Agus Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana", *Jurnal Kewarganegaraan,* Vol. 6 No. 1, 2022.
[20] Sahat Maruli Tua Situmeang, *Cyber Law*, Bandung: Penerbit Cakra, 2020, hlm. 20.

dari itu terhadap maksud dan tujuan mengenai *strafbaarfeit* tersebut sering dipergunakan oleh pakar hukum pidana dengan istilah tindak pidana, perbuatan pidana, peristiwa pidana, serta delik. Di antara istilah-istilah itu, yang paling tepat dan baik digunakan adalah istilah tindak pidana dengan pertimbangan selain mengandung pengertian yang tepat dan jelas dengan istilah hukum juga sangat praktis untuk diucapkan.[21] Unsur-unsur Tindak Pidana ialah unsur formal meliputi:[22] Perbuatan manusia, yaitu perbuatan dalam arti luas, artinya tidak berbuat yang termasuk perbuatan dan dilakukan oleh manusia;

a. Melanggar peraturan pidana, dalam artian bahwa sesuatu akan dihukum apabila sudah ada peraturan pidana sebelumnya yang telah mengatur perbuatan tersebut, jadi hakim tidak dapat menuduh suatu kejahatan yang telah dilakukan dengan suatu peraturan pidana, maka tidak ada tindak pidana;

b. Diancam dengan hukuman, hal ini bermaksud bahwa KUHP mengatur tentang hukuman yang berbeda berdasarkan tindak pidana yang telah dilakukan;

c. Dilakukan oleh orang yang bersalah, dimana unsur-unsur kesalahan yaitu harus ada kehendak, keinginan atau kemauan dari orang yang melakukan tindak pidana serta Orang tersebut berbuat sesuatu dengan sengaja, mengetahui dan sadar sebelumnya terhadap akibat perbuatannya. Kesalahan dalam arti sempit dapat diartikan kesalahan yang disebabkan karena si pembuat kurang memperhatikan akibat yang tidak dikehendaki oleh undang-undang; dan

d. Pertanggungjawaban yang menentukan bahwa orang yang tidak sehat ingatannya tidak dapat diminta pertanggungjawabannya. Dasar dari pertanggungjawaban seseorang terletak dalam keadaan jiwanya.

Sedangkan Unsur material dari tindak pidana bersifat bertentangan dengan hukum, yaitu harus benar-benar dirasakan oleh masyarakat sehingga perbuatan yang tidak patut dilakukan. Jadi meskipun perbuatan itu memenuhi rumusan undang-undang, tetapi apabila tidak bersifat melawan hukum, maka perbuatan itu bukan merupakan suatu tindak pidana diucapkan.[23] Sebagai sebuah bagian dari tindak pidana, kejahatan dunia maya juga memiliki pelaku dan korban. Pelaku kejahatan adalah orang yang telah melakukan kejahatan, yang dalam arti luasnya lagi seseorang yang melakukan pelanggaran dalam perundang-undangan yang ada, melanggar hak orang lain serta melanggar norma-norma yang ada dan hidup di

[21] Rianda Prima Putri, "Asesmen Sebagai Salah Satu Bentuk Rehabilitasi Bagi Pencandu Narkoba", *Ensiklopedia Social Review*, Vol.1 No.1, 2019.
[22] *Ibid.*
[23] *Ibid.*

masyarakat, tetapi orang yang melakukan kejahatan tidak hanya orang dewasa tanpa terkecuali seorang anak, karena seorang anak pun dapat melakukan sesuatu kejahatan dikarenakan beberapa faktor baik secara langsung maupun tidak langsung.[24]

Sedangkan korban kejahatan adalah mereka yang menderita jasmaniah dan rohaniah sebagai akibat tindakan orang lain yang mencari pemenuhan kepentingan diri sendiri atau orang lain yang bertentangan dengan kepentingan dan hak asasi yang menderita. Korban kejahatan dapat diklasifikasikan menjadi korban individual (*individual victims*) dan kolektif (*collective victims*), korban kejahatan bersifat langsung yaitu korban kejahatan itu sendiri dan tidak langsung (korban semu/abstrak) yaitu masyarakat, seseorang, kelompok masyarakat maupun masyarakat luas dan selain itu kerugian korban juga dapat bersifat materiil yang lazimnya dinilai dengan uang dan immateriil yakni perasaan takut, sakit, sedih, kejutan psikis dan lain sebagainya.[25]

Dampak Globalisasi Digital Terhadap Meningkatnya Kejahatan Siber Di Indonesia

Kemajuan teknologi telah mengubah struktur masyarakat dari yang bersifat lokal menjadi global. Perubahan ini disebabkan oleh hadirnya teknologi informasi. Perkembangan teknologi informasi yang terintegrasi dengan media dan komputer telah melahirkan perangkat baru yang dikenal sebagai internet. Kehadiran internet menciptakan paradigma baru dalam kehidupan manusia, yang beralih dari realitas fisik (real) ke realitas baru yang bersifat virtual (maya). Realitas ini sering kali terkait dengan internet dan *cyberspace.*[26] Perkembangan internet yang terus meningkat, baik dalam hal perangkat maupun penggunaannya, memberikan dampak positif maupun negatif. Teknologi tidak hanya mempermudah kehidupan manusia, tetapi juga memfasilitasi tindakan kriminal. Selain itu, teknologi berpengaruh signifikan terhadap pemahaman mengenai kejahatan, terutama dalam aliran kriminologi yang menekankan pada faktor manusia, baik secara fisik maupun psikologis. Kejahatan telah ada sejak zaman purba dan terus berkembang seiring waktu. Seiring dengan perkembangan zaman, bentuk-bentuk kejahatan pun semakin bervariasi. Perkembangan teknologi menjadi salah satu faktor penyebab timbulnya kejahatan. Dengan

[24] Zinedine De Carvalho et al, "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia", *Jurnal Publiciana,* Vol.9 No.1, 2023.
[25] *Ibid.*
[26] Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)", *Jurnal Jurisprudentie,* Vol.6 No.2, 2019.

kemajuan teknologi, jenis-jenis kejahatan semakin berkembang dan beragam, dengan banyak kejahatan baru muncul, terutama yang berkaitan dengan teknologi internet.[27]

Tantangan Hukum Dalam Penegakan Keadilan Terhadap Kejahatan Siber Lintas Negara Di Indonesia

Hukum kejahatan siber di Indonesia sendiri telah diatur dalam beberapa undang-undang dan peraturan yang mengatasi berbagai bentuk kejahatan yang dilakukan melalui media elektronik. Pada awal 2000-an, perkembangan teknologi informasi dan internet di Indonesia semakin pesat. Namun, belum ada regulasi yang jelas untuk mengatur transaksi elektronik, perlindungan data pribadi, serta penegakan hukum terhadap kejahatan siber. Pemerintah menyadari pentingnya memiliki regulasi yang jelas untuk mengatur penggunaan teknologi informasi secara legal dan aman. Maka, lahirlah inisiatif untuk menyusun UU ITE.[28] Pada akhirnya, Undang-Undang Nomor l l Tahun 2008 tentang Informasi dan Transaksi Elektronik pada 21 April 2008. Undang-undang ini adalah peraturan pertama di Indonesia yang mengatur aspek-aspek penggunaan teknologi informasi, termasuk transaksi elektronik, perlindungan data, dan penegakan hukum terhadap tindak pidana siber.

Pasal 30 Undang-Undang Nomor l l Tahun 2008 tentang Informasi dan Transaksi Elektronik telah menyatakan bahwa:

1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3) 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.

UU ITE sendiri telah mengalami dua kali perubahan sejak diundangkan, Pertama, perubahan menjadi Undang-Undang Nomor 19 Tahun 2016 yang menunjukkan dinamika

[27] *Ibid.*
[28] Irfan Santoso, Alvi Syahrin, Mahmud Mulyadi, Agusmidah Agusmidah, "Kebijakan Hukum Pidana Terhadap Perbuatan Melawan Hukum Dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE", *Locus Journal Of Academic Literature Review*, Vol.3 No.4, 2024.

dan keinginan masyarakat akan adanya penyempurnaan pasal-pasal UU ITE, khususnya akan ketentuan pidana konten ilegal. Kemudian, pada 21 November 2023, naskah Rancangan Undang-Undang tentang Perubahan Kedua atas UU ITE disahkan. Naskah ini kemudian ditandatangani pada tanggal 4 Januari 2024, sehingga Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi perubahan kedua UU ITE di Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dalam Pasal 27B Ayat (1) juga memuat pengaturan mengenai setiap orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan informasi elektronik dan dokumen elektronik dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum. Pasal 28 Ayat (1) UU ITE 2024 kemudian mengatur kembali larangan bagi setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan informasi elektronik dan dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan, yang dapat mengakibatkan kerugian materil bagi konsumen dalam transaksi elektronik. Aturan ini digunakan untuk melindungi konsumen dalam transaksi online. Pasal 32 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi juga mengatur tentang larangan penyalahgunaan jaringan telekomunikasi, termasuk untuk kegiatan ilegal. Selanjutnya, Pasal 3 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga mengatur tentang penyelenggaraan sistem elektronik dan kewajiban penyelenggara dalam menjaga keamanan data. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik juga mengatur akses masyarakat terhadap informasi publik dan sanksi bagi pihak yang melanggar hak atas informasi.

Akan tetapi, aturan-aturan tersebut belum secara khusus mengatur kejahatan siber yang dilakukan oleh pelaku di luar Indonesia. Saat ini, masyarakat internasional telah mengenal Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*) yang dibuat pada tahun 2001 oleh Uni Eropa. Substansi konvensi ini telah mencakup berbagai aspek yang luas, termasuk kebijakan kriminal yang bertujuan melindungi masyarakat dari kejahatan siber, baik melalui undang-undang maupun kerja sama internasional. Langkah ini diambil dengan kesadaran akan meningkatnya digitalisasi, konvergensi, dan globalisasi teknologi informasi, yang berpotensi disalahgunakan untuk tindak pidana.[29] Prioritas utama perjanjian ini adalah mendorong kerja sama internasional untuk melindungi masyarakat dari kejahatan siber

[29] Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional" *Jurnal Ilmu Hukum,* tanpa nomor, 2014.

melalui regulasi yang sesuai. Konvensi ini telah melahirkan panduan untuk menyelaraskan kerangka hukum nasional. Terdapat tiga tujuan utama Konvensi Budapest, termasuk penyelarasan kerangka nasional, peningkatan teknik penyelidikan kejahatan siber, dan perluasan kerja sama internasional. Sejak 2001, 66 negara non-Eropa telah meratifikasi perjanjian ini, menjadikannya acuan global dalam menangani kejahatan siber.[30] Indonesia sendiri telah meratifikasi konvensi ini di tahun 2009.[31] Ratifikasi ini menunjukkan komitmen Indonesia dalam mengatasi kejahatan siber di tingkat internasional. Konvensi ini memberikan landasan hukum yang lebih luas serta kerangka kerja untuk koordinasi antarnegara dalam menghadapi kejahatan siber. Dengan mengadopsi Konvensi Kejahatan Siber, Indonesia ikut berkontribusi dalam upaya global untuk menyelaraskan hukum dan langkah-langkah pencegahan kejahatan siber. Meskipun terdapat dasar hukum yang kuat, tantangan utama dalam penanganan kejahatan siber tetap terkait dengan peningkatan kapasitas, pelatihan personel, dan koordinasi yang efektif antara lembaga penegak hukum dan sektor swasta. Diperlukan pendekatan holistik dan berkelanjutan agar Indonesia mampu menghadapi dinamika kejahatan siber yang terus berubah. Penanganan kejahatan siber yang kompleks membutuhkan pendekatan melalui kerja sama bilateral, regional, dan multilateral. Kerja sama antara lembaga penegak hukum, pemerintah, dan masyarakat sangat penting untuk mengatasi ancaman kejahatan siber. Beberapa rekomendasi untuk memperkuat upaya penanganan kejahatan siber mencakup penguatan regulasi yang lebih komprehensif, peningkatan kerja sama internasional melalui perjanjian dan kolaborasi antarlembaga, serta peningkatan kesadaran masyarakat tentang bahaya kejahatan siber. Dengan langkah-langkah ini, diharapkan masyarakat dapat lebih efektif melindungi diri dari ancaman kejahatan siber yang terus berkembang.[32]

Salah satu masalah utama dalam penegakan kejahatan siber yang bersifat transnasional adalah masalah yurisdiksi. Yurisdiksi sendiri merujuk pada kekuasaan suatu negara untuk menerapkan hukum dan mengadili tindakan yang dilakukan oleh individu atau entitas, terlepas dari lokasi atau kewarganegaraan mereka.[33] Dalam kejahatan siber yang pelakunya bisa bertempat di luar negara Indonesia, masalah dapat muncul ketika lebih dari satu negara mengklaim yurisdiksi atas tindakan yang sama. Hal ini dapat menyebabkan

[30] Agus Nilmada Azmi, Syarah Shabrina**, "**Challenges of Universal Adoption of The Budapest Convention on Cybercrime**",** *Prosiding The 5th International Conference on Technology, Education, And Social Science***,** Vol. 1, No. 1, 2023.
[31] Aisyah Putri Nabila, Nathania Aurell Manabung, Aquilla Cinta Ramadhansha, "Peran Hukum Internasional Dalam Menanggulangi Cyber Crime Pada Kejahatan Transnasional", *Indonesian Journal of Law,* Vol.1 No.1, 2024.
[32] Akbar Kurnia Putra, *Op Cit.*
[33] Septi Dyah Tirtawati, Joko Setiyono, "Menilik Penerapan Prinsip Yurisdiksi Universal Negara Terhadap Kejahatan Perompakan Di Laut Lepas Menurut Hukum Internasional", *Jurnal Al-Daulah,* Vol.10 No.2, 2022.

ketidakpastian hukum dan konflik antara negara-negara tersebut. Dalam situasi ini, negara-negara seringkali diharapkan untuk bernegosiasi dan menentukan yurisdiksi mana yang paling tepat untuk mengadili kasus tersebut. Dalam kejahatan siber, ada pengaturan lebih lanjut yang tercantum dalam Konvensi tentang Kejahatan Dunia Siber khususnya Pasal 22 yang mencakup lima paragraf. Paragraf pertama menjelaskan bahwa negara-negara pihak konvensi dapat mengambil tindakan legislasi untuk melaksanakan yurisdiksi atas kejahatan siber yang terjadi di wilayah mereka atau di luar wilayah mereka. Paragraf 2 menyebutkan setiap negara memiliki hak untuk memilih apakah akan menerapkan ketentuan yurisdiksi atau tidak, dengan mempertimbangkan keadaan dan kasus kejahatan. Paragraf 3 menyebutkan jika pelaku kejahatan berada di wilayah negara dan ekstradisi tidak dilakukan karena status kewarganegaraan mereka, negara tersebut masih dapat melaksanakan yurisdiksi Meskipun pasal-pasal tersebut memberikan kerangka untuk yurisdiksi dalam penanganan kejahatan siber, masih terdapat kemungkinan konflik yurisdiksi antara negara-negara yang mengklaim yurisdiksi atas suatu kejahatan, terutama ketika kejahatan tersebut melibatkan sistem komputer dan internet yang dapat menargetkan korban dari berbagai negara. Oleh karena itu, perlu ada kesepakatan dan kolaborasi antara negara untuk menentukan yurisdiksi yang paling tepat dalam menangani kejahatan siber.[34]

Tantangan kejahatan siber juga dapat muncul dalam pelaksanaan Pilkada di Indonesia yang akan datang pada bulan November. Salah satu tantangan terbesar adalah penyebaran disinformasi dan hoaks. Dalam proses pemilihan umum dan daerah, umum terjadi pihak-pihak yang tidak bertanggung jawab dapat menyebarkan berita palsu atau informasi menyesatkan melalui media sosial, aplikasi pesan instan, dan platform online lainnya.[35] Ini bisa berupa penyebaran informasi palsu tentang kandidat untuk menjatuhkan lawan politik, hoaks tentang sistem pemilu yang dianggap diretas, atau konten yang memecah belah masyarakat dengan menekankan isu-isu sensitif seperti etnisitas, agama, atau kelompok tertentu. Disinformasi yang cepat menyebar dapat mengurangi kepercayaan publik terhadap proses pemilu dan memicu ketidakstabilan sosial.[36] Untuk mencegah penyebaran hoaks dan disinformasi, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjadi dasar

[34] Fazrul Rahman Mukhsin, Aurora Tifani Suci, Fadhila Triza Nandrini, Achmad Rofiq, M. Ongko Khoirurozy, "The Review Of Cybercrime Case Handling Based On Indonesian Jurisdiction And International Law", *International Journal Of Law And Legal Ethics* (IJLLE), Vol.12, 2022.
[35] Christiany Juditha, "Buzzer di Media Sosial Pada Pilkada dan Pemilu Indonesia", *Prosiding Seminar Nasional Komunikasi dan Informatika #3,* 2019.
[36]Febriansyah Putra, Haldi Patra, "Analisis Hoax pada Pemilu: Tinjauan dari Perspektif Pendidikan Politik", *Naradidik: Journal of Education & Pedagogy,* Vol.2, No.1, 2023.

hukum yang penting. Pasal 28 ayat (1) UU ITE menyatakan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang menyebabkan kerugian konsumen dalam transaksi elektronik dapat dipidana. Selain itu, Pasal 27 ayat (3) UU ITE mengatur tentang pencemaran nama baik di dunia maya, termasuk penyebaran fitnah dan ujaran kebencian.

Serangan peretasan atau *hacking* juga menjadi ancaman serius. Website KPU sendiri telah dilaporkan dibobol hacker dimana 204 juta data DPT bocor dalam kejadian ini. 200 juta data dilaporkan telah dijual oleh peretas yang menggunakan nama Jimbo dengan harga US$74 ribu atau sekitar Rp 1,2 miliar.[37] Serangan semacam ini bisa mempengaruhi transparansi dan akuntabilitas proses pemilu. Data pemilih yenag telah dicuri dapat dimodifikasi, misalnya untuk menghilangkan pemilih dari daftar atau membocorkan data pribadi untuk tujuan yang tidak sah. Hal ini bisa mengganggu legitimasi Pilkada dan menimbulkan ketidakpercayaan terhadap sistem pemilu. Untuk mengatasi ancaman peretasan, Undang-Undang Nomor 5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat serta Undang-Undang Nomor 1 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan dasar hukum untuk penanganan kejahatan siber. Pasal 30 UU ITE menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses sistem elektronik milik orang lain dengan cara apa pun dapat dipidana. Selain itu, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memperkuat regulasi terkait perlindungan data pribadi dan keamanan siber. Untuk mencegah berbagai bentuk kejahatan siber dalam Pilkada, beberapa langkah pencegahan hukum harus diterapkan. Pertama, penguatan infrastruktur keamanan digital di lembaga-lembaga yang terlibat dalam Pilkada, termasuk Komisi Pemilihan Umum (KPU), agar lebih tahan terhadap serangan siber. Hal ini dapat dilakukan dengan memperkuat sistem enkripsi dan meningkatkan pengawasan terhadap aktivitas jaringan. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik juga menjadi dasar penting dalam melindungi data pemilih.

Kedua, kolaborasi dengan *platform* media sosial untuk memantau dan mengatasi hoaks perlu dilakukan. Undang-Undang Nomor 40 Tahun 1999 tentang Pers juga dapat diteraplan ini, karena *platform digital* dan media massa harus menjalankan peran mereka secara profesional dan etis dalam menyebarkan informasi yang benar dan faktual selama masa kampanye Pilkada. Ketiga, peningkatan kapasitas penegak hukum dalam menangani kejahatan siber

[37] Diakses dari https://www.cnbcindonesia.com/tech/20231129062825-37-492819/kpu-dibobol-hacker-data-204-juta-warga-ri-dijual-di-internet pada 19 Oktober 2024 pukul 16.51 WIB.

harus menjadi prioritas. Aparat penegak hukum harus memiliki kemampuan dan sarana teknologi yang cukup untuk mendeteksi dan merespons kejahatan siber secara cepat dan efektif. Peningkatan kerja sama internasional juga diperlukan, mengingat banyak serangan siber berasal dari luar negeri. Keempat, sosialisasi kepada masyarakat tentang ancaman kejahatan siber dan pentingnya menjaga keamanan data pribadi harus dilakukan secara terus-menerus. Pemerintah bersama dengan lembaga terkait dapat melakukan edukasi melalui kampanye publik yang fokus pada keamanan siber dan dampak negatif dari penyebaran hoaks. Hal ini akan meningkatkan kewaspadaan masyarakat dan mengurangi risiko menjadi korban serangan siber selama Pilkada. Dengan penerapan langkah-langkah hukum yang kuat tersebut, diharapkan ancaman kejahatan siber dapat ditekan dan pelaksanaan Pilkada dapat berjalan dengan lancar dan transparan.

KESIMPULAN

Globalisasi digital telah membawa perubahan signifikan dalam struktur masyarakat, dengan internet menjadi salah satu pendorong utama dalam transisi ini. Meskipun memberikan banyak kemudahan dan peluang, perkembangan teknologi informasi juga memfasilitasi munculnya berbagai bentuk kejahatan siber yang semakin kompleks. Undang-undang di Indonesia, meskipun telah mengatur beberapa aspek kejahatan siber, masih menghadapi tantangan, terutama dalam kejahatan lintas negara.

Ratifikasi Konvensi tentang Kejahatan Siber oleh Indonesia menunjukkan komitmen untuk bekerja sama di tingkat internasional dalam penanganan kejahatan ini. Namun, tantangan utama tetap ada pada peningkatan kapasitas dan koordinasi antar lembaga, serta penanganan masalah yurisdiksi yang sering kali menjadi hambatan dalam penegakan hukum. Upaya bersama dari pemerintah, lembaga penegak hukum, dan masyarakat sangat penting untuk menciptakan lingkungan yang lebih aman di dunia maya. Selain itu, dalam menghadapi tantangan kejahatan siber pada Pilkada mendatang, berbagai ancaman seperti penyebaran disinformasi, hoaks, dan serangan peretasan dapat merusak integritas pemilu. Disinformasi dapat memicu ketidakpercayaan publik, sedangkan peretasan terhadap data pemilih dapat mengganggu legitimasi Pilkada. Untuk mengatasinya, UU ITE menjadi landasan hukum penting dalam menangani penyebaran hoaks, pencemaran nama baik, serta akses ilegal terhadap sistem elektronik. Selain itu, penguatan infrastruktur keamanan digital di lembaga pemilu dan perlindungan data pribadi juga diperlukan. Kolaborasi dengan platform media sosial, peningkatan kapasitas penegak hukum, dan sosialisasi publik tentang keamanan siber

harus dilakukan. Dengan langkah-langkah ini, diharapkan ancaman kejahatan siber dalam Pilkada dapat diminimalkan sehingga proses pemilu berjalan lancar, aman, dan transparan.

SARAN

Sebagai tindak lanjut dari penelitian ini, direkomendasikan agar peneliti selanjutnya fokus pada pengembangan model kerja sama internasional yang efektif dalam penegakan hukum siber. Mengingat tantangan lintas batas negara, penelitian dapat diarahkan untuk menggali perbandingan antara kebijakan penegakan hukum siber di berbagai negara dan mekanisme perjanjian internasional yang telah ada. Studi lebih lanjut juga dapat mengeksplorasi keterbatasan peraturan nasional dalam menghadapi perkembangan kejahatan siber yang kian kompleks dan melibatkan pelaku dari berbagai yurisdiksi.

Penelitian yang lebih mendalam tentang penerapan pendekatan teknologi dalam pengawasan kejahatan siber juga sangat diperlukan. Penggunaan teknologi seperti kecerdasan buatan dan analitik data besar dalam deteksi kejahatan siber dapat menjadi subjek penelitian yang potensial untuk mendukung penegakan hukum. Selain itu, pemetaan kerangka hukum dan analisis kasus mengenai penanganan kejahatan siber di berbagai negara dapat membantu dalam mengidentifikasi kelemahan regulasi domestik serta merancang kerangka kolaborasi yang lebih efisien. Dengan mengembangkan kebijakan yang adaptif dan kolaboratif, Indonesia diharapkan mampu memperkuat ketahanan hukum dalam menghadapi ancaman kejahatan siber lintas negara.

DAFTAR PUSTAKA

Buku

Hermawanto, Ariesani dan Melaty Anggraini. *Globalisasi, Revolusi Digital dan Lokalitas: Dinamika Internasional dan Domestik di Era Borderless World*. Yogyakarta: LPPM Press. 2020.

Situmeang, Sahat Maruli Tua. *Cyber Law*. Bandung: Penerbit Cakra. 2020.

Wibowo, Agus. *Globalisasi Digital*. Semarang: Yayasan Prima Agus Teknik. 2023.

Jurnal

Aldriano, Muhammad Anthony, Mas Agus Priyambodo, "Cyber Crime dalam Sudut Pandang Hukum Pidana", *Jurnal Kewarganegaraan*. Vol. 6. No. 1. 2022.

Aryeetey, Ernest and Natalia Dinello (eds). *Testing Global Interdependence Issues on Trade. Aid, Migration and Development*. Massachusetts: Edward Elgar Publishing, Inc. 2007.

Azmi, Agus Nilmada, Syarah Shabrina. "Challenges of Universal Adoption of The Budapest Convention on Cybercrime". *Prosiding The 5th International Conference on Technology, Education, And Social Science*. Vol. 1. No. 1. 2023.

Carvalho, Zinedine De, et al. "Pengaruh Media Sosial terhadap Perubahan Sosial Masyarakat di Indonesia". *Jurnal Publiciana*. Vol. 9. No.1. 2023.

Damargara, Muhammad Izzar, Muhammad Alhidayah, Muhammad Raihan Faiqy, Jatnika Maulana. "Urgensi Realisasi Pengaturan Data Protection Officer (DPO) pada Sektor Kesehatan Ditinjau dari Hukum Pelindungan Data Pribadi". *Padjadjaran Law Review*. Vol. 10. No. 1. 2022.

Fordoński, Radoslaw, Wojciech Kasprzak. "WannaCry Ransomware Cyberattack as Violation of International Law". *Studia Prawnoustrojowe Journal*. No. 44. 2019.

Greco, Gianpiero, Nicola Montinaro. "The Phenomenon Of Cybercrime: From The Transnational Connotation To The Need For Globalization Of Justice". *European Journal of Social Sciences Studies*. Vol. 6. No. 1. 2021.

Hopkins, A. G. "Globalisation and Decolonisation", *The Journal of Imperial and Commonwealth History*. Vol. 45. No.5. 2017.

Marita, Lita Sari. "Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia". *Cakrawala: Jurnal Humaniora Universitas Bina Sarana Informatika*. Vol. 15. No. 2. 2015.

Mukhsin, Fazrul Rahman, Aurora Tifani Suci, Fadhila Triza Nandrini, Achmad Rofiq, M. Ongko Khoirurozy. "The Review of Cybercrime Case Handling Based on Indonesian Jurisdiction and International Law". *International Journal of Law and Legal Ethics (IJLLE)*. Vol. 12. 2022.

Nabila, Aisyah Putri, Nathania Aurell Manabung, Aquilla Cinta Ramadhansha. "Peran Hukum Internasional dalam Menanggulangi Cyber Crime pada Kejahatan Transnasional". *Indonesian Journal of Law*. Vol. 1. No.1. 2024.

Nanda, Sendi Eka, Winda Widyaningsih. "Pengaruh Terpaan Berita Peretasan Tokopedia terhadap Reputasi Perusahaan". *Broadcasting Communication Journal*. Vol. 3. No.1. 2021.

Putra, Akbar Kurnia. "Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional". *Jurnal Ilmu Hukum*. tanpa nomor. 2014.

Putri, Rianda Prima. "Asesmen Sebagai Salah Satu Bentuk Rehabilitasi Bagi Pencandu Narkoba". *Ensiklopedia Social Review*. Vol. 1. No.1. 2019.

Ramadhan, Gilang. "Perlidungan Hukum bagi Korban Ransomware Wannacry: Tindak Pidana Ransomware". *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat*. Vol. 1. No.2. 2023.

Raodia. "Pengaruh Perkembangan Teknologi terhadap Terjadinya Kejahatan Mayantara (Cybercrime)". *Jurnal Jurisprudentie*. Vol. 6. No. 2. 2019.

Santoso, Irfan, Alvi Syahrin, Mahmud Mulyadi, Agusmidah. "Kebijakan Hukum Pidana terhadap Perbuatan Melawan Hukum dalam UU ITE Pasca Berlakunya Pedoman Implementasi Pasal - Pasal Tertentu UU ITE". *Locus Journal of Academic Literature Review*. Vol. 3. No. 4. 2024.

Speer, David L. "Redefining Borders: The Challenges Of Cybercrime". *Crime, Law & Social Change Journal*. No. 34. 2000.

Tirtawati, Septi Dyah Tirtawati, Joko Setiyono. "Menilik Penerapan Prinsip Yurisdiksi Universal Negara Terhadap Kejahatan Perompakan Di Laut Lepas Menurut Hukum Internasional". *Jurnal Al-Daulah*. Vol. 10. No. 2. 2022.

Tranggono, et al. "Pengaruh Perkembangan Teknologi di Era Globalisasi dan Peran Pendidikan terhadap Degradasi Moral pada Remaja". *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*. Vol. 3. No. 2. 2023.