VOLUME 4 NOMOR 2 TAHUN 2024
EDISI OKTOBER
E-ISSN 2807-372X P-ISSN 2807-6095
Diserahkan : 30/07/2024 Disetujui : 20/08/2024 Diterbitkan : 30/10/2024
Submitted : 30/07/2024 Accepted : 20/08/2024 Published : 30/10/2024

KEJAHATAN DI DUNIA MAYA DALAM SISTEM HUKUM INDONESIA

Afwa Hilman Hidayat, Aina Shafira Rohiman, Thoriq Faraaj Mumtaaz, Valerie Liony Yuliana Naomi
Fakultas Hukum, Universitas Singaperbangsa Karawang
2010631010047@student.unsika.ac.id, 2010631010175@student.unsika.ac.id,
2010631010041@student.unsika.ac.id, 2010631010155@student.unsika.ac.id

ABSTRAK

Setiap interaksi yang terjalin antara sesama manusia bisa menimbulkan gesekan yang mengarah perselisihan dan permusuhan, untuk itu penyelesaian gesekan agar tidak meruncing menjadi permusuhan, maka peran hukum sangatlah penting dan dibutuhkan. Mengutip dari Kamus Besar Bahasa Indonesia Daring (KBBI), peretas memiliki makna, di antaranya, orang yang terobsesi untuk mengetahui lebih banyak tentang komputer atau orang yang mengakses komputer orang lain tanpa izin, biasanya dengan bantuan teknologi komunikasi. Metode yang digunakan ialah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah suatu pendekatan yang mengacu pada peraturan perundang-undangan yang berlaku. Adapun sumber data menggunakan data-data sekunder. Cyber crime Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU cyber crime secara khusus.
Kata Kunci: **Cybercrime, Yuridis, Undang-Undang.**

ABSTRACT

Every interaction that exists between fellow human beings can cause friction that leads to disputes and hostility, for this reason the settlement of friction so that it does not escalate into hostility, the role of law is very important and needed. Quoting from the Big Indonesian Online Dictionary (KBBI), a hacker means, among other things, a person who is obsessed with knowing more about a computer or a person who accesses other people's computers without permission, usually with the help of communication technology. The method used is a normative juridical approach. The normative juridical approach is an approach that refers to the applicable laws and regulations. The data source uses secondary data. Indonesian cyber crime is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) as amended to become Law Number 19 of 2016. So, there is no specific cyber crime law yet.

Keywords*: *Cybercrime, Juridical, Constitution

KEJAHATAN DI DUNIA MAYA DALAM SISTEM HUKUM INDONESIA

A. PENDAHULUAN

Indonesia adalah negara hukum sebagaimana secara tersurat pernyataan bahwa negara yang selalu menyandarkan roda kehidupan yang ada pada hukum yang berlaku.[1] Keberlakuan hukum yaitu sebagai suatu jaminan dan kepastian perlindungan tiap warga negara. *Ubi societas ibi ius* dengan arti di mana ada masyarakat disitu ada hukum, hukum itu ada ialah karena adanya masyarakat. Masyarakat sebagai makhluk sosial dalam situasi kondisi akan menyesuaikan diri dengan perubahan-perubahan yang ada tersebut. Keberadaan hukum selalu berjalan beriringan dengan keberadaan masyarakat, ataupun sebaliknya jikalau tidak ada masyarakat tidak mungkin ada hukum, dan jika pun ada masyarakat tanpa hukum, yang terjadi adalah masyarakat liat dan tak terkendali, karena dalam berperilaku tidak ada pembatasan atau pencegahan dan tidak ada sanksi sebagai suatu efek yang ditimbulkan dari pelanggaran ataupun kejahatan yang dilakukan.

Setiap interaksi yang terjalin antara sesama manusia bisa menimbulkan gesekan yang mengarah perselisihan dan permusuhan, untuk itu penyelesaian gesekan agar tidak meruncing menjadi permusuhan, maka peran hukum sangatlah penting dan dibutuhkan. Fungsi keberadaan hukum ialah untuk mengatur masyarakat jika fungsi hukum tercapai maka akan terwujudlah kesejahteraan. Seiring berkembangnya kemajuan teknologi atas respon dari revolusi yang terjadi selain memberikan dampak positif, tetapi juga memberikan dampak negatif. dampak negatif sebagai contoh yang akan diangkat oleh penulis yaitu mengenai *cybercrime*.

Cybercrime atau kejahatan siber merupakan tindakan ilegal dengan menggunakan pengetahuan teknologi komputer untuk melakukan tindak kejahatan. Pencurian perangkat keras dan perangkat lunak, manipulasi data, pengaksesan sistem komputer secara ilegal dengan telepon, dan mengubah program. Mengutip dari Kamus Besar Bahasa Indonesia Daring (KBBI), peretas memiliki makna, di antaranya, orang yang terobsesi untuk mengetahui lebih banyak tentang komputer atau orang yang mengakses komputer orang lain tanpa izin, biasanya dengan bantuan teknologi komunikasi. Adapun, jenis *cybercrime*

[1]Undang – Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 1 ayat (3).

yang kerap kali ditemui ketika beraktivitas di dunia maya diantaranya, yaitu: akses illegal, phising, penipuan otp, kejahatan konten illegal, dan cyber terrorism. *Cyber crime* Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU *cyber crime* secara khusus.

B. METODE PENELITIAN

Metode penelitian merupakan suatu kegiatan ilmiah yang disasarkan pada metode, sistematika dan pemikiran tertentu yang bertujuan mempelajari satu atau beberapa gejala hukum tertentu dengan jalan menganalisisnya.[2] Menurut Peter Mahmud Marzuki penelitian hukum normatif merupakan suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi.[3] Dalam makalah ini menggunakan penelitian hukum normatif, yaitu penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka. Metode yang digunakan ialah pendekatan yuridis normatif. Pendekatan yuridis normatif adalah suatu pendekatan yang mengacu pada peraturan perundang-undangan yang berlaku. Adapun sumber data menggunakan data-data sekunder.[4] Dalam jurnal ini memuat beberapa dokumen bersumber dari jurnal, buku, internet, perundang-undangan dan lain sebagainya. Pengumpulan data dalam penelitian hukum normatif dilakukan dengan cara studi pustaka berupa data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur-literatur lain berkaitan dengan permasalahan yang diteliti atau penelitian hukum kepustakaan.[5]

C. PEMBAHASAN

1. Jenis-Jenis Cyber Crime

[2] Khudzaifah Dimiyati dan Kelik Wardiono, 2004, Metode Penelitian Hukum, Surakarta: Fakultas Hukum UMS, hal 1.
[3] Peter Mahmud Marzuki, Penelitian Hukum, Cet. 6, (Jakarta: Kencana Prenada Media Group, 2005), hlm. 3.
[4]Johanes Supranto, Metode Penelitian Hukum dan Statistik. (Rineka Cipta: Jakarta. 2003), hlm. 13.
[5]Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, (Jakarta:PT Raja Grafindo Persada, 2001), hlm. 13.

Cyber crime adalah kejahatan di dunia maya. Salah satu jenis kejahatan yang meningkat di tengah pandemi akibat perubahan gaya hidup masyarakat serba *online*.Modus *cyber crime* macam-macam. Mulai dari pencurian data, pembobolan rekening, hingga minta-minta sumbangan atas nama korban pandemi.

Cyber crime adalah tindakan ilegal yang dilakukan pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk menyerang sistem informasi korban.Misalnya melakukan *hack* sosial media, membobol perangkat teknologi serta data korban. Lalu kemudian menyikat habis saldo rekening ataupun kartu kredit korban.*Cyber crime* Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU *cyber crime* secara khusus.

Cyber crime termasuk dalam kategori perbuatan yang dilarang dalam UU ITE.

a. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.
b. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi dan/atau dokumen elektronik.
c. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Ada beberapa jenis kejahatan *cyber crime* yang harus menjadi perhatian masyarakat, antara lain: [6]

a. *Identity Theft*

Identity Theft atau pencurian identitas adalah jenis kejahatan *cyber crime* yang pertama. Di mana, biasanya pelaku akan meyalahgunakan identitas orang lain, seperti, nama, nomor telepon, hingga nomor identitas diri dan nomor kartu kredit guna mengambil keuntungan finansial. Seperti, mengambil pinjaman, masuk ke

[6]Cermati.com :"14 Jenis Cyber Crime, Kejahatan Internet yang Merugikan", November 21, 2022, https://www.cermati.com/artikel/jenis-cyber-crime.

rekening bank atau akun keuangan online, atau mengklaim asuransi.

b. Kejahatan *Phising*

Phishing adalah contoh *cyber crime* untuk melakukan penipuan dengan mengelabui korban. Umumnya aksi kejahatan ini dilancarkan melalui email maupun media sosial lain, seperti mengirimi *link* palsu, membuat *website* bodong, dan sebagainya.

Tujuannya mencuri data penting korban, seperti identitas diri, *password*, kode PIN, kode OTP (*one time password*) pada akun-akun keuangan, seperti *mobile banking*, *internet banking*, *paylater*, dompet digital, sampai kartu kredit.

c. Kejahatan *Carding*

Carding adalah jenis kejahatan dunia maya yang dilakukan dengan bertransaksi menggunakan kartu kredit milik orang lain. Jadi, setelah mengetahui nomor kartu kredit korban, pelaku kemudian berbelanja *online* dengan kartu kredit curian itu.

Nomor kartu kredit tersebut dicuri dari situs atau *website* yang tidak aman. Bisa juga diperoleh dengan cara membeli dari jaringan *spammer* atau pencuri data. Selanjutnya data kartu kredit itu disalahgunakan oleh *carder*, sebutan pelaku kejahatan *carding*.

d. Serangan *Ransomware*

Ransomware adalah *malware* atau *software* jahat yang bukan hanya bisa menginfeksi komputer, tapi juga menyandera data pengguna. Tindak kejahatan ini dapat menimbulkan kerugian besar bagi korbannya.

Pelaku akan meminta uang tebusan ke korban jika ingin *ransomware*dihapus atau dimusnahkan. Apabila korban tidak mengabulkan permintaan tersebut, pelaku tak segan-segan mengancam akan membuat data menjadi korup alias tidak bisa digunakan lagi.

e. Penipuan *Online*

Penipuan *online* atau penipuan digital yang saat ini makin banyak modusnya. Di antaranya adalah modus penipuan berkedok foto selfie dengan KTP atau identitas diri.

Foto selfie bersama KTP biasanya menjadi salah satu syarat registrasi online akun keuangan, seperti dompet digital, *paylater*, pinjaman *online*, sampai daftar rekening bank *online*.

Bisa saja kamu terjebak aplikasi pinjaman online palsu yang dibuat sedemikian rupa. Kemudian oleh pelaku, data kamu dipakai untuk pencucian uang, dijual di pasar gelap, atau digunakan sesuka hati untuk pinjaman *online* ilegal.

f. SIM *Swap*

SIM *swap* adalah modus penipuan dengan mengambilalih nomor ponsel atau kartu SIM ponsel seseorang. Tujuannya untuk meretas akun perbankan seseorang.

Akibatnya, kartu SIM ponsel yang kemudian aktif dan berlaku adalah milik pelaku, bukan lagi punya korban. Oleh karena itu, jika ingin membuang kartu SIM lama, sebaiknya dipatahkan atau digunting agar tidak disalahgunakan orang lain.

g. Peretasan Situs dan Email

Kejahatan ini istilahnya *deface website* dan email. Yakni jenis kejahatan *cyber crime* dengan cara meretas sebuah situs ataupun email, serta mengubah tampilannya.

Dengan kata lain, penampilan *website* atau email kamu mendadak berubah akibat peretasan ini. Contoh, halaman situs bukan yang biasanya, jenis huruf ganti, muncul iklan tidak jelas, bahkan mencuri data yang kamu tidak menyadarinya.

h. Kejahatan *Skimming*

Jenis kejahatan *cyber crime* lain yang harus diwaspadai, yakni *skimming*. *Skimming* adalah kejahatan perbankan dengan cara mencuri data kartu debit atau kartu kredit untuk menarik dana di rekening.

Cara kerjanya membobol informasi pengguna memakai alat yang dipasang pada mesin Anjungan Tunai Mandiri (ATM) atau di mesin gesek EDC. Dengan teknik tersebut, pelaku bisa menggandakan data yang terdapat dalam pita magnetik di kartu kredit maupun debit.

Kemudian memindahkan informasi ke kartu ATM kosong. Akhirnya, pelaku bisa dengan mudah menguras saldo rekening nasabah.

Skimming dapat terjadi ketika kamu sedang transaksi belanja online. Saat kartu

debit atau kartu kredit terhubung pada gawai, risiko terkena skimming menjadi lebih tinggi.

Ponsel atau laptop terkoneksi dengan internet sehingga memudahkan pelaku meretas atau mengambil data kartu kredit atau kartu debit. Terlebih jika menggunakan koneksi *wifi* publik. Jadi, pastikan setiap transaksi *online* pakai jaringan internet pribadi.

i. OTP *Fraud*

Kode OTP ini ibarat kunci. Kunci akhir untuk bisa mengakses atau menyelesaikan transaksi keuangan. Jika kode 6 digit ini sampai diketahui orang lain, bisa berbahaya.

Saat ini, marak kejahatan pencurian kode OTP atau OTP *fraud*. Penyebab OTP fraud adalah *malware* atau semacam virus yang menyerang perangkat lunak.

Penyebab lainnya bisa juga melalui aplikasi, *social engineering* seperti via telepon, SMS, email. Contohnya lewat *call center* palsu.

j. Pemalsuan Data atau *Data Forgery*

Jenis kejahatan *cyber crime* Indonesia berikutnya adalah *data forgery*. Adalah kejahatan dengan memalsukan data atau dokumen penting melalui internet.

Biasanya kejahatan ini menyasar pada dokumen penting milik*e-commerce* atau penyedia situs belanja *online*. Seolah-olah terjadi salah ketik yang merugikan pengguna atau masyarakat.

k. Kejahatan Konten Ilegal

Divisi Hubungan Internasional Polri juga menyebut konten ilegal termasuk dalam jenis kejahatan *cyber crime*. Konten ilegal adalah kejahatan memasukkan data atau informasi yang tidak benar, tidak etis, melanggar hukum atau mengganggu ketertiban umum.

Sebagai contoh, berita bohong atau fitnah, pornografi, maupun informasi yang menyangkut rahasia negara, propaganda untuk melawan pemerintah yang sah.

l. "Teroris" Dunia Maya atau *Cyber Terrorism*

Cyber terrorism adalah kejahatan yang mengganggu, atau membuat kerusakan terhadap suatu data di jaringan komputer. Pelaku menawarkan diri kepada korban

untuk memperbaiki data tersebut yang sudah disabotase dengan bayaran tertentu.

m. Mata-mata atau *Cyber Espionage*

Jenis kejahatan *cyber crime* yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer korban.

Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

n. Menjiplak Situs Orang Lain

Kejahatan melanggar Hak Atas Kekayaan Intelektual (HAKI) orang lain di internet. Misalnya meniru tampilan situs orang lain secara ilegal, menyiarkan informasi yang merupakan rahasia dagang orang lain.

2. Sistem Hukum dan Penanggulangan *Cyber Crime*

A. Sistem Hukum *Cyber Crime* di Indonesia

Sistem hukumIndonesia tidak secara spesifik mengontrol tentang hukum siber, namun beberapa undang-undang telah mengatur pencegahan kejahatansiber, seperti Undang-undang No.36tentang 1999 tentang Telekomunikasi, Undang-undang No.19 Tahun 2002 tentang Hak Cipta, Undang-undang No.15 Tahun 2003 tentang PemberantasanTerorisme, serta Undang-undang No.11Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-Undang dan peraturan tersebut ini telah mengkriminalisasi jenis kejahatan dunia maya (*cybercrime*) dan ancaman hukuman buat setiap pelanggarnya.[7]

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 Pidanaterhadap Informatika dan Telematika, yang mengatur tindak pidana *illegal access, illegal interception, data interferencedan system interference*, penyalahgunaan nama domain, dan pornografi anak.

[7]Thantawi, "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia," Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala2, no. 1 (Februari 2014): 37.

Dalam pembahasan perkembangan hukum pidana yang akan datang,penyelesaian dan pencegahan *cyber crime* harus 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 dalamUndang-undang No. 11Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-undang No.19Tahun 2016 tentang Perubahan atas Undang-undang No 11Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagai berikut :

1. Tindakan yang melanggar kesusilaan

   Pada Pasal 27 ayat (1) Undang-undang No. 11Tahun 2008 disebutkan bahwa"Setiap Orang dengan sengaja dan tanpa hak membagikan atau menyebarkan atau membuat dapat diaksesnya Informasi Elektronik atau Dokumen Elektronik yang memiliki isi yang melanggar kesusilaan". Termasuk pornografi online dan prostitusi online. Salah satu permasalahan yang diakibatkan olehperkembangan teknologi informasi melalui jaringan internet adalah banyaknya situs yang menampilkan adegan porno. Tampaknya saat ini, sangat sulit melindungi Internet dari gangguan pedagang hiburan yang menjual pornografi.[8]

2. Perjudian

   Perjudian online diatur pada Pasal 27 ayat (2) Undang-undang Informasi dan Transaksi Elektronik. Dalam peraturan ini juga sama disebutkan bahwa:"Setiap orang dengan sengaja dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan perjudian".

3. Penghinaan atau pencemaran nama baik

   Pencemaran nama baik ataupun penghinaan di dunia maya merupakan larangan yang diatur pada Pasal 27 ayat (3) Undang-undang No. 11Tahun 2008,yang berbunyi

[8]Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime)(Bandung: Refika Aditama, 2005), 146.

: “Setiap Orang dengan sengaja, dan tanpa hak membagikan/menyebarkan/membuat dapat diaksesnya informasi elektronik/dokumen elektronik yang mempunyai muatan penghinaan atau pencemaran nama baik.” Pembuat undang-undang menyamakan antara penghinaan dan pencemaran. Penghinaan sendiri ialah sebuah perbuatan, sedangkan salah satu bentuk penghinaan ialah pencemaran.[9]

4. Pemerasan atau pengancaman

Pada Pasal 27 ayat (4) Undang-undang No. 11 Tahun 2008 melarang pemerasan atau pengancaman di dunia maya. Dalam pasal tersebut dijelaskan: “Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman”.

5. Penguntitan (*Cyber Stalking*)

Undang-undang No. 11 Tahun 2008 Pasal 29 mengaturbahwa: “Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi”.Ketentuan mengenai informasidan transaksi elektronik dalam Pasal 29 mengatur mengenai tindakan pelecehan, ancaman, atau tindakan lain yang dilakukan untuk menimbulkan ketakutan, termasuk kata-kata atau tindakan tertentu.[10]

6. Penyebaran berita bohong (*Hoax*)

Penyebaran berita palsu diatur dalam Undang-undang No. 11/2008 Pasal 28 ayat (1), berbunyi : “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong/palsu serta menyesatkan, yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.”

7. Ujaran Kebencian

Pasal 28 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tentangpidana tersebut, yang berbunyi: “Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang dirancang untuk

[9]Adami Chazawi, Hukum Pidana Positif Penghinaan, Edisi Revisi (Malang: Media Nusa Creative, 2013), 81.
[10]Sigid Suseno, Yurisdiksi Tindak Pidana Siber(Bandung: Refika Aditama, 2012), 177–78.

menimbulkan kebencian atau permusuhan individu/kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA)".

8. Akses ilegal

   Undang-undang No. 11Tahun 2008, dalam Pasal 30mengatur sebagai berikut:

   a. Siapapun yang dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik orang lain dengan cara apapun.
   b. Siapapun dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses (membuka) Komputer atau Sistem Elektronik dengan cara apapun dengan maksud untuk memperoleh Informasi Elektronik atau Dokumen Elektronik.
   c. Siapapun yang melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dengan sengaja, tanpa hak atau melawan hukum (ilegal) mengakses Komputer atau Sistem Elektronik."

B. Penanggulangan *Cyber Crime* di Indonesia

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:[11]

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*)

[11]Dista Amalia Arifah, "Kasus Cybercrime di Indonesia," Jurnal Bisnis dan Ekonomi (JBE)18, no. 2 (September 2011): 189.

6. *Firewall*
7. AntiVirus

Adapun beberapa langkah yang harus diambil dalam menanggapi *Cyber crime*, sebagai berikut :

1. Melakukan pembaruan hukum pidana nasional dan hukum acara, sesuai dengan kesepakatan internasional yang terkait dengan kejahatan tersebut.
2. Meningkatkan sistem keamanan jaringan komputer nasional sesuai dengan standar internasional.
3. Meningkatkan pengetahuandan keahlian aparat penegak hukum dalam upaya pencegahan, investigasi, dan penuntutan kasus-kasus yang berkaitan dengan *cyber crime*.
4. Meningkatkan kesadaran warga negara tentang masalah *cyber crime*dan pentingnya mencegah kejahatan itu terjadi.
5. Meningkatkan kerjasama dari berbagai negara, baik kerja sama bilateral, regional maupun multilateral dalam upaya mengatasi *cyber crime*, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik (*mutual assistance treaties*).

Adapun beberapa contoh dari bentuk penanggulangan yang lain yaitu :

1. IDCERT (Indonesia *Computer Emergency Response Team*)

   Salah satu cara untuk membuat masalah keamanan lebih mudah ditangani adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Dengan munculnya "*sendmail worm*" (sekitar tahun 1988), masalah keamanan semacam ini mulai dikenali di luar negeri, ketika worm menutup sistem email Internet era itu. Selepasnya dibentuk sebuah (CERT) *Computer Emergency Response Team*, sejak itu di negara lain juga mulai membentuk CERT untuk dijadikan *point of contact*guna orang untuk mengadukan problem kemanan. IDCERT merupakan CERT Indonesia.[12]
2. Sertifikasi perangkat *security*

[12]Ibid. Hlm 190

Peralatan yang dipakai guna membereskan keamanan harus memiliki tingkat karakteristik. Tentunya peralatan yang digunakan untuk tujuan pribadi berbeda dengan yang digunakan untuk tujuan militer. Tetapi sejauh ini di Indonesia belum ada institusi yang menangani problem evaluasi perangkat keamanan.

Negara Indonesia telah membuat kebijakan yang berhubungan dengan hukum teknologi informasi (*law of information technology*) setelah diundangkannya Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada tanggal 21 April 2008. Produk hukum yang berkaitan dengan ruang siber (*cyber space*) atau mayantara ini dianggap oleh pemerintah perlu untuk memberikan keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Landasan filosofi lahirnya Undang-Undang pemanfaatan informasi teknologi informasi, adalah untuk mensiasati dan mengantisipasi globalisasi yang sekarang sedang bergulir kencang. Era globalisasi adalah era dimana pemanfaatan teknologi informasi,internet sudah melekat bahkan menjadi gaya hidup masyarakat global. Dalam aspek hukum, era globalisasi dengan *icon* pemanfaatan teknologi informasi di segala bidang telah melahirkan tingkah laku baru yang sebelumnya sama sekali tidak terantisipasi baik yang bersifat positif maupun negatif. Proses pemanfaatan teknologi agar tetap bisa terus berlangsung sesuai dengan koridor yang berlaku, maka diperlukan perangkat hukum untuk memagari perilaku yang mungkin timbul sebagai akibat pemanfaatan teknologi informasi secara salah.

Kritik masyarakat baik dari akademisi, aparat penegak hukum, para *bloggers* terutama *hackers* pada saat disahkannya UU ITE adalah hal yang wajar di era demokratisasi seperti saat ini. Karena dalam merumuskan peraturan hukum dewasa ini harus mempertimbangkan secara komprehensif beragam dimensi persoalan. Di sini orang akan mempersoalkan hak-hak warga seperti kebebasan berekspresi, kebebasan media, dan masalah-masalah HAM seperti : persoalan privasi, hak untuk memperoleh informasi, dan sebagainya yang saat ini sangat diperhatikan dalam legislasi positif nasional. Di sinilah relevansi persoalan hak dan kewajiban menjadi penting.

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah ʻpolitik kriminalʻ menurut Sudarto politik kriminal merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan. Oleh karena itu tujuan pembuatan UU ITE tidak terlepas dari tujuan politik kriminal, yaitu sebagai upaya untuk kesejahteraan sosial (*social welfare*) dan untuk perlindungan masyarakat (*social defence*).

Evaluasi terhadap kebijakan di dunia mayatetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief, evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legislative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal policy*). Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegakan hukum pidana dan kebijakan penanggulangan kejahatan.

Kegiatan pemanfaatan teknologi informasi perlu terus dikembangkan tanpa mengesampingkan persatuan dan kesatuan nasional dan penegakan hukum secara adil, sehingga pelanggaran-pelanggaran yang berkaitan dengan pemanfaatan teknologi informasi dapat dihindari melalui penerapan keseragaman asas dan peraturan perundang undangan.

D. PENUTUP (*Times New Roman* 12, *bold*, Kapital)

Cyber crime atau kejahatan siber merupakan tindakan ilegal dengan menggunakan pengetahuan teknologi komputer untuk melakukan tindak kejahatan. Pencurian perangkat keras dan perangkat lunak, manipulasi data, pengaksesan sistem komputer secara ilegal dengan telepon, dan mengubah program. Adapun, jenis *cyber crime* yang kerap kali ditemui ketika beraktivitas di dunia maya diantaranya, yaitu: akses *illegal*, *phising*, penipuan otp, kejahatan konten *illegal*, dan *cyber terrorism*. *Cyber crime* Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU *cyber crime* secara khusus. Kebijakan kriminalisasi yang tertulis dalam golongan *cybercrime* 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 Pidanaterhadap Informatika dan Telematika, yang mengatur tindak pidana *illegal access*, *illegal interception*, data *interferencedan system interference*, penyalahgunaan nama domain, dan pornografi anak. 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. Menurut Barda Nawawi Arief, evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legislative policy*) dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal policy*).

DAFTAR PUSTAKA

Dista Amalia Arifah, "Kasus Cybercrime di Indonesia," Jurnal Bisnis dan Ekonomi (JBE)18, no. 2 (September 2011): 189. Di unduh dari https://media.neliti.com/media/publications/24189-ID-kasus-cybercrime-di-indonesia.pdf

Thantawi, "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia," Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala2, no. 1 (Februari 2014): 37. Di unduh darihttps://jurnal.unsyiah.ac.id/MIH/article/view/4574.

Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime) (Bandung: Refika Aditama, 2005), 146.

Adami Chazawi, Hukum Pidana Positif Penghinaan, Edisi Revisi (Malang: Media Nusa Creative, 2013), 81.

Johanes Supranto, Metode Penelitian Hukum dan Statistik. (Rineka Cipta: Jakarta. 2003), hlm. 13.

Khudzaifah Dimiyati dan Kelik Wardiono, 2004, Metode Penelitian Hukum, Surakarta: Fakultas Hukum UMS, hal 1.

Peter Mahmud Marzuki, Penelitian Hukum, Cet. 6, (Jakarta: Kencana Prenada Media

Group, 2005), hlm. 3.

Sigid Suseno, Yurisdiksi Tindak Pidana Siber(Bandung: Refika Aditama, 2012), 177–78.

Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat, (Jakarta:PT Raja Grafindo Persada, 2001), hlm. 13.

Undang – Undang Dasar Negara Republik Indonesia Tahun 1945 Pasal 1 ayat (3)

Cermati.com : "14 Jenis Cyber Crime, Kejahatan Internet yang Merugikan", November 21, 2022, https://www.cermati.com/artikel/jenis-cyber-crime.