Asas ini memberikan kekuasaan kepada negara untuk mengadili para pelaku kejahatan dengan menggunakan hukum dari negara tersebut sehubungan dengan tindakan kejahatan ekstrateritorial yang mengancam dan membahayakan kepentingan negara[28].

BAB III

[28] "*Criminal Jurisdiction of States under International Law"*, *Max Planck Encyclopedia of International Law, Oxford Public International Law,* 2011.

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Penelitian

Penerapan Ketentuan-Ketentuan dalam Hukum Internasional kedalam Proses penegakan Hukum Nasional

Hukum internasional merupakan suatu sumber hukum yang biasanya digunakan oleh komunitas internasional. Tidak hanya untuk kepentingan internasional, hukum internasional juga berguna untuk kepentingan nasional atau domestik. Suatu negara dapat mengadopsi norma-norma yang ada dalam suatu hukum internasional maupun konvensi-konvensi untuk diberlakukan di dalam hukum nasional negaranya[29]. Pernyataan ini didukung oleh pendapat bahwa hukum internasional dapat berperan sebagai norma dan ketentuan yang sangat efektif dalam sebuah masyarakat karena memiliki hubungan yang efektif dengan pengaturan dalam hukum nasional[30]. Hal tersebut menunjukan bahwa hukum internasional dan hukum nasional dapat digunakan berdampingan. Jika norma-norma dalam hukum nasional itu dinilai kurang dalam mengatur suatu tindak pidana, norma-norma dalam suatu hukum internasional yang mengatur tentang tindak pidana yang sama dapat digunakan. Kemudian, jika yang terjadi itu adalah suatu tindak pidana transnasional, kasus tersebut memerlukan kerjasama antar negara. Jika sudah seperti itu, negara-negara tersebut dapat membuat forum, misalnya forum tersebut dapat berbentuk konvensi, dimana forum itu kemudian menghasilkan suatu konsensus. Konsensus ini yang kemudian menjadi suatu ketentuan internasional, dimana ketentuan tersebut dapat mengatur tentang, bagaimana bentuk kerjasama dalam proses penegakan hukum, atau bagaimana ketentuan pemidanaannya. Intinya, konsensus ini yang kemudian membentuk suatu keseragaman praktik dalam proses

[29] Berdasarkan hasil wawancara dengan Ninon Melatyugra, S.H., M.H. pada tanggal 26 Maret 2022
[30] Dina Sunyowati, 2013, "Hukum Internasional Sebagai Sumber Hukum Dalam Hukum Nasional", *Jurnal Hukum dan Peradilan*, Vol. 2, Nomor 1, hlm. 76, diakses pada tanggal 14 April 2022 dari https://www.jurnalhukumdanperadilan.org/index.php/jurnalhukumperadilan.

penegakan hukum tersebut. Jika praktik penegakan hukum tersebut itu seragam, akan memudahkan negara-negara lain jika ada kasus serupa dan meminimalisir terjadinya ketegangan antar negara[31].

Lalu bagaimana dengan penerapan *Convention on Cybercrime*, sebagai alat penegakan hukum meskipun belum diratifikasi? Penerapan *Convention on Cybercrime* sebagai alat penegakan hukum meskipun belum diratifikasi dinilai sangat memungkinkan. Selain melalui proses ratifikasi, suatu negara juga dapat mengadopsi norma-norma yang ada dalam suatu hukum internasional maupun konvensi-konvensi untuk diberlakukan di dalam hukum nasional negaranya[32]. Ada juga pendapat bahwa norma-norma dalam suatu hukum internasional dapat diterima sebagai bagian dari pembentukan hukum melalui prosedur dan tata cara tertentu karena dinilai sebagai suatu bidang hukum yang berdiri sendiri[33].

Sebelum suatu negara memakai suatu hukum internasional sebagai alat penegakan hukum di negara tersebut, ada beberapa hal yang harus diperhatikan. Pertama yang harus diperhatikan adalah kedudukan hukum internasional sebagai norma hukum. Seperti disebut di awal, hukum internasional dapat berperan sebagai norma dan ketentuan yang sangat efektif dalam sebuah masyarakat karena memiliki hubungan yang efektif dengan pengaturan dalam hukum nasional. Salah satu contoh yang ada adalah Indonesia yang membuat Undang-undang nomor 24 tahun 2000 tentang Perjanjian Internasional, yang dimana isinya hampir 80% mengadopsi norma-norma dari Konvensi Wina 1969, meski tidak meratifikasi Konvensi tersebut[34]. Kedua adalah kesesuaian konstitusi sebagai aspek penting dalam mengadopsi sebuah hukum internasional[35]. Produk hukum yang terbentuk secara formal berdasarkan suatu hukum internasional bukan merupakan turunan dari suatu

---

[31] Ninon Melatyugra, *Loc.cit.*
[32] *Ibid.*
[33] Dina Sunyowati, *Loc.cit.,* hlm. 75.
[34] Ninon Melatyugra, *Loc.cit.*
[35] *Ibid.*

hukum internasional, melainkan hukum yang dapat terbentuk berdasarkan kesesuaian konstitusi negara sebagai dasar hukum tertinggi[36]. Suatu negara harus terlebih dahulu memperhatikan substansi dari hukum internasional tersebut apakah norma-norma dan substansi yang terkandung dalam hukum internasional tersebut sesuai dengan konstitusi negaranya. Ketiga adalah yurisdiksi suatu negara berdasarkan suatu hukum internasional[37]. Hal ini penting sebab negara memiliki hak untuk mengatur negaranya sendiri tanpa campur tangan dari pihak dan negara lain[38].

Pada dasarnya, hukum internasional tidak memiliki otorisasi langsung untuk mengatur suatu tindak pidana karena menurut peraturan perundang-undangan, pemidanaan terhadap suatu tindakan itu merupakan ranah dari hukum nasional. Hal ini terjadi demikian agar warga negara tahu bahwa ada hak asasi manusia yang dibatasi oleh negaranya melalui undang-undang. Pasal 2 ayat (4) Piagam PBB menyatakan bahwa hukum internasional menjamin kalau negara-negara mempunyai kedaulatan dalam mengatur urusan dalam negerinya sendiri[39]. Oleh sebab itu undang-undang tentang pemidanaan adalah ranah dari hukum nasional. Tetapi setelah dibentuk PBB, pengaturan soal HAM dalam forum internasional mengalami perkembangan. Kebiasaan forum internasional juga menunjukkan bahwa penegakan HAM yang dilakukan oleh suatu negara tidak dapat terlepas dari ranah hukum internasional[40]. Peran hukum internasional dalam pemidanaan suatu tindak pidana hanya sebatas tindakan persuasif, dimana biasanya hukum internasional itu mengajak negara-negara membentuk suatu kesamaan praktik. Contohnya soal *cybercrime*,

---

[36] Isharyanto, 2017, Hukum Internasional dalam Pusaran Politik dan Kekuasaan, Tangerang Selatan: Pustakapedia, hlm 31, Diakses pada tanggal 17 Mei 2022 dari https://layanan.hukum.uns.ac.id/.
[37] Ninon Melatyugra, *Loc.cit.*
[38] Raisamba, 2021, "Tinjauan Yuridis Konvensi Budapest 2001 Dalam Aktivitas Ilegal Pada *Deep Web*", Skripsi: Fakultas Hukum Universitas Pasundan, hlm. 28. diakses pada tanggal 17 Mei 2022 dari http://repository.unpas.ac.id/.
[39] Nadia Maulida Zuhra, 2020, "Kategorisasi Kejahatan Agresi Atas Tindakan Penggunaan Kekerasan Negara Perancis Pada Konflik Republik Mali Dalam Hukum Pidana Internasional", *Jurnal Hukum De'Rechtsstaat*, Vol. 6, Nomor 2, hlm. 174, diakses pada tanggal 17 Mei 2022 dari https://ojs.unida.ac.id/.
[40] Yustina Trihoni Nalesti Dewi, 2013, Kejahatan Perang Dalam Hukum Internasional Dan Hukum Nasional, Jakarta: PT Rajagrafindo Persada, hlm 55.

forum internasional hanya dapat mengajak negara-negara untuk menentukan apa saja bentuk-bentuk *cybercrime*, baru kemudian negara membuat undang-undangnya sendiri soal *cybercrime* berdasarkan ketentuan tersebut.

B. Pembahasan

1. Ketentuan Dalam *Convention on Cybercrime* Terhadap *Cybercrime* Khususnya Peretasan

A. Pandangan Uni Eropa terhadap *Cybercrime*

Prinsip-prinsip dalam *Convention on Cybercrime* yang tertuang dalam bagian pembuka konvensi ini menunjukan bagaimana pandangan Uni Eropa terhadap *cybercrime*. Uni Eropa menilai *Convention on Cybercrime* diperlukan sebagai pemersatu negara-negara dalam melawan *cybercrime*. Banyak sekali perubahan-perubahan akibat perkembangan teknologi dan jaringan komputer yang sangat maju. Perkembangan teknologi dan jaringan komputer yang cepat dan tidak terkendali dapat digunakan untuk melakukan tindakan kejahatan serta bukti-bukti kejahatan tersebut dapat disimpan atau dialihkan dalam jaringan komputer, sehingga dibutuhkan suatu kebijakan dan aturan untuk melindungi pihak-pihak yang berkepentingan baik. Berdasarkan pandangan Uni Eropa, *cybercrime* perlu ditangani sebab Uni Eropa khawatir dengan resiko yang dapat ditimbulkan. Resiko-resiko seperti pelanggaran pidana serta kepentingan-kepentingan yang dapat terancam akibat adanya *cybercrime* dinilai Uni Eropa memerlukan penanganan bersama dari masyarakat internasional. Uni Eropa juga menilai bahwa masyarakat internasional memerlukan kebijakan yang bertujuan untuk melindungi masyarakat internasional terhadap *cybercrime*. Penilaian ini yang kemudian melatarbelakangi terbentuknya *Convention on Cybercrime* yang bertujuan untuk mendorong kerjasama internasional dalam menangani *cybercrime*. Pembentukan *Convention on Cybercrime* oleh Uni

Eropa juga karena Uni Eropa beserta negara-negara peserta menilai bahwa cara paling efektif dalam melawan *cybercrime* adalah dengan kerjasama internasional[41].

B. Ketentuan Mengenai *Cybercrime* di dalam *Convention on Cybercrime*

Dalam *Convention on Cybercrime,* ditetapkan ada tiga hal yang disedikan *Convention on Cybercrime* selaku hukum internasional. Pertama adalah kriminalisasi pelanggaran-pelanggaran yang termasuk ke dalam *cybercrime*, Kedua adalah hukum acara untuk menyelidiki *cybercrime* serta alat bukti elektronik terkait, dan ketiga adalah mengenai kerjasama internasional.[42] Pengaturan mengenai *cybercrime* diatur dalam pasal 2 sampai dengan pasal 11. Dalam pasal-pasal ini disebut definisi serta pelanggaran-pelanggaran apa saja yang termasuk ke dalam cybercrime. *Convention on Cybercrime* juga menyebutkan bahwa pelanggaran-pelanggaran yang terjadi dapat juga dikriminalisasi oleh hukum domestik suatu negara yang berwenang mengadili kasus tersebut. Jenis-jenis *Cybercrime* Berdasarkan *Convention on Cybercrime*[43]:

1) Akses Ilegal

Berdasarkan pasal 2 *Convention on Cybercrime*, akses ilegal adalah tindakan mengakses seluruh atau sebagian dari suatu sistem komputer dengan melanggar keamanan, yang dilakukan dengan sengaja dan tanpa hak.

2) Penyadapan Ilegal

Berdasarkan pasal 3 *Convention on Cybercrime*, penyadapan ilegal adalah tindakan penyadapan atas suatu transmisi data yang terjadi antara sistem komputer, dimana data tersebut merupakan data rahasia atau bukan data publik, yang dilakukan dengan sengaja dan tanpa hak.

---

[41] *Council of Europe*, "*Convention On Cybercrime*", Budapest, 23 November 2001, diakses pada tanggal 19 April 2022 dari https://rm.coe.int/.
[42] *Council of Europe*, "*Convention On Cybercrime: Benefits and Impact in Practice*", Stasbourg, 13 July 2020,hlm. 4, diakses pada tanggal 28 Juni 2022 dari https://rm.coe.int/.
[43] *Council of Europe*, "*Convention On Cybercrime*", Budapest, 23 November 2001, diakses pada tanggal 19 April 2022 dari https://rm.coe.int/.

3) Gangguan terhadap Data

Berdasarkan pasal 4 *Convention on Cybercrime*, gangguan terhadap data adalah tindakan menghancurkan, menghapus, merusak, merubah, atau menyembunyikan data dari suatu sistem komputer, dimana akibat dari tindakan-tindakan tersebut menyebabkan suatu pihak mengalami kerugian, dan tindakan-tindakan tersebut dilakukan dengan sengaja dan tanpa hak.

4) Gangguan terhadap Sistem

Berdasarkan pasal 5 *Convention on Cybercrime*, gangguan terhadap sistem adalah tindakan menghambat fungsi dari suatu sistem komputer dengan cara memasukan, mengirim, menghancurkan, menghapus, merusak, merubah, atau menyembunyikan data dari atau ke suatu sistem komputer yang dilakukan dengan sengaja dan tanpa hak.

5) Penyalahgunaan Gawai Elektronik

Berdasarkan pasal 6 *Convention on Cybercrime*, penyalahgunaan gawai elektronik adalah tindakan membuat, menjual, menyediakan untuk penggunaan, mengimpor, menyebarkan, atau memiliki suatu alat, program komputer, data komputer, kata sandi, atau kode akses dengan tujuan untuk melakukan pelanggaran yang disebutkan dalam pasal 2 sampai pasal 5 *Convention on Cybercrime*. Tindakan-tindakan dalam pasal ini tidak dapat diartikan sebagai tindakan pidana jika tindakan-tindakan tersebut dilakukan bukan untuk melakukan pelanggaran yang disebut dalam pasal 2 sampai pasal 5 *Convention on Cybercrime*.

6) Pemalsuan yang Berkaitan dengan Komputer

Berdasarkan pasal 7 *Convention on Cybercrime*, pemalsuan yang berkaitan dengan komputer adalah tindakan memasukan, merubah, menghapus, atau menyembunyikan data komputer, dimana berakibat data tersebut menjadi data yang tidak asli (otentik), kemudian data tersebut dianggap dan digunakan secara hukum

selayaknya data asli (otentik). Tindakan tersebut dilakukan secara sengaja dengan tanpa hak, dan data tersebut digunakan dengan maksud menipu dan maksud tidak jujur lainnya.

7) Penipuan yang Berkaitan dengan Komputer

Berdasarkan pasal 8 *Convention on Cybercrime*, penipuan yang berkaitan dengan komputer adalah tindakan memasukan, merubah, menghapus, atau menyembunyikan data komputer, dan tindakan menghambat suatu fungsi dari suatu sistem komputer yang dilakukan secara sengaja dan tanpa hak dengan tujuan mendapat keuntungan ekonomi.

8) Pelanggaran yang Berkaitan dengan Pornografi Anak

Berdasarkan pasal 9 *Convention on Cybercrime*, pelanggaran yang berkaitan dengan pornografi anak adalah tindakan membuat, menawarkan, menyediakan, menyebarkan, atau mengirim pronografi anak melalui suatu sistem komputer untuk diri sendiri maupun orang lain. Jenis yang termasuk pornografi anak dalam pasal ini adalah pornografi yang secara visual menampilkan seseorang di bawah umur, seseorang yang sepertinya masih di bawah umur, dan gambar-gambar realistis yang menampilkan seseorang di bawah umur dalam konten suatu konten seksual yang spesifik. Istilah di bawah umur dalam pasal ini mencakup seluruh orang yang berumur dibawah 18 tahun.

9) Pelanggaran yang Berkaitan dengan Hak Cipta dan Hak Terkait

Berdasarkan pasal 10 *Convention on Cybercrime*, pelanggaran yang berkaitan dengan hak cipta dan hak terkait adalah tindakan yang didefinisikan berdasarkan hukum nasional suatu negara, sesuai dengan Ketentuan Paris pada tanggal 24 Juli 1971 yang merevisi Konvensi Bern untuk Perlindungan Karya Sastra dan Artistik, perjanjian terkait tentang HAKI dan Perjanjian Hak Cipta WIPO, dimana tindakan tersebut dilakukan secara sengaja dan tanpa hak.

10) Percobaan dan Dukungan atau Persengkongkolan

Berdasarkan pasal 11 *Convention on Cybercrime*, percobaan dan dukungan atau persengkongkolan adalah tindakan membantu, mendukung atau bersekongkol dalam melakukan pelanggaran yang disebutkan dalam pasal 2 sampai pasal 10 *Convention on Cybercrime* yang dilakukan dengan sengaja.

C. Ketentuan Mengenai Tindakan Pidana Peretasan dalam *Convention on Cybercrime*

Dalam *Convention on Cybercrime*, sebenarnya kata 'peretasan' tidak ditemukan. Namun, jika melihat pengertian peretasan secara umum, pengaturan tentang tindak pidana peretasan di dalam *Convention on Cybercrime* sendiri ada di dalam pasal 2, pasal 3 dan pasal 4. Menurut pasal 2 *Convention on Cybercrime,* tindakan yang termasuk dalam akses ilegal adalah tindakan kejahatan yang dilakukan dengan sengaja untuk mengakses seluruh atau sebagian dari suatu sistem komputer. Menurut pasal 3, tindakan yang termasuk ke dalam pencegatan atau penyadapan ilegal adalah pencegatan yang dilakukan secara teknis melalui satu sistem komputer pribadi dengan target komputer lain. Menurut pasal 4, tindakan yang termasuk gangguan terhadap data adalah merusak, menghapus, menurunkan kualitas, mengubah atau menekan data dalam suatu sistem komputer. Semua tindakan tersebut dilakukan secara ilegal, tanpa hak dan tanpa izin. Tindakan-tindakan tersebut juga dilakukan dengan melanggar keamanan, dengan tujuan untuk mendapat data atau maksud tidak jujur lainnya, atau berhubungan dengan sistem komputer yang terhubung dengan komputer lainnya. Pengertian-pengertian tersebut didukung dengan pengertian peretasan yang dikemukakan oleh Eliasta Ketaren, yaitu peretasan adalah kegiatan menyusup ke dalam suatu sistem dan jaringan komputer secara tidak sah. Maksud kata tidak sah disini adalah tanpa izin dan tanpa sepengetahuan dari pemilik sistem dan jaringan komputer tersebut. Tindakan yang termasuk tindakan-tindakan yang diatur dalam pasal 2, pasal 3 dan pasal 4 juga termasuk tindakan yang diatur

dalam hukum nasional, dimana tindakan itu dilakukan dengan sengaja untuk mengakses seluruh atau sebagian dari suatu sistem komputer tanpa izin. Tindakan yang diatur dalam hukum nasional berarti tindakan yang ditetapkan dan masih diberlakukan di dalam peraturan perundang-undangan suatu negara. Dalam hukum nasional indonesia, peretasan diatur dalam pasal 30 Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, dimana dalam 3 ayat dalam pasal tersebut diatur bahwa kegiatan yang dilarang adalah kegiatan mengakses komputer dan/atau sistem elektronik secara sengaja dan tidak sah. Akses tidak sah ini maksudnya dilakukan dengan melawan hukum dan akses dilakukan dengan menerobos, melampaui atau menjebol sistem keamanan komputer tersebut dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik. Berdasarkan bunyi pasalnya, pasal 2, pasal 3 dan pasal 4 *Convention on Cybercrime* ini mengatur tentang hukum pidana materiil. Sebagai bagian dari hukum pidana materiil, negara harus menetapkan kebijakan-kebijakan mengenai penggolongan suatu tindakan yang termasuk kedalam tindakan kriminal, sehingga tercipta suatu kriteria. Kriteria tersebut kemudian dipakai sebagai dasar-dasar pembentukan peraturan[44].

Dalam pasal 2,pasal 3 dan pasal 4 *Convention on Cybercrime* disebut juga tindakan-tindakan tersebut dilakukan dengan melanggar keamanan, dengan tujuan untuk mendapat data atau maksud tidak jujur lainnya, atau berhubungan dengan sistem komputer yang terhubung dengan komputer lainnya. Berdasarkan bunyi tersebut, delik yang dinyatakan dalam pasal-pasal *Convention on Cybercrime* ditetapkan sebagai serangan terhadap suatu kerahasiaan, ketersediaan, serta kredibilitas data suatu sistem komputer[45].

1. Penerapan Ketentuan dalam *Convention on Cybercrime* terhadap Warga Negara Indonesia Pelaku Kejahatan Peretasan Transnasional

[44] Muhamad Amirulloh, Ida Padmanegara, dan Tyas Dian Anggraeni, *Op. cit.,* hlm. 7.
[45] *ibid.,* hlm. 23.

A. Hal-hal yang Harus Diperhatikan sebelum Menerapkan Suatu Hukum Internasional

1) Hukum Internasional Sebagai Norma Hukum

Hukum internasional awalnya dibuat sebagai sumber hukum untuk komunitas-komunitas internasional. Hukum internasional berperan sebagai norma-norma bagi masyarakat internasional dalam membuat kepentingan-kepentingan internasional[46]. Kemudian peran hukum internasional berkembang. Tidak hanya berguna untuk kepentingan internasional, hukum internasional juga berguna untuk kepentingan nasional atau kepentingan domestik. Suatu negara dapat mengadopsi norma-norma yang ada dalam suatu hukum internasional maupun konvensi-konvensi untuk diberlakukan di dalam hukum nasional negaranya. Hukum internasional dapat berperan sebagai norma dan ketentuan yang sangat efektif dalam sebuah masyarakat karena memiliki hubungan yang efektif dengan pengaturan dalam hukum nasional[47]. Salah satu contoh yang ada adalah Indonesia yang membuat Undang-undang nomor 24 tahun 2000 tentang Perjanjian Internasional, yang dimana isinya hampir 80% mengadopsi norma-norma dari Konvensi Wina 1969, meski tidak meratifikasi Konvensi tersebut. Hal tersebut yang kemudian menunjukan bahwa hukum internasional itu ada karena dibutuhkan sebagai norma hukum, yang dibutuhkan dalam level internasional maupun level nasional.

2) Kesesuaian Konstitusi Sebagai Aspek Penting dalam Mengadopsi Sebuah Hukum Internasional

Dalam mengadopsi hukum internasional menjadi hukum nasional sebuah negara, ada aspek penting yang harus diperhatikan. Sebelum meratifikasi atau mengadopsi sebuah hukum internasional, negara harus terlebih dahulu memperhatikan substansi serta norma-norma dari hukum internasional tersebut.

[46] Dina Sunyowati, *Loc.cit.,* hlm. 75.
[47] *Ibid.,* hlm. 76.

Produk hukum yang terbentuk secara formal berdasarkan suatu hukum internasional bukan merupakan turunan dari suatu hukum internasional, melainkan hukum yang dapat terbentuk berdasarkan kesesuaian konstitusi negara sebagai dasar hukum tertinggi[48]. Suatu negara harus terlebih dahulu memperhatikan substansi dari hukum internasional tersebut apakah norma-norma dan substansi yang terkandung dalam hukum internasional tersebut sesuai dengan konstitusi negaranya. Untuk Indonesia sendiri, konstitusi Indonesia sebenarnya tidak mengatur tentang bagaimana posisi hukum internasional di hukum nasional Indonesia. Akibatnya, praktik hukum internasional yang terjadi di Indonesia kadang tidak seragam dengan negara-negara lain. Tapi negara masih bisa menentukan hal-hal apa saja yang tidak sesuai dengan konstitusi tersebut. Dengan menentukan hal-hal apa saja yang tidak sesuai dengan konstitusi, negara kemudian dapat menilai suatu hukum internasional dapat digunakan atau tidak. Menentukan hal-hal tersebut mengacu kepada tiga hal. Yang pertama penegakan hukum harus memperhatikan sistem penerimaan suatu negara terhadap suatu aturan internasional. Yang kedua adalah bagaimana aturan internasional tersebut ditafsirkan secara universal. Yang ketiga adalah bagaimana tolak ukur pembatasan-pembatasan di dalam aturan internasional tersebut. Konstitusi berperan sebagai *filter* terhadap hukum-hukum internasional tersebut dapat diterapkan dalam wilayah nasional atau tidak[49].

3) Yurisdiksi Negara Berdasarkan Suatu Hukum Internasional

Dalam pasal 22 ayat (1) *Convention on Cybercrime* dinyatakan bahwa suatu negara dapat menerapkan yurisdiksinya atas tindakan-tindakan pidana mayantara yang dicantumkan dalam pasal 2 hingga pasal 11 *Convention on Cybercrime*. Dalam pasal 22 ayat (1) *Convention on Cybercrime* juga dinyatakan juga bahwa yurisdiksi tersebut dapat diterapkan saat tindakan-tindakan pidana mayantara yang dicantumkan

[48] Isharyanto, *Op.cit.*
[49] Ninon Melatyugra, 2016, "Mendorong Sikap Lebih Bersahabat Terhadap Hukum Internasional: Penerapan Hukum Internasional Oleh Pengadilan Indonesia", *Jurnal Refleksi Hukum*, Vol. 1, Nomor 1, hlm. 53, diakses pada tanggal 14 April 2022 dari https://ejournal.uksw.edu/refleksihukum.

dalam pasal 2 hingga pasal 11 *Convention on Cybercrime* terjadi di dalam wilayah negara tersebut, di atas kapal yang berbendera negara tersebut, di atas pesawat yang terdaftar berdasarkan hukum negara tersebut, dan saat suatu tindakan dilakukan oleh seseorang yang merupakan warga negara dari negara tersebut, dimana tindakan tersebut termasuk tindak kejahatan berdasarkan hukum negara tersebut dan tindakan itu terjadi dan berlangsung di luar wilayah negara tersebut. Kedaulatan ini hadir sebagai jaminan bahwa negara lain tidak akan mengintervensi yurisdiksi eksklusif yang dimiliki negara tersebut. Kedaulatan ini juga mengharuskan negara yang bersangkutan untuk menghormati kedaulatan serta tidak mengintervensi yurisdiksi negara lain[50].

Berdasarkan isi dari pasal 22 ayat (1) *Convention on Cybercrime*, dapat diperhatikan bahwa isi ayat tersebut menganut asas-asas hukum internasional. Yang pertama adalah asas teritorial. Penerapan yurisdiksi suatu negara saat tindak pidana dilakukan di dalam wilayah negara tersebut menganut asas teritorial. Ini berarti negara mempunyai yurisdiksi eksklusif atas wilayah, atas segala yang ada dan/atau yang terjadi di dalam batas-batas wilayah negara tersebut, serta atas penduduk negara tersebut[51]. Salah satu wujud yurisdiksi teritorial tersebut yaitu negara dapat memberlakukan hukum nasionalnya terhadap warga negaranya maupun warga negara asing selama orang tersebut melakukan tindakan hukum di dalam wilayah negara tersebut. Asas ini juga diperluas dan berlaku saat tindakan pidana dilakukan di atas kapal yang berbendera negara tersebut dan di atas pesawat yang terdaftar berdasarkan hukum negara tersebut[52]. Kemudian berdasarkan isi dari pasal 22 ayat (1) *Convention on Cybercrime* yang menyebutkan saat suatu tindakan dilakukan oleh seseorang yang merupakan warga negara dari negara tersebut, dimana tindakan tersebut termasuk tindak kejahatan berdasarkan hukum negara tersebut dan tindakan itu terjadi dan

[50] Yustina Trihoni Nalesti Dewi, *Op. cit*, hlm 54.
[51] *Ibid.*
[52] Afitrahim M.R., 2009, "Yurisdiksi Berdasarkan *Convention On Cybercrime*", Skripsi: Fakultas Hukum Universitas Indonesia, hlm. 58. diakses pada tanggal 14 April 2022 dari https://lib.ui.ac.id/file?file=digital/2016-9/20326369-S26248/.

berlangsung di luar wilayah negara tersebut, dapat dikatakan bahwa isi dari pasal ini menganut asas nasionalitas aktif. Asas nasionalitas aktif menyatakan bahwa suatu warga negara harus tunduk pada hukum negaranya meskipun tidak berada di wilayah negaranya tersebut. Pada pasal ini juga tercantum mengenai asas *protective principle*, dimana suatu negara berwenang mengadili suatu tindak pidana jika negara tersebut terancam kepentingannya akibat suatu tindak pidana meskipun tindak pidana tersebut tidak terjadi di dalam wilayah negaranya, maupun pelaku dan negara yang menjadi target kejahatan bukan negara tersebut.

Selain ditentukan berdasarkan pasal 22 ayat (1) *Convention on Cybercrime,* ayat (4) pada pasal tersebut juga menyatakan bahwa konvensi ini tidak mengecualikan hukum nasional suatu negara sebagai dasar untuk menetapkan yurisdiksi. Lalu bagaimana jika ada lebih dari satu pihak yang menuntut yurisdiksi atas tindakan-tindakan pidana yang dicantumkan dalam pasal 2 hingga pasal 11 *Convention on Cybercrime*? Dalam pasal 22 ayat (5) *Convention on Cybercrime* menyatakan bahwa para pihak yang terlibat harus berdiskusi untuk menentukan yurisdiksi yang paling cocok untuk ditetapkan.

B. Ketentuan Menurut *Convention on Cybercrime* Mengenai Ratifikasi

Pada pasal 36 ayat (1) *Convention on Cybercrime* dinyatakan kalau *Convention on Cybercrime* bebas diratifikasi oleh negara-negara anggota Majelis Eropa (*Council of Europe*) dan oleh negara-negara yang bukan anggota dari Majelis Eropa (*Council of Europe*). Dalam ayat (2) disebutkan pula bahwa *Convention on Cybercrime* tunduk kepada proses ratifikasi, yang kemudian akan diterima dan disahkan, lalu perangkat ratifikasi tersebut akan diberikan oleh Sekretaris Jenderal Majelis Eropa. Dalam *Convention on Cybercrime* tidak disebutkan bagaimana kedudukan *Convention on Cybercrime* terhadap negara yang tidak meratifikasi konvensi ini. Dalam *Convention on Cybercrime* hanya disebut bahwa konvensi ini

terbuka untuk diratifikasi oleh negara manapun, termasuk negara-negara negara-negara yang bukan anggota dari Majelis Eropa (*Council of Europe*).

Indonesia sendiri belum meratifikasi *Convention on Cybercrime*. Jika ikut meratifikasi, berarti Indonesia sebagai negara peratifikasi wajib mengikuti peraturan yang tertuang dalam konvensi tersebut, dimana biasanya suatu konvensi mewajibkan negara-negara yang terlibat untuk membuat peraturan-peraturan yang dapat mempidanakan jenis-jenis kejahatan yang diatur dalam konvensi tersebut[53]. Di dalam peraturan *Convention on Cybercrime, Convention on Cybercrime* mengharuskan negara-negara yang terlibat untuk membuat peraturan-peraturan yang dapat mempidanakan jenis-jenis kejahatan yang diatur dalam konvensi ini, seperti kejahatan mengenai akses ilegal, penyadapan ilegal, gangguan terhadap data dan sistem, serta penyalahgunaan gawai dan sistem yang berkaitan dengan jaringan komputer. Untuk saat ini, pemerintah Indonesia saat ini sudah memiliki peraturan hukum yang mengatur tentang hal-hal tersebut, yaitu Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Meratifikasi *Convention on Cybercrime* serta membuat pengaturan untuk mengimplementasikannya kedalam hukum nasional juga bisa menjadi strategi alternatif dalam membuat regulasi dalam bidang *cybercrime*[54]. Jika Indonesia ikut meratifikasi *Convention on Cybercrime*, pengesahan *Convention on Cybercrime* sebagai undang-undang akan didukung dengan adanya Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai implementasi nyata nilai-nilai dalam *Convention on Cybercrime*.

Dengan ratifikasi, Indonesia akan terikat dan berhak atas keuntungan-keuntungan yang sama dengan negara-negara peserta konvensi. Keuntungan-keuntungan yang ditawarkan antara lain kerjasama internasional terkait ekstradisi, investigasi, pelaksanaan yang efektif terkait penerapan prinsip yurisdiksi

[53] Wisnu Aryo Dewanto, 2015, "Akibat Hukum Peratifikasian Perjanjian Internasional Di Indonesia: Studi Kasus Konvensi Palermo 200l", *Jurnal Hukum Veritas Et Justitia*, Vol. 1, Nomor 1, hlm. 50, diakses pada tanggal 9 Juni 2022 dari https://journal.unpar.ac.id/index.php/veritas/article/view/1416.
[54] Muhamad Amirulloh, Ida Padmanegara, dan Tyas Dian Anggraeni, *Op. cit.,* hlm. 7.

ekstra teritorial serta keuntungan lainnya[55]. Menjadi pihak dalam konvensi ini juga artinya Indonesia dapat berkontribusi pada pengembangan lebih lanjut dari *Convention on Cybercrime* melalui catatan panduan atau penambahan protokol[56]. Kewajiban yang mungkin akan memberatkan Indonesia jika meratifikasi *Convention on Cybercrime* adalah Indonesia sebagai negara anggota peratifikasi wajib ikut serta dalam jaringan praktisi titik kontak 24/7 yang didirikan berdasarkan perjanjian antar negara anggota peratifikasi.[57] Tetapi di dalam pasal 39 nomor 3 *Convention on Cybercrime* menjamin tidak ada satu pun ketentuan dalam Konvensi ini yang akan mempengaruhi hak, batasan, kewajiban, dan tanggung jawab lainnya dari sebuah pihak.

C. Penerapan *Convention on Cybercrime* Sebagai Alat Penegakan Hukum di Indonesia

Suatu hukum internasional biasanya tidak berperan langsung dalam penegakan hukum Indonesia. Konstitusi Indonesia tidak mengatur tentang bagaimana posisi hukum internasional dalam proses penegakan hukum nasional. Penerapan suatu hukum internasional sebagai alat penegakan hukum di Indonesia biasanya dilakukan dengan cara meratifikasi suatu hukum atau peraturan internasional. Undang-undang hasil ratifikasi tersebut yang kemudian dipakai sebagai alat penegakan hukum. Selain melalui proses ratifikasi, suatu negara juga dapat mengadopsi norma-norma yang ada dalam suatu hukum internasional maupun konvensi-konvensi untuk diberlakukan di dalam hukum nasional negaranya. Norma-norma dalam suatu hukum internasional dapat diterima sebagai bagian dari pembentukan hukum melalui prosedur dan tata cara tertentu karena dinilai sebagai suatu bidang hukum yang berdiri sendiri[58]. Ini yang dilakukan oleh Indonesia terhadap *Convention on Cybercrime. Convention on Cybercrime* sendiri belum diratifikasi oleh Indonesia. Jika kita memperhatikan

[55] *Ibid.,* hlm. 59.
[56] *Council of Europe*, *Op.cit.,* hlm. 3.
[57] *Ibid*.
[58] Dina Sunyowati, *Loc.cit.,* hal. 75.

substansi dan norma-norma hukum dalam *Convention on Cybercrime*, norma-norma dalam *Convention on Cybercrime* sudah diadopsi dalam pembentukan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Semua jenis tindakan yang dipertimbangkan dalam *Convention on Cybercrime* telah diatur di dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, hanya tata letak dan urutan dari tindakan tersebut yang diubah dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik[59]. Adopsi norma-norma dalam *Convention on Cybercrime* ke dalam Undang-Undang nomor 11 tahun 2008 tentang Informasi Dan Transaksi Elektronik ini menunjukan bahwa Indonesia menggunakan paham dualisme, dimana suatu hukum internasional tidak dapat memaksa Indonesia untuk patuh terhadap hukum tersebut. Indonesia kemudian membuat sendiri hukumnya berdasarkan hukum internasional tersebut[60].

D. Penerapan *Convention on Cybercrime* Kepada Warga Negara Indonesia Pelaku Kejahatan Peretasan Transnasional

Pada dasarnya *Convention on Cybercrime* telah menetapkan norma-norma kebijakan dan penanggulangan kejahatan mayantara. Norma-norma ini yang kemudian dipakai sebagai dasar pembentukan hukum-hukum di berbagai negara. Beberapa negara juga meratifikasi *Convention on Cybercrime* menjadi hukum nasional di negaranya. Di Indonesia sendiri, *Convention on Cybercrime* belum diratifikasi, tetapi norma-norma dalam *Convention on Cybercrime* sudah diadopsi dalam pembentukan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Semua jenis tindakan yang dipertimbangkan dalam *Convention on Cybercrime* telah diatur di dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, hanya tata letak dan urutan dari tindakan tersebut

[59] Akbar Kurnia Putra, *Loc.cit.*, hlm. 106.
[60] Ninon Melatyugra, *Loc.cit.,* hlm. 48.

yang diubah dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik[61].

Penerapan ketentuan dalam *Convention on Cybercrime* kepada WNI pelaku kejahatan peretasan transnasional dapat dilakukan dengan cara menerapkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini dapat dilakukan karena Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan adopsi dari norma-norma dalam *Convention on Cybercrime*. Jadi menerapkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang merupakan penerapan dari *Convention on Cybercrime* sendiri dapat dilakukan berdasarkan teori voluntaris, yang menganggap hukum nasional dan hukum internasional merupakan kesatuan yang berjalan secara berdampingan dan terpisah[62]. Penerapan *Convention on Cybercrime* dalam kasus tersebut dapat dilakukan berdasarkan paham monism, dimana dinyatakan bahwa suatu negara dapat menerapkan suatu hukum internasional secara langsung kedalam sistem hukum nasional[63]. Penerapan ini dapat dilaksanakan sebagai penetapan ketentuan tentang yurisdiksi suatu negara yang berwenang dalam penegakan serta mengadili pelaku dan sebagai penyelesaian sengketa. Hal ini dapat dilakukan berdasarkan pasal 22 ayat (4) *Convention on Cybercrime* menyatakan bahwa konvensi ini tidak mengecualikan hukum nasional suatu negara sebagai dasar untuk menetapkan yurisdiksinya.

Yurisdiksi menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diatur dalam pasal 2 yang menyatakan bahwa undang-undang ini berlaku bagi setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di dalam maupun di

[61] *Ibid.*
[62] Dina Sunyowati, *Loc.cit.,* hal. 76.
[63] Ninon Melatyugra, *Ibid.*

luar wilayah hukum Indonesia, yang memiliki akibat hukum di dalam maupun di luar wilayah hukum Indonesia dan merugikan Indonesia[64]. Berdasarkan pasal tersebut jelas bahwa Indonesia memiliki wewenang untuk menerapkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dalam proses penegakan hukum tersebut. Perbuatan hukum yang dimaksud adalah peretasan berdasarkan pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dari tiga ayat yang ada dalam pasal tersebut, disebutkan bahwa peretasan adalah kegiatan mengakses komputer dan/atau sistem elektronik secara sengaja dan tidak sah. Akses tidak sah ini maksudnya dilakukan dengan melawan hukum dan akses dilakukan dengan menerobos, melampaui atau menjebol sistem keamanan komputer tersebut dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik[65]. Penuntutan dan keputusan pengadilan akan mengacu pada pasal-pasal hukum nasional dan bukan pada *Convention on Cybercrime*, kecuali untuk kasus-kasus di mana bukti telah diperoleh melalui ketentuan kerjasama internasional.[66]

Mengingat kejahatan yang terjadi bersifat transnasional, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sendiri tidak cukup karena tidak mengatur bagaimana penyelesaian sengketa yang dapat terjadi akibat tindakan pidana yang dilakukan secara transnasional tersebut. Sengketa yang mungkin dapat terjadi adalah ada negara atau pihak lain menuntut yurisdiksi atas penegakan hukum tersebut. Untuk mengatur hal tersebut, dapat diterapkan pasal 22 ayat (5) *Convention on Cybercrime* menyatakan bahwa para pihak yang terlibat harus berdiskusi untuk menentukan yurisdiksi yang paling cocok untuk ditetapkan.

---

[64] Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[65] *Ibid.*
[66] *Council of Europe*, "*Convention On Cybercrime: Benefits and Impact in Practice*", Stasbourg, 13 July 2020, diakses pada tanggal 28 Juni 2022 dari https://rm.coe.int/.

BAB IV

KESIMPULAN DAN SARAN

A. Kesimpulan