 ISSN : 2089-5940

PELANGGARAN CYBERCRIME DAN KEKUATAN YURISDIKSI DI INDONESIA

Andysah Putera Utama Siahaan[1,2]
[1]Faculty of Computer Science, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Ph.D. Student of School of Computer and Communication Engineering,
Universiti Malaysia Perlis, Kangar, Malaysia
andiesiahaan@gmail.com

***Abstrak* — *Cybercrime adalah kejahatan digital yang dilakukan untuk menuai keuntungan melalui Internet sebagai media. Setiap aktivitas kriminal yang terjadi di dunia digital atau melalui jaringan internet disebut sebagai kejahatan internet. Cybercrime juga mengacu pada aktivitas kriminal pada komputer dan jaringan komputer. Kegiatan ini bisa dilakukan di lokasi tertentu atau bahkan dilakukan antar negara. Kejahatan ini termasuk pemalsuan kartu kredit, penipuan kepercayaan, penyebaran informasi pribadi, pornografi, dan sebagainya. Di zaman kuno tidak ada hukum yang kuat untuk memerangi kejahatan dunia maya. Karena ada undang-undang dan transaksi informasi elektronik, yurisdiksi hukum kejahatan komputer telah diterapkan. Jaringan komputer tidak hanya dipasang di satu area lokal tertentu namun dapat diterapkan ke jaringan di seluruh dunia. Inilah yang membuat cybercrime bisa terjadi antar negara secara bebas. Masalah ini membutuhkan yurisdiksi universal. Sebuah negara memiliki kewenangan untuk memberantas kejahatan yang mengancam masyarakat internasional. Yurisdiksi ini diterapkan tanpa menentukan di mana kejahatan tersebut dilakukan dan warga yang melakukan kejahatan dunia maya. Yurisdiksi ini dibuat tanpa kehadiran lembaga peradilan internasional khusus untuk mencoba kejahatan perorangan. Cybercrime tidak bisa dimusnahkan secara total. Menerapkan yurisdiksi internasional setidaknya mengurangi jumlah cybercrime di dunia.*

Kata Kunci* — *Cybercrime, Yuridiksi, Kekuatan, Hukum

I. PENDAHULUAN

Kemajuan teknologi membuka peluang kejahatan besar. Hal ini bisa dilihat dari banyaknya kasus yang datang ke pengadilan tentang kejahatan digital. Kasus yang ditangani adalah tentang penyalahgunaan teknologi seperti internet, hoax, fake photos dan lain-lain. Salah satu fakta yang menyebabkan cybercrime adalah kebutuhan akan teknologi jaringan komputer semakin meningkat. Kegiatan komersil masyarakat menjadi hal penting dilakukan dengan menggunakan jaringan komputer. Ini bisa tersebar di seluruh negeri. Kegiatan dunia akan berlangsung selama 24 jam dan bisa dipantau selama 24 jam juga. Kegiatan ini meliputi perdagangan saham, perbankan, dan aktivitas keuangan lainnya. Di dunia maya, aktivitas apapun bisa dilakukan. Hal ini berdampak positif pada kemajuan teknologi dan menambah kenyamanan bagi orang untuk bertukar informasi. Tapi ini tak luput dari dampak negatifnya. Saat pornografi berkembang di internet, hukum tidak bisa berbuat banyak di masa lalu. Perkembangan teknologi internet memicu munculnya cybercrime. Tindakan ini akan merugikan orang lain. Aktivitas cybercrime meliputi pencurian kartu kredit, hacking beberapa situs, mencegat transmisi data orang lain, dan memanipulasi data dengan menyiapkan beberapa program seperti virus untuk melakukan kejahatan tersebut. Cybercrime telah menjadi ancaman bagi stabilitas internasional, sehingga pemerintah sulit mengkompensasi teknik kejahatan yang dilakukan dengan teknologi komputer, terutama jaringan internet dan intranet.

Cyberspace adalah media tanpa batas karena terhubung dengan jaringan komputer yang terhubung dengan dunia. Ini tidak mengenali batas wilayah atau negara. Kejahatan ini akan menimbulkan masalah, terutama dalam hukum pidana dan yurisdiksi. Yurisdiksi adalah kekuatan atau kompetensi hukum negara terhadap orang, benda atau peristiwa. Inilah prinsip kedaulatan negara, persamaan negara dan prinsip non-interferensi. Yurisdiksi juga merupakan bentuk kedaulatan penting dan sentral yang dapat mengubah, menciptakan, atau mengakhiri hubungan hukum atau kewajiban.

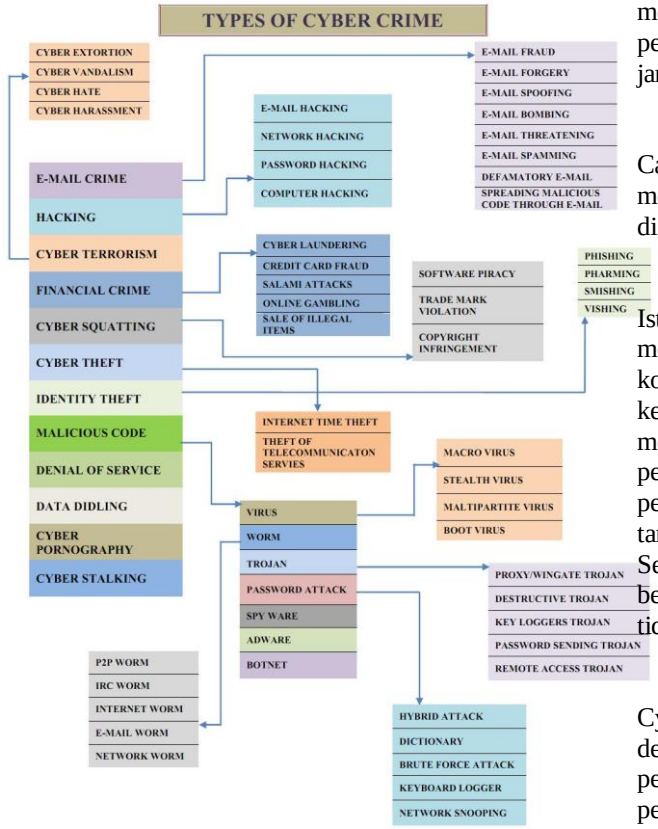
Penelitian ini mencoba untuk menjelaskan bagaimana sistem hukum akan diterapkan pada pelaku kejahatan dunia maya berdasarkan pelanggaran tertentu. Setiap pelanggaran memiliki tindakan hukum yang berbeda. Dengan menerapkan yurisdiksi, aktor cybercrime akan berkurang demi stabilitas dan kedaulatan negara.

II. TEORI

A. *Cybercrime*

Cybercrime adalah kegiatan ilegal yang dilakukan di dunia maya dengan perantara komputer atau peralatan elektronik lainnya. Ini mencakup teknologi yang mendukung sarana teknologi seperti ponsel, smartphone dan lainnya yang bisa dilakukan melalui jaringan elektronik global [2] [5]. Cybercrime mencoba memasuki jaringan komputer tanpa izin. Cybercrime dianggap bertentangan atau bertentangan dengan hukum yang berlaku. Bedanya dengan tindak pidana serupa dapat dilihat dari kemampuan serbaguna yang ditunjukkan oleh perkembangan informasi dan teknologi komunikasi yang canggih. Gambar 1 menggambarkan jenis cybercrime [1].

 ISSN : 2089-5940



Gambar 1: Tipe cybercrime

Ada beberapa jenis kejahatan pada cybercrime yang bisa diklasifikasikan berdasarkan aktivitas seperti [3] [4] [6]:

- Akses tidak sah

Ini adalah kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dimilikinya. Contoh kejahatan ini adalah Probing dan port.

- Konten Ilegal

Ini adalah kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang hal yang tidak benar, tidak etis, dan dapat dianggap sebagai tindakan hukum yang melanggar hukum atau mengganggu, misalnya penyebaran pornografi atau berita yang tidak benar.

- Penyebaran Virus

Penyebaran virus umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terpapar virus tidak menyadari hal ini. Virus ini kemudian dikirim ke tempat lain via email.

- Cyber Spionase, Sabotase, dan Pemerasan

Cyber Spionase adalah kejahatan dengan cara memanfaatkan jaringan internet untuk melakukan spionase pihak lain, dengan memasukkan sistem jaringan komputer target. Sabotase dan Pemerasan adalah jenis kejahatan yang dilakukan dengan melakukan gangguan, penghancuran atau penghancuran data, program komputer atau sistem jaringan komputer yang terhubung ke internet.

- Carding

Carding adalah kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

- Hacking dan Cracking

Istilah hacker biasanya mengacu pada seseorang yang memiliki minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kemampuannya. Aktivitas cracking di internet memiliki cakupan yang sangat luas, mulai dari pembajakan akun orang lain, pembajakan situs web, penyelidikan, penyebaran virus, hingga penonaktifan target. Tindakan terakhir disebut DoS (Denial Of Service). Serangan DoS adalah serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak bisa memberikan layanan.

- Cybersquatting dan Typosquatting

Cybersquatting adalah kejahatan yang dilakukan dengan mendaftarkan nama domain perusahaan perusahaan lain dan kemudian mencoba menjualnya ke perusahaan dengan harga yang lebih tinggi. Typosquatting adalah kejahatan dengan menciptakan domain palsu yang merupakan domain yang mirip dengan nama domain orang lain.

- Cyber Terrorism

Tindakan cybercrime termasuk terorisme cyber jika mengancam pemerintah atau warga negara, termasuk melakukan cracking ke lokasi pemerintah atau militer.

B. Konstitusi Informasi Elektronik

Undang-undang ini pada awalnya melindungi kepentingan negara, masyarakat, dan sektor swasta dari cybercrime. Ada tiga kategori besar yang mencakup undang-undang yang terkait dengan penghinaan, penghujatan, dan ancaman online. Hukum menjerat tidak hanya penulis tetapi juga mereka yang mendistribusikan, mentransmisikan, atau membuat konten dapat diakses secara elektronik. Kesalahannya adalah mendistribusikannya adalah untuk mengirim dan menyebarkan informasi dan dokumen elektronik kepada banyak orang atau berbagai pihak melalui jaringan internet [7] [8]. Mengirim mengirimkan informasi yang diarahkan ke satu pihak melalui dunia maya. Membuat konten yang dapat diakses publik adalah semua perbuatan cybercrime lainnya. Mereka yang berbagi informasi atau konten yang melanggar hukum dapat dikenai biaya dan dikenakan sanksi. Pengguna media sosial harus lebih berhati-hati dan tidak membagikan hal-hal di depan umum tanpa verifikasi yang baik dan benar. Informasi tersebut harus diperiksa ulang sebelum dipublikasikan secara terbuka. Berbagi, mendistribusikan dan melukai orang lain adalah

 ISSN : 2089-5940

tindakan kriminal yang bisa dikriminalisasi [9] [10] [11].

III. HASIL

A. *Yuridiksi Kejahatan dalam Transaksi Cybercrime*

Yurisdiksi adalah wewenang negara untuk menjalankan hukum nasionalnya terhadap orang, objek, atau peristiwa hukum. Yurisdiksi negara dalam hukum internasional berarti hak suatu Negara untuk mengatur dan mempengaruhi tindakan legislatif, eksekutif, dan yudisial dan tindakan terhadap hak individu, properti atau properti, perilaku atau kejadian yang merupakan masalah di dalam suatu negara dan luar negeri.

Yurisdiksi berkaitan dengan masalah hukum, wewenang atau wewenang peradilan atau badan hukum lainnya yang didasarkan pada hukum yang berlaku. Ada batas lingkup kemampuan untuk membuat, menerapkan dan menerapkan undang-undang tersebut kepada mereka yang tidak menaatinya. Meski yurisdiksi terkait erat dengan wilayah, keterkaitan ini tidak mutlak. Negara bagian lain mungkin juga memiliki kewenangan untuk melakukan tindakan yang dilakukan di luar negeri.

Yurisdiksi hukum selalu menjadi masalah serius yang dihadapi oleh penegak hukum terutama jika pelaku adalah warga negara asing. Cybercrime dan yurisdiksi memperjelas bahwa untuk menangani masalah cybercrime di dalam yurisdiksi hukum yang melibatkan antar negara

B. *Kekuatan Hukum dalam Penanganan Cybercrime*

Penegakan hukum terhadap cybercrime terutama di Indonesia sangat dipengaruhi oleh lima faktor seperti hukum, mentalitas, perilaku sosial, sarana, dan budaya. Hukum yang tidak bisa tegak dengan sendirinya selalu melibatkan manusia di dalamnya dan juga melibatkan perilaku manusia di dalamnya. Hukum juga tidak dapat dibangun dengan sendirinya tanpa ada penegak hukum. Penegak hukum tidak hanya diadili karena profesionalisme dan pandai dalam menerapkan norma hukum tetapi juga berurusan dengan seseorang bahkan sekelompok orang yang dicurigai melakukan kejahatan.

Penegak hukum diharuskan bekerja keras karena penegakan hukum merupakan subyek utama perang melawan kejahatan cyber. Misalnya, Resolusi PBB No. 5 tahun 1963 tentang upaya pemberantasan kejahatan penyalahgunaan Teknologi Informasi pada tanggal 4 Desember 2001, mengindikasikan bahwa ada masalah internasional yang parah, serius dan segera terjadi. KUHP masih digunakan sebagai dasar hukum untuk meliput cybercrime, terutama cybercrime yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Beberapa alasan konstitusional dalam KUHP yang digunakan oleh aparat penegak hukum meliputi:

- Pasal 167 KUHP
- Pasal 406 Ayat 1 KUHP
- Pasal 282 KUHP
- Pasal 378 KUHP
- Pasal 112 KUHP
- Pasal 362 KUHP
- Pasal 372 KUHP

Ada hukum lain yang terkait dengan masalah ini. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (IET). Aturan tindak pidana yang dilakukan di dalamnya terbukti mengancam pengguna internet. Sejak diberlakukannya UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada tanggal 21 April 2008, telah menyebabkan banyak korban. Berdasarkan pemantauan yang telah dilakukan aliansi setidaknya ada empat orang yang disebut polisi dan menjadi tersangka karena diduga melakukan tindak pidana yang diatur dalam UU ITE. Tersangka atau korban dari ITE Act adalah pengguna internet aktif yang dituduh menghina atau terkait dengan konten penghinaan di internet. Mereka yang dituduh berdasarkan Undang-Undang Hukum IET cenderung tunduk pada Pasal 27 ayat 3 jo dengan Pasal 45 ayat 1 UU IET yang enam tahun penjara dan denda 1 miliar rupiah. Hukum IET bisa digunakan untuk mengalahkan semua aktivitas cybercrime di internet tanpa terkecuali.

IV. KESIMPULAN

Cybercrime adalah kejahatan yang timbul dari dampak negatif perkembangan teknologi. Berarti digunakan dalam bentuk komputer, smartphone, dan perangkat yang terhubung dengan internet. Hal itu juga terjadi karena ketidakmampuan hukum termasuk aparat dalam mencapainya. Kejahatan ini bersifat virtual karena pelaku tidak tampil secara fisik. Penegakan hukum cybercrime adalah kegiatan yang menyelaraskan nilai-nilai yang digariskan dalam hukum melawan cybercrime. Cybercrime merupakan kegiatan yang melanggar hukum yang dilakukan dengan menggunakan internet berdasarkan kecanggihan teknologi komputer dan telekomunikasi. Yurisdiksi di dunia maya membutuhkan prinsip-prinsip yang jelas yang berakar pada hukum internasional. Setiap negara dapat mengembangkan peraturan untuk mengadopsi solusi yang sama terhadap pernyataan mengenai yurisdiksi internet. Prinsip yurisdiksi akan memudahkan negara untuk melakukan kerjasama untuk menyelaraskan ketentuan pidana untuk mengatasi kejahatan dunia maya. Indonesia telah menerapkan sistem yurisdiksi yang kuat dalam menangani cybercrime. Ketentuan ini telah diatur dalam KUHP yang sesuai.

 ISSN : 2089-5940

Berdasarkan hukum yang berlaku, penjahat dunia maya akan diadili oleh ketentuan.

REFERENSI

[1] D. Sudyana, "Pengenalan Cyber Crime," 1 10 2015. [Online]. Available: http://blog.didiksudyana.com/2015 /10/pengenalan-cyber-crime.html. [Accessed 20 12 2017].

[2] Y. M. Saragih and A. P. U. Siahaan, "Cyber Crime Prevention Strategy in Indonesia," *International Journal of Humanities and Social Science*, vol. 3, no. 6, pp. 22-26, 2016.

[3] V. Tasril, M. B. Ginting, Mardiana and A. P. U. Siahaan, "Threats of Computer System and its Prevention," *International Journal of Scientific Research in Science and Technology*, vol. 3, no. 6, pp. 448-451, 2017.

[4] S. Ramadhani, Y. M. Saragih, R. Rahim and A. P. U. Siahaan, "Post-Genesis Digital Forensics Investigation," *International Journal of Scientific Research in Science and Technology*, vol. 3, no. 6, pp. 164-166, 2017.

[5] Hariyanto and A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and Investigation," *IOSR Journal of Computer Engineering*, vol. 18, no. 6, pp. 115-121, 2016.

[6] Y. Triwahyuni, "Pengertian, Jenis-jenis, dan Contoh Kasus Cyber Crime," Wordpress, 5 12 2015. [Online]. Available: https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-kasus-cyber-crime/. [Accessed 20 12 2017].

[7] Rusmiatiningsih, "Yuridiksi Hukum Pidana dalam Transaksi Cybercrime," Blogspot, 19 10 2013. [Online]. Available: http://rusmiatiningsih.blogspot.co.id/2013/10/yuridiksi-hukum-pidana-dalam-transaksi.html. [Accessed 20 12 2017].

[8] S. Muslimah and N. Hidayati, "7 Hal di UU ITE yang Wajib Kamu Tahu Agar Tak Bernasib Seperti Jonru," Kumparan, 29 9 2017. [Online]. Available: https://kumparan.com/@kumparannews/7-hal-di-uu-ite-yang-wajib-kamu-tahu-agar-tak-bernasib-seperti-jonru. [Accessed 20 12 2017].

[9] D. Manurung, "Cyber Crime: Hukum dan Sanksi," Blogspot, 27 11 2013. [Online]. Available: http://desrianimanroe.blogspot.co.id/2013/11/hukum-dan-sanksi.html. [Accessed 10 12 2017].

[10] C. S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," *International Journal of Cyber Criminology*, vol. 9, no. 1, pp. 55-119, 2015.

[11] A. A. S. A. Hait, "Jurisdiction in Cybercrimes: A Comparative Study," *Journal of Law, Policy and Globalization*, vol. 22, pp. 75-84, 2014.