Jurnal Hukum Non Diskriminatif
Vol 1, No 2, Januari 2023, Hal. 39-43
ISSN 2962-4231 (Media Online)
DOI 10.56854/jhdn.v1i2.112
http://ejurnal.bangunharapanbangsa.com/index.php/jhdn

Cybercrime Kejahatan Yang Berbasis Komputer

Nova Andrian*, Budi Santoso
Fakultas ilmu hukum Universitas Lancang Kuning
Email: novandryani06@gmail.com

Abstrak-Teknologi informasi memegang peran yang penting, baik di masa kini maupun masa yang akan datang. Internet adalah salah satu bagian dari perkembangan teknologi informasi yang telah membuka cakrawala baru dalam kehidupan manusia. Internet dapat diartikan sebuah ruang informasi dan komunikasi yang menembus batas-batas antarnegara dan mempercepat penyebaran ilmu pengetahuan serta mempermudah segala kegiatan yang dilakukan manusia Walaupun begitu, setiap sisi positif pasti memiliki sisi negative. Internet berlaku dalam hal ini banyak kejahatan yang dapat terjadi dalam cyberspace yang dinamakan cybercrime. Saat ini, kata "aman" belum dapat kita rasakan dalam dunia cyber. Berbagai penanggulangan yang dianggap efektif masih dilakukan hingga saat ini, walaupun tidak menghindari para pelaku Cybercrime, setidaknya dapat mengecilkan kemungkinan seseorang menjadi salah satu korban dari Cybercrime atau penanggulangan saat Cybercrime terjadi. Dengan begitu banyak Cybercrime yang muncul, diperlukan segera sebuah hukum. Hukum yang cocok dan metode preventif untuk mencegah Cybercrime

Kata Kunci: Cybercrime, Komputer, Internet

Abstract-Information technology plays an important role, both in the present and in the future. The Internet is one part of the development of information technology that has opened new horizons in human life. The Internet can be interpreted as an information and communication space that penetrates the boundaries between countries and accelerates the spread of science and simplifies all human activities however, every positive side must have a negative side. The Internet applies in this casemany crimes that can occur in cyberspace called cybercrime. Currently, we cannot feel the word "safe" in the cyber world. Various countermeasures that are consideredeffective are still being done to date, although not avoiding Cybercrime perpetrators, at least it can downplay the possibility of someone becoming one of the victims of Cybercrime or countermeasures when Cybercrime occurs. With so many emerging Cybercrime, a law is urgently required. The right laws and methods to prevent Cybercrime

Keywords: Cybercrime, Computer, Internet

1. PENDAHULUAN

Internet sudah menjadi salah satu kew-ajiban dalam hidup saat ini. Kemudahan yang ditawarkan *Internet* semakin mem- buat manusia terlena. *Internet* meng-hubungkan setiap penggunanya. Tidak ada batasan waktu, wilayah ataupun *gender*. Teknologi Informasi saat iniseolah-olah menjadi pedang bermata dua,karena selain memberikan kontribusi bagipeningkatan kemajuan, kesejahteraan,dan peradaban manusia, sekaligus men- jadi sarana efektif perbuatan melawan hukum.

Kebutuhan akan teknologi jaringan kom- puter semakin meningkat. Selain sebagai media penyedia informasi, melalui *inter- net* pula kegiatan komunitas komersial menjadi bagian terbesar dan pesat per-tumbuhannya serta menembus berbagai batas Negara. Bahkan melalui jaringan ini, segala macam informasi di dunia bisadiketahui selama 24 jam. Melalui dunia *internet* atau bisa disebut juga *cyber- space*, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja akanmenambah trend dalam perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Akan tetapi dampak negaif pun tidak bisa dihindari. Tatkala pornografi marak dimedia *internet*, ma- syarakat pun tak bisa berbuat banyak. Seiring dengan berkembangnya teknologi *internet*, menyebabkan munculnya keja- hatan yang disebut dengan *cybercrime* atau kejahatan melalui jaringan *internet*.

Munculnya beberapa kasus *cybercrime*, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya *email* dan memani- pulasi data dengan cara menyiapkan pe- rintah yang tidak dikehendaki ke dalam program Komputer. Sehingga dalam ke- jahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki Komputer orang lain tanpa ijin, sedangkan delik materil adalah per- buatan yang menimbulkan akibat keru-gian bagi orang lain. Adanya *cybercrime* telah menjadi ancaman stabilitas, se-hingga pemerintah sulit mengimbangiteknik kejahatan yang dilakukan dengan teknoligo komputer, khususnya jaringan *internet*.

2. KERANGKA TEORI

2.1 Pengertian *Cybercrime*

Cybercrime atau kejahatan berbasis komputer, adalah kejahatan yang me- libatkan komputer dan jaringan (*net-work*).[1] Komputer mungkin telah diguna- kan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.[2] *Cybercrimes* dapat didefinisikan sebagai: "Pelanggaranyang dilakukan terhadap perorangan atau sekelompok individu dengan motif krimi-nal untuk secara sengaja menyakiti repu- tasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepadakorban baik secara langsung maupuntidak langsung, menggunakan jaringan telekomunikasi modern seperti *Internet* (jaringan termasuk namun tidak terbatas pada ruang *Chat*, *email*, *notice boards* dan kelompok) dan telepon genggam(*Bluetooth* / SMS / MMS)". *Cybercrime* dapat

Jurnal Hukum Non Diskriminatif
Vol 1, No 2, Januari 2023, Hal. 39-43
ISSN 2962-4231 (Media Online)
DOI 10.56854/jhdn.v1i2.112
http://ejurnal.bangunharapanbangsa.com/index.php/jhdn

mengancam seseorang, keamanannegara atau kesehatan finansial. Isu seputar jenis kejahatan ini telah menjadi sangat populer, terutama seputar *hacking*, pelanggaran hak cipta, penyadapan yang tidak beralasan dan pornografi. Ada pula masalah privasi pada saat informasi rahasia dicegat atau diungkapkan, secara sah atau tidak. Debarati Halder dan K.Jaishankar lebih jauh mendefinisikan *cybercrime* dari perspektif *gender* dan mendefinisikan *"cybercrime againstwomen"* sebagai "Kejahatan yang di- targetkan pada wanita dengan motif untuk secara sengaja menyakiti korban secara psikologis dan fisik, menggunakanjaringan telekomunikasi modern seperti*internet* dan telepon genggam". Secara sengaja, baik pemerintah dan swasta terlibat dalam *cybercrimes*, termasuk spionase, pencurian keuangan dankejahatan lintas batas (*cross-border*) lainnya. Kegiatan yang melintasi batas negara dan melibatkan kepentingan setidaknya satu negara ter-kadang disebutsebagai *cyberwarfare*.

Sebuah laporan (disponsori oleh *McAfee*) memperkirakan bahwa kerusakan tahun- an yang disebabkan oleh *cybercrimes* pada ekonomi global mencapai $445miliar.[5] Namun, sebuah laporan dari *Microsoft* menunjukkan bahwa perkiraan berbasis survei semacam itu "sangat tidaksempurna" dan membesar-besarkan keru- gian yang sebenarnya.[6] Sekitar $1,5 miliar hilang pada tahun 2012 untuk penipuan kartu kredit dan debit *online* di Amerika Serikat.[7] Pada tahun 2016, se- buah studi oleh Juniper Research memperkirakan bahwa biaya *cybercrime* bisa mencapai 2,1 triliun pada tahun 2019.[8]

2.2 Penipuan dan kejahatan finansial

Penipuan dengan menggunakan komputeradalah salah representasi fakta yang tidakjujur yang dimaksudkan untuk membiar-kan orang lain melakukan sesuatu yang menyebabkan kerugian. Dalam konteks ini, kecurangan tersebut dilakukan de-ngan cara:

- Mengubah dengan cara yang tidak sah.Ini memerlukan sedikit keahlian teknisdan merupakan bentuk pencurianumum oleh seorang karyawan yang mengubah data atau memasukkan datapalsu atau dengan memasukkan in- struksi yang tidak sah atau meng- gunakan proses yang tidak sah.
- Mengubah, menghancurkan atau men- curi output, biasanya untuk menyem- bunyikan transaksi yang tidak sah. Ini sulit dideteksi;
- Mengubah atau menghapus data yang tersimpan.

Bentuk kecurangan lainnya dapat difasili-tasi dengan menggunakan sistem kom- puter, termasuk penipuan bank, *carding*, pencurian identitas, pemerasan dan pen- curian informasi rahasia.

Berbagai penipuan internet banyak ber-basis *phishing* dan *social engineering* yang menjadi sasaran biasanya konsumendan pelaku bisnis. Pejabat pemerintah dan spesialis ke- amanan teknologi informasi telah men-dokumentasikan peningkatan yang signi- fikan dalam masalah Internet dan pemin daian *server* sejak awal 2001. Namun, ada kekhawatiran yang berkembang di antara lembaga pemerintah seperti BiroInvestigasi Federal (*Federal Bureau of Investigations* / FBI) dan Badan Intelijen Pusat (*Central Intelligence Agency* / CIA)bahwa intrusi semacam itu adalah bagian dari usaha terorganisir oleh *cyber-terrorist*, dinas intelijen asing atau kelompok lain untuk memetakan potensi celah keamanan dalam sistem kritis.[9]Seorang *cyberterrorist* adalah seseorang yang mengintimidasi atau menggalang pemerintah atau organisasi untuk mema- jukan tujuan politik atau sosialnya de- ngan meluncurkan serangan berbasis komputer terhadap komputer, jaringan atau informasi yang tersimpan di dalamnya.

> *Cyberterrorisme* secara umum dapat didefinisikan sebagai tindakan terorisme yang dilakukan melalui penggunaandunia maya atau sumber daya komputer (Parker 1983). Sebagai contoh, sebuah propaganda sederhana di Internet akan terjadi serangan bom saat liburan tahun baru bisa dianggap sebagai *cyber-terrorism*. Ada juga kegiatan *hacking* yang diarahkan pada individu atau ke- luarga yang diselenggarakan oleh ke- lompok-kelompok di dalam jaringan, cenderung menimbulkan ketakutan di ka-langan orang-orang, mengumpulkan in-formasi yang relevan untuk menghancur- kan kehidupan masyarakat, perampokan, pemerasan, dll.[10]

2.3 Cyberextortion

Cyberextortion terjadi saat sebuah situs*web*, *server e-mail* atau sistem komputer dikenai atau diancam dengan penolakan berulang (*Denial of Service* / DoS) terhadap layanan atau serangan lainnyaoleh *hacker* jahat. Para h*acker* ini me-nuntut uang sebagai imbalan dengan janjiakan menghentikan serangannya dan ataumenawarkan "perlindungan". Menurut Biro Investigasi Federal, saat ini semakin banyak serangan yang dilakukan para pelaku *cyberextortion* pada situs *web*perusahaan dan jaringan, melumpuhkankemampuan / kinerja mereka untuk ber-operasi dan menuntut pembayaran untuk memulihkan layanan mereka. Lebih dari 20 kasus dilaporkan setiap bulan ke FBI dan banyak yang tidak dilaporkan untuk menjaga agar nama korban tidak keluar dan tersebar ke publik. Pelaku biasanya menggunakan serangan *denial-of-service* terdistribusi (*distributed denial-of-service*DDoS). Contoh *cyberextortion* adalah serangan terhadap perusahaan *Sony Pictures* pada tahun 2014

Jurnal Hukum Non Diskriminatif
Vol 1, No 2, Januari 2023, Hal. 39-43
ISSN 2962-4231 (Media Online)
DOI 10.56854/jhdn.v1i2.112
http://ejurnal.bangunharapanbangsa.com/index.php/jhdn

3. METODE PENELITIAN

Dalam penelitian ini, peneliti menggunakan metode penelitian normatif yuridis yaitu suatu penelitian kepustakaan yang dilakukan dengan cara mengkaji berbagai litelatur-literatur hukum terkait yang berkenaan dengan topik pembahasan penelitian ini yang juga dikaitkan dengan beberapa sumber hukum dalam bentuk hukum positif (undang-undang).

4. HASIL

Difusi luas aktivitas *cybercriminal* adalahmasalah dalam deteksi dan penuntasan kejahatan komputer. Menurut Jean-Loup Richet (*Research Fellow* di ESSEC ISIS), keahlian teknis dan aksesibilitas tidak lagi bertindak sebagai penghalang masuk ke *cybercrime*.[33] Memang, *hack- ing* jauh lebih rumit daripada beberapatahun yang lalu, karena komunitas *hacker*telah menyebarkan pengetahuan merekamelalui Internet. *Blog* dan komunitas *hacker* sangat berkontribusi dalam ber-bagi informasi: seorang *hacker* pemulabisa mendapatkan keuntungan dari pe- ngetahuan dan saran dari *hacker* yang lebih senior.

Selanjutnya, *hacking* lebih murah dari sebelumnya: sebelum era *cloud com-puting*, untuk *spam* atau *scam* dibutuhkan *server* yang berdedikasi, ketrampilan da- lam manajemen *server*, konfigurasi jari- ngan dan pemeliharaan, pengetahuan ten-tang standar penyedia layanan Internet dan lain-lain.

Sebagai perbandingan, *mail software-as- a-service* adalah layanan pengiriman *email* terukur, murah, massal dan transak-sional untuk tujuan pemasaran dan dapat dengan mudah disiapkan untuk *spam*.[34] Jean-Loup Richet menjelaskan bahwa *cloud computing* dapat membantu *cyber- criminal* sebagai cara untuk meman- faatkan serangannya - *brute-force pass- word*, meningkatkan jangkauan *botnet* atau memfasilitasi kampanye *spamm- ing*.

Komputer bisa menjadi sumber bukti (forensik digital). Bahkan di mana kom- puter tidak digunakan secara langsung untuk tujuan kriminal, catatan itu mung- kin berisi catatan nilai bagi penyidik kri- minal dalam bentuk *logfile*. Di kebanyak-an negara penyedia layanan internet (*Internet Service Providers*) secara hu- kum diharuskan untuk menyimpan *logfiles* mereka untuk jumlah waktu yang telah ditentukan. Sebagai contoh; Petun- juk Penyimpanan Data Eropa yang luas (berlaku untuk semua negara anggota UniEropa) menyatakan bahwa semua lalu lintas *E-mail* harus dipertahankan mini- mal selama 12 bulan.

Ada banyak cara untuk kejahatandunia maya bisa terjadi dan penyelidikan cenderung dimulai denganjejak alamat IP (*IP Address*), namunitu belum tentu merupakan basis faktual dimana penyidik dapat me- nyelesaikan sebuah kasus. Berbagaijenis kejahatan teknologi tinggi mung-kin juga mencakup unsur-unsur ke- jahatan teknologi rendah dan sebalik-nya, membuat penyidik dunia mayamenjadi bagian tak terpisahkan dari penegakan hukum modern. Metodo-logi kerja penyidik *cybercrime* bersifatdinamis dan terus membaik, baik di unit polisi khusus, maupun dalam ke-rangka kerjasama internasional.

Karena undang-undang yang mudah di- eksploitasi, penjahat dunia maya meng- gunakan negara-negara berkembang un- tuk menghindari deteksi dan penuntutan dari penegak hukum. Di negara ber- kembang, seperti Filipina, hukum mela- wan *cybercrime* sangat lemah atau ter-kadang tidak ada. Undang-undang yang lemah ini memungkinkan penjahat dunia maya menyerang dari perbatasan inter-nasional dan tetap tidak terdeteksi. Bah- kan ketika diidentifikasi, penjahat ini menghindari hukuman atau ekstradisi ke negara lain, seperti Amerika Serikat,yang telah mengembangkan undang- undang yang memungkinkan penuntutan.

Meskipun hal ini terbukti sulit dalam beberapa kasus, agensi seperti FBI, telah menggunakan tipu muslihat dan dalih untuk menangkap penjahat. Sebagai con- toh; dua *hacker* Rusia telah menghindari FBI untuk beberapa lama. FBI mendiri- kan sebuah perusahaan komputasi palsu yang berbasis di Seattle, Washington. Mereka melanjutkan untuk memancing dua pria Rusia ke Amerika Serikat de-ngan menawarkan mereka bekerja denganperusahaan ini. Setelah selesai wawanca- ra, tersangka ditangkap di luar gedung.Trik pintar seperti ini terkadang merupa- kan bagian penting dari penangkapan penjahat dunia maya saat undang-undang yang lemah membuat hal itu menjadi tidak mungkin lain. Presiden Barack Obama mengeluarkan perintah eksekutif pada bulan April 2015 untuk

Jurnal Hukum Non Diskriminatif
Vol 1, No 2, Januari 2023, Hal. 39-43
ISSN 2962-4231 (Media Online)
DOI 10.56854/jhdn.v1i2.112
http://ejurnal.bangunharapanbangsa.com/index.php/jhdn

memerangi kejahatan dunia maya. Perintah eksekutif ini memungkinkan Amerika Serikat untuk membekukan aset kejahatan dunia maya dan memblokiraktivitas ekonomi mereka di Amerika Serikat. Ini adalah beberapa undang-undang padat pertama yang memerangi *cybercrime* dengan cara ini. Uni Eropa mengadopsi arahan 2013/40/ EU. Semua pelanggaran terhadap direktif tersebut dan institusi prosedural lainnya juga ada dalam Konvensi Dewan Eropa tentang *Cybercrime*.

Sanksi untuk kejahatan terkait komputer di Negara Bagian New York dapat ber- kisar dari denda dan masa hukuman penjara yang singkat untuk pelanggaran ringan Kelas A seperti penggunaan kom- puter yang tidak sah sampai gangguan komputer pada tingkat pertama yang me- rupakan tindak pidana Kelas C dan dapat dilakukan. 3 sampai 15 tahun penjara. Namun, beberapa *hacker* telah dipeker-jakan sebagai pakar keamanan informasi oleh perusahaan swasta karena pengeta- huan mereka tentang kejahatan komputer, sebuah fenomena yang secara teoritis da- pat menciptakan insentif yang menyimpang.

Kemungkinan penghindaran ini adalah agar pengadilan melarang para *hacker* yang dipidana menggunakan komputer dan internet dalam bentuk apapun, bah- kan setelah mereka dibebaskan dari penjara, meskipun saat komputer dan internet menjadi sangat lebih penting bagikehidupan sehari-hari, hukuman jenis ini dapat artikan sebagai hukuman lebih keras dan kejam. Namun, pendekatan laintelah dikembangkan untuk me-*manage* para pelaku kejahatan *cyber* tanpa lara- ngan total dalam menggunakan komputer atau internet.[40] Pendekatan ini melibatkan pembatasan individu terhadap perangkat tertentu yang dapat dilakukan dengan cara pemantauan komputer atau penelu- suran komputer oleh petugas percobaan atau pembebasan bersyarat.

5. KESIMPULAN

Seiring kemajuan teknologi dan lebih ba- nyak orang mengandalkan internet untuk menyimpan informasi sensitif seperti in- formasi kartu kredit atau perbankan, pen- jahat akan berusaha mencuri informasi itu. Kejahatan *cyber* menjadi lebih me-rupakan ancaman bagi orang di seluruh dunia. Meningkatkan kesadaran tentangbagaimana informasi dilindungi dan me- ngetahui taktik yang digunakan penjahat *cyber* untuk mencuri informasi itu pen- ting di dunia sekarang ini. Menurut Pusat Pengaduan Kejahatan Internet FBI pada tahun 2014 ada 269.422 keluhan yang diajukan. Dengan semua klaim gabungan terjadi kerugian total yang dilaporkan sebesar $800.492.073.[42] Tapi kejahatan *cyber* sepertinya tidak diketahui oleh ke- banyakan orang. Ada 1,5 juta serangan *cyber* setiap tahunnya, itu berarti ada lebih dari 4.000 serangan sehari, 170 serangan setiap jam, atau hampir tiga serangan setiap menit, dengan penelitian menunjukkan bahwahanya 16% korban telah meminta orang- orang yang melakukan serangan untuk menghentikan serangannya.[43] Siapa saja yang menggunakan internet karena alasan apapun bisa menjadi korban, karena itu- lah penting untuk mengetahui bagaimana seseorang dilindungi saat *online*

DAFTAR PUSTAKA

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) *Cybercrime: Digital Cops in a Networked Environment*, NewYork University Press, New York.

Bowker, Art (2012) "The Cybercrime Handbook for CommunityCorrections: Managing Risk inthe 21st Century" Charles C. Thomas Publishers, Ltd. Springfield.

Brenner, S. (2007) *Law in an Era of Smart Technology*, Oxford: Oxford University Press

Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1- 4614-5217-1)

Chang, L.Y. C. (2012) *Cybercrime in the Greater China Region: Regulatory Responses andCrime Prevention across the Taiwan Strait*. Cheltenham:Edward Elgar. (ISBN 978-0- 85793-667-7)

Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world", in M. Gill (ed)Handbook of Security (pp. 321– 339). NY: Palgrave.

Csonka P. (2000) Internet Crime; the Draft council of Europeconvention on cyber-crime: A response to the challenge ofcrime in the age of the internet? *Computer Law & Security Report* Vol.16 no.5.

Easttom C. (2010) *Computer Crime Investigation and the Law*

Fafinski, S. (2009) *Computer Misuse: Response, regulation and thelaw* Cullompton: Willan

Glenny, Misha, *DarkMarket:cyberthieves, cybercops, and you*, New York, NY : Alfred A. Knopf, 2011. ISBN 978-0-307- 59293-4

Grabosky, P. (2006) *Electronic Crime*, New Jersey: Prentice Hall Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women inIndia. New Delhi: SAGE Publishing. ISBN 978- 9385985775.

Halder, D., & Jaishankar, K. (2011)Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

Jaishankar, K. (Ed.) (2011). CyberCriminology: Exploring Internet Crimes and Criminal behavior.Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.

Vol 1, No 2, Januari 2023, Hal. 39-43
ISSN 2962-4231 (Media Online)
DOI 10.56854/jhdn.v1i2.112
http://ejurnal.bangunharapanbangsa.com/index.php/jhdn

McQuade, S. (2006) *Understanding and Managing Cybercrime*, Boston:Allyn & Bacon.
McQuade, S. (ed) (2009) *TheEncyclopedia of Cybercrime*,Westport, CT: Greenwood Press ciberespacio, Latin American's New Security Thinking, Clacso, 2014, pp. 167/182
Richet, J.L. (2013) From Young Hackers to Crackers, *International Journal of Technology andHuman Interaction (IJTHI)*, 9(3), 53-62.
Wall, D.S. (2007) *Cybercrimes: The transformation of crime in theinformation age*, Cambridge:Polity.
Williams, M. (2006) *Virtually Criminal: Crime, Deviance and RegulationOnline*, Routledge, London.
Yar, M. (2006) *Cybercrime and Society*, London: Sage