De Jure: Jurnal Hukum dan Syar'iah
Vol. 14, No. 1, 2022, h. 140-159
ISSN (Print): 2085-1618, ISSN (Online): 2528-1658
DOI: http://dx.doi.org/10.18860/j-fsh.v14i1.15731
Available online at http://ejournal.uin-malang.ac.id/index.php/syariah

Penerapan Prinsip *Aut Dedere Aut Judicare* Terhadap Pelaku *Cybercrime* Lintas Negara Melalui Ratifikasi *Budapest Convention*

Ermanto Fahamsyah
Universitas Jember
ermanto_fahamsyah@yahoo.co.id

Vicko Taniady
Universitas Jember

Kania Venisa Rachim
Universitas Jember

Novi Wahyu Riwayanti
Universitas Jember

Abstract:

The presence of cybercrime in Indonesia is challenging to handle, especially for cybercrime actors who come from across countries. This study aims to examine the problem of taking global cybercriminals and examine solutions to applying the Aut Dedere Aut Judicare principle through the ratification of the *Budapest Convention*. The research method used in this study is normative legal research with a regulatory approach, cases, and comparative analysis. The study results indicate that Indonesia does not yet have a special regulation regulating cybercrimes; however, two rules cover cybercrimes offences, namely, the Criminal Code and the ITE Law. However, these two regulations can still not deal with transnational cybercriminals specifically for fun issues. Therefore, applying the Aut Dedere Aut Judicare principle through the *Budapest Convention* ratification becomes urgent for implementation. The Aut Dedere Aut Judicare principle states that every country will understand with other countries to arrest, prosecute and prosecute perpetrators of international crimes. So it is necessary to ratify the *Budapest Convention* as a legal basis to apply the Aut Dedere Aut Judicare principle.

Keywords: Aut Dedere Aut Judicare; *Budapest Convention*; Cybercrime Perpetrators; Cross Country.

Abstrak:

Kehadiran *cybercrime* di Indonesia sangat sulit ditangani terkhusus bagi pelaku *cybercrime* yang berasal dari lintas negara. Tujuan penelitian ini adalah untuk mengkaji problematika penanganan bagi pelaku *cybercrime* lintas negara, serta mengkaji solusi penerapan prinsip *Aut Dedere Aut Judicare* melalui upaya ratifikasi *Budapest Convention*. Metode penelitian yang digunakan adalah dalam penelitian ini, penelitian hukum normatif, dengan pendekatan peraturan perundang-undangan, kasus, serta analisis komparatif. Hasil penelitian menunjukkan bahwa Indonesia hingga saat ini belum memiliki pengaturan khusus yang mengatur *cybercrime,* namun demikian terdapat dua peraturan yang mencakup delik *cybercrime* yakni, KUHP dan UU ITE. Namun demikian, dua peraturan tersebut masih belum bisa menangani para pelaku *cybercrime* lintas negara terkhusus permasalahan yurisdiksi. Oleh karena itu, penerapan prinsip *Aut Dedere Aut Judicare* melalui ratifikasi *Budapest Convention* menjadi urgensi yang harus dilakukan. Prinsip *Aut Dedere Aut Judicare* menyatakan setiap negara akan bekerjasama bersama negara lain untuk menangkap, menuntut, dan mengadili para pelaku kejahatan internasional. Sehingga perlu upaya ratifikasi *Budapest Convention* sebagai dasar hukum untuk menerapkan prinsip *Aut Dedere Aut Judicare.*

Kata Kunci: Aut Dedere Aut Judicare; *Budapest Convention*; Pelaku Cybercrime; Lintas Negara.

Pendahuluan

Pesatnya perkembangan teknologi, khususnya teknologi informasi dan komunikasi pada saat ini, telah menumbuhkan interkoneksitas antar masyarakat dunia tanpa terhambat oleh batas-batas wilayah negara. Perkembangan dari teknologi informasi dan komunikasi yang berkolaborasi dengan media serta komputer, memunculkan sebuah piranti baru yang dikenal sebagai internet.[1] Penggunaan internet semakin hari semakin meningkat, terkhusus di Indonesia. Berangkat dari data *internetworldstats* menyebutkan jumlah pengguna internet di Indonesia telah mencapai 212,35 juta jiwa terhitung pada Maret 2021, dan menempati urutan ketiga dengan jumlah pengguna internet terbanyak di Asia.[2]

Perkembangan internet diibaratkan sebagai pedang bermata dua, karena selain memberikan dampak positif bagi kehidupan manusia, internet bisa juga menjadi cara efektif untuk melakukan perbuatan melawan hukum.[3] Salah satu perbuatan melawan hukum akibat perkembangan internet adalah kejahatan *cybercrime* atau yang dikenal sebagai kejahatan yang dilakukan melalui jaringan internet. Berdasarkan

---

1 Donovan Typhano Rachmadie & Supanto, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 1 Tahun 2016" (2020) 9:2 J Huk Pidana Dan Penanggulangan Kejahatan 128–156, hlm. 129.

2 Viva Budy Kusnandar, "Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia | Databoks," Katadata.co.id, 2021, https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia.

3 Fiorida Mathilda, "Cyber Crime Dalam Sistem Hukum Indonesia," *Sigma-Mu* 4, no. 2 (2012): 34–45, https://doi.org/10.35313/sigmamu.v4i2.870.

International Telecommunication Union (ITU) menyatakan bahwa *cybercrime* merupakan kejahatan yang dilakukan melalui komputer baik sebagai alat, target, maupun sarana untuk melakukan kejahatan.[4] Sehingga, pendekatan sistem hukum terhadap pemanfaatan internet tidak dapat lagi dilakukan secara konvensional,[5] mengingat aktivitasnya dilakukan secara lintas negara, mudah memperoleh akses dari lintas negara, serta kerugian dapat terjadi meskipun pelaku dan korban tidak pernah berhubungan sekaligus.[6]

International Criminal Police Organization (Interpol) dalam laman resminya mencatat sebanyak hampir 270 situs web yang disusupi, termasuk portal pemerintah di wilayah Asia Tenggara, serta 26 situs web pemerintah yang terpengaruh oleh enam kelompok peretas dan beberapa peretas individu, khususnya di Indonesia berdasarkan data Badan Siber dan Sandi Negara (BSSN) mencatat serangan siber tahun 2020 angka mencapai angka 495,3 juta atau meningkat 41 persen dari tahun sebelumnya 2019 yang sebesar 290,3 juta. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Dimana pada tahun 2019 terdapat 4.586 laporan polisi diajukan melalui Patrolisiber pada Januari sampai Agustus 2020, hampir 190 juta terjadi upaya serangan siber di Indonesia yang dilakukan oleh hacker nasional hingga internasional.[7] Bahkan, Akhman Muqowam, Ketua Komite 1 DPD RI menyatakan tingkat *cybercrime* di Indonesia berada pada peringkat kedua di dunia.[8] Pada tahun 2017 kerugian ekonomi akibat *cybercrime* di Indonesia mencapai Rp478,8 triliun.[9] Lebih lanjut, disampaikan oleh Direktur Tindak Pidana Siber Bareskrim Polri, Brigadir Jenderal Polisi Slamet Uliandi, S.I.K., menyampaikan sejak 2020 hingga 2021, terjadi 649 laporan penipuan dan 39 kali pencurian data yang masuk Siber Polri. Terjadi juga 18 kali aduan peretasan sistem elektronik.[10]

Di Indonesia, pengaturan *cybercrime* tertuang dalam beberapa regulasi, salah satunya adalah Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP) dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Menurut pandangan Mardjono Reksodiputro, Kriminolog dari Universitas Indonesia menyatakan *cybercrime* sebenarnya bukanlah

---

4 Galuh Kartiko, "Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional" (2013) 8:2 Rechtidee 136–153, hlm. 137.

5 Cahyo Handoko, "Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime di Pengadilan" (2017) 6:1 J Jurisprud 1–15, hlm. 1-4.

6 Raida L Tobing, *Laporan Akhir Penelitian Hukum tentang Efektifitas UU No. 11 Tahun 2008 tetang Informasi dan Transaksi Elektronik* (Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2010), hlm. 5.

7 Putri Zakia Salsabila, "Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi," Kompas.com, 2020, https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi.

8 Dessy Suciati Saputri, "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber," Republika Online, 2015, https://republika.co.id/berita/nasional/umum/15/04/09/nmjajy-indonesia-peringkat-ke2-dunia-kasus-kejahatan-siber.

9 Ratna Christianingrum & Ade Nurul Aida, *Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan* (Jakarta: Pusat Kajian Anggaran Badan Keahlian-Sektretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia, 2021), hlm. 5.

10 TBNews, *Sejak 2020 Polri Sebut Total Kerugian Kejahatan Siber Mencapai...*, diakses 10 Mei 2022, https://tribratanews.polri.go.id/read/5780/2/sejak-2020-polri-sebut-total-kerugian-kejahatan-siber-mencapai-123-t-1615705417.

kejahatan baru yang masih bisa diakomodir oleh KUHP.[11] Lebih lanjut, meskipun Indonesia belum memiliki regulasi khusus *cybercrime,* namun terdapat UU ITE sebagai *lex specialis* yang mengatur *cybercrime.* Namun demikian, terdapat kelemahan dalam pengaturan *cybercrime* di Indonesia, terkhusus permasalahan yurisdiksi. Meskipun pengaturan mengenai *cybercrime* yang dilakukan oleh pelaku lintas negara telah diatur dalam Pasal 2 dan Pasal 37 UU ITE, namun dalam praktiknya sangat sulit untuk dilakukan. Hal ini karena akan menimbulkan konflik yurisdiksi karena menggunakan pendekatan yang berbeda[12] dan belum tentu setiap negara akan menyampaikan kejahatan tersebut.[13] Lebih lanjut, permasalahan yurisdiksi berkaitan dengan sejauh mana suatu negara dapat menerapkan kedaulatan hukumnya, serta mengukur kemampuan suatu negara menyidangkan suatu kasus bernuansa internasional. Bahkan menurut Debra L. Shinder menyebutkan bahwa *"*kasus *cybercrime,* lebih dari kebanyakan kasus lainnya, sering kali melibatkan masalah yurisdiksi yang kompleks dan dapat menghadirkan hambatan hukum serta praktis untuk penuntutan*".*[14]

Oleh karena itu, perlu adanya penerapan prinsip *Aut Dedere Aut Judicare.* Prinsip *Aut Dedere Aut Judicare* dilahirkan dari pemikiran Cherif Bassiouni yang memiliki arti bahwa setiap negara berkewajiban menuntut dan untuk mengadili para pelaku kejahatan internasional dan bekerja sama dengan negara lain untuk menangkap serta mengadili para pelaku kejahatan internasional.[15] Untuk menerapkan prinsip *Aut Dedere Aut Judicare* terhadap *cybercrime* diperlukannya upaya untuk ratifikasi *Budapest Convention* sebagai payung hukum. *Budapest Convention* menekankan kepada semua negara yang telah meratifikasi untuk melakukan kerjasama internasional dalam memberantas *cybercrime.*[16] Sehingga penerapan prinsip *Aut Dedere Aut Judicare* melalui ratifikasi *Budapest Convention* menjadi urgensi yang harus dilakukan untuk menindak pelaku kejahatan *cybercrime* lintas negara.

Kajian mengenai *cybercrime* dan prinsip *Aut Dedere Aut Judicare* sejatinya telah beberapa kali dilakukan, seperti: 1) Penelitian yang dilakukan oleh David Wicki dan Birchler dengan judul "*The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime".*[17] Penelitian ini mengkaji dua kerangka hukum yakni Konvensi Budapest dan *the General Data Protection Regulation* (GDPR). Penelitian ini mengungkapkan bahwa Konvensi Budapest tentang *cybercrime* memainkan peran penting dalam memerangi kejahatan dunia maya dengan menetapkan standar hukum pidana berbasis prinsip yang mutakhir dan aturan prosedural penting terkait dengan penyimpanan sementara data yang berpotensi digunakan sebagai bukti dalam menuntut tindak pidana; 2) Penelitian

---

[11] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: Rajawali Press, 2013), hlm. 48.

[12] Hendra Kusuma Wardana, *Yurisdiksi Terhadap Cybercrime* (thesis, Universitas Airlangga, 2010), hlm. 1-2.

[13] Kartiko, *supra* note 2, hlm. 136.

[14] Michael Cross, *Scene of Cybercrime Second Edition* (Burlington: Syngress, 2008), hlm. 669.

[15] Novalinda Nadya Putri, "Penerapan Prinsip Aut Dedere Aut Judicare Dalam Penegakan Hukum Pidana Internasional" (2021) 6:1 LEGA LATA J Ilmu Huk 139–167, hlm. 145.

[16] Farouq Ahmad Faleh Al Azzam, "The adequacy of the international cooperation means for combating cybercrime and ways to modernize it" (2019) 10:1 JANUSNET 67–83, hlm 67.

[17] David Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?," *International Cybersecurity Law Review* 1 (2020): 63–72, https://doi.org/10.1365/s43439-020-00012-5.

yang dilakukan oleh Novalinda Nadya Putri dengan judul "Penerapan Prinsip *Aut Dedere Aut Judicare* Dalam Penegakan Hukum Pidana Internasional".[18] Penelitian ini mengkaji penerapan prinsip-prinsip hukum pidana internasional, salah satunya adalah *Aut Dedere Aut Judicare.* Penelitian ini menyebutkan bahwa penerapan *Aut Dedere Aut Judicare* telah kerap kali dilakukan, baik mengekstradisi pelaku kejahatan internasional maupun mengadilinya. Prinsip ini mampu mencegah pelaku kejahatan agar tidak dapat menemukan perlindungan di negara manapun; dan 3) Penelitian yang dilakukan oleh Ranty Mahardika Jhon dengan judul "*Existence of Criminal Law on Dealing Cybercrime in Indonesia".*[19] Penelitian ini mengungkapkan bahwa *cybercrime* adalah bagian buruk dari perkembangan teknologi, yang berimplikasi negative bagi kehidupan masyarakat, terutama bagi kejahatan ekonomi. Di Indonesia, pengaturan *cybercrime* memiliki berbagai kendala, salah satunya adalah yurisdiksi. Lebih lanjut, penelitian ini menginginkan perlu adanya kerjasama bilateral untuk mengatasi *cybercrime* yang dilakukan oleh pelaku Warga Negara Asing maupun Warga Negara Indonesia yang melibatkan negara Indonesia dari tindak kejahatan Internasional *cybercrime,* karena prinsip *Aut Dedere Aut Judicare* merupakan salah satu bagian dari hukum pidana internasional yang berarti bahwa setiap negara berkewajiban menuntut dan untuk mengadili para pelaku kejahatan internasional dan bekerja sama dengan negara lain untuk menangkap serta mengadili para pelaku kejahatan internasional.

Melihat penelitian terdahulu yang telah disajikan**,** penelitian ini memiliki kesamaan tema yakni terkait *cybercrime* dan prinsip *Aut Dedere Aut Judicare.* Namun, dalam penelitian ini terdapat isu kebaruan hukum sehingga tidak mengulang penelitian terdahulu, dan menguatkan penanganan *cybercrime,* terkhusus bagi pelaku lintas negara. Adapun isu kebaruan hukum dalam penelitian ini dan akan menjadi penelitian pertama adalah mengkaji penerapan prinsip *Aut Dedere Aut Judicare* terhadap pelaku *cybercrime* melalui upaya ratifikasi *Budapest Convention*. Sehingga, terdapat dua isu hukum yang akan dikaji, yakni: Pertama, bagaimana problematika pengaturan pidana bagi pelaku *cybercrime* lintas negara di Indonesia?; dan Kedua, bagaimana penerapan prinsip *Aut Dedere Aut Judicare* melalui ratifikasi *Budapest Convention* terhadap pertanggungjawaban pidana bagi pelaku *cybercrime* lintas negara?

Penelitian ini menggunakan penelitian hukum normatif[20], dengan pendekatan peraturan perundang-undangan (*statute approach*) dan kasus (*case approach*). Pendekatan peraturan perundang-undangan ini ditujukan untuk menganalisis dan mengidentifikasi ketentuan yang mengatur *cybercrime* yang dilakukan oleh pelaku lintas negara. Pendekatan kasus ini dimaksudkan untuk menelaah kasus-kasus *cybercrime* sehingga dapat ditarik benang merah terkait langkah solutif penanganan *cybercrime* yang dilakukan oleh pelaku lintas negara. Penelitian ini juga menggunakan analisis komparatif dibeberapa negara yang telah melakukan ratifikasi *Budapest*

---

[18] Putri, "Penerapan Prinsip Aut Dedere Aut Judicare Dalam Penegakan Hukum Pidana Internasional."

[19] Ranty Mahardika Jhon, "Existence of Criminal Law on Dealing Cybercrime in Indonesia," *IJCLS (Indonesian Journal of Criminal Law Studies)* 3, no. 1 (31 Mei 2018): 25–34, https://doi.org/10.15294/ijcls.v3i1.16945.

[20] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif : Suatu Tinjauan Singkat* (Jakarta: Raja Grafindo Persada, 2003). Jenis penelitian hukum normatif merupakan jenis penelitian yang mengkaji asas-asas hukum, sistematik hukum, taraf sinkronisasi vertikal dan horizontal, *legal history*, dan *comparative law*.

Convention, baik dari sejarah, regulasi, hingga contoh kasus. Pada penelitian ini akan mengelola data sekunder, yang mencakup bahan hukum primer, sekunder, dan tersier. Adapun bahan hukum primer yang digunakan adalah peraturan perundang-undangan yang berkaitan dengan *cybercrime,* dan penggunaan konvensi internasional. Bahan hukum sekunder seperti buku, jurnal ilmiah, dan penelitian ahli terdahulu. Dan bahan hukum tersier, seperti kamus hukum misalnya *black's law dictionary*, dan media *online* yang memiliki kredibilitas.

Peneliti setelah mengumpulkan dan menginventarisasi bahan hukum melalui teknik studi pustaka, akan dilakukan preskripsi terkait masalah hukum yang dikaji. Selanjutnya, analisis data dilakukan melalui pola deduksi untuk menggambarkan beberapa norma peraturan yang berkaitan dengan masalah hukum yang dikaji serta menjelaskan fakta hukum. Penganalisisan data dilakukan secara sistematis, teratur, logis, menyeluruh, serta diuraikan secara holistic dan rinci. Sehingga, melalui pola penalaran yang disusun secara sistematikan akan mempu melahirkan kesimpulan dari masalah hukum yang dikaji.

Problematika Pengaturan Pidana Bagi Pelaku *Cybercrime* Lintas Negara di Indonesia

Kehadiran teknologi informasi saat ini dimanfaatkan oleh semua golongan, baik masyarakat, instansi pemerintah, bahkan hingga swasta. Salah satu wujud kehadiran teknologi informasi adalah internet. Internet merupakan ruang informasi dan komunikasi yang tidak terbatas antar negara.[21] Indonesia merupakan negara yang menggunakan internet terbanyak dengan hasil penilaian di urutan ketiga di Asia dengan jumlah 212,35 juta jiwa pada Maret 2021.[22] Namun demikian, kehadiran internet yang membawa kita masuk ke dunia maya, dalam perkembangannya juga memberikan dampak negatif bagi kehidupan. Internet sebagai media tanpa batas dapat digunakan untuk melakukan *cybercrime*[23] seperti, penipuan, *cyberporn,* terorisme, pelanggaran Hak Kekayaan Intelektual, dan kejahatan lainnya yang memberikan dampak kerugian materil dan non-materil kepada pengguna, dan bahkan merupakan tatatan kehidupan bangsa dan negara.[24]

Oleh karena itu, perlu adanya perlakuan tegas terkait segala ancaman *cybercrime* yang meresahkan keamanan warga negara dan kedaulatan negara, sehingga perlu adanya perhatian lebih terhadap keamanan siber terkhusus pertanggungjawaban pidana bagi pelaku *cybercrime* lintas negara. Merujuk pada pendapat Barda (2005) terdapat tiga hal problematika sulitnya menjerat pelaku *cybercrime*, yakni:[25] 1) Kejahatan ini dilakukan secara elektronik sehingga sulit untuk diidentifikasi, serta

---

[21] Rosemary Thackeray & MaryAnne Hunter, "Empowering Youth: Use of Technology in Advocacy to Affect Social Change" (2010) 15:4 J Comput-Mediat Commun 575–591, hlm. 575-576.

[22] Muhammad Najamuddin Dwi Miharja & Ahmad Fauzi, "Peningkatan Keamanan Login Pada Content Management System (CMS) Wordpress Dengan Implementasi Notifikasi Login Dengan Whatsapp Gateway" (2021) 12:4 J SIGMA 41–44, hlm. 42.

[23] Miko Aditiya Suharto & Maria Novita Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional" (2021) Risal Huk 98–107, hlm. 98-99.

[24] Regner Sabillon et al, "Cybercrime and cybercriminals: A comprehensive study" (2016) 4:6 Int J Comput Netw Commun Secur 165–176, hlm. 165-167.

[25] Hamsu Abdul Gani & Andika Wahyudi Gani, "Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No.11 Tahun 2008 dan UU No.19 Tahun 2016" (2019) Pros Semin Nas LP2M UNM, online: <https://ojs.unm.ac.id/semnaslemlit/article/view/11257>, hlm 128.

pengaturan terkait asas legalitas masih bersifat konvensional dan bertolak dari perbuatan nyata serta kepastian hukum; 2) *Cybercrime* memiliki kaitan dengan pesatnya pertumbuhan teknologi, sedangkan pengaturan hukum (asas legalitas) bersifat konvensional serta sumber hukum formasi bersifat statis; dan 3) *Cybercrime* dilakukan dengan melewati perbatasan antar negara, sedangkan peraturan disuatu negara pada umumnya hanya berlaku diwilayah teritorialnya sendiri. Pada saat ini, pengaturan *cybercrime* belum diatur secara khusus dan masih diatur secara tersebar dibeberapa peraturan perundang-undangan yang bersifat sektoral dan parsial.[26] Berikut beberapa peraturan yang mengatur terkait *cybercrime*: 1) Kitab Undang-Undang Hukum Pidana; 2) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE); 3) Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta (UU Hak Cipta); 4) Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang (UU TPPU); 5) Undang-Undang Nomor 20 Tahun 2001 tentang Perubahan Atas Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Tipikor); dan 6) Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran (UU Penyiaran).

Dari peraturan yang ada terkait *cybercrime* dapat dikatakan belum komprehensif. Jika dikaji berdasarkan UU Penyiaran dimana masih belum adanya kualifikasi delik.[27] Lebih lanjut dalam UU Tipikor dan TPPU masih mengalami permasalahan terkait *electronic record,* serta hanya berfokus terhadap satu tindak pidana.[28] Salah satu pengaturan yang kerap kali menjadi senjata utama dalam penanggulangan *cybercrime* adalah KUHP dan UU ITE.[29] Sehingga, penelitian ini akan mengkaji bagaimana pengaturan *cybercrime* dari KUHP dan UU ITE.

Tabel 1. Analisis Jenis Delik *Cybercrime* di KUHP.

No.	Jenis Delik *Cybercrime* di KUHP	Diatur Pada Pasal- KUHP
1.	Pencurian	Pasal 364
2.	Perusakan/Penghancuran Barang	Pasal 406
3.	Pornografi	Pasal 282
4.	Penipuan	Pasal 378
5.	Perbuatan memasuki atau melewati wilayah orang lain	Pasal 167
6.	Penggelapan	Pasal 372
7.	Kejahatan terhadap ketertiban umum	Pasal 154

[26] Muhamad Hasan Rumlus & Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik" (2020) 11:2 J HAM 285–299, hlm. 286-288.

[27] Anriyan Ridwan Tahir, *Analisis Hukum Terhadap Kejahatan Siber (Cybercrime) Pencurian Data Berupa Hak Cipta (Copyright) Milik Stasiun Televisi Swasta* Universitas Hasanuddin, 2018), hlm. 17.

[28] Marwin Marwin, "Penanggulangan Cyber Crime Melalui Penal Policy" (2013) 5:1 ASAS 1–9, hlm. 5.

[29] Penulis mengkaji beberapa Putusan Pengadilan Negeri yang berkaitan dengan delik *cybercrime,* yakni Putusan Nomor: 50/PID.B/2015/PN Mgg; Putusan Nomor 258/PID.S/2012/PN.SBY; Putusan Nomor 349/Pid.Sus/2019/PN. DPS. Pada tiga putusan tersebut menggunakan KUHP dan UU ITE sebagai dasar hukum menjerat pelaku *cybercrime* di Indonesia.

8.	Penghinaan	Pasal 310, 311, 315, 317, dan 318.
9.	Pemalsuan Surat	Pasal 263
10.	Pembocoran Rahasia	Pasal 97
11.	Perjudian	Pasal 303

Pengaturan dalam KUHP sejatinya telah mengatur kaitan hukum tentang kejahatan yang berhubungan dengan *cybercrime.*[30] Namun demikian, KUHP yang merupakan produk Belanda nyatanya masih bersifat konvensional sehingga tidak dapat diandalkan untuk penanggulangan *cybercrime.* Lebih lanjut, pengaturan KUHP juga menghadapi kelemahan dan keterbatasan karena *cybercrime* merupakan kejahatan dengan menggunakan sarana atau *high tech crime* yang bervariasi. Bahkan, masih banyak lagi delik-delik *cybercrime* yang belum diatur dalam KUHP.[31] Permasalahan lainnya adalah terkait pelaku *cybercrime* lintas negara. Jika dikaji dalam Pasal 4 KUHP memiliki makna asas nasionalitas pasif, yang dimana hukum pidana Indonesia berlaku bagi setiap orang (WNI dan WNA) yang melakukan perbuatan pidana diluar wilayah Indonesia namun melanggar kepentingan Indonesia.[32] Dalam perkembangannya asas ini memiliki keterbatasan dalam menjerat seseorang yang melakukan *cybercrime* diluar wilayah Indonesia dengan kualifikasi tindak pidana tertentu.[33] Sehingga, dengan melihat delik *cybercrime* dalam KUHP masih bersifat konvensional membuat asas nasionalitas pasif tidak mampu dilakukan serta tidak adanya kerjasama internasional membuat sulitnya penanganan pelaku *cybercrime* lintas negara.

Lebih lanjut, peraturan *cybercrime* juga diatur dalam UU ITE. UU ITE merupakan perwujudan dari pemerintah untuk melakukan perlindungan terhadap masyarakat dalam bidang informasi dan transaksi elektronik. Jika dikaji dalam UU ITE, terdapat dua kategori kriminalisasi *cybercrime,* yakni tindakan dengan menggunakan sarana komputer untuk melakukan kejahatan, dan tindakan yang menggunakan komputer untuk sasaran kejahatan. Terdapat beberapa delik *cybercrime* yang diatur dalam UU ITE, yakni:

Tabel 2. Jenis Delik *Cybercrime* di UU ITE.

No.	**Jenis Delik *Cybercrime* di UU ITE**	**Diatur Pada Pasal- UU ITE**

[30] Andri Winjaya Laksana, "Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif" (2019) 35:1 J Huk 52–76, hlm. 53-55.

[31] Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional" (2014) 5:2 J Ilmu Huk Jambi 95–109, hlm 95-97.

[32] Rahel Octora, "Penerapan Asas Nasionalitas Pasif dan Pemidanaan Pembantu Tindak Pidana Perdagangan Orang Dalam Rkuhp" (2018) 40:3 Kertha Patrika 155–174, hlm. 160-162.

[33] Lailatul Mustaqimah, "Penerapan Asas Nasionalitas Pasif Terhadap Tindak Pidana Teknologi Informasi" (2016) 1:2 Badamai Law J 322–342, hlm 330-332.

1.	Melanggar Kekusilaan, Perjudian, Penghinaan, Pencemaran Nama Baik, Pemerasan dan/atau Pengancaman	Pasal 27
2.	Menyebarkan berita palsu, dan menyebarkan *hate speech.*	Pasal 28
3.	Melakukan ancaman kekerasan atau menakut-nakuti	Pasal 29
4.	Mengakses komputer orang lain dengan tujuan memperoleh informasi dengan melanggar sistem pengamanan (aktivitas *Hacking*)	Pasal 30
5.	Melakukan penyadapan	Pasal 31
6.	*Defacing*	Pasal 32
7.	Pengangguan Melalui Internet	Pasal 33
8.	Fasilitator *Cybercrime*	Pasal 34
9.	Plagiat/Pembajakan Melalui Internet	Pasal 35
10.	Mengakibatkan kerugian	Pasal 36
11.	Wilayah Yurisdiksi	Pasal 37

Namun demikian, kehadiran UU ITE hingga sekarang masih belum mampu menekan keberadaan *cybercrime* karena masih terdapat kekurangan dalam Undang-Undang tersebut, seperti banyak delik *cybercrime* yang belum diatur,[34] cara penanganan, dan lainnya terkhusus pada pelaku *cybercrime* lintas negara atau yurisdiksi.[35] Sejatinya, pengaturan terkait pelaku *cybercrime* lintas negara telah diatur dalam Pasal 2 UU ITE yang menganut asas universal atau lintas teritorial.[36] Sehingga, baik pelaku perbuatan hukum dilakukan diluar wilayah hukum (yurisdiksi) Indonesia yang dilakukan oleh WNI, WNA, Badan Hukum Indonesia, dan Badan Hukum Asing yang mengakibatkan kerugian terhadap kepentingan Indonesia maka akan dihukum berdasarkan UU ITE. Bahkan pengaturan terkait yurisdiksi juga telah diatur dalam Pasal 37 UU ITE[37] yang menyatakan seluruh perbuatan yang dilarang dalam Pasal 26-Pasal 36 UU ITE (yang dimana pasal tersebut masuk dalam delik *cybercrime*) dilakukan diluar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah yurisdiksi Indonesia.

---

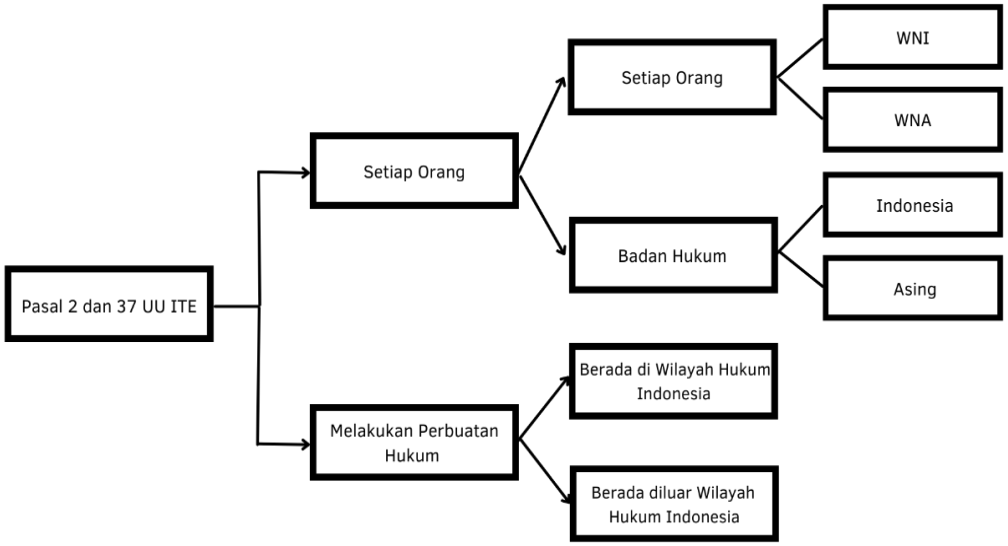
[34] Putra, "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional."

[35] Apripari Irham, "Penegakkan Yurisdiksi International Criminal Court atas Kejahatan Agresi Pasca Kampala Amendments Diadopsi dalam Rome Statute" (2020) 26:4 SASI 540–556, hlm 543-545.

[36] Yuliana Surya Galih, "Yurisdiksi Hukum Pidana Dalam Dunia Maya" (2019) 7:1 J Ilm Galuh Justisi 59–74, hlm. 59-62.

[37] Melani Melani, Hari Disemadi & Nyoman Jaya, "Kebijakan Hukum Pidana Dibidang Transaksi Elektronik Sebagai Tindak Pidana Non-Konvensional" (2020) 15:1 Pandecta Res Law J 111–120, hlm. 116.

Gambar 1: Arah Pengaturan Terkait Yurisdiksi Pasal 2 dan Pasal 37 UU ITE.



Sumber: Analisis dari Penulis

Namun, fakta dilapangan menunjukkan implementasi terkait penanganan pidana bagi pelaku *cybercrime* lintas negara nyatanya masih menuai problematika.[38] Hal ini karena akan menimbulkan konflik yurisdiksi dan belum tentu setiap negara akan menyampaikan kejahatan tersebut.[39] Lebih lanjut, permasalahan yurisdiksi berkaitan dengan sejauh mana sebuah negara dapat mengimplementasikan kedaulatan hukum yang berlaku di negaranya, serta sejauh mana kemampuan suatu negara menyidangkan perkara bernuansa internasional.[40] Terdapat banyak contoh kasus *cybercrime* di Indonesia yang dilakukan oleh pelaku lintas negara, namun tidak pernah sekalipun para pelaku mendapatkan hukuman. Salah satunya adalah kasus grup hacker Naikon yang berasal dari China melakukan serangan *malware backdoor* Aria-body yang membuat virus di komputer pemerintahan.[41] Lebih lanjut, *cyberwar* antara Indonesia dan Australia juga terjadi pada November 2013, yang diawali oleh aksis penyadapan yang dilakukan oleh Badan Intelijen Australia terhadap Presiden Susilo Bambang Yudhoyono dan sejumlah Menteri.[42] Hal ini membuat hubungan antara Indonesia dan Australia terkesan tidak lagi harmonis.

Problematika yurisdiksi terhadap penanganan *cybercrime* masih menjadi masalah yang serius apabila pelaku berasal dari lintas negara. Barbara Etter menjelaskan penyebab timbulnya masalah yurisdiksi dalam konteks internasional, yakni:[43] 1) Tidak adanya konsesus global mengenai jenis kejahatan komputer; 2)

---

38 Dewi Bunga, "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime" (2019) 16:1 J Legis Indones 1–15, hlm. 2-4.

39 Kartiko, "Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional."

40 *Kartiko*.

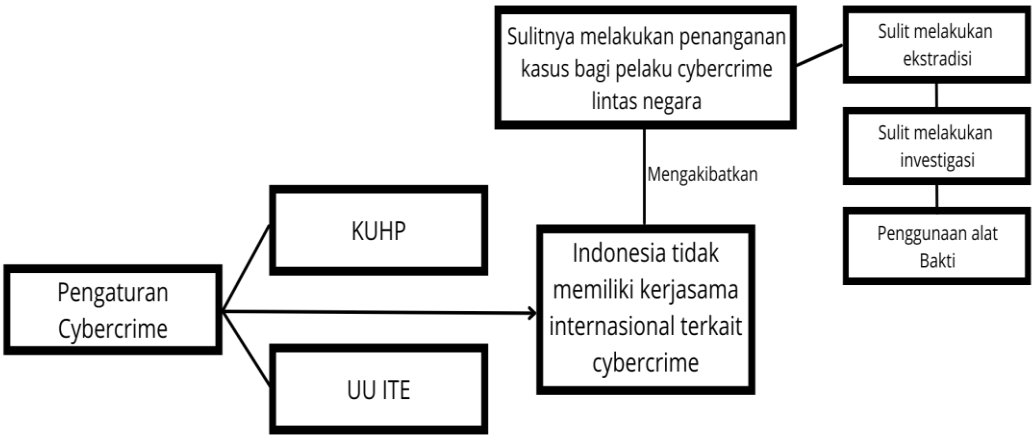
41 Anggoro Suryo Jati, "Mengenal Naikon, Grup Hacker China yang Serang Indonesia," Detik.com, 2020, https://inet.detik.com/security/d-5034437/mengenal-naikon-grup-hacker-china-yang-serang-indonesia.

42 Iskandar, "Kilas Balik Perang Hacker Indonesia vs Australia," liputan6.com, 2014, https://www.liputan6.com/tekno/read/826144/kilas-balik-perang-hacker-indonesia-vs-australia.

43 Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia* (Jakarta: PT RajaGrafindo Persada, 2006).

Kurangnya kualitas para penegak hukum terhadap penanganan *cybercrime,* serta terjadi kekosongan hukum; 3) Bersifat transnasional; 4) Ketidakharmonisan hukum acara terkait *cybercrime;* dan 5) Tidak adanya upaya melakukan sinkronisasi dalam hal penegakan hukum, ekstradisi, bantuan hukum, maupun kerjasama internasional terhadap investigas *cybercrime.* Oleh karena itu, dengan meminjam pandangan David R. Johnson perlu adanya upaya kerjasama internasional dalam penanganan *cybercrime.*[44] Penerapan prinsip *Aut Dedere Aut Judicare* menjadi urgensi yang harus dilakukan. Prinsip *Aut Dedere Aut Judicare* akan memberikan keharusan kepada setiap negara untuk menuntut dan mengadili para pelaku *cybercrime* serta bekerja sama dengan negara lain untuk menangkap dan mengadili para pelaku *cybercrime.*[45] Sehingga, perlu adanya ratifikasi *Budapest Convention* sebagai wujud dasar hukum.

Gambar 2: Problematika Pengaturan Pidana Bagi Pelaku *Cybercrime* Lintas Negara di Indonesia



Sumber: Analisis dari Penulis

Penerapan Prinsip *Aut Dedere Aut Judicare* Melalui Ratifikasi *Budapest Convention*

Hasil Dewasa ini, kehadiran *cybercrime* telah masuk dalam segi kehidupan manusia. Di Indonesia, pengaturan *cybercrime* tidak memiliki regulasi khusus,[46] namun demikian terdapat beberapa peraturan seperti KUHP dan UU ITE. Dua peraturan tersebut nyatanya masih mengalami problematika, salah satunya adalah sulitnya menangkap/memproses para pelaku *cybercrime* lintas negara. Hal ini berkaitan erat dengan yurisdiksi dan kedaulatan suatu negara. Selain itu, peliknya pembuktian *locus delicti* pelaku *cybercrime* yang menimbulkan multi yurisdiksi, mengakibatkan perlunya hukum internasional untuk bertindak mengatasi hal tersebut. Salah satu yang harus dilakukan adalah dengan menerapkan prinsip-prinsip

---

[44] David R Johnson & David Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48:5 Stanford Law Rev 1367–1402, hlm. 1367-1369.

[45] Andrea Caligiuri, "Governing International Cooperation in Criminal Matters: The Role of the aut dedere aut judicare Principle" (2018) 18:2 Int Crim Law Rev 244–274, hlm 244.

[46] Muhamad Rizal & Yanyan Yani, "Cybersecurity Policy and Its Implementation in Indonesia" (2016) 4:1 JAS J ASEAN Stud 61–78, hlm. 70.

hukum internasional yang sejalan hukum nasional.[47] Hal tersebut sejalan dengan pemikiran Darrel Menthe bahwa yurisdiksi di *cybercrime* memerlukan pengadopsian prinsip yang pasti yang berasal dari *international law*.[48] Dengan menggunakan prinsip-prinsip yurisdiksi dalam hukum internasional tersebut, negara-negara bersangkutan kiranya dapat mengadopsi pemecahan masalah yang sama terhadap pertanyaan mengenai yurisdiksi internet. Oleh karena itu, perlu adanya pengaturan terbarukan dalam upaya menjerat dan meminta pertanggungjawaban kepada pelaku *cybercrime* lintas negara.

Oleh karena itu, perlu adanya penerapan prinsip *Aut Dedere Aut Judicare* terhadap para pelaku *cybercrime* lintas negara. Prinsip *Aut Dedere Aut Judicare* dilahirkan dari pemikiran Cherif Bassiouni,[49] dimana setiap negara memiliki kewajiban untuk menuntut dan untuk mengadili pelaku kejahatan internasional dan melakukan kerjasama dengan negara lain untuk menangkap serta mengadili pelaku kejahatan internasional. Pada dasarnya, jika seorang tersangka kriminal ditemukan di suatu negara tertentu, negara tersebut harus memilih antara mengekstradisi individu tersebut untuk diadili di Negara lain atau di hadapan pengadilan pidana internasional, atau mengadili individu itu sendiri.[50] Menurut *International Law Commission* (ILC), tujuan mendasar dari prinsip ini adalah "untuk memastikan bahwa individu yang bertanggung jawab atas kejahatan yang sangat serius dibawa ke pengadilan dengan menyediakan penuntutan dan penghukuman yang efektif terhadap individu tersebut oleh yurisdiksi yang kompeten".[51] Sehingga dapat disimpulkan bahwa pemberlakuan prinsip *Aut Dedere Aut Judicare* dimaksudkan untuk para pelaku yang melakukan kejahatan internasional, maupun transnasional harus diadili tanpa adanya impunitas atau alasan apapun.[52]

Prof. Eddy O.S. Hiariej juga menyatakan bahwa kejahatan internasional merupakan tindakan yang oleh konvensi internasional dimaksudkan sebagai kejahatan yang bertentangan dengan hukum internasional, kejahatan dilakukan kepada masyarakat internasional, yang penuntutan dan penghukumnya dapat dilandasi melalui prinsip *Aut Dedere Aut Judicare.*[53] *Cybercrime* yang merupakan kejahatan internasional[54] dapat menggunakan prinsip *Aut Dedere Aut Judicare* dalam menghadapi problematika penanganan pidana bagi pelaku *cybercrime* lintas negara. Hal tersebut juga dinyatakan dalam *transmission control protocol internet protocol* sebagai basis baru yang menghubungkan antar negara bahkan antar pulau melalui jaringan

---

47 Firdaus Firdaus, "Kedudukan Hukum Internasional Dalam Sistem Perundang-Undang Nasional Indonesia" (2014) 8:1 Fiat Justisia J Ilmu Huk 36–52, hlm. 45.

48 Yuliana Surya Galih, "Yurisdiksi Hukum Pidana Dalam Dunia Maya" (2019) 7:1 J Ilm Galuh Justisi 59–74, hlm. 68.

49 M. Cherif Bassiouni dan Edward M. Wise, *Aut Dedere Aut Judicare: The Duty to Extradite or Prosecute in International Law* (London: Martinus Nijhoff, 1995).

50 Penny Brouma, "Aut Dedere Aut Judicare: To Extradite or to Prosecute? That Is the Question," *the SAFIA Blog* (blog), 2021, https://thesafiablog.com/2021/05/06/aut-dedere-aut-judicare-to-extradite-or-to-prosecute-that-is-the-question/.

51 *Brouma.*

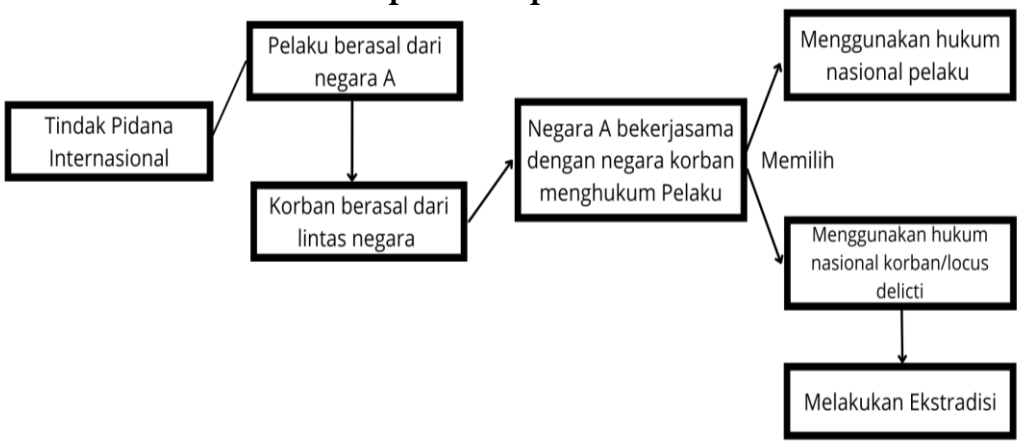
52 Harry D Gould, "The Principle of Universal Jurisdiction" in *Leg Punishm Int Law* (New York: Palgrave Macmillan US, 2010), hlm. 81-86.

53 Eddy O S Hiariej, *Pengantar Hukum Pidana Internasional*, pertama ed (Jakarta: Erlangga, 2009), hlm. 46-54.

54 Andri Winjaya Laksana, "Cybercrime Comparsion Under Criminal Law in Some Countries" (2018) 5:2 J Pembaharuan Huk 217–226, hlm. 217-218.

internet telah mengubah jarak dan waktu menjadi tidak terbatas, sehingga *cybercrime* tidak lagi menjadi kejahatan yang bersifat nasional melainkan internasional. Oleh sebab itu, intrumen hukum internasional harus mengakomodir kebutuhan hukum kejahatan *cybercrime* tersebut. Indikator *cybercrime* dapat dikatakan sebagai kejahatan internasional menurut M. Cherif Bassiouni adalah terdapatnya tiga (3) unsur sebagai berikut:[55] 1) Unsur internasional termasuk di dalamnya ancaman secara langsung dan tidak langsung atas perdamaian dunia dan menggoyah perasaan kemanusiaan; 2) Unsur transnasional termasuk didalamnya bahwa dampak yang ditimbulkan memiliki dampak terhadap lebih dari satu negara, terhadap warga negara lebih dari satu negara, dan sarana dan prasarana serta metode yang digunakan melampaui batas-batas territorial suatu negara; dan 3) Unsur kebutuhan termasuk didalamnya kebutuhan akan kerjasama antar negara-negara untuk melakukan penanggulangan.

Gambar 3. Penerapan Prinsip *Aut Dedere Aut Judicare*.



Sumber: Analisis dari Penulis

Melalui uraian unsur kejahatan internasional tersebut, asas *aut dedere aut judicare* dapat digunakan terhadap pelaku bebrbagai jenis *cybercrime* lintas negara selama memenuhi ketiga unsur tersebut. Dengan penerapan prinsip tersebut, Indonesia memiliki kewajiban untuk mengekstradisi, dan mengadili pelaku kejahatan internasional serta memiliki kewajiban untuk menjalin kerjasama dengan negara lain guna menahan, menuntut, dan mengadili pelaku *cybercrime.* Pengadopsian atau ratifikasi *Budapest Convention* sebagai wujud pelaksanaan prinsip *Aut Dedere Aut Judicare* urgen untuk dilakukan. Sejatinya, Indonesia pada tahun 2009 telah mempersiapkan Rancangan Undang-Undang Ratifikasi Budapest *EU Convention on Cybercrime* 2001, namun gagal karena substansi pengaturan dalam konvensi tersebut tidak sesuai dengan hukum nasional terkhusus *cyberporn.*[56] Padahal jika dikaji pada saat ini, *cybercrime* dengan jenis *cyberporn* telah marak terjadi dan

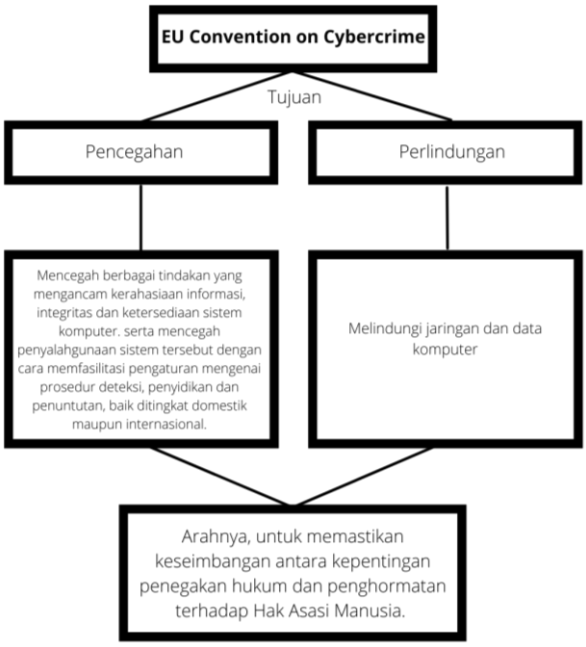
---

[55] Maskun Maskun dkk., "Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer," *Masalah-Masalah Hukum* 42, no. 4 (2013): 511–19, hlm. 515.

[56] Dilihat pada Putusan Mahkamah Konstitusi (MK) Nomor 78/PUU-XVll/2019 tentang Perkara Pengujian Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta terhadap Undang- Undang Dasar Negara Republik Indonesia Tahun 1945, hlm. 128.

bahkan meresahkan masyarakat.[57] Namun demikian, *Budapest Convention* hanya dijadikan sebagai inspirasi kehadiran UU ITE, tanpa adanya upaya untuk melakukan ratifikasi.[58] Sehingga, Indonesia yang tidak meratifikasi konvensi tersebut bukan merupakan anggota *Budapest Convention*, yang membuat Indonesia harus menghadapi problematika karena tidak adanya ikatan kerjasama internasional. Hal ini berimbas terhadap tidak memungkinkannya untuk melakukan ekstradisi, tidak mendapatkan investigasi dan keterbukaan informasi, serta tidak terfasilitasi penggunaan alat bukti sesuai dengan prinsip yurisdiksi ekstra teritorial. Sehingga upaya untuk melakukan ratifikasi *Budapest Convention* sebagai wujud pelaksanaan prinsip *Aut Dedere Aut Judicare* menjadi urgensi yang harus dilakukan.

Gambar 4. Tujuan Kehadiran *Budapest Convention*.[59]



Sumber: Analisis dari Penulis

Adanya *Budapest Convention* yang menerapkan prinsip *Aut Dedere Aut Judicare* menjadi angin segar bagi negara-negara yang memiliki permasalahan terkait yurisdiksi teritorial *cybercrime.* Prinsip *Aut Dedere Aut Judicare* sejatinya telah tertuang dalam Pasal 22 ayat 1 huruf d yang menyatakan bahwa apabila terjadi pelanggaran oleh salah satu warga negaranya, maka dapat dihukum sesuai dengan hukum yang berlaku dimana pelanggaran tersebut dilakukan atau dilakukan diluar wilayah kewenangan negara manapun. Sehingga dalam pelaksanaannya juga harus melakukan kerjasama internasional yang tertuang dalam Pasal 23 *Budapest*

---

[57] Made Julia Mahayanti & I Dewa Gede Dana Sugama, "Tindak Pidana Cyberpornography Yang Melibatkan Anak Di Bawah Umur" (2021) 10:8 Kertha Wicara J Ilmu Huk 586–598, hlm. 589.

[58] Radita Setiawan & Muhammad Okky Arista, "Efektivitas Undang-Undang Informasi dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana" (2013) 2:2 J Huk Pidana Dan Penanggulangan Kejahatan 139–146, hlm. 144.

[59] Dianalisis melalui EU Convention on Cybercrime 2001 dan penelitian Muhamad Amirulloh, *Arti Penting Ratifikasi European Union Convention on Cybercrime 2001 Bagi Indonesia* Universitas Padjajaran, 2008), hlm. 25-29.

Convention yang mengungkapkan bahwa seluruh negara yang telah menyepakati konvensi ini melakukan kerjasama satu sama lain yang bersifat timbal balik hingga tahap penyidikan atau proses-proses terkait perbuatan melawan hukum yang berkaitan dengan *cybercrime.* Bahkan, *Budapest Convention* juga terbuka untuk setiap negara[60] melalui persetujuan, ratifikasi, penyimpanan instrumen, dan penerimaan, yang tertuang dalam Pasal 36 *Budapest Convention*. Lebih lanjut, *Budapest Convention* juga telah memiliki pengaturan pidana substantif kepada pelaku *cybercrime* yang tertuang dalam Pasal 2 hingga Pasal 13. Terkait Hukum Acara juga telah diatur dalam Pasal 14 hingga Pasal 21 *Budapest Convention*. Pemberlakuan pidana subtantif dilandaskan terhadap ketentuan yurisdiksi negara pada Pasal 22 *Budapest Convention*, yang mengatur terkait prinsip yurisdiksi negara sebagai wujud pemberlakuan yurisdiksi kriminal bagi pelaku *cybercrime.*

Berdasarkan data *Council of Europe*, telah ada sebanyak 75 negara yang meratifikasi *Budapest Convention* hingga Juli 2020.[61] Jika dikaji di Negara Senegal memiliki sejarah yang sama di Indonesia, karena menjadikan *Budapest Convention* hanya sebagai inspirasi tanpa adanya ratifikasi yakni dengan peraturan *Law 2008-11 of 25 Jan 2008 on cybercrime*. Namun demikian, pada tahun 2017, Senegal melakukan upaya ratifikasi dan menjadi negara ke 51 yang meratifikasi *Budapest Convention*.[62] Sama halnya dengan Republik Dominika yang awalnya memiliki peraturan *Law 53-07 on High Technology Crimes and Offences* pada tahun 2007 serta melakukan ratifikasi *Budapest Convention* pada tahun 2016.[63] Lebih lanjut, terdapat banyak kasus *cybercrime* yang telah dituntaskan melalui *Budapest Convention*, seperti: Pertama, Kasus Pornografi Anak Internasional. Pada 2019, polisi Georgia menangkap warga Australia, Warga negara Georgia dan AS atas tuduhan eksploitasi seksual anak dan pornografi anak. Dalam operasi multinasional polisi membongkar jaringan perdagangan anak yang mengeksploitasi gadis semuda 8 tahun untuk memproduksi pornografi. Materi pornografi adalah dijual baik secara lokal maupun internasional sebagian besar melalui web gelap. Operasi polisi didahului oleh kerjasama intensif antara Georgia, Australia dan Amerika Otoritas negara bagian serta Europol. Tiga telah dihukum oleh pengadilan Georgia dan divonis masing-masing 19 tahun penjara, sedangkan 21 lainnya masih diadili.[64]

Kedua, Kasus Malware GozNym. Pada tahun 2019 Georgia berpartisipasi dalam hukum multinasional berskala besar operasi penegakan di mana kejahatan dunia maya terorganisir yang kompleks dan beroperasi secara global jaringan dibongkar. Jaringan kriminal menggunakan malware GozNym untuk mencuri dan diperkirakan $100 juta dari lebih dari 41.000 korban, terutama bisnis dan mereka lembaga keuangan. Jaringan kriminal dipimpin oleh seorang warga negara Georgia

---

60 T Mhd Aulia Fitra, *Tinjauan Hukum Internasional Atas Perbuatan Hacking dan Cracking Sebagai Bentuk Dari Kejahatan Cybercrime* Universitas Sumatera Utara, 2018), hlm. 69.

61 Cybercrime Convention Committee, *The Budapest Convention on Cybercrime: benefits and impact in practice* (France: Council of Europe, 2020).

62 T-CY News, "Accession by Senegal to the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism," 2016, https://www.coe.int/en/web/cybercrime/-/accession-by-senegal-to-the-budapest-convention-on-cybercrime-and-its-protocol-on-xenophobia-and-racism.

63 Sandeep Mittal & Prof Priyanka Sharma, "A Review of International Legal Framework to Combat Cybercrime" (2017) 8:5 Int J Adv Res Comput Sci 1372–1374, hlm. 1372.

64 ABC News, "Australian Arrested in Georgia after International Child-Trafficking Ring Bust," 2019, https://www.abc.net.au/news/2019-09-20/australian-arrested-in-georgia-after-child-trafficking-ring-bust/11531194.

dan terdiri dari anggota sebagian besar dari Eropa Timur. Operasi tersebut mencapai puncaknya pada inisiasi penuntutan pidana terhadap anggota jaringan di empat berbeda negara sebagai hasil kerjasama antara Georgia, Amerika Serikat, Ukraina, Moldova, Jerman, Bulgaria, Europol dan Eurojust. Georgia berhasil menuntut pimpinan sindikat dan rekannya yang divonis 7 tahun 5 tahun di penjara, masing masing. Penuntutan Georgia sangat bergantung pada bukti yang dibagikan oleh mitra operasi internasional.[65]

Sehingga, dengan melihat bukti keefektivan dalam penerapan prinsip *Aut Dedere Aut Judicare* dan keuntungan melakukan ratifikasi *Budapest Convention*, sudah seyogyanya Indonesia turut meratifikasi konvensi tersebut. Dengan diterapkannya prinsip *Aut Dedere Aut Judicare* dan diratifikasinya *Budapest Convention* kedalam hukum nasional Indonesia, maka negara akan lebih mudah dalam menghadapi berbagai kasus kejahatan *cybercrime*. Apalagi jika merujuk pada pendapat J. E Sahetapy yang mengatakan bahwa sebenarnya meski terdapat UU ITE negara Indonesia sebenarnya masih belum mampu menghadapi berbagai jenis kejahatan dalam *cybercrime*, karena tidak semudah itu apabila hanya menilai kejahatan komputer berupa pencurian data sebagai pencurian.[66] Lebih lanjut juga, keuntungan Indonesia melakukan ratifikasi *Budapest Convention* akan menyangkut kerjasama internasional, sehingga akan memudahkan ekstradisi, investigasi, keterbukaan informasi, alat bukti, dan pelaksanaan secara efektif prinsip yurisdiksi ekstra teritorial.[67] Melalui penerapan prinsip *Aut Dedere Aut Judicare* melalui upaya ratifikasi *Budapest Convention* diharapkan mampu memecahkan problematika penanganan *cybercrime* di Indonesia serta menangani pelaku *cybercrime* lintas negara.

Kesimpulan

Kemajuan teknologi pada saat ini tidak hanya memberikan dampak positif, tetapi juga halnya membawa dampak negatif dengan munculnya berbagai kejahatan seperti *cybercrime. Cybercrime* memiliki jenis karakteristik yang berbeda dengan tindak pidana lainnya, sehingga pendekatan konvensional tidak dapat dilakukan lagi. Negara Indonesia pada saat ini masih belum memiliki regulasi khusus yang mengatur *cybercrime,* namun demikian beberapa delik *cybercrime* telah diatur dalam KUHP dan UU ITE. Kehadiran KUHP dan UU ITE pada saat ini juga menuai problematika, salah satunya adalah ketidakmampuan menjerat pelaku *cybercrime* yang berasal dari lintas negara. Jika dikaji dalam KUHP, pengaturan masih bersifat konvensional, serta tidak adanya delik terkajian kejahatan yang dilakukan melalui komputer atau internet. Lebih lanjut juga, Pasal 2 dan Pasal 37 UU ITE sejatinya telah mengenal prinsip universal atau lintas teritorial. Namun, polemik terkait yurisdiksi membuat peraturan tersebut sulit untuk dilakukan, bahkan memungkinkan munculnya konflik yurisdiksi, terlebih Indonesia pada saat ini masih belum memiliki kerjasama internasional dalam memberantas *cybercrime.* Hingga saat

---

65 Europol, "Goznym Malware: Cybercriminal Network Dismantled In International Operation," 2019, https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation.

66 Abdul Rauf & Hardi, "Implementasi Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Di Bidang Komputer" (2016) 5:1 SISITI Semin Ilm Sist Inf Dan Teknol Inf 75–86, hlm. 79.

67 Muhammad Amirulloh, Ida Padmanegara, dan Tyas Dian Anggraeni, *Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi* (Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2009).

ini, permasalahan tersebut belum mampu terselesaikan, meskipun kejahatan *cybercrime* semakin marak dan menimbulkan kerugian ekonomi yang tidak sedikit.

Oleh karena itu, perlu adanya pengadopsian prinsip *Aut Dedere Aut Judicare* bagi pelaku *cybercrime* lintas negara. Prinsip *Aut Dedere Aut Judicare* memiliki makna bahwa setiap negara memiliki kewajiban untuk menuntut dan untuk mengadili pelaku kejahatan internasional dan melakukan kerjasama dengan negara lain untuk menangkap serta mengadili pelaku kejahatan internasional. Namun demikian, untuk menerapkan prinsip tersebut diperlukannya upaya untuk melakukan ratifikasi *Budapest Convention*. Prinsip *Aut Dedere Aut Judicare* tertuang dalam Pasal 22 ayat 1 huruf d *Budapest Convention*. Sehingga dengan adanya upaya ratifikasi konvensi tersebut, maka terjalinlah kerjasama internasional yang akan memudahkan ekstradisi, investigasi, keterbukaan informasi, alat bukti, dan pelaksanaan secara efektif prinsip yurisdiksi ekstra teritorial. Terlebih, hingga Juli 2020 telah ada sebanyak 75 negara yang meratifikasi *Budapest Convention*. Sehingga, dengan adanya pengadopsian prinsip *Aut Dedere Aut Judicare* melalui ratifikasi *Budapest Convention* mampu memecahkan permasalahan *cybercrime* di Indonesia.

Daftar Pustaka:

ABC News. "Australian Arrested in Georgia after International Child-Trafficking Ring Bust," 2019. https://www.abc.net.au/news/2019-09-20/australian-arrested-in-georgia-after-child-trafficking-ring-bust/11531194.

Amirulloh, Muhamad. "Arti Penting Ratifikasi European Union Convention on Cybercrime 2001 Bagi Indonesia." Universitas Padjajaran, 2008.

Amirulloh, Muhammad, Ida Padmanegara, dan Tyas Dian Anggraeni. Kajian EU Convention on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi. Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2009.

Arief, Barda Nawawi. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia. Jakarta: PT RajaGrafindo Persada, 2006.

Aries, Albert. "Jangkauan Yurisdiksi UU ITE Menjerat Pelaku Cracking Server Milik Asing." hukumonline.com, 2018. https://www.hukumonline.com/klinik/a/jangkauan-yurisdiksi-uu-ite-menjerat-pelaku-icracking-server-i-milik-asing-lt517d0337ad845.

Azzam, Farouq Ahmad Faleh Al. "The Adequacy of the International Cooperation Means for Combating Cybercrime and Ways to Modernize It." JANUS.NET 10, no. 1 (2019): 67–83.

Bassiouni, M. Cherif, dan Edward M. Wise. Aut Dedere Aut Judicare: The Duty to Extradite or Prosecute in International Law. London: Martinus Nijhoff, 1995.

Brouma, Penny. "Aut Dedere Aut Judicare: To Extradite or to Prosecute? That Is the Question." the SAFIA Blog (blog), 2021. https://thesafiablog.com/2021/05/06/aut-dedere-aut-judicare-to-extradite-or-to-prosecute-that-is-the-question/.

Bunga, Dewi. "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime." Jurnal Legislasi Indonesia 16, no. 1 (22 April 2019): 1–15. https://doi.org/10.54629/jli.v16i1.456.

Caligiuri, Andrea. "Governing International Cooperation in Criminal Matters: The Role of the Aut Dedere Aut Judicare Principle." International Criminal Law Review 18, no. 2 (2018): 244–74. https://doi.org/10.1163/15718123-01802005.

Christianingrum, Ratna, dan Ade Nurul Aida. Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan. Jakarta: Pusat Kajian Anggaran Badan Keahlian-Sektretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia, 2021.

Cross, Michael. Scene of Cybercrime Second Edition. Burlington: Syngress, 2008.

Cybercrime Convention Committee. The Budapest Convention on Cybercrime: benefits and impact in practice. France: Council of Europe, 2020.

Europol. "Goznym Malware: Cybercriminal Network Dismantled In International Operation," 2019. https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation.

Firdaus, Firdaus. "Kedudukan Hukum Internasional Dalam Sistem Perundang-Undang Nasional Indonesia." Fiat Justisia: Jurnal Ilmu Hukum 8, no. 1 (2014): 36–52. https://doi.org/10.25041/fiatjustisia.v8no1.285.

Fitra, T. Mhd Aulia. "Tinjauan Hukum Internasional Atas Perbuatan Hacking dan Cracking Sebagai Bentuk Dari Kejahatan Cybercrime." Universitas Sumatera Utara, 2018. https://repositori.usu.ac.id/handle/123456789/5434.

Galih, Yuliana Surya. "Yurisdiksi Hukum Pidana Dalam Dunia Maya." Jurnal Ilmiah Galuh Justisi 7, no. 1 (2019): 59–74. https://doi.org/10.25157/jigj.v7i1.2138.

Gani, Hamsu Abdul, dan Andika Wahyudi Gani. "Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No.11 Tahun 2008 dan UU No.19 Tahun 2016." Prosiding Seminar Nasional LP2M UNM, 2019. https://ojs.unm.ac.id/semnaslemlit/article/view/11257.

Gould, Harry D. "The Principle of Universal Jurisdiction." Dalam The Legacy of Punishment in International Law, 81–108. New York: Palgrave Macmillan US, 2010. https://doi.org/10.1057/9780230113077_5.

Handoko, Cahyo. "Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime di Pengadilan." Jurnal Jurisprudence 6, no. 1 (2017): 1–15. https://doi.org/10.23917/jurisprudence.v6i1.2992.

Hiariej, Eddy O. S. Pengantar Hukum Pidana Internasional. Pertama. Jakarta: Erlangga, 2009.

Irham, Apripari. "Penegakkan Yurisdiksi International Criminal Court Atas Kejahatan Agresi Pasca Kampala Amendments Diadopsi Dalam Rome Statute." SASI 26, no. 4 (2020): 540–56. https://doi.org/10.47268/sasi.v26i4.272.

Iskandar. "Kilas Balik Perang Hacker Indonesia vs Australia." liputan6.com, 2014. https://www.liputan6.com/tekno/read/826144/kilas-balik-perang-hacker-indonesia-vs-australia.

Jati, Anggoro Suryo. "Mengenal Naikon, Grup Hacker China yang Serang Indonesia." Detik.com, 2020. https://inet.detik.com/security/d-5034437/mengenal-naikon-grup-hacker-china-yang-serang-indonesia.

Jhon, Ranty Mahardika. "Existence of Criminal Law on Dealing Cybercrime in Indonesia." IJCLS (Indonesian Journal of Criminal Law Studies) 3, no. 1 (31 Mei 2018): 25–34. https://doi.org/10.15294/ijcls.v3i1.16945.

Johnson, David R., dan David Post. "Law and Borders: The Rise of Law in Cyberspace." Stanford Law Review 48, no. 5 (1996): 1367–1402. https://doi.org/10.2307/1229390.

Kartiko, Galuh. "Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional." Rechtidee 8, no. 2 (2013): 136–53. https://doi.org/10.21107/ri.v8i2.695.

Kusnandar, Viva Budy. "Pengguna Internet Indonesia Peringkat ke-3 Terbanyak di Asia | Databoks." Katadata.co.id, 2021. https://databoks.katadata.co.id/datapublish/2021/10/14/pengguna-internet-indonesia-peringkat-ke-3-terbanyak-di-asia.

Laksana, Andri Winjaya. "Cybercrime Comparsion Under Criminal Law in Some Countries." Jurnal Pembaharuan Hukum 5, no. 2 (14 Agustus 2018): 217–26. https://doi.org/10.26532/jph.v5i2.3008.

———. "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif." Jurnal Hukum 35, no. 1 (2019): 52–76. https://doi.org/10.26532/jh.v35i1.11044.

Mahayanti, Made Julia, dan I. Dewa Gede Dana Sugama. "Tindak Pidana Cyberpornography Yang Melibatkan Anak Di Bawah Umur." Kertha Wicara : Journal Ilmu Hukum 10, no. 8 (15 Juli 2021): 586–98. https://doi.org/10.24843/KW.2021.v10.i08.p02.

Marwin, Marwin. "Penanggulangan Cyber Crime Melalui Penal Policy." ASAS 5, no. 1 (2013): 1–9. https://doi.org/10.24042/asas.v5i1.1693.

Maskun, Maskun, Alma Manuputty, S. M. Noor, dan Juajir Sumardi. "Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer." Masalah-Masalah Hukum 42, no. 4 (2013): 511–19.

Mathilda, Fiorida. "Cyber Crime Dalam Sistem Hukum Indonesia." Sigma-Mu 4, no. 2 (2012): 34–45. https://doi.org/10.35313/sigmamu.v4i2.870.

Melani, Melani, Hari Disemadi, dan Nyoman Jaya. "Kebijakan Hukum Pidana Dibidang Transaksi Elektronik Sebagai Tindak Pidana Non-Konvensional." Pandecta Research Law Journal 15, no. 1 (18 Juni 2020): 111–20. https://doi.org/10.15294/pandecta.v15i1.19469.

Miharja, Muhammad Najamuddin Dwi, dan Ahmad Fauzi. "Peningkatan Keamanan Login Pada Content Management System (CMS) Wordpress Dengan Implementasi Notifikasi Login Dengan Whatsapp Gateway." Jurnal SIGMA 12, no. 4 (2021): 41–44.

Mittal, Sandeep, dan Prof Priyanka Sharma. "A Review of International Legal Framework to Combat Cybercrime." International Journal of Advanced Research in Computer Science 8, no. 5 (2017): 1372–74. https://doi.org/10.2139/ssrn.2978744.

Mustaqimah, Lailatul. "Penerapan Asas Nasionalitas Pasif Terhadap Tindak Pidana Teknologi Informasi." Badamai Law Journal 1, no. 2 (26 September 2016): 322–42. https://doi.org/10.32801/damai.v1i2.1826.

Octora, Rahel. "Penerapan Asas Nasionalitas Pasif Dan Pemidanaan Pembantu Tindak Pidana Perdagangan Orang Dalam Rkuhp." Kertha Patrika 40, no. 3 (2018): 155–74. https://doi.org/10.24843/KP.2018.v40.i03.p03.

Putra, Akbar Kurnia. "Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasional." Jurnal Ilmu Hukum Jambi 5, no. 2 (2014): 95–109.

Putri, Novalinda Nadya. "Penerapan Prinsip Aut Dedere Aut Judicare Dalam Penegakan Hukum Pidana Internasional." DE LEGA LATA: Jurnal Ilmu Hukum 6, no. 1 (7 Januari 2021): 139–67. https://doi.org/10.30596/delegalata.v6i1.5537.

Rachmadie, Donovan Typhano, dan ' Supanto. "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 1 Tahun 2016." Jurnal Hukum Pidana Dan Penanggulangan Kejahatan 9, no. 2 (2 Mei 2020): 128–56.

Rauf, Abdul, dan Hardi. "Implementasi Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan Di Bidang Komputer." SISITI : Seminar Ilmiah Sistem Informasi dan Teknologi Informasi 5, no. 1 (2016): 75–86.

Rizal, Muhamad, dan Yanyan Yani. "Cybersecurity Policy and Its Implementation in Indonesia." JAS (Journal of ASEAN Studies) 4, no. 1 (2016): 61–78. https://doi.org/10.21512/jas.v4i1.967.

Rumlus, Muhamad Hasan, dan Hanif Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik." Jurnal HAM 11, no. 2 (2020): 285–99. https://doi.org/10.30641/ham.2020.11.285-299.

Sabillon, Regner, Jeimy Cano, Víctor Reyes, dan Jordi Serra Ruiz. "Cybercrime and Cybercriminals: A Comprehensive Study." International Journal of Computer Networks and Communications Security 4, no. 6 (2016): 165–76.

Salsabila, Putri Zakia. "Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi." Kompas.com, 2020. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi.

Saputri, Dessy Suciati. "Indonesia Peringkat ke-2 Dunia Kasus Kejahatan Siber." Republika Online, 2015. https://republika.co.id/berita/nasional/umum/15/04/09/nmjajy-indonesia-peringkat-ke2-dunia-kasus-kejahatan-siber.

Setiawan, Radita, dan Muhammad Okky Arista. "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana." Jurnal Hukum Pidana Dan Penanggulangan Kejahatan 2, no. 2 (2013): 139–46.

Soekanto, Soerjono, dan Sri Mamudji. Penelitian Hukum Normatif : Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada, 2003.

Suhariyanto, Budi. Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya. Jakarta: Rajawali Press, 2013.

Suharto, Miko Aditiya, dan Maria Novita Apriyani. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." Risalah Hukum, 2021, 98–107. https://doi.org/10.30872/risalah.v17i2.705.

Tahir, Anriyan Ridwan. "Analisis Hukum Terhadap Kejahatan Siber (Cybercrime) Pencurian Data Berupa Hak Cipta (Copyright) Milik Stasiun Televisi Swasta." Universitas Hasanuddin, 2018. http://digilib.unhas.ac.id/opac/detail-opac?id=45438.

T-CY News. "Accession by Senegal to the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism," 2016. https://www.coe.int/en/web/cybercrime/-/accession-by-senegal-to-the-budapest-convention-on-cybercrime-and-its-protocol-on-xenophobia-and-racism.

Thackeray, Rosemary, dan MaryAnne Hunter. "Empowering Youth: Use of Technology in Advocacy to Affect Social Change." Journal of Computer-Mediated Communication 15, no. 4 (2010): 575–91. https://doi.org/10.1111/j.1083-6101.2009.01503.x.

Tobing, Raida L. Laporan Akhir Penelitian Hukum tentang Efektifitas UU No. 11 Tahun 2008 tetang Informasi dan Transaksi Elektronik. Jakarta: Badan Pembinaan Hukum Nasional Kementrian Hukum dan HAM RI, 2010.

Wardana, Hendra Kusuma. "Yurisdiksi Terhadap Cybercrime." Thesis, Universitas Airlangga, 2010. http://lib.unair.ac.id.

Wicki-Birchler, David. "The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?" International Cybersecurity Law Review 1 (2020): 63–72. https://doi.org/10.1365/s43439-020-00012-5.