PENERAPAN KEBIJAKAN DIGITAL DALAM RANGKA PENCEGAHAN CYBER CRIME DITINJAU DARI UNDANG-UNDANG ITE

Hery Firmansyah[1], Amad Sudiro[2], Sindhi Cintya[3], Charina Putri Besila[4], dan Shrishti[5]

[1]Jurusan Ilmu Hukum, Universitas Tarumanagara
Email: Heryf@fh.untar.ac.id
[2] Jurusan Ilmu Hukum, Universitas Tarumanagara
Email: amads@fh.untar.ac.id
[3]Jurusan Ilmu Hukum, Universitas Tarumanagara
Email: sindhi.205180001@stu.untar.ac.id
[4]Jurusan Ilmu Hukum, Universitas Tarumanagara
Email: charina.205180089@stu.untar.ac.id
[5]Jurusan Hukum, Tarumanagara Jakarta
Email: shrishti.205190263@stu.untar.ac.id

ABSTRACT

The development of social media (medsos) is getting faster and reaching all levels of society. Social media has become a phenomenal and inseparable need of the Indonesian people. Some of the features of social media include upload status, share news links, chat comumunication, audiovisual communication and more. Even though all people's behavior on social media platforms has been regulated by law, criminal acts as cybercrime still occur. Cybercrime is not a foreign thing among Indonesian people. Even the government through the National Police has formed a special team to monitor and eradicate cyber crime in Indonesia. However, in the eradication process, there is still a problem, namely in proving the defendant's guilt. This fact becomes a challenge for law enforcement circles to solve all problems that occur due to very rapid technological developments. The Criminal Procedure Code (KUHAP) and the Law on Information and Electronic Transactions (UU ITE), namely Law No. 19 of Year 2016 Amendment to Law No. 11 of Year 2008 have been applied to cyber crimes. Unfortunately, the Indonesian people do not understand these regulations. This is because digital literacy focuses more on searching for hoax information rather than explaining various actions that can be classified as cyber crime.

***Keywords**: Cybercrime, ITE Law, Prevention, Social Media, Criminal Law*

ABSTRAK

Perkembangan media sosial (medsos) semakin pesat dan menembus seluruh lapisan masyarakat. Medsos telah menjadi kebutuhan masyarakat Indonesia yang sangat fenomenal dan tidak dapat dipisahkan. Beberapa fitur yang dimiliki oleh medsos termasuk mengunggah status, membagi halaman berita, *chatting*, komunikasi audiovisual dan fitur lainnya. Walaupun semua perilaku masyarakat pada platform medsos telah diatur oleh hukum, tetap saja terjadi tindak pidana sebagai cybercrime terjadi. Cybercrime tidak merupakan hal yang asing antar masyarakat Indonesia. Bahkan pemerintah telah membentuk tim khusus untuk memantau dan memberantas cyber crime di Indonesia melalui Polri. Akan tetapi dalam proses pembrantasan, tetap saja terdapat suatu permasalahan, yaitu pada pembuktian kesalahan terdakwa. Fakta ini menjadi tantangan bagi aparat penegak hukum untuk menyelesaikan segala permasalahan yang ditimbulkan oleh perkembangan teknologi yang sangat pesat. Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-Undang Tentang Informasi dan Trsansaksi Elektonik (UU ITE) yaitu Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 telah diterapkan untuk perbuatan cyber crime. Sayangnya, masyarakat Indonesia belom paham dengan peraturan-peraturan tersebut. Ini dikarenakan literasi digital lebih banyak berfokus pada penelusuran informasi hoaks dari pada menjelaskan berbagai perbutan yang dapat digolongkan sebagai cyber crime.

.

Kata kunci: *Cybercrime*, UU ITE, Pencegahan, Media Sosial, Pidana

1. PENDAHULUAN

Penggunaan Teknologi Informasi, media dan komunikasi telah mengubah perilaku masyarakat dan peradaban manusia di seluruh dunia. Perkembangan teknologi informasi dan komunikasi berarti bahwa hubungan dunia melintasi batas-batas negara dan menyebabkan perubahan sosial, ekonomi, dan budaya secara besar yang terjadi dengan cepat. Tidak disangka bahwa teknologi

informasi akan membawa manfaat yang besar bagi negara-negara di dunia (Budi Suhariyanto, 2013) yang dapat menyumbangkontribusi bagi perkembangan dan kemajuan kesejahteraan peradaban manusia, seperti e-commerce, e-learning, internet banking dan lain-lain, akan tetapi sekaligus menjadi wadah yang efektif untuk melakukan perbuatan melanggar hukum.

Kemajuan teknologi internet, menimbulkan keberadaan kejahatan yang dapat dilihat dari munculnya istilah Cyber crime atau kejahatan yang dilakukan dengan mengunakan jaringan Internet. Cyber Crime merupakan segala kejahatan/perilaku ilegal yang dilakukan oleh seseorang, sekelompok orang atau korporasi dengan menggunakan teknologi komputer, jaringan internet dan juga perangkat digital lainnya sebagai alat utama (Agus Rahardjo, 2002). Kejahatan tersebut dapat dilihat ketika timbul dampak negatif ketika kesalahan terjadi karena perangkat komputer dan menyebabkan kerugian besar bagi pengguna atau pemangku kepentingan. Kesalahan yang disengaja tersebut mengarah kepada penyalahgunaan komputer (Andi Hamzah, 1990). Dalam jaringan komputer seperti internet, masalah kejahatan menjadi lebih kompleks karena cakupannya yang luas.

Cyber crime yang juga disebut sebagai kejahatan dunia maya (*virtual)* memanfaatkan perkembangan teknologi untuk melakukan perbuatan melawan hukum dengan berbagai motif, mulai dari kesenangan diri sendiri atau kejahilan sampai tindakan kriminal yang menyebabkan kerugian finansial atau politik. Jenis kejahatan ini juga tergantung pada kemampuan pelaku dalam menguasai bidang teknologi. Dengan ini, munculah beberapa kasus Cybercrime di Indonesia seperti pembobolan kartu kredit, peretasan beberapa situs, penipuan jual-beli, penyadapan transmisi data, pendistribusian konten ilegal di medsos, ujaran kebencian, pembajakan akun medsos dan memanipulasi data.

Kejahatan tersebut tidak berhenti disini, berdasarkan lokakarya Measures to Combat Computer-related Crime Kongres XI PBB dijelaskan bahwa dengan teknologi baru yang akan muncul di bidang komunikasi dan informasi akan memberikan bayangan gelap (a dark shadow), karena memungkinkan terjadinya bentuk-bentuk eksploitasi baru, kesempatan baru untuk aktivitas kejahatan, dan bentuk-bentuk baru dari kejahatan cyber.

Karakteristik pelaku cyber crime berdeda dengan pelaku kejahatan lain. Walaupun para hakim menggunakan hukum pidana konvensional yang berlaku di Indonesia dapat untuk mengadili pelaku cyber crime, pada prakteknya hukum tersebut memiliki banyak keterbatasan yaitu dari sisi unsur tindak pidana maupun pertanggungjawaban pidananya. Hal tersebut mengakibatkan banyak pelaku cyber crime lolos dari jeratan hukum.

Maka untuk itu pemahaman mengenai ruang lingkup kejahatan telematika sangat penting agar aparat penegak hukum dapat memberi batasan cakupan kejahatan telematika. Menurut beberapa literature, cyber crime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut: (Antoni, 2017)

a. Unauthorized access to computer system and service, yaitu kejahatan yang dilakukan kedalam suatu sistem jaringan computer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan computer yang dimasukinya.
b. Illegal contents, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah:
c. Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
d. Pemuatan hal-hal yang berhubungan dengan pornografi.
e. Pemuatan suatu informasi yang merupakan rahasia Negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.
f. Data forgecy, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless dokumen melalui internet. Kejahatan ini biasanya ditunjukkan

pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.

g. Cyber espionage, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan computer pihak sasarannya.
h. Cyber sabotage and extortion, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan computer yang tersambung dengan internet.
i. Offence against intellectual property, yaitu kekayaan yang ditunjukkan terhadap hak kekayaan intelektuan yang dimiliki seorang di internet.
j. Infringements of privacy, yaitu kejahatan yang ditunjukkan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

2. METODE PELAKSANAAN PKM

Langkah-langkah/tahapan pelaksanaan

Kegiatan sosialisasi tentang Penerapan Kebijakan Dijital Dalam Rangka Pencegahan Cyber Crime Ditinjau Dari Undang-Undnag ITE mengikuti prinsip-prinsip transparansi/ keterbukaan, partisipasi, koordinasi, dan keterpaduan. Sosialisasi Penerapan Kebijakan Dijital Dalam Rangka Pencegahan Cyber Crime Ditinjau Dari Undang-Undnag ITE harus mampu menguraikan berbagai aspek penting mengenai kejahatan cybercrime, penerapan UU ITE, tata cara menghindari kejahatan cybercrime, serta berbagai ketentuan teknis lainnya. Metode sosialiasi berupa pemaparan materi dan diskusi interaktif antara penyaji dengan peserta sosialiasi.

Partisipasi mitra dalam kegiatan PKM

SMA Yadika 1 Duri Kepa sebagai mitra dalam kegiatan PKM akan membantu tim dalam memfasilitasi tempat dan sarana, serta menyebarkanluaskan informasi mengenai sosialisasi yang diadakan. Mitra juga akan menugaskan perangkat Sekolah untuk mengikuti sosialisasi ini.

Uraian kepakaran dan tugas masing-masing anggota tim

Materi yang akan disampaikan pada sosialisasi ini antara lain:

1. Kejahatan Cybercrime dan Implementasi UU ITE oleh
2. Moderator oleh
3. Tim Administrasi oleh

3. HASIL DAN PEMBAHASAN

Era globalisasi membawa pengaruh terhadap bidang teknologi informasi dengan munculnya berbagai bentuk kejahatan yang dapat disebut sebagai cybercrime, suatu fenomena yang memerlukan penanggulangan secara cepat dan akurat.

Semua negara sudah pasti memiliki hukum yang mengatur cybercrime tersebut, termasuk Indonesia. Pengaturan teknologi informasi yang diterapkan oleh suatu negara berlaku untuk setiap orang yang melakukan kejahatan cyber baik di wilayah negara tersebut maupun di luar negara apabila perbuatan tersebut memiliki akibat di Indonesia. Indonesia termasuk negara yang menetapkan cybercrime dalam hukum pidana. Kejahatan tersebut tidak hanya di atur dalam Hukum Pidana akan tetapi juga dibeberapa Undang-undnag di luar KUHP yaitu termasuk UU ITE.

UU ITE tersebut terbentuk untuk menjaga ruang digital Indonesia agar lebih bersih, sehat, beretika, dan bisa dimanfaatkan secara produktif. Peraturan tersebut juga meminta Kapolri dan jajaran agar lebih selektif dalam mensikapi dan menerima pelaporan pelanggaran UU ITE.

Selain UU ITE, peraturan yang menjadi landasan dalam penanganan kasus *cybercrime* di Indonesia ialah peraturan pelaksana UU ITE dan juga peraturan teknis dalam penyidikan di masing-masing instansi penyidik.

Kini, untuk memberantas kejahatan dunia maya, Polri melakukan terobosan dengan mengedepankan pengaduan umum tentang kejahatan ini. Pada bulan Agustus, unit investigasi kriminal polisi (Dittipidcyber) secara resmi meluncurkan situs web patroli cyber. Kejahatan dunia maya dapat dilaporkan langsung di halaman ini. Website ini juga membantu menghubungkan setiap unit kepolisian untuk mendeteksi kasus cybercrime. Penjahat sering melakukan kejahatan secara langsung di berbagai daerah.

Dengan pembaruan segala macam, dengan berjalannya waktu kejahatan cyber crime tetap saja meningkat dan menjadi lebih luas. Dalam kondisi tersebut timbul permasalahan hukum yang harus dihadapi oleh apparat penegak hukum ketika dilakukan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal melakukan pembuktian dengan hal yang terkait dengan tindakan hukum yang dilaksanakan dengan mengunakan sistem elektronik.

Secara umum kejahatan cyber tersebut dapat dicegah melalui beberapa cara yaitu:

1. Pendidikan komputer oleh sekolah, sebagai akibatnya bisa menaikkan pengetahuan dan kesadaran atas bentuk bentuk perbuatan dalam menggunakan sarana komputer yang salah.
2. Pengawasan terhadap warnet-warnet yang ada di masyarakat, untuk mencegah warnet sebagai sarang penggunaan situs yang melanggar hukum.
3. Pengawan orang tua terhadap anak pengguna komputer dan internet.
4. Membuat wadah bagi anak-anak yang memiliki kelebihan dibidang jaringan internet. Filterisasi situs-situs yang merusak norma anak muda oleh pemerintah.
5. Sanksi yang tegas bagi pemilik warnet jika tidak menegur users nya yang sedang menggunaan situs cyber gambling, cyberporn , dll.
6. Banyaknya komunitas black hat (hacker hitam) di Indonesia sebagai salah satu dampak penyebab maraknya terjadi kejahatan di dunia maya, lemahnya system computer, dan begitu kecilnya gaji para ahli IT di Indonesia menyebabkan para master computer berbuat criminal demi mencukupi kebutuhan financialnya, jadi perlu peningkata taraf hidup bagi para ahli IT.

4. KESIMPULAN DAN SARAN

Kesimpulan dan saran yang dapat kami sampaikan dari sosiolisasi tersebut adalah metode langkah-langkah/upaya penanggulangan cybercrime yaitu upaya preventif dan represif.

a. Upaya Preventif

Dalam melaksanakan kegiatan preventif tersebut, kepolisian khususnya unit polisi cybercrime telah melakukan berbagai langkah, termasuk melakukan sosialisasi kepada masyarakat luas. Selain itu, sosialisasi juga diberikan kepada masyarakat umum melalui media surat kabar dan radio, dan polisi terus melakukan himbauan kepada masyarakat luas saat mengisi acara talk show.

b. Upaya Represif

Polisi akan bekerja sama dengan pemangku kepentingan yang ada. Artinya, menangkap pelaku kejahatan yang terlibat dalam perbuatan tersebut, atau menangkap dan menangkap tersangka dalam kasus kejahatan dunia maya pasca penangkapan melalui laporan masyarakat dan kunjungan tempat kejadian perkara (TKP) selanjutnya. Merujuk ke kejaksaan, diadakan konferensi pers media, dan media hadir untuk mewawancarai tersangka dan petugas polisi yang menangani kasus tersebut. Hasil wawancara tersebut kemudian akan disiarkan atau disebarluaskan untuk menginformasikan kepada masyarakat tentang kasus-kasus yang ditangani polisi.

c. Pelaksanaan Undang Informasi dan Transaksi

Ketika berhadapan dengan cybercrime di Indonesia, hukum positif masih rapuh di *lex locus delicti*. Namun berbeda dengan situasi atau situasi pelanggaran hukum yang dihadapi oleh pelaku dan korban kejahatan dunia maya dalam kejahatan dunia maya di tempat yang berbeda. Bidang kejahatan dunia maya yang luas namun mudah diakses telah menyebabkan kejahatan merajalela. Kepolisian Negara Republik Indonesia (POLRI), sebagai salah satu lembaga penegak hukum negara, tak mampu lagi berdiam diri setelah lahir Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Aparat penegak hukum dalam hal ini penyidik kepolisian harus bergerak secara aktif dalam menindak kejahatan di dunia maya. Aparat kepolisian harus dapat menangani kasus kejahatan yang terjadi di dunia maya (M. Ramli, Ahmad, 2006).

Melainkan dari upaya tersebut, penyempurnaan UU ITE oleh pihak berkepentingan sangat dibutuhkan agar Indonesia dapat mewujudkan UU ITE yang sempurna dan bersifat lex specialist. Dengan ini harus juga dilakukan perubahan pada beberapa ketentuan Kitab Undang-Undang Hukum Pidana agar dapat mengatasi berbagai jenis kejahatan cyber crime.

Dengan diperlakukannya berbagai perubahan dalam Kitab Undang-Undang Hukum Pidana Nasional diharapkan berdampak pada pulihnya kepercayaan masyarakat terhadap hukum.

Ucapan Terima Kasih (*Acknowledgement*)

Ucapan terimakasih sampaikan kepada Abdimas UNTAR yang telah mendukung kami dalam melaksanakan sosialisasi ini. Apresiasi juga kami sampaikan kepada SMA YADIKA 1 DURI KEPA yang telah mengikuti sosialisasi dengan baik dan antusiasme yang tinggi.

REFERENSI

Antoni. (2017). Kejahatan Dunia Maya (Cybercrime) dalam Simak Online, Jurnal Nuraini.

Hamza, A. (1990). Aspek-Aspek Pidana di Bidang Komputer. Sinar Grafika, Jakarta.

M.Ramli, Ahmad. (2006). Cyber Law dan HAKI Dalam Sistem Hukum Indonesia, PT Refika Aditama, Bnadung.

Rahardjo, A. (2002). Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologo. PT Citra Aditya Bakti, Bandung.

Suhariyanto, Budi. (2013). Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan dan Celah Hukumnya. PT Rajagrafindo, Depok.

(halaman kosong)