Pintar
Opini Untar

Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

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

* Hery Firmansyah

** Sindhi Cintya | **Charina Putri Besila | **Rony Mart Panjaitan | **Shrishti Shrishti

Editor: Frangky Selamat

Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi menyebabkan hubungan dunia menjadi *borderless* dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Tidak disangka bahwa teknologi informasi membawa keuntungan yang besar bagi negara-negara di dunia yang dapat memberi kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, seperti *e-commerce, e-learning, internet banking* dan lain-lain, akan tetapi sekaligus menjadi sarana efektif perbuatan melawan hukum.

Perkembangan teknologi internet, menyebabkan keberadaan kejahatan yang dapat dilihat dari munculnya istilah *cybercrime* atau kejahatan melalui jaringan internet. *Cybercrime* merupakan segala kejahatan/perilaku ilegal yang dilakukan oleh seseorang, sekelompok orang atau korporasi dengan menggunakan teknologi komputer, jaringan internet dan juga perangkat-perangkat digital lainnya sebagai alat utama. Kejahatan tersebut dapat dilihat ketika timbul dampak negatif saat terjadi kesalahan yang ditimbulkan oleh piranti komputer yang akan mengakibatkan kerugian besar bagi pengguna atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja tersebut mengarah pada penyalahgunaan komputer. Dalam jaringan komputer seperti internet, masalah kejahatan menjadi lebih kompleks karena cakupannya yang luas.

Cybercrime yang juga disebut sebagai kejahatan dunia maya (*virtual)* memanfaatkan perkembangan teknologi untuk melakukan perbuatan melawan hukum dengan beragam motif, mulai dari kepuasan diri atau keisengan sampai kejahatan yang merugikan secara ekonomi maupun

Pintar
Opini Untar
Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

politik. Jenis kejahatan ini pun beragam sesuai dengan kemampuan pelaku dalam penguasaan bidang teknologi. Dengan ini, munculah beberapa kasus *cybercrime* di Indonesia seperti pembobolan kartu kredit, *hacking* beberapa situs, penipuan jual beli, menyadap transmisi data orang lain, penyebaran konten ilegal di medsos, ujaran kebencian, pembajakan akun medsos dan memanipulasi data.

Kejahatan tersebut tidak berhenti di sini, 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 cybercrime berbeda dengan pelaku kejahatan lain. Walaupun para hakim menggunakan hukum pidana konvensional yang berlaku di Indonesia dapat untuk mengadili pelaku *cybercrime*, pada praktiknya hukum tersebut memiliki banyak keterbatasan yaitu dari sisi unsur tindak pidana maupun pertanggungjawaban pidananya. Hal tersebut mengakibatkan banyak pelaku *cybercrime* lolos dari jeratan hukum.

Karakteristik *cyber crime*

Maka untuk itu pemahaman mengenai ruang lingkup kejahatan telematika sangat penting agar aparat penegak hukum dapat memberi batasan cakupan kejahatan telematika. Menurut beberapa literatur, *cybercrime* merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:

a) *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer 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: pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, pemuatan hal-hal yang berhubungan

Pintar
Opini Untar
Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

dengan pornografi, dan pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.

c) *Data forgery*, yaitu kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scripless* 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.
d) *Cyber espionage*, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasarannya.
e) *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
f) *Offence against intellectual property*, yaitu kekayaan yang ditunjukkan terhadap hak kekayaan intelektual yang dimiliki seorang di internet.
g) *Infringements of privacy*, yaitu kejahatan yang ditunjukkan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

Penegakan hukum

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 diatur dalam Hukum Pidana akan tetapi juga di beberapa Undang-undang 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 menyikapi dan menerima pelaporan pelanggaran UU ITE.

Pintar
Opini Untar
Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

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.

Dalam rangka memberantas *cybercrime*, Polri kini telah melakukan terobosan dengan memudahkan pengaduan masyarakat terkait kejahatan ini. Dittipidcyber Bareskrim Polri pada Agustus resmi meluncurkan situs "Patroli Cyber". Dalam situs ini, aksi kejahatan *cyber* bisa langsung dilaporkan. Situs tersebut juga membantu agar tiap satuan wilayah kepolisian saling terkoneksi untuk mengungkap kasus tindak pidana *cyber*. Pasalnya pelaku kejahatan sering kali melakukan aksi kejahatan langsung di berbagai wilayah.

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

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

1. Pendidikan komputer oleh sekolah, sehingga dapat meningkatkan 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. Pengawasan orangtua terhadap anak pengguna komputer dan internet.
4. Membuat wadah bagi anak-anak yang memiliki kelebihan di bidang 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 menggunakan situs *cyber gambling*, *cyber porn*, dan lain-lain.
6. Banyaknya komunitas *black hat* (*hacker* hitam) di Indonesia sebagai salah satu dampak penyebab maraknya terjadi kejahatan di dunia maya, lemahnya sistem komputer, dan begitu kecilnya gaji para ahli IT di Indonesia menyebabkan para master komputer berbuat kriminal demi mencukupi kebutuhan finansialnya, jadi perlu peningkatan taraf hidup bagi para ahli IT.

Pintar
Opini Untar
Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

Selain Langkah-langkah tersebut, pihak kepolisian telah melakukan berbagai upaya penanggulangan *cybercrime* yaitu dengan upaya preventif dan represif.

a. Upaya Preventif

   Dalam melakukan upaya preventif ini pihak kepolisian khususnya unit *cybercrime*, polisi telah melakukan berbagai upaya seperti memberikan himbauan ke masyarakat melalui media elektronik maupun media sosial dengan menyebarkan broadcast berupa himbauan-himbauan terkait *cybercrime* untuk diteruskan ke masyarakat luas. Selain itu dilakukan juga penerangan ke masyarakat melalui media surat kabar dan radio, serta pada saat mengisi acara *talk show* pihak kepolisian tidak henti-hentinya memberikan himbauan ke masyarakat.

b. Upaya Represif

   Pihak kepolisian bekerja sama dengan *stakeholder* yang ada yaitu bagaimana menangkap pelaku yang tertangkap tangan melakukan kejahatan ataupun melalui laporan masyarakat kemudian mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap tersangka kasus *cybercrime*. Setelah dilakukan penangkapan kemudian diproses di kepolisian dan sebelum dilimpahkan berkas perkaranya ke kejaksaan terlebih dahulu diadakan konferensi pers dengan media di mana pihak media hadir untuk mewawancarai tersangka dan petugas yang menangani kasus tersebut. Lalu hasil wawancara tersebut disiarkan atau disebarkan ke masyarakat luas, sehingga masyarakat mengetahui kasus-kasus yang ditangani oleh aparat kepolisian

Selain upaya tersebut, penyempurnaan UU ITE oleh pihak berkepentingan sangat dibutuhkan agar Indonesia dapat mewujudkan UU ITE yang sempurna dan bersifat *lex specialis*. Dengan ini harus juga dilakukan perubahan pada beberapa ketentuan Kitab Undang-Undang Hukum Pidana agar dapat mengatasi berbagai jenis kejahatan *cybercrime*. Dengan diberlakukannya berbagai perubahan dalam Kitab Undang-Undang Hukum Pidana Nasional diharapkan berdampak pada pulihnya kepercayaan masyarakat terhadap hukum.

Berbagai kasus pelanggaran hukum melalui media internet kini kerap terjadi di Indonesia, negeri yang merupakan negara hukum *(recht-staats)*. Kelemahan hukum sering dijadikan kambing hitam, sehingga banyak perbuatan pidana terlepas dari jerat hukum. Hukum itu sangat dinamis, hukum

Pintar
Opini Untar
Volume 2 | Halaman 391 – 396 | 30 Desember 2021
ISSN: 2746 - 9018

bukan barang mati. Soal kebenaran dalam hukum tidak dapat hanya dilihat dari satu sisi kelompok, karena hukum itu pada hakikatnya harus dapat merespons rasa keadilan yang tumbuh di tengah masyarakat. Hukum bukan hanya sekedar permainan pasal-pasal secara legalitas, akan tetapi hukum harus mengikat secara sosiologis.

Dalam menjamin keamanan, keadilan dan kepastian hukum, penegakan hukum *(law enforcement)* di dunia *cyber* maka harus memenuhi 4 (empat) syarat sebagai berikut:

a) Adanya aturan perundang-undangan khusus yang mengatur dunia *cyber*.
b) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus menangani *cybercrime*.
c) Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu.
d) Kesadaran hukum dari masyarakat yang terkena peraturan.

Selain ke 4 (empat) syarat tersebut penegakan hukum di dunia maya juga sangat tergantung dari pembuktian dan yurisdiksi yang ditentukan oleh undang-undang. Oleh karena itu, peraturan mengenai *cyber law* harus dapat mencakup perbuatan yang dilakukan di luar wilayah Indonesia tapi merugikan kepentingan orang atau negara dalam wilayah Indonesia. Sebagaimana diterapkan dalam UU ITE mengenai asas universal.

Dengan ini, dalam berbagai kesempatan, keamanan jaringan merupakan mencegah terjadinya *cybercrime*. Pengalaman dari negara berkembang seperti Filipina yang secara teknologi dapat dikatakan tertinggal jika dibandingkan dengan negara Singapura. Namun dalam menyikapi *cybercrime*, negara tersebut jauh lebih siap melalui undang-undang yang begitu tegas untuk mencegah terjadinya *cybercrime*.

* Dosen Fakultas Hukum Universitas Tarumanagara

** Mahasiswa Fakultas Hukum Universitas Tarumanagara