p-ISSN : 0215-3092
e- ISSN : 2443-0013

PENEGAKAN HUKUM *CYBER CRIME* DALAM UPAYA PENANGGULANGAN TINDAK PIDANA TEKNOLOGI INFORMASI

Muhammad Satrio Purnomo Wikantomo,
Ida Aryati Dyah Purnomo Wulan, Ismiyanto
Magister Hukum Universitas Islam batik Suarakarta

A B S T R A K

This article aims to let us learn more about cyber crime. This is due to the weakness of cyberspace can become a global disaster that threatens the business sector, national and global security, behavior, child protection, and government systems. The results showed that the public is currently still misusing social media to spread crime in cyberspace. Most of the perpetrators of cybercrime on social media will be caught by Law No.11 of 2008 concerning Electronic Information and Transactions (UU ITE), whether intentional or unintentional. The law should provide protection for internet users with good intentions, and provide firm action for perpetrators of cyber crime. However, the legal system has not solved all computer crimes over the Internet. Likewise in the investigation, there were many obstacles related to legal instruments, the ability of investigators, evidence, and computer forensic facilities. This is why cyber crime law enforcement is still weak

A R T I C L E I N F O

Article History:
Accepted 03 okt 2022
Available online 24 Des 2022

Kata kunci: ***Cyber crime, Criminal policy, Information technology***

I. PENDAHULUAN

Perkembangan teknologi dan informasi berdampak kepada semua bidang kehidupan. Dengan adanya kemajuan teknologi jarak dan waktu seolah-olah bukan lagi menjadi masalah. Dengan kata lain bahwa teningkatan teknologi informasi bertujuan untuk mempermudah serta mempercepat pekerjaan. Manfaat tersebut dapat dirasakan apabila dikerjakan dalam ruang lingkup dan oleh oleh yang memiliki fungsi dan tugasnya serta dapat dipertanggungjawabkan.

Namun, disisi lain peningkatan teknologi informasi tersebut dapat mengakibatkan kerugian dan korban apabila disalahgunakan oleh seseorang yang memanfaatkan demi mencapai tujuan demi menguntungkan dirinya sendiri, ataupun kelompoknya dengan cara yang bersifat melawan hukum. Pelaku tindak pidana memanfaatkan media teknologi informasi untuk mencari dan memanfaatkan korbannya. Salah satu modus nya yaitu penipuan undian berhadiah yang dikirim melalui *short message service* (SMS) dan melalui whatsapp. Biasanya korban mendapatkan informasi kemudian diminta untuk membayar uang sebagai pembayaran pajak, administrasi dan lain-lain atas hadiah yang akan diterimanya, namun alih-alih setelah membayar sesuai arahan pelaku, korban tidak mendapatkan hadiah yang dijanjikannya.

Modus lain adalah arisan online, dimana korban mengikuti arisan melalui media online setelah membayar beberapa kali pengelola tidak bisa dihubungi dan uang arisan yang telah dibayarkan oleh korban tidak dikembalikan. Ada juga korban akibat pinjaman online, dimana korban meminjam sejumlah uang kepada pengelola pinjaman dengan memberikan identitas pribadi yang kemudian bunganya sangat besar dan korban

p-ISSN : 0215-3092
e- ISSN : 2443-0013

dipermalukan dan mendapatkan tekenan psikologis yang luar biasa ketika telat membayar.

Selain itu ada juga yang mengalami pembelian barang secara online namun setelah korban melakukan pembayaran barang yang dibeli tersebut tidak sesuai bahkan tidak datang, dan tindak pidana siber lainnya. Fenomena tersebut tentu sangat meresahkan masyarakat, dimana masyarakat tidak semuanya memahami akan pentingnya perlindungan data pribadi serta pentingnya kehati-hatian dalam bertransaksi melalui media online. Bahkan tidak hanya masyarakat biasa pada umumnya di daerah desa, korbannya pun ada yang berasal dari aparatur perangkat desa meskipun tidak sampai menjadi korban aparatur desa juga pernah mengalaminya. Berangkat dari permasalahan tersebut maka pentingnya edukasi kepada masyarakat Desa Cilame terkait pemahaman tentang berbagai macam tindak pidana *cyber crime* serta penanggulangannya.

Semakin banyaknya kasus *cyber crime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cyber crime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya. Penentuan sebagai tindak pidana merupakan kebijakan kriminal, yang menurut Sudarto sebagai usaha yang rasional dari masyarakat untuk menanggulangi kajahatan. Di dalam kebijakan kriminal mencakup kebijakan hukum pidana yang disebut juga sebagai kebijakan penanggulangan kejahatan dengan hukum pidana, karena di samping dengan hukum pidana untuk menanggulangi kejahatan, dapat dengan sarana-sarana non-hukum pidana.

Hukum pidana selaku fungsi kontrol sosial digunakan untuk memberantas tindak pidana berbentuk pelanggaran norma terkait penggunaan teknologi informasi yang berpotensi pidana, buat melindungi masyarakat dari bahaya tindak pidana tersebut. Korupsi tidak mustahil diredakan sekiranya semua pihak turut benar-benar komited dalam membasmi. Suatu kejahatan apabila tidak dilakukan pembasmian atau penanggulangan, maka secara kriminologis akan memberikan beberapa dampak buruk, antara lain: (1) meningkatnya kejahatan, baik dari aspek kuantitas maupun kualitas; (2) memunculkan bentuk-bentuk kejahatan baru di luar perhitungan umat manusia, yang bisa saja merupakan derivasi dari "kejahatan konservatif"; dan (3) tidak dapat teridentifikasinya sebuah kejahatan sebagai kejahatan.[1]

II. METODE PENELITIAN

Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundangundangan terkait *cyber crime*. Metode pengumpulan data dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain.

Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan *cyber law* di Indonesia. Pendekatan yang dipergunakan adalah pendekatan perundang-undangan dan pendekatan konseptual.

Penulis mengkaji Undang-Undang mengenai *cyber law* sedangkan Bahan Hukum yang dipergunakan adalah bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundangundangan

[1] Nafi' Mubarok, *Kriminologi dalam perspektif Islam* (Sidoarjo: Dwiputra Pustaka Jaya, 2017), 2–3

p-ISSN : 0215-3092
e- ISSN : 2443-0013

yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari buku, jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.

III. HASIL PENELITIAN DAN PEMBAHASAN

Di antara negara berkembang, Indonesia merupakan salah satu negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia kurang memprioritaskan pengembangan teknologi dan penguasaan strategi. Yang terjadi saat itu adalah transfer teknologi dari negara maju tidak otomatis dikuasai oleh negara berkembang seperti Indonesia. Sungguh ironis, karena pada sekitar tahun 1980 Indonesia merupakan negara Asia Tenggara yang memiliki satelit komunikasi pertama kali. Namun sekarang Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, sudah menjadi negara maju berbasis teknologi komunikasi modern.

Walaupun masih ada kontroversi, bisa dikatakan bahwa Indonesia ialah negara dengan kesenjangan digital yang cukup besar. Kesenjangan digital bisa dijelaskan sebagai adanya kesenjangan antara mereka yang bisa menggunakan teknologi komunikasi dan mereka yang tidak bisa. Selain kesenjangan tingkat pendidikan dan ekonomi di Indonesia, akses teknologi komunikasi Indonesia juga belum merata. Ketimpangan, kurangnya informasi dan telekomunikasi dapat dibagi menjadi beberapa kategori. Tentunya yang paling banyak dikunjungi adalah yang paling dekat dengan pusat informasi komunitas (masyarakat).

Terlepas dari kesenjangan digital, kejahatan dunia maya (*cyber crime*) di Indonesia masih merajalela. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para hacker hitam. Mereka dapat menggunakan kartu kredit orang lain untuk mendapatkan apa pun yang mereka butuhkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16. Kejahatan tersebut biasa disebut dengan (*credit card fraud*) atau *carding*. Indradi memaparkan, carding ialah penipuan terhadap kartu kredit apabila pelaku mengerti nomor kartu kredit seseorang yang masih berlaku, kemudian pelaku dapat membeli perlengkapan secara online dan mengirimkan tagihan kepada pemilik asli kartu kredit tersebut, pelaku carding biasa disebut carder. Dalam kejahatan ini, pemilik kartu kredit akan kehilangan uangnya karena orang lain menggunakannya untuk berbelanja dengan mencuri rekening kartu kreditnya. Pencurian akun ini bisa dilakukan dengan cara membobol keamanan toko online tempat pembelian dilakukan.

Apalagi jika keamanan toko online tersebut tidak kuat, maka akun kartu kredit yang kemungkinan dibajak oleh para pelaku carding (carder) akan bertambah. Berdasarkan kasus dan keadaan *cyber crime* yang berlangsung di Indonesia, bisa terlihat bahwa *cyber crime* melahirkan ancaman serius bagi departemen keamanan non tradisional. Di Indonesia, kejahatan *cyber crime* merupakan salah satu kejahatan tertinggi di dunia. Istilah keamanan disebut sebagai kemampuan negara untuk mendeskripsikan konsep ancaman dengan mengedepankan aspek militer dalam penyelesaiannya. Seperti yang dikatakan oleh Walt, penelitian keamanan adalah fenomena perang yang ditegaskan sebagai, "*the study of threat, use, and control of military force*".

Namun, setelah tuntasnya perang dingin, makna dari istilah keamanan mengalami perubahan, keamanan meliputi sudutsudut yang lebih luas, semacam masalah lingkungan hidup, hak asasi manusia, ekonomi, sosial masyarakat, budaya, dan sebagainya. Perubahan makna dan konsep keamanan ini disebabkan oleh berbagai perkembangan, seperti tren global. Revolusi di bidang teknologi komunikasi menunjukkan salah satu tren perkembangan, perubahan ini memungkinkan jarak dapat dihilangkan dan didukung oleh fasilitas transportasi dunia yang semakin kompleks. Situasi ini akan berdampak pada perkembangan problematis masalah politik global, termasuk masalah keamanan.

p-ISSN : 0215-3092
e- ISSN : 2443-0013

Sistem hukum Indonesia tidak secara spesifik mengontrol tentang hukum siber, namun beberapa undangundang telah mengatur pencegahan kejahatan siber, seperti Undang-undang No. 36 tentang 1999 tentang Telekomunikasi, Undang-undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang dan peraturan tersebut ini telah mengkriminalisasi jenis kejahatan dunia maya (*cyber crime*) dan ancaman hukuman buat setiap pelanggarnya.

Selain itu, kebijakan kriminalisasi yang tertulis dalam golongan *cyber crime* telah dirumuskan dalam RKUHP yang terdapat pada Buku Kedua (Bab VIII): Tindak Pidana yang membahayakan keamanan Umum bagi Orang, Barang, Lingkungan Hidup. Bagian Kelima: Pasal 373- 379 tentang Tindak Pidana terhadap Informatika dan Telematika, yang mengatur tindak pidana *illegal access, illegal interception, data interference* dan *system interference*, penyalahgunaan nama domain, dan pornografi anak.

Dalam pembahasan perkembangan hukum pidana yang akan datang, penyelesaian dan pencegahan *cyber crime* kudu diimbangi dengan penertiban dan pengembangan seluruh sistem hukum pidana, yang mencakup pembangunan struktur, budaya, serta substansi hukum pidana. Dalam kondisi demikian, kebijakan hukum pidana menempati letak yang strategis dalam perkembangan hukum pidana modern. Kebijakan hukum pidana berniat untuk mencapai kedamaian dan kesejahteraan semua orang.

Berikut tindakan kejahatan dunia maya (*cyber crime*) yang di atur dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undangundang No. 19 Tahun 2016 tentang Perubahan atas Undangundang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagai berikut:

a. Tindakan yang melanggar kesusilaan
b. Perjudian
c. Penghinaan atau pencemaran nama baik
d. Pemerasan atau pengancaman
e. Penguntitan (cyberstalking)
f. Penyebaran berita palsu (hoax)
g. Ujaran kebencian
h. Akses illegal

Tindak pidana *cyber crime* memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Kebanyakan dari korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka saat ini, dan yang perlu dilakukan sekarang adalah mencegah kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan tersebut dapat berupa:

1) *Educate user* (memberikan pengetahuan baru tentang *Cyber crime* dan dunia internet)
2) *Use hacker's perspective* (menggunakan pemikiran hacker untuk melindungi sistem anda)
3) *Patch system* (menutup lubang-lubang kelemahan pada sistem)
4) *Policy* (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5) IDS (*Intrusion Detection System*) bundled with IPS (*Intrusion Prevention System*)
6) *Firewall.*
7) *AntiVirus.*

Tindakan penegak hukum terhadap pelaku tindak pidana dunia maya adalah untuk melindungi pengguna *cyberspace* dari para *cracker* yang menggunakan media internet dalam melakukan kejahatannya. Meskipun Indonesia belum memiliki "*cyberlaw*" yang secara khusus menargetkan kepentingan korban, namun Indonesia tetap perlu tindakan hukum dengan menggunakan hukum yang ada sebelumnya seperti: perundang-undangan, yurisprudensi maupun konvensi-konvensi Internasional yang sudah diratifikasi untuk melindungi kepentingan penduduk dunia maya di Indonesia Berbagai upaya dapat diambil untuk menyelesaikan kejahatan Internet, baik secara premetif, preventif, maupun represif.

p-ISSN : 0215-3092
e- ISSN : 2443-0013

Upaya prevetif dapat dijalankan dengan meratifikasi kesepakatan *cyber crime* internasional kedalam sistem hukum di Indonesia. Kesepakatan Dewan Eropa ialah salah satu wujud kesepakatan internasional, dan sebagian kovenannya telah diratifikasi kedalam sistem perundangundangan di Indonesia. Penanggulangan *cyber crime* secara preventif dapat dijalankan dengan cara mengembangkan pengamanan, meningkatkan energi guna fitur komputer, kemampuan dan kedisplinan dalam memakai fitur tersebut di dunia maya. Aktifitas tersebut bisa berbentuk aksi yang dapat dijalankan baik secara individu, kebijakan nasional, ataupun global.

Sementara itu tindakan penanggulangan *cyber crime* secara represif dapat dilaksanakan dengan menjerat para pelaku tindak pidana untuk ditangani sesuai dengan undangundang. Undang-undang menentukan kepentingan korban dengan memberikan restitusi, kompensasi, ataupun asistensi yang merupakan tanggung jawab pelaku dengan Negara sebagai penyedianya.

IV. KESIMPULAN

Berdasarkan kasus dan kondisi *cyber crime* yang terjadi di Indonesia, dapat terlihat bahwa *cyber crime* merupakan ancaman serius bagi departemen keamanan non tradisional. Di Indonesia, kejahatan penggunaan perangkat komputer dan internet (*cyber crime*) merupakan salah satu kejahatan tertinggi di dunia. Sistem hukum Indonesia tidak secara spesifik mengatur tentang hukum siber (*cyber crime*), namun beberapa undang-undang telah mengatur pencegahan kejahatan siber, seperti Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi, Undang-undang No. 19 Tahun 2002 tentang Hak Cipta, Undang-undang No. 15 Tahun 2003 tentang Pemberantasan Terorisme, serta Undangundang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dalam pembahasan perkembangan hukum pidana dimasa mendatang, penanggulangan dan pencegahan cybercrime kudu diimbangi dengan pembenahan serta pengembangan seluruh sistem hukum pidana, yang meliputi pembangunan struktur, budaya, serta substansi hukum pidana. Dalam kondisi demikian, kebijakan hukum pidana menempati posisi yang strategis dalam kemajuan hukum pidana modern. Serta penegakan hukum pidana hendaknya lebih memperhatikan kepada sistem keadilan restoratif (Restorative Justice), sepertinya ini merupakan solusi yang adil untuk mengaitkan pelaku, korban, keluarganya, serta pihak lain yang terlibat dalam tindak pidana untuk bersamasama berupaya menyelesaikan tindak pidana tersebut

DAFTAR PUSTAKA

Chazawi, Adami. (2013). *Hukum Pidana Positif Penghinaan*. Edisi Revisi. Malang: Media Nusa Creative,.

Fitriani, Yuni, dan Roida Pakpahan. (2020). “Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace.” *Cakrawala: Jurnal Humaniora* 20, no. 1.

Mubarok, Nafi’. (2017). *Kriminologi dalam perspektif Islam*. Sidoarjo: Dwiputra Pustaka Jaya,.

Thantawi. (2014). “Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia.” *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala* 2, no. 1