HUKUM CYBER

Tim Penulis:
Juanrico Alfaromona Sumarezs Titahelu, Kasmanto Rinaldi, Ika Atikah,
La Ode Ali Mustafa, Margie Gladies Sopacua, Nanda Dwi Rizkia, Judy Marria Saimima,
Yanti Amelia Lewerissa, Fahririn, Betsy A Kapugu, Irwanto, Stefanus Don Rade,
Deasy Soeikromo, Henny Saida Flora.

www.penerbitwidina.com

HUKUM CYBER

Tim Penulis:
Juanrico Alfaromona Sumarezs Titahelu, Kasmanto Rinaldi, Ika Atikah,
La Ode Ali Mustafa, Margie Gladies Sopacua, Nanda Dwi Rizkia, Judy Marria Saimima,
Yanti Amelia Lewerissa, Fahririn, Betsy A Kapugu, Irwanto, Stefanus Don Rade,
Deasy Soeikromo, Henny Saida Flora.

Penerbit Widina

HUKUM *CYBER*

Tim Penulis:
Juanrico Alfaromona Sumarezs Titahelu, Kasmanto Rinaldi, Ika Atikah,
La Ode Ali Mustafa, Margie Gladies Sopacua, Nanda Dwi Rizkia, Judy Marria Saimima,
Yanti Amelia Lewerissa, Fahririn, Betsy A Kapugu, Irwanto, Stefanus Don Rade,
Deasy Soeikromo, Henny Saida Flora.

Desain Cover:
Septian Maulana

Sumber Ilustrasi:
www.freepik.com

Tata Letak:
Handarini Rohana

Editor:
N. Rismawati

ISBN:
978-623-459-725-7

Cetakan Pertama:
Oktober, 2023

PENERBIT:
WIDINA MEDIA UTAMA
Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 360/JBA/2020
Website: www.penerbitwidina.com
Instagram: @penerbitwidina
Telepon (022) 87355370

PRAKATA

Rasa syukur yang teramat dalam dan tiada kata lain yang patut kami ucapkan selain mengucap rasa syukur. Karena berkat rahmat dan karunia Tuhan Yang Maha Esa, buku yang berjudul Hukum *Cyber* telah selesai di susun dan berhasil diterbitkan, semoga buku ini dapat memberikan sumbangsih keilmuan dan penambah wawasan bagi siapa saja yang memiliki minat terhadap pembahasan Hukum *Cyber*.

Buku ini merupakan salah satu wujud perhatian penulis terhadap Hukum *Cyber*. Setiap negara yang memfasilitasi kehidupan bernegara dengan penggunaan sistem elektronik dan internet yang maju, secara tidak langsung perkembangan *cyber law* di dalamnya turut maju. Hukum Siber atau *Cyber law* erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya. *Cyber Law* ini merupakan istilah yang berasal dari *cyberspace law*.

Istilah hukum diartikan sebagai padanan dari kata *cyber law*, yang saat ini secara *international* digunakan untuk istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain yang juga digunakan adalah Hukum TI (*Law of Information Teknologi*), Hukum dunia maya (*Virtual Word Law*), dan Hukum Mayantara.

Kegiatan siber/*cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan siber/*cyber* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Sehingga Hukum Siber/*Cyber law* bukan saja keharusan, melainkan sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu dengan banyaknya berlangsung kegiatan *cyber crime*.

Akan tetapi pada akhirnya kami mengakui bahwa tulisan ini terdapat beberapa kekurangan dan jauh dari kata sempurna, sebagaimana pepatah menyebutkan “tiada gading yang tidak retak” dan sejatinya kesempurnaan hanyalah milik Tuhan semata. Maka dari itu, kami dengan senang hati secara terbuka untuk menerima berbagai kritik dan saran dari para pembaca sekalian, hal tersebut tentu sangat diperlukan sebagai bagian dari upaya kami untuk terus melakukan perbaikan dan penyempurnaan karya selanjutnya di masa yang akan datang.

Terakhir, ucapan terima kasih kami sampaikan kepada seluruh pihak yang telah mendukung dan turut andil dalam seluruh rangkaian proses penyusunan dan penerbitan buku ini, sehingga buku ini bisa hadir di hadapan sidang pembaca. Semoga buku ini bermanfaat bagi semua pihak dan dapat memberikan kontribusi bagi pembangunan ilmu pengetahuan di Indonesia.

Oktober, 2023

Tim Penulis

DAFTAR ISI

HUKUM *CYBER*

BAB 1: PENGERTIAN DAN SEJARAH PERKEMBANGAN

Dr. Juanrico Alfaromona Sumarezs Titahelu, S.H., M.H

Fakultas Hukum Universitas Pattimura

BAB 1

PENGERTIAN DAN SEJARAH PERKEMBANGAN

A. PENDAHULUAN

Setiap negara yang memfasilitasi kehidupan bernegara dengan penggunaan sistem elektronik dan internet yang maju, secara tidak langsung perkembangan *cyber law* di dalamnya turut maju.

Hukum Siber atau *Cyber law* erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya. *Cyber Law* ini merupakan istilah yang berasal dari *cyberspace law*.

Istilah hukum diartikan sebagai padanan dari kata *cyber law*, yang saat ini secara *international* digunakan untuk istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain yang juga digunakan adalah Hukum TI (*Law of Information Teknologi*), Hukum dunia maya (*Virtual Word Law*), dan Hukum Mayantara.

Secara Akademik, Terminologi "*cyber law*" belum menjadi teknologi yang umum. Terminologi lain untuk tujuan yang sama seperti *The Law of Internet, Law and The Information Superhighway, Information Technologi Law, The Law of Information*, dan lain-lain.

Ruang lingkup hukum siber/*cyber law* dalam beberapa hal diantaranya:

1. *Copyright* (hak cipta)
2. *Trademark* (hak merek)
3. *Defamation* (pencemaran nama baik)
4. *Hate Speech* (penistaan, penghinaan, fitnah)
5. *Hacking, Viruses*, *Illegal Access*, (penyerangan terhadap komputer lain)
6. *Regulation Internet Resource* (pengaturan sumber daya internet)
7. *Privacy* (kenyamanan pribadi)
8. *Duty Care* (kehati-hatian)
9. *Criminal Liability* (kejahatan menggunakan IT)
10. *Procedural Issues* (yurisdiksi, pembuktian, penyelidikan, dll.)
11. *Electronic Contract* (transaksi elektronik),
12. Pornografi
13. *Robbery* (pencurian lewat internet)
14. *Consumer Protection* (perlindungan konsumen)
15. *E-Commerce*, *E-Government* (pemanfaatan internet dalam keseharian).

Karena erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana maka hukum siber/*cyber law* menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan elektronik yang termasuk juga di dalamnya kejahatan pencucian uang dan kejahatan terorisme.

Kegiatan siber/*cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan siber/*cyber* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Sehingga Hukum Siber/*Cyber law* bukan saja keharusan, melainkan sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu dengan banyaknya berlangsung kegiatan *cyber crime*.

B. DEFINISI HUKUM SIBER/*CYBER LAW*

Sebelum membahas lebih jauh mengenai Hukum Siber, maka perlu kita ketahui dahulu apa yang dimaksud dengan Hukum. Pengertian hukum ini sendiri dapat kita temukan dalam berbagai literatur hukum. Disini penulis akan memberikan beberapa pengertian hukum yang berasal dari pendapat para ahli yang terkenal dan juga para ahli yang ada di Indonesia yaitu:

a. C.S.T Kansil menyatakan bahwa hukum itu ialah peraturan-peraturan yang bersifat memaksa, yang menentukan tingkah laku manusia dalam lingkungan masyarakat yang dibuat oleh badan-badan resmi yang berwajib, pelanggaran mana terhadap peraturan-peraturan tadi berakibat diambilnya tindakan, yaitu dengan hukuman tertentu. (Kansil, 1982)
b. E.M. Meyers dalam bukunya "*De Algemene begrippen van het Burgerlijk Recht",* yang artinya hukum ialah semua aturan yang mengandung pertimbangan kesusilaan, ditujukan kepada tingkah laku manusia dalam masyarakat dan yang menjadi pedoman bagi penguasa-penguasa negara dalam melakukan tugasnya. Sedangkan menurut Immanuel Kant, "hukum ialah keseluruhan syarat-syarat yang dengan ini kehendak bebas dari orang yang satu dapat menyesuaikan diri dengan kehendak bebas dari orang yang lain menuruti peraturan hukum tentang kemerdekaan". (Titahelu, 2021a)
c. Hukum adalah alat atau sarana untuk mengatur & menjaga ketertiban guna mencapai suatu masyarakat yang berkeadilan dalam menyelenggarakan kesejahteraan sosial yang berupa peraturan-

> peraturan yang bersifat memaksa & memberikan sanksi bagi yang melanggarnya, baik itu untuk mengatur masyarakat maupun aparat pemerintah sebagai penguasa. (Titahelu, 2021:151)

Kata “hukum” itu sendiri untuk sebagian besar orang merupakan hal yang sangat dihindari atau bahkan ditakuti karena keakrabannya dengan kata sanksi dan penjara. Semua orang secara alami, takut untuk terkena konsekuensi yang akan didapat dari melanggar hukum tersebut. Olehnya bagi orang awam, eksistensi hukum itu sendiri telah memberikan mereka batasan dalam berperilaku dan berbuat dalam lingkungan bermasyarakat. (Titahelu, 2022:43)

Pengertian siber *(cyber)* adalah sesuatu yang berhubungan dengan sistem komputer dan informasi. Dalam perkembangannya, siber dapat diartikan yang berhubungan dengan internet.

Kehadiran hukum *cyber* di Indonesia sudah diinisiasi sebelum 1999. Di masa itu, hukum siber adalah perangkat hukum yang menjadi dasar dan peraturan yang menyinggung transaksi elektronik. Pendekatan dengan perangkat hukum ini dimaksudkan agar ada pijakan yang dapat digunakan oleh undang-undang dan peraturan lainnya. Banyaknya berbagai kejahatan dan pelanggaran hukum dalam pemanfaatan teknologi maka dibuat sebuah undang-undang sebagai dasar hukum atas segala kejahatan dan pelanggaran yang terjadi. (Wahyuni, 2022)

Dunia *cyber* atau dalam istilah Indonesia dikenal dengan dunia maya (atau disebut juga ruang siber atau mayantara; bahasa Inggris: *cyberspace*) merupakan sebuah media elektronik dalam jaringan komputer yang banyak dipakai untuk keperluan komunikasi satu arah maupun timbal-balik secara *online* (terhubung langsung).

Dunia maya ini merupakan gabungan dari berbagai peralatan teknologi komunikasi dan jaringan komputer yang dapat menghubungkan peralatan komunikasi (komputer, telepon genggam, instrumentasi elektronik, dan lain-lain) yang tersebar di seluruh penjuru dunia secara interaktif.

Kata "*cyberspace*" (dari *cybernetics* dan *space*) berasal dan pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, William Gibson dalam buku ceritanya, "*Burning Chrome*", 1982 dan menjadi populer pada novel

berikutnya, Neuromancer, 1984 yang menyebutkan bahwa: *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*.

Dalam buku yang berjudul *Investigating Computer-Related Crime*, Peter Sthepenson menjelaskan bahwa *Cybercrime* yaitu sebuah kejahatan yang ditujukan pada sebuah komputer atau *system computer*. Peter menambahkan bahwa sifat kejahatan *cyber* sangat kompleks, dari hal sederhana seperti penyadapan atau pengintaian ke dalam sistem komputer yang mana kita tidak memiliki otorisasi terhadap komputer tersebut, atau kejahatan berupa penyebaran virus yang dilakukan oleh seorang karyawan yang merasa tidak puas terhadap kebijakan dalam organisasinya. (Sthepenson & Keith, 2013)

Sedangkan Sussan Brenner menjelaskan *cybercrimes* dalam tiga kategori, yakni:

1. Kejahatan dimana komputer menjadi sasaran atau target kriminal.
2. Kejahatan dimana komputer merupakan alat yang digunakan untuk melakukan kejahatan.
3. Kejahatan di mana penggunaan komputer merupakan aspek insidental dari perbuatan kejahatan tersebut. (Brenner, 2001)

Menurut instrumen PBB dalam *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders* yang diselenggarakan di Vienna, 10-17 April 2000, kategori *cyber crime* dapat dilihat secara sempit maupun secara luas, yaitu:

1. Kejahatan dunia maya dalam arti sempit ("kejahatan komputer"): setiap perilaku ilegal yang diarahkan melalui operasi elektronik yang menargetkan keamanan sistem komputer dan data yang diproses olehnya;
2. Kejahatan dunia maya dalam arti yang lebih luas ("kejahatan terkait komputer") adalah setiap perilaku ilegal yang dilakukan melalui, atau terkait dengan, sistem atau jaringan komputer, termasuk kejahatan

seperti kepemilikan ilegal, menawarkan atau mendistribusikan informasi melalui komputer sistem atau jaringan.

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) pada saat ini sudah memasuki semua aspek kehidupan masyarakat di dunia. Pemanfaatan TIK tersebut mendorong terbentuknya satu komunitas yang terhubung secara elektronik dalam satu ruang yang sering disebut ruang siber (*cyber space*). Sistem elektronik termasuk jaringan internet pada saat ini dimanfaatkan untuk mendukung berbagai kegiatan di sektor usaha, perdagangan, layanan kesehatan, komunikasi dan kepemerintahan, serta sektor pertahanan.

Semakin meluasnya dan meningkatnya pemanfaatan TIK khususnya melalui jaringan internet diiringi pula dengan meningkatnya aktivitas ancaman. Ancaman itu antara lain upaya membobol kerahasiaan informasi, merusak sistem elektronik dan berbagai perbuatan melawan hukum lainnya. Dengan memperhatikan hal di atas, ruang siber perlu mendapatkan perlindungan yang layak guna menghindari potensi yang dapat merugikan pribadi, organisasi bahkan negara. Istilah pertahanan siber muncul sebagai upaya untuk melindungi diri dari ancaman dan gangguan tersebut.

Pertahanan siber bertingkat dari lingkup perorangan, kelompok kerja, organisasi sampai dengan skala nasional. Perhatian yang khusus diberikan pada sektor yang mengelola infrastruktur kritis seperti pertahanan keamanan, energi, transportasi, sistem keuangan, dan berbagai layanan publik lainnya. Gangguan pada sistem elektronik pada sektor-sektor ini bisa menyebabkan kerugian ekonomi, turunnya tingkat kepercayaan kepada pemerintah, terganggunya ketertiban umum dan lain-lain. Risiko ini yang menjadi pertimbangan diperlukannya pertahanan siber yang kuat dalam satu negara. (Indonesia, 2014)

Hukum Siber/*Cyber Law* sendiri diperlukan untuk menanggulangi kejahatan siber. Hukum Siber sendiri sangat berkaitan dengan upaya pencegahan tindak pidana, ataupun penanganannya. Hukum Siber akan menjadi dasar hukum untuk proses penegakan hukum dalam sarana elektronik dan *computer*. Dengan kata lain, hukum siber sangat dibutuhkan karena menurut pihak yang pro terhadap hukum siber, sudah

saatnya Indonesia memiliki aturan/hukum yang mengaturnya, mengingat hukum-hukum konvensional tidak mampu mengantisipasi perkembangan dunia maya yang pesat.

Adapun aturan yang telah dibentuk oleh pemerintah yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

C. ISTILAH SIBER

Berikut ini beberapa istilah yang menggunakan kata siber (*cyber*):

a. *Cyberspace* (Ruang siber) adalah ruang dimana komunitas saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari-hari;
b. *Cyberphobia* adalah ketakutan terhadap komputer yang tidak rasional;
c. *Cyberpunk* adalah genre fiksi ilmiah yang sangat mengandalkan ide-ide ilmu komputer;
d. *Cyber University* (kampus siber) kampus atau perguruan tinggi yang dikembangkan dengan berbasis teknologi dan informasi;
e. *National cyber security* (Keamanan Siber Nasional) adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor;
f. *Cyber defense* (Pertahanan siber) adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara;
g. *Cyber Attack (*Serangan siber) adalah serangan untuk mengganggu, menonaktifkan, menghancurkan, atau mengendalikan lingkungan komputasi atau untuk mengakses informasi yang dikendalikan;
h. *Cyber crime* (Kejahatan siber) adalah kejahatan yang dilakukan dengan menggunakan teknologi informasi atau yang menargetkan teknologi informasi;
i. *Cyber Law* (hukum siber) yaitu hukum yang menyangkut teknologi informasi, termasuk komputasi dan internet;
j. *CDC Cyber* berbagai komputer *mainframe*;

k. *Cyberbullying* adalah Penindasan di dunia maya, intimidasi, atau pelecehan menggunakan cara elektronik;
l. *Cybercafé* adalah bisnis yang menyediakan akses internet;
m. *Cyberculture,* budaya yang muncul berdasarkan penggunaan jaringan komputer;
n. *Cyberstalking* merupakan penggunaan Internet atau sarana elektronik lainnya untuk membuntuti atau melecehkan individu, kelompok, atau organisasi;
o. *Cyber Party* adalah partai politik yang diciptakan oleh John McAfee untuk Pemilihan Presiden AS 2016.

D. ASAS-ASAS HUKUM SIBER/*CYBER LAW*

Hukum siber juga memiliki asas dalam penentuan berlakunya hukum. Asas-asas tersebut sangat penting dikarenakan keberadaan aturan yang bersifat nasional dan berlakunya dalam wilayah hukum negara yang membuat aturan tersebut. Tetapi tidak menutup kemungkinan diperlukan asas-asas lain yang bisa memberlakukan aturan tersebut diluar wilayah suatu negara.

Adapun asas-asas umum yang berada dalam hukum siber yaitu:

1. *Subjective territoriality*, hal ini menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan yang dilakukan dan penyelesaian tindak pidana dilakukan di negara lain.
2. *Objective territoriality*, menyatakan bahwa hukum yang berlaku adalah hukum akibat sebuah perbuatan terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
3. *Nationality*, menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
4. *Passive nationality*, menekankan yurisdiksi berdasarkan kewarganegaraan korban.
5. *Protective principle*, menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya yang umumnya digunakan jika korban adalah negara atau pemerintah.

6. *Universality*, asas ini memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus *cyber*. Asas ini menentukan bahwa setiap negara berhak menangkap dan menghukum para pelaku pembajakan, lalu kemudian asas ini diperluas hingga mencakup kejahatan terhadap kemanusiaan dan terus dikembangkan untuk kejahatan sangat serius berdasarkan perkembangan hukum internasional.

E. METODE ANCAMAN SIBER DAN JENIS KEAMANANNYA

Ancaman siber juga sangat penting untuk diketahui, khususnya bagi kita yang awam atau tidak terlalu memahami secara detail bentuk-bentuk ancaman siber. Apalagi penggunaan komputer, laptop bahkan *smart phone* dengan berbagai jenis serta didukung dengan fasilitas internet yang semakin mumpuni mewajibkan kita sebagai pengguna untuk lebih berhati-hati.

Berikut dibawah ini metode ancaman siber yang dapat menyerang perangkat elektronik yang perlu kita ketahui bersama yaitu:

1. *Malware*;
   Malware adalah singkatan dari *malicious software* merupakan salah satu ancaman siber yang paling umum. Perangkat lunak ini diciptakan untuk mengganggu bahkan merusak komputer. Ancaman ini kerap menyebar melalui lampiran email atau unduhan yang terlihat ilegal. Beberapa jenis *malware* adalah virus, *trojans*, *spyware*, *ransomware*, *adware*, dan *botnet*.
2. Injeksi SQL (*Structured Query Language*):
   Jenis metode ancaman selanjutnya adalah injeksi SQL yang digunakan untuk mengambil kendali serta mencuri data dari pusat data. Kerentanan ini dimanfaatkan oleh penjahat siber dengan memasukkan kode berbahaya pada aplikasi berbasis data melalui pertanyaan SQL. Hal ini dilakukan untuk mencuri informasi pribadi pengguna.
3. *Phishing*
   Umumnya, metode ancaman *phising* dikirimkan dalam bentuk email resmi perusahaan, tetapi mengandung permintaan terkait informasi sensitif. Ancaman ini digunakan dalam penipuan guna mendapatkan data dan informasi pribadi.

4. Serangan *Man-in-the-Middle*
   Serangan *Man-in-the-Middle* adalah jenis metode ancaman dalam bentuk penyadapan komunikasi antara dua individu untuk mencuri data. Salah satu contoh ancaman *Man-in-the-Middle* adalah penggunaan jaringan wi-fi yang tidak aman sehingga memungkinkan penjahat siber menghalangi data yang dikirimkan dari perangkat menuju jaringan korban.
5. Serangan *Denial-of-Service*
   Jenis metode ancaman yang terakhir adalah serangan *Denial-of-Service*, yakni serangan terhadap jaring internet dengan menghabiskan *resource* yang dimiliki suatu sistem sehingga fungsinya tidak dapat bekerja dengan benar. Tidak hanya itu, serangan *Denial-of-Service* secara tidak langsung juga menghambat pengguna lain dalam mengakses layanan sistem yang diserang tersebut.

Setelah kita mengetahui ancaman siber diatas maka kita juga perlu mempelajari cara mengamankan perangkat elektronik kita. Adapun jenis keamanannya yaitu:

1. *Could Security*;
   Jenis keamanan siber satu ini mengacu pada upaya untuk melindungi data yang tersimpan di *cloud*. Beberapa hal yang dilibatkan dalam perlindungan ini adalah teknologi, kebijakan kontrol, dan layanan yang mendukung keamanan *cloud*. *Cloud security* adalah salah satu aspek penting dalam memastikan keamanan data. Beberapa ancaman bagi *cloud security* di antaranya pencurian data, penyalahgunaan data, dan pembajakan lalu lintas layanan.
2. *Network Security*;
   Network security atau keamanan jaringan merupakan upaya perlindungan jaringan internal dengan meningkatkan keamanan jaringan. *Network security* sangat penting bagi perusahaan yang menggunakan sistem jaringan untuk setiap aktivitasnya. Tindakan perlindungan ini dapat melindungi aset perusahaan dari ancaman *cyber crime* dan juga dapat mengelola lalu lintas jaringan agar lebih efisien. Salah satu contoh *network security* adalah penggunaan

antivirus dan *firewall* guna mendeteksi ancaman yang berasal *malware*.

3. *Application Security*;
   Application security adalah jenis keamanan siber yang digunakan untuk meningkatkan keamanan aplikasi dari berbagai ancaman. Aplikasi dapat diakses dari berbagai jaringan yang memungkinkan adanya serangan siber. Hal ini menjadikan aplikasi rentan terhadap ancaman siber sehingga perlu menerapkan *application security*.

Beberapa cara yang dapat memastikan bahwa proses keamanan bekerja dengan baik adalah prosedur autentikasi, otorisasi, enkripsi, *logging*, dan uji keamanan aplikasi.

F. SEJARAH PERKEMBANGAN SIBER

Perkembangan teknologi tentu berimplikasi terhadap berbagai aspek kehidupan manusia, hal ini tidak dapat dielakkan lagi. Dilihat dari segi positifnya, dapat memudahkan berbagai pelaksanaan pekerjaan. Namun di sisi lain pemanfaatannya juga berbanding lurus dengan ancaman terhadap keamanan. Hal itu dapat dilihat dari ribuan kasus kejahatan siber yang terjadi di Indonesia. Demikian pula dengan negara-negara lain di dunia menghadapi ancaman yang sama.

Tahun 2010 disepakati apa yang disebut *Salvador Declaration*. Salah satu elemen utama dari deklarasi ini adalah memberikan mandat kepada UNODC, khususnya kepada organnya *Commission on Crime Prevention and Criminal Justice*, untuk membahas isu kejahatan siber dengan membentuk suatu *open-ended intergovernmental expert group on cybercrime*.

Memang kejahatan siber kala itu baru diatur dalam *Budapest Convention* yang merupakan konvensi hasil susunan negara-negara Eropa yang tergabung dalam *Council of Europe*. Sehingga, dunia internasional terbagi dalam 2 pandangan berbeda terkait instrumen hukum untuk menangani kejahatan siber. Antara pihak yang merasa cukup dengan pengaturan *Budapest Convention*. Di pihak lain terdapat kalangan negara yang berpandangan bahwa diperlukan instrumen hukum yang inklusif dan transparan dapat menampung seluruh kepentingan negara.

Oleh karenanya, kini telah terbentuk *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* dengan Indonesia diantaranya sebagai *Rapporteur*. *Rapporteur* itu tugasnya kalau di PBB bukan notulensi, kalau notulensi hanya mencatat saja. Tapi *Rapporteur* itu yang mengesahkan hasil perdebatan.

Indonesia secara aktif terlibat dalam berkontribusi, baik secara tertulis mengenai cakupan, struktur dan objektivitas maupun melalui diskusi bilateral intensif dengan sejumlah negara. Lebih lanjut perihal cakupan, isu terkait yang diusulkan yakni tentang kedaulatan, perlindungan hak asasi manusia, bantuan dan perlindungan bagi korban dan berbasis gender, *crime* oleh badan hukum (*legal persona*), langkah konkret tangani hasil pelanggaran termasuk pemulihan aset, dan pencegahan.

Kemajuan teknologi informasi telah mendorong sistem komputasi dan informasi atau siber meningkat pesat. Kemajuan siber ini telah melahirkan kemudahan di berbagai sektor kehidupan, seperti pada sektor finansial, transportasi, wisata dan lainnya. Namun, kemajuan ini telah membawa dampak baru apa yang disebut dengan kerentanan siber atau bahkan serangan siber.

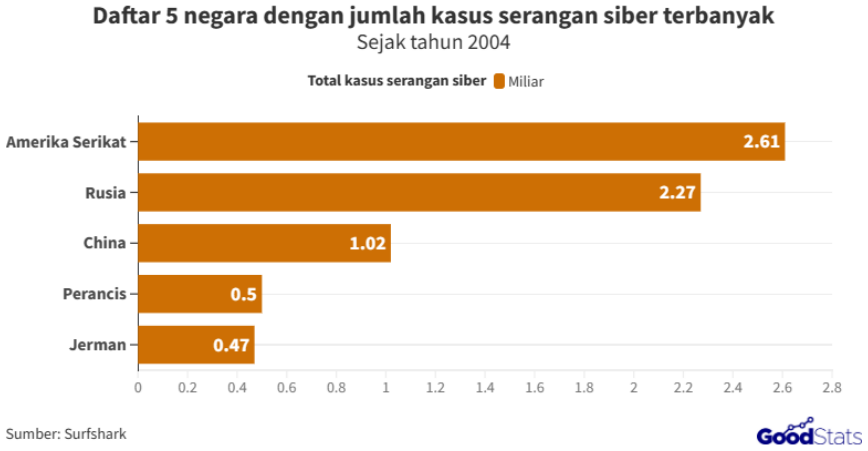
Dunia maya atau ruang siber dianggap sebagai dimensi terpenting setelah darat, laut, udara, dan ruang angkasa. Minat terhadap keamanan siber telah meningkat selama beberapa tahun terakhir untuk tujuan defensif dan ofensif, terlebih karena peningkatan jumlah serangan siber yang terjadi secara global.

Di antara tren keamanan siber untuk tahun 2030 yang disorot oleh Forum Ekonomi Dunia (WEF), kekhawatiran seputar penyalahgunaan kemampuan AI (*artificial intelligence*) dalam serangan di dunia maya meliputi *malware*, *ransomware*, rekayasa sosial (*social engineering*), dan propaganda.

Berdasarkan laporan *Grand View Research*, pasar keamanan siber global bernilai US$203 miliar di tahun 2022, dan diproyeksikan tumbuh sebesar 12,3% selama periode 2023-2030. Adapun, nilainya diprediksi mencapai US$500 miliar pada tahun 2030 mendatang.

Sedangkan, biaya rata-rata operasional yang dikeluarkan oleh perusahaan secara global karena kasus pembobolan data mencapai US$4,35 juta pada tahun 2021 menurut laporan dari International Business Machines Corporation. Jumlah kasus serangan siber juga tercatat telah meningkat sebesar 13%.

Daftar 5 negara dengan jumlah kasus serangan siber terbanyak di dunia



Melansir laman perusahaan keamanan siber Surfshark, Amerika Serikat (AS) menjadi negara dengan jumlah kasus serangan siber terbanyak di dunia sejak tahun 2004. Negeri Paman Sam tersebut dilaporkan memiliki jumlah serangan siber mencapai lebih dari dua miliar kasus.

Sementara, Indonesia menempati urutan ke-13 dalam daftar dengan jumlah serangan mencapai 142 juta kasus sejak tahun 2004. Selain itu, akun yang mengalami kebocoran data pada kuartal II/2022 naik sebesar 2% (*quarter to quarter*/qtq) secara global menjadi 459 akun dibobol per menitnya, dibanding kuartal sebelumnya sebanyak 450 akun per menit.

Seiring perkembangan teknologi informasi dan komunikasi, keamanan siber di Indonesia mengalami perubahan dan peningkatan yang signifikan. Cikal bakal perkembangan siber di Indonesia tak terlepas dari peristiwa di

awal kemerdekaan RI, pada tanggal 4 April 1946. Menteri Pertahanan saat itu, Mr. Amir Sjarifuddin memerintahkan dr. Roebiono Kertopati, seorang dokter kepresidenan di Kementerian Pertahanan Bagian B (bagian intelijen) untuk membentuk badan pemberitaan rahasia yang disebut dengan Dinas *Code*.

dr. Roebiono kemudian membentuk kamar sandi yang kelak di kemudian hari menjadi embrio berdirinya Lembaga Sandi Negara yang kini berubah nama menjadi Badan Siber dan Sandi Negara (BSSN). Saat itu, operasional Dinas *Code* menggunakan sistem yang dikenal dengan 'Buku *Code* C' yang merupakan karya dr. Roebiono yang memuat 10.000 sandi berupa kode rahasia seperti kata, tanda baca, awalan dan akhiran, hingga penamaan dan lainnya. Ia membuat enkripsi tersebut menggunakan sistem kode angka secara mandiri.

Menghadapi perubahan tantangan zaman dan ancaman keamanan, BSSN RI terus melakukan pemutakhiran dalam sistem keamanan siber. Berdasarkan Perpres Nomor 18 Tahun 2020 tentang RPJMN 2020-2024, BSSN membentuk 121 Tim Tanggap Insiden Siber atau *Computer Security Incident Response Team* (CSIRT). CSIRT menjadi salah satu *major project* guna memperkuat keamanan siber Indonesia.

Pembentukan CSIRT sejalan pula dengan penerapan Sistem Pemerintah Berbasis Elektronik (SPBE) sebagaimana tertuang dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE. Menjadi bagian unsur keamanan SPBE adalah penjaminan keutuhan, ketersediaan data dan informasi. Dalam konteks tersebut, maka fungsi CSIRT adalah sebagai penyediaan pemulihan dari insiden keamanan siber. CSIRT memiliki otoritas untuk menangani berbagai insiden keamanan siber yang terjadi atau mengancam sistem informasi BSSN berupa *web defacement*, DDOS, *malware*, *phising*, dan sebagainya.

Pembentukan CSIRT ini memiliki misi *'Secure The Future'*. Di mana Indonesia diharapkan siap menghadapi ancaman kejahatan di ruang siber termasuk kejahatan penyalahgunaan data. Pemanfaatan ruang siber harus diikuti tiga hal, yaitu keamanan siber, pemaksimalan penggunaan ruang siber untuk memajukan kepentingan nasional di tingkat global, penguatan kuantitas dan kualitas ruang siber yang kompetitif di tingkat dunia pada seluruh lapisan ruang siber, baik lapisan fisik, logika, dan sosial.

G. RANGKUMAN MATERI

Hukum Siber atau *Cyber law* erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya. *Cyber Law* ini merupakan istilah yang berasal dari *cyberspace law*.

Istilah hukum diartikan sebagai padanan dari kata *cyber law*, yang saat ini secara *international* digunakan untuk istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain yang juga digunakan adalah Hukum TI (*Law of Information Teknologi*), Hukum dunia maya (*Virtual Word Law*), dan Hukum Mayantara.

Upaya pencegahan tindak pidana dan penanganan tindak pidana maka hukum siber/*cyber law* menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan elektronik yang termasuk juga di dalamnya kejahatan pencucian uang dan kejahatan terorisme.

Kegiatan siber/*cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan siber/*cyber* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata.

Hukum siber adalah perangkat hukum yang menjadi dasar dan peraturan yang menyinggung transaksi elektronik. Pendekatan dengan perangkat hukum ini dimaksudkan agar ada pijakan yang dapat digunakan oleh undang-undang dan peraturan lainnya. Banyaknya berbagai kejahatan dan pelanggaran hukum dalam pemanfaatan teknologi maka dibuat sebuah undang-undang sebagai dasar hukum

Kemajuan teknologi informasi telah mendorong sistem komputasi dan informasi atau siber meningkat pesat. Kemajuan siber ini telah melahirkan kemudahan di berbagai sektor kehidupan, seperti pada sektor finansial, transportasi, wisata dan lainnya. Namun, kemajuan ini telah membawa dampak baru apa yang disebut dengan kerentanan siber atau bahkan serangan siber.

Seiring perkembangan teknologi informasi dan komunikasi, keamanan siber di Indonesia mengalami perubahan dan peningkatan yang signifikan. Cikal bakal perkembangan siber di Indonesia tak terlepas dari peristiwa di awal kemerdekaan RI, pada tanggal 4 April 1946. Menteri Pertahanan saat itu, Mr. Amir Sjarifuddin memerintahkan dr. Roebiono Kertopati, seorang dokter kepresidenan di Kementerian Pertahanan Bagian B (bagian intelijen) untuk membentuk badan pemberitaan rahasia yang disebut dengan Dinas *Code*.

Menghadapi perubahan tantangan zaman dan ancaman keamanan, BSSN RI terus melakukan pemutakhiran dalam sistem keamanan siber. Berdasarkan Perpres Nomor 18 Tahun 2020 tentang RPJMN 2020-2024, BSSN membentuk 121 Tim Tanggap Insiden Siber atau *Computer Security Incident Response Team* (CSIRT). CSIRT menjadi salah satu *major project* guna memperkuat keamanan siber Indonesia.

TUGAS DAN EVALUASI

1. Sebutkan ruang lingkup hukum siber?
2. Apa yang dimaksud dengan kegiatan siber ?
3. Berikan pendapatmu terkait pengertian hukum siber !
4. Apa saja asas yang digunakan dalam pemberlakuan hukum siber?
5. Jelaskan metode ancaman siber !
6. Ada 5 negara di dunia yang memiliki tingkat penyerangan siber tertinggi. Sebutkan 3 dari kelima Negara tersebut !

DAFTAR PUSTAKA

Brenner, S. W. (2001). *Defining Cybercrime: A review of State and Federal Law di dalam Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime* (R. D. Clifford (ed.); 3rd ed.). Carolina Academic Press.

Indonesia, K. P. R. (2014). *Peraturan Menteri Pertahanan RI Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber*.

Kansil, C. S. T. (1982). *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*. Balai Pustaka.

Sthepenson, P., & Keith, G. (2013). *Investigating Computer-Related Crime : A Handbook For Corporate Investigators* (Second). CRC Press.

Titahelu, J. A. S. (2021a). Etika dan Hukum Dalam Public Relations. In A. Masruroh (Ed.), *Public Relations (Komunikasi Strategis, Digital dan Bertanggung Jawab Sosial)* (pp. 37–49). Widina Bhakti Persada.

Titahelu, J. A. S. (2021b). Hukum dan Kebijakan Publik. In *Kebijakan Publik* (pp. 149–167). Widina Bhakti Persada.

Titahelu, J. A. S. (2022). Sumber-Sumber Hukum Pidana. In E. Damayanti (Ed.), *Hukum Pidana* (pp. 41–60). Widina Bhakti Persada.

Wahyuni, W. (2022). *Mengenal Cyber Law dan Aturannya*. Hukum Online. https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/?page=2

HUKUM *CYBER*

BAB 2: ASPEK HUKUM DALAM MEDIA SOSIAL

Dr. Kasmanto Rinaldi, S.H., M.Si

Universitas Islam Riau

BAB 2

ASPEK HUKUM DALAM MEDIA SOSIAL

A. PENDAHULUAN

Pada bab ini penulis akan membahas tentang media sosial, media sosial dan investigasi, media sosial dan penyimpangan, aspek hukum media sosial di berbagai negara, dan aspek hukum dalam media sosial di Indonesia. Perkembangan sosial media membawa dampak positif kepada keberlangsungan hidup manusia pada era globalisasi ini. Namun kehadirannya juga memberikan dampak negatif bagi penggunanya. Dibalik banyaknya dampak positif yang ditawarkan dari sosial media, ternyata sosial media menyimpan banyak sisi gelap yang dapat membahayakan penggunanya.

Di media sosial media pengguna rentan terjadi kejahatan siber atau *Cyber Crime* yang siap merugikan korban-korbannya. Pengguna sosial media berasal dari berbagai kalangan, mulai dari anak-anak hingga lansia menggunakan sosial media tanpa mengetahui efek samping yang ditimbulkan dari media sosial tersebut. Sehingga tidak sepenuhnya para pengguna sosial media paham terkait etika penggunaannya, sehingga berpotensi terjadi penyimpangan-penyimpangan saat bersosial media.

Menurut penelitian yang dilakukan oleh Ubaidillah tentang kejahatan *cyber crime* di era 4.0, terdapat 60% masyarakat yang tidak mendapatkan kejahatan siber dan 30% pernah mendapatkan kejahatan siber (Ubaidillah, Kurnia, & Octaviany, 2022, p. 779). Dari 30% tersebut mereka mendapatkan kejahatan siber seperti akun media sosial Facebook yang dicuri, akun Instagram yang di*hacking*, penipuan pesan singkat, hingga terkena *phising.* Bagi beberapa individu, media sosial merupakan sarana

atau alat untuk melakukan perbuatan merugikan orang lain atau melakukan kejahatan.

Maraknya kejahatan yang muncul di media sosial menimbulkan kekhawatiran dan menjadikan para aparat yang berwenang mengambil tindakan tegas dalam memerangi kejahatan di media sosial. Kehadiran serta berlakunya peraturan UU ITE diharapkan para pengguna media sosial dapat lebih bijak dan berhati-hati dalam menggunakan media sosial dan menyikapi informasi-informasi yang beredar di media sosial.

B. MEDIA SOSIAL

Perkembangan media sosial pada era globalisasi saat ini sangat pesat. Masyarakat bahkan dapat mengakses seluruh jenis media sosial yang mereka inginkan dengan bermodalkan internet. Beragam aktivitas dan kepentingan dilakukan di media sosial, mulai dari mengakses informasi, berkomunikasi, berbagi dokumentasi, dan lain sebagainya. Masyarakat dapat mengakses media sosial dimana pun dan kapanpun tanpa terbatas ruang dan waktu.

Revolusi digital memberikan kemudahan akses dan kenyamanan bagi keberlangsungan hidup manusia sehingga mengubah sendi-sendi kehidupan, kebudayaan, dan masyarakat. Hal tersebut ditandai dengan lahirnya fenomena abad kreatif (abad ke-21) yang menempatkan informasi, pengetahuan, kreativitas, inovasi, dan jejaring sebagai sumber daya strategis yang positif dan juga negatif (Buchori, 2018). Media sosial mengalami perkembangan dari waktu ke waktu yaitu sebagai berikut:

1. Pada tahun 1978 merupakan sebuah awal penemuan sistem papan buletin yang memungkinkan untuk dapat berhubungan dengan orang lain menggunakan surat elektronik maupun mengunggah. Semua ini dilakukan dengan menggunakan saluran telepon yang terhubung dengan benda yang bernama modem.
2. Pada tahun 1995 merupakan kelahiran situs *GeoCities*, situs ini melayani *Web Hosting* yaitu layanan penyewaan penyimpanan data-data *website* agar dapat diakses di mana saja. Kemunculan *GeoCities* ini merupakan awal dari berdirinya *website-website* lainnya.

3. Pada tahun 1997 muncul situs jejaring sosial pertama yang bernama *Sixdegree.com.* Meskipun pada tahun 1995 terdapat situs *Classmates.com* yang memiliki tujuan yang sama, namun *Sixdegree.com* dianggap lebih dapat menawarkan situs jejaring sosial jika dibandingkan dengan *Classmates.com*
4. Pada tahun 1999 adalah kemunculan situs untuk membuat *blog* pribadi yang bernama *Blogger*. Situs ini memberikan penawaran kepada penggunanya untuk dapat membuat halaman situsnya sendiri. pengguna dari *blogger* ini bisa memuat dan meng*upload* hal apapun termasuk hal pribadi maupun hal untuk mengkritisi pemerintah. Sehingga *blogger* dapat disebut sebagai tonggak berkembangnya sebuah media sosial.
5. Pada tahun 2002 merupakan berdirinya *Friendster*, yaitu merupakan situs jejaring sosial yang *booming* dan keberadaannya menjadi fenomenal.
6. Pada tahun 2003 merupakan berdirinya LinkedIn. LinkedIn berguna untuk bersosial dan mencari pekerjaan, sehingga fungsi dari sebuah media sosial semakin mengalami perkembangan dan menghadirkan inovasi baru.
7. Pada tahun 2003 merupakan berdirinya *MySpace* yang menawarkan kemudahan. Sehingga situs ini disebut-sebut sebagai situs jejaring sosial yang *user friendly*
8. Pada tahun 2004 merupakan tahun kemunculan *Facebook*. *Facebook* merupakan situs jejaring sosial yang terkenal hingga sampai saat ini. *Facebook* merupakan jejaring sosial yang memiliki anggota terbanyak dibandingkan situs lainnya.
9. Pada tahun 2006 merupakan tahun lahirnya *Twitter*, yaitu jejaring sosial yang berbeda dari yang ainnya karena pengguna dari *Twitter* hanya dapat meng*update* status yang dibatasi sebanyak 140 karakter.
10. Pada tahun 2007 kemunculan *Wiser*. *Wiser* merupakan situs jejaring sosial yang diharapkan dapat menjadi sebuah direktori *online* organisasi lingkungan seluruh dunia termasuk pergerakan lingkungan baik dilakukan individu maupun kelompok.
11. Pada tahun 2011 merupakan lahirnya Google+.

Kemajuan teknologi terus menciptakan inovasi. Peningkatan jumlah pengguna media sosial dari tahun ke tahun juga mengalami peningkatan drastis. Berdasarkan laporan *We Are Social* yang menyatakan bahwa per Januari 2021 terdapat sekitar 170 juta penduduk Indonesia yang dinyatakan sebagai pengguna aktif media sosial dan rata-rata mereka menghabiskan waktu berselancar di media sosial dengan kurun waktu sekitar 3 jam 14 menit per harinya (Hayati, 2021).

Media sosial merupakan suatu media *online*, dengan para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, wiki, forum, dan dunia virtual (Hendrawan, Sari, 2021). Dengan begitu media sosial dapat diartikan sebagai sarana berinteraksi antara pengguna dengan berbagi pesan, cerita, pendapat, informasi, baik yang mengandung nilai positif maupun negatif. Orang-orang dapat dengan mudah terhubung dalam skala gobal. Media sosial pada dasarnya merupakan perkembangan mutakhir dari teknologi informasi berbasis internet yang dapat memudahkan para penggunanya untuk berkomunikasi, berpartisipasi, saling berbagi dengan menciptakan sebuah jaringan secara maya sehingga dapat menyebarluaskan konten-konten mereka sendiri (Abdullah, Mutalib, 2020).

Media sosial merupakan media *online* yang mendukung interaksi sosial. Andreas Kaplan dan Michael Haenlein mendefinisikan media sosial sebagai "sebuah kelompok aplikasi berbasis internet yang membangun di atas dasar ideologi dan teknologi web 2.0 dan yang memungkinkan penciptaan dan pertukaran *user-generated content*. (Cahyono, 2016, p. 142). Di sisi lain, media sosial merupakan media yang dapat dilihat oleh publik. Hal ini dapat diartikan bahwa seluruh curahan, ketikan, opini, bahkan emosi yang dituangkan seseorang di media sosialnya dapat dilihat dan diketahui oleh orang lain (Rizana, Utama, Svinarky, 2021). Pada dasarnya media sosial adalah perkembangan mutakhir dari teknologi web baru yang berbasis internet yang dapat memudahkan semua orang dapat berkomunikasi, berpartisipasi, saling berbagi dan membentuk sebuah jaringan secara *online,* sehingga dapat menyebarluaskan konten mereka sendiri. (Emilsyah, 2021).

Media sosial menempati posisi tertinggi dalam kehidupan masyarakat karena sering digunakan untuk berkomunikasi. Peran media sosial dalam keberlangsungan hidup manusia berperan sebagai alat berdialog atau berinteraksi antar manusia dengan menggunakan internet dan teknologi web. Namun tidak jarang banyak masyarakat yang menyalahgunakan fungsi dan kegunaan dari media sosial untuk kepentingan-kepentingan tertentu dengan cara melakukan kejahatan atau penyimpangan. Berdasarkan hal tersebut, media sosial mempunyai dampak kepada masyarakat yaitu sebagai berikut:

1. **Dampak positif:** media sosial memfasilitasi masyarakat untuk saling berkomunikasi. Media sosial menyediakan fasilitas untuk bertukar pesan, menyampaikan informasi, mempermudah manusia dalam menjalin silaturahmi, mengeratkan hubungan pertemanan, memberikan kesempatan masyarakat untuk dapat berjualan, mendapatkan informasi lowongan pekerjaan, memperoleh dengan mudah informasi beasiswa maupun pendidikan lainnya, dan menambah wawasan masyarakat.
2. **Dampak negatif:** Menggunakan media sosial bagi segelintir masyarakat merupakan hal yang candu, akibat dari kecanduan tersebut dapat berdampak pada aktivitas sehari-hari. Media sosial dapat menimbulkan rasa malas belajar. Pornografi dalam media sosial juga sangat rentan diakses karena memiliki akses yang mudah. Media yang cenderung membahas berita sering dimanfaatkan oleh orang dewasa. Media yang membahas informasi dan hiburan merupakan posisi yang penting bagi kalangan ibu-ibu, remaja, serta anak-anak. Penggunaan media sosial secara berlebihan yang menghabiskan waktu seharian sehingga menjadikan seseorang individu tersebut menjadi individualis dan tidak peduli dengan lingkungan dan masyarakat di sekitarnya (Rizana, Utama, & Svinarky, 2021). Keseringan dalam menggunakan media sosial juga menjadikan seseorang individu tidak fokus dan produktif dalam bekerja. Data-data pribadi juga sangat rawan bocor secara *online* (Putri & Rinaldi, 2022)

Media diibaratkan mempunyai peran sebagai *agent of change* dan sarana interaksi. Media mempunyai peranan penting, pentingnya media dapat dilihat dari pengaruh yang diberikan dan dirasakan oleh masyarakat mulai dari aspek kognitif, efektif, hingga konatif dari media. Media sosial mengambil berbagai macam bentuk termasuk majalah, forum internet, weblog, blog sosial, podcast, foto, video, dan lainnya. Menurut Achmad Buchori (2018) media memberikan manfaat bagi keberlangsungan hidup masyarakat. Berikut manfaat bagi masyarakat terkait penggunaan media sebagai berikut:

1. Membantu interaksi sosial dan memberdayakan masyarakat. Media dapat menghubungkan hal yang biasanya dipisahkan dan dibatasi oleh sosial, ekonomi, budaya, politik, agama, dan ideologi.
2. Menawarkan sarana untuk meningkatkan partisipasi masyarakat dan memfasilitasi terciptanya suatu komunitas dengan tujuan kepentingan bersama.
3. Memfasilitasi pendidikan dan pembelajaran. Media memudahkan akses terhadap pendidikan dan memudahkan pembelajaran.
4. Meningkatkan fleksibilitas untuk pekerja dan pengusaha yang meningkatkan produktivitas.

Berbagai macam jenis informasi yang bersumber dari media sosial, selalu dapat menjadi andalan utama bagi jurnalis, apalagi yang berkaitan dengan opini publik (Sumartono, 2017). Hanya dengan mengandalkan sumber informasi yang didapatkan dari media sosial, jurnalis dengan mudah untuk mendapatkan ide-ide untuk membuat berita bagi media elektronik maupun media cetak (Nisa, Disemadi, & Roisah, 2020). Haenlein menciptakan skema klasifikasi untuk berbagai jenis media sosial dalam artikel Horizons Bisnis. Menurut Kaplan dan Haenlein dalam Anang Sugeng Cahyono (2016) terdapat enam jenis media sosial yaitu sebagai berikut:

1. Proyek kolaborasi
   Website memberikan izin penggunanya untuk dapat mengubah, menambah, ataupun me-*remove* konten-konten yang ada di *website* ini. Salah satu contohnya adalah Wikipedia.

2. Blog dan microblog
   Pengguna lebih bebas dalam mengekspresikan sesuatu di blog tersebut. Seperti curhat maupun memberikan kritikan terhadap kebijakan pemerintah. Contoh media sosial tersebut adalah Twitter.
3. Konten
   Para pengguna *website* tersebut saling membagikan konten-konten media seperti video, *ebook*, gambar, dan lain sebagainya. Contoh media sosial tersebut adalah Youtube.
4. Situs jejaring sosial
   Aplikasi akan memberikan izin pengguna untuk terhubung dengan cara membuat informasi pribadi sehingga dapat terhubung dengan orang lain. Informasi tersebut seperti foto-foto. Contoh media sosial tersebut adalah Facebook.
5. Virtual *game world*
   Dunia virtual mereplikasikan lingkungan 3D, pengguna dapat muncul dalam bentuk avatar yang diinginkan serta berinteraksi dengan prang lain seperti di dunia nyata. Contohnya adalah *game online*.
6. Virtual *social world*
   Dunia virtual yang penggunanya merasa hidup di dunia virtual, persis seperti virtual *game world* yang berinteraksi dengan pengguna lain. Akan tetapi virtual *social world* lebih bebas. Contohnya *second life*.

C. MEDIA SOSIAL DAN INVESTIGASI

Media sosial merupakan salah satu alat dalam perangkat investigasi lembaga untuk membantu menetapkan petunjuk investigasi dan mengumpulkan bukti tentang calon tersangka. Tidak ada aturan yang khusus mengatur penggunaan informasi lembaga penegak hukum yang diperoleh dari situs media sosial, tetapi kemampuan mereka untuk mendapatkan atau menggunakan informasi tertentu dapat dipengaruhi oleh kebijakan perusahaan media sosial serta kebijakan media sosial lembaga penegak hukum itu sendiri dan aturan acara pidana. Ketika individu mem*posting* konten di media sosial tanpa adanya batasan *audiens*, siapapun bahkan lembaga penegak hukum dapat mengakses *posting*an konten tersebut di *platform* media sosial.

Penegak hukum menggunakan informasi tertentu yang dibagikan di platform media sosial untuk membantu mencegah dan menyelidiki aktivitas kriminal. Penegak hukum menggunakan media sosial untuk mengumpulkan informasi dan bukti sebagai bagian dari tugas investigasinya. Media sosial selain untuk berkomunikasi juga sebagai pengumpulan intelijen. Banyak contoh penegakan hukum menggunakan media sosial dalam mendukung penilaian dan investigasi intelijen. Media sosial sebagai alat yang dapat digunakan oleh para penegak hukum untuk dapat terhubung dengan masyarakat. Ada banyak cara untuk membantu menetapkan petunjuk investigasi dan mengumpulkan bukti, termasuk mengumpulkan informasi dari media sosial (Finklea, 2022).

D. PENYIMPANGAN SOSIAL DALAM MEDIA SOSIAL

Masyarakat menghasilkan berbagai isi dan konten di media sosial. Di sisi lain, media sosial mempunyai sisi dan dampak yang buruk. Media sosial dapat menjadi sumber timbulnya penyimpangan sosial atau perilaku menyimpang (Hayati, 2021). Perbuatan kejahatan dapat diartikan sebagai tindakan anti sosial yang mendapat reaksi buruk dari masyarakat karena dianggap menyimpang dengan norma yang berlaku di masyarakat (Lubis, Rinaldi , & Mianita, 2022). Tindakan kriminal atau tindak pidana pada umumnya dilakukan pelaku karena dimotivasi oleh dorongan pemenuhan kebutuhan yang relatif sulit (Al Hadi & Rinaldi, 2023). Melalui media sosial dapat memicu peluang terjadinya penyimpangan. *Platform* media sosial harus berhati-hati untuk tidak melakukan pelanggaran-pelanggaran dalam melaksanakan fungsinya sebagai media.

Semakin banyaknya menghabiskan waktu untuk berinteraksi di media sosial mengakibatkan banyaknya timbul perilaku menyimpang yang dilakukan di media sosial. Jenis perilaku menyimpang yang timbul sangat bervariasi, salah satunya adalah perilaku kekerasan berbasis gender *online* yang mengandung pelecehan seksual, ancaman, *grooming,* mencemarkan nama baik, dan lain sebagainya. Perilaku kekerasan berbasis gender *online* merupakan salah satu tipologi kejahatan di media sosial yang tidak sesuai dengan norma yang berlaku di masyarakat.

Akibat adanya penyimpangan yang timbul di media sosial tersebut menjadikan interaksi sosial dalam media sosial menjadi rusak dan berpotensi memberikan dampak negatif bagi penggunanya. Penyimpangan sosial yang dilakukan di media sosial merupakan bentuk kekerasan berbasis gender *online* adalah melakukan pelecehan seksual *(cyber sexual harassment).* Penyimpangan yang dilakukan di media sosial semakin marak terjadi. Seperti pelecehan yang dilakukan di media sosial yang dilakukan secara tidak langsung. Anak-anak dan remaja menjadi kalangan yang sangat rentan dalam menyalahgunakan media sosial dan menjadi korban media sosial (Windarto, Oktaviany, 2020). Tindakan menyimpang yang dilakukan oleh remaja dikenal dengan istilah kenakalan remaja (Rinaldi, Afrizal, dan Maulana, 2022).

Di media sosial siapapun dapat dengan bebas menyebarkan konten, memberikan pendapat, mengirimkan *chat*, baik bersifat positif maupun negatif tanpa khawatir. Hal itu disebabkan karena di media sosial dapat membuat akun anonim. Akun anonim cenderung digunakan agar tidak dikenali ketika memberikan opini, komentar, hingga konten di media sosial. Hal tersebut berpotensi untuk menciptakan penyimpangan di media sosial. Pelaku kejahatan dan penyimpangan dengan mudah dan berani untuk melancarkan aksi kejahatan dan penyimpangannya karena menggunakan akun anonim yang identitasnya tidak diketahui.

Banyak dari pengguna media sosial tidak memahami aturan-aturan dan etika dari penggunaan dan efek yang akan muncul dari media sosial itu sendiri. Pentingnya literasi digital untuk memiliki kecakapan dalam menggunakan media sosial. Literasi digital merupakan pengetahuan dan kecakapan untuk menggunakan media digital, alat-alat komunikasi, atau jaringan dalam menemukan, mengevaluasi, menggunakan, membuat informasi, dan memanfaatkannya secara sehat, bijak, cerdas, cermat, tepat, dan patuh terhadap hukum dalam tujuan membina komunikasi dan interaksi dalam kehidupan sehari-hari (Buchori, 2018). Media sosial dianggap sebagai tempat untuk menyalurkan konten maupun informasi yang tidak jarang mengandung hal yang negatif yang dapat menimbulkan persepsi yang berbeda akan dapat menimbulkan perselisihan antar pengguna itu sendiri (Perdana & Yusuf, 2020, p. 229). Contohnya yaitu ujaran kebencian, *hoax*, *bullying,* SARA, dan kejahatan lainnya.

E. ASPEK HUKUM MEDIA SOSIAL DI BERBAGAI NEGARA

Aspek hukum media sosial di berbagai negara tentunya berbeda-beda. Seperti di negara Jerman yang memiliki Undang-Undang Penegakan Jaringan Jerman *(Netzwerkdurchsetzungsgesetz atau NetzDG)* mulai berlaku sepenuhnya pada 1 Januari 2018. Undang-undang ini umumnya dikenal dengan "undang-undang ujaran kebencian". Undang-undang ini merupakan upaya ambisius dari negara barat untuk meminta pertanggungjawaban platform media sosial untuk memerangi ujaran *online* yang dianggap ilegal menurut hukum domestik. Tujuannya adalah untuk menegakkan 22 undang-undang di ruang *online* yang sudah ada dalam hukum pidana Jerman dan untuk meminta pertanggungjawaban platform media sosial besar atas penegakannya. Ke-22 undang-undang tersebut mencakup kategori seperti hasutan untuk kebencian, penyebaran penggambaran kekerasan, dan lainnya.

NetzDG juga berlaku untuk kategori lainnya seperti penyebaran pornografi anak, penghinaan, pencemaran nama baik, pencemaran nama baik agama, perkumpulan keagamaan dan ideologi dengan cara yang dapat mengganggu ketenteraman masyarakat, pelanggaran hubungan intim (Heidi & Leerseen, 2019). NetzDG menargetkan platform media sosial besar dengan lebih dari 2 juta pengguna berlokasi di Jerman. *Platform* ini harus menyediakan mekanisme bagi pengguna untuk mengajukan keluhan tentang konten ilegal. Ketika menerima keluhan, *platform* harus menyelidiki apakah konten tersebut ilegal. Jika ditemukan konten tersebut secara nyata melanggar hukum, *platform* harus menghapusnya dalam waktu 24 jam. Konten ilegal lainnya harus dihapus dalam waktu 7 hari. Di Malaysia mempunyai Undang-Undang Kejahatan Komputer, *Digital Signature Act*, *Telemedicine act* (tiga dari mereka berlaku sejak 1997), *Multimedia Act* (1998), *Payment System Act* (2003), Dan *Personal Data Act* (2010). Singapura juga mempunyai satu set peraturan yang serupa dengan Malaysia.

F. ASPEK HUKUM MEDIA SOSIAL DI INDONESIA

Media sosial menjadi ruang tempat manusia menarik dirinya dari realitas, menarik diri dari tubuhnya, menarik diri dari permasalahan sosial untuk masuk ke dalam realitas-realitas yang bersifat halusinasi (Fahrimal,

2018). Pada ruang media sosial identitas dibangun dalam wujud virtual. Masyarakat yang menggunakan media sosial dapat beraktivitas secara bebas tanpa memerlukan adanya pengendalian sosial, moral, spiritual, dan etika. Maka media sosial sangat lekat dengan hal yang berhubungan dengan pelanggaran etika, moral, dan nilai-nilai yang bersifat universal.

Pelanggaran, kejahatan, dan penyimpangan yang terjadi di media sosial dapat berwujud penyebaran informasi palsu, transaksi ilegal, penipuan, *cyber bullying,* pornografi, *human trafficking,* ujaran kebencian, dan lainnya. Riset Andina (2010) dalam Fahrimal (2018) menyatakan penemuannya bahwa media sosial Facebook merupakan salah satu media sosial yang paling banyak digunakan dan menjadi aplikasi media sosial yang paling berdampak negatif terhadap masyarakat.

Media sosial tidak memiliki pengawas yang mengawasi berbagai macam media sosial dalam berinteraksi (Khatimah, 2018). Hal ini justru berbanding terbalik dengan media massa yang mempunyai pengawas contohnya pengawas media penyiaran yang umumnya dikenal dengan sebutan Kemenkominfo yang berwenang mengatur alokasi frekuensi, dan Komisi Penyiaran Indonesia (KPI) dengan berbagai undang-undang yang telah tercantum dalam buku Pedoman Perilaku Penyiaran dan Standar Program Siaran (P3SPS) yang berfungsi mengawasi hal yang berkaitan dengan penyiaran.

Dari permasalahan tersebut, pemerintah Indonesia mengambil tindakan dengan mengeluarkan peraturan tentang media sosial agar dapat mengendalikan atau mengontrol media sosial menjadi lebih kondusif. Pemerintah dan kementrian komunikasi dan informatika telah membuat sebuah regulasi untuk dapat mengontrol dan mencegah kejahatan siber di media sosial. Kejahatan siber atau *cyber crime* merupakan kejahatan yang dilakukan di media *online* dengan menggunakan komputer menjadi media utama mencari korban yang akan dituju (Ubaidillah, Kurnia, & Octaviany, 2022). Oleh sebab itu terdapat batasan-batasan yang diatur dalam perundang-undangan yang wajib dipatuhi oleh siapapun dalam menggunakan media sosial. Batasan dalam menggunakan media sosial tersebut diatur dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Tujuan dari regulasi tersebut dibuat untuk menjawab permasalahan yang terjadi saat menggunakan media sosial yang sering dihadapkan dengan penyampaian informasi, komunikasi, dan transaksi yang di dalamnya banyak yang melanggar dan melawan hukum. Regulasi tersebut adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah Undang-undang Nomor 19 tahun 2016. Undang-undang ITE merupakan bentuk keseriusan dan tindakan tegas negara dalam mencegah kejahatan internet. Undang-undang ini dimaksudkan untuk menjawab permasalahan yang terjadi oleh pengguna media sosial yang dihadapkan oleh perbuatan melawan hukum.

Pemerintah memberikan perlindungan dan jaminan keamanan terhadap pengguna internet. Perlindungan yang diberikan berlaku kepada seluruh pengguna. Esensi Undang-undang ITE melingkupi semua transaksi berbasis elektronik seperti komputer serta jaringan dan memiliki kekuatan hukum. Undang-undang ITE diharapkan berguna untuk mengatur seluruh sistem yang terlibat kendala hukum dengan hukum berhubungan dengan dunia internet *(cyber)*. Undang-undang ini ditujukan kepada pengguna yang berada di Indonesia.

Undang-undang ITE dikhususkan berlaku untuk setiap orang di Indonesia dan seluruh masyarakat Indonesia yang tinggal di luar Indonesia yang berhubungan dengan hukum Indonesia. Pelaku dan korban dari undang-undang ITE merupakan pengguna aktif media sosial yang dituduh melakukan pelanggaran dan penyimpangan terkait konten yang mengandung unsur negatif di internet. Undang-undang ITE digunakan dengan tujuan untuk mengalahkan dan meniadakan segala aktivitas yang berhubungan dengan *cyber crime* di internet tanpa terkecuali.

Undang-undang ITE hanya dapat meminimalisir dan menurunkan hal yang menyimpang dan melanggar ketentuan hukum. Undang-undang ITE membangun generasi yang modern dan berilmu dalam melalui perubahan sosial melalui media sosial yang ada. Media sosial yang saat ini digunakan jadi lebih bermanfaat dan berguna dalam memenuhi aspek kehidupan. Undang-undang Informasi dan Transaksi Elektronik (UU ITE) pasal 40 ayat (2a) memberi kewenangan pada pemerintah untuk dapat mencegah dan memblokir situs-situs yang memuat informasi-informasi tertentu.

Pada pasal 40 ayat (2b) Undang-undang ITE juga menjelaskan dan menegaskan bahwasanya dalam tujuan mencegah menyebarnya konten negatif atau konten yang dinilai melanggar peraturan, pemerintah dapat memerintahkan pihak penyelenggara informasi (dalam hal ini penyedia jaringan internet) agar melakukan pemutusan akses terhadap layanan akses informasi, termasuk media sosial. Adapun bentuk-bentuk tindak pidana di media sosial menurut Teguh Prasetyo (2018) yang diatur dalam Undang-undang tentang Informasi dan Transaksi Elektronik adalah sebagai berikut:

1. Setiap orang yang dilarang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi dan dokumen elektronik yang mengandung muatan yang melanggar kesusilaan.
2. Setiap orang dilarang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi dan dokumen elektronik yang mengandung perjudian.
3. Setiap orang dilarang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan informasi dan dokumen elektronik yang mengandung muatan penghinaan dan pencemaran nama baik.
4. Setiap orang dilarang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan atau membuat dapat diaksesnya informasi elektronik dan dokumen yang mengandung muatan pemerasan dan ancaman.
5. Setiap orang dengan sengaja menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
6. Setiap orang dilarang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian dan permusuhan kelompok atau individu masyarakat tertentu berdasarkan suku, agama, ras, dan antar golongan (SARA).
7. Setiap orang dilarang dengan sengaja mengirimkan informasi dan dokumen elektronik
8. Mengandung ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Undang-undang ITE merupakan salah satu bentuk kepedulian pemerintah terhadap pengguna media sosial. Dengan adanya undang-undang ITE diharapkan penyimpangan dan pelanggaran di media sosial menurun. Undang-undang ini mengkriminalisasi kejahatan yang terjadi di dunia maya termasuk di media sosial dan mengancam akan menghukum pelakunya. Ruang lingkup Undang-undang ITE sangat terbatas dan masih membutuhkan undang-undang lain untuk melengkapi (Chintia, Nadiah, Ramadhani, Haedar, Febriansyah, & Rakhmawati, 2018).

Akibat keterbatasan ini kasus-kasus kejahatan siber yang terjadi di media sosial dihukum dengan KUHP Hukum Acara Pidana (UU KUHAP), Perlindungan Konsumen UU No. 8 tahun 1999, UU Hak Cipta No. 19 tahun 2002, atau UU Anti-Pornografi No. 44 Tahun 2008. Undang-undang ITE mengacu pada model yang bersifat komprehensif. Materi muatan yang diatur di dalam undang-undang ITE tersebut mengandung hal yang luas dan mencakup banyak aspek hukum, yaitu aspek hukum perdata materiil, hukum pidana materiil, hukum acara perdata, hukum acara pidana, dan hukum pembuktian (Angkupi, 2014). Undang-undang ITE memuat ketentuan tentang larangan melakukan perbuatan tertentu yang diancam dengan sanksi. Tindak-tindak pidana tersebut sebagaimana yang di uraikan di bawah ini. Tindak pidana komputer yang sering terjadi di media sosial yang diatur oleh UU ITE adalah:

1. Pornografi
   Larangan melakukan perbuatan yang berisi melanggar kesusilaan diatur dalam pasal 27 Ayat (1) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (1). Pasal 27 Ayat (1) menentukan: Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan mentransmisikan dan membuat dapat diaksesnya informasi elektronik yang memiliki muatan yang melanggar kesusilaan.
2. Perjudian *online*
   Larangan perjudian dengan menggunakan sistem elektronik dan dilakukan secara *online (online gambling)* diatur pada Pasal 27 Ayat (2) dan diancam sanksi pidana berdasarkan Pasal 45 Ayat (1). Pasal 27 Ayat (2) menentukan bahwa setiap orang dengan sengaja dan tanpa hak mendistribusikan dan mentransmisikan dan membuat diaksesnya

informasi elektronik dan dokumen elektronik yang memiliki muatan perjudian.

3. Penghinaan dan Pencemaran Nama Baik
   Larangan penghinaan dan pencemaran nama baik dengan menggunakan sistem komputer atau yang dilakukan di media sosial diatur dalam Pasal 27 Ayat (3) dan diancam sanksi pidana berdasarkan Pasal 45 Ayat (1). Pasar 27 Ayat (3) menentukan bahwa setiap orang dengan sengaja mendistribusikan dan mentransmisikan dan membuat dapat diaksesnya informasi elektronik dan dokumen elektronik yang memiliki muatan penghinaan dan pencemaran nama baik.
4. Penyebaran Informasi yang Bermuatan SARA
   Larangan melakukan perbuatan menyebarkan informasi yang bermuatan SARA diatur dalam Pasal 28 Ayat (2) dan diancam sanksi pidana berdasarkan Pasal 45 ayat (2). Pasal 28 Ayat (2) menentukan bahwa setiap orang yang secara sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).
5. Pemerasan dan Pengancaman
   Pada pasal 27 ayat (4) undang-undang nomor 19 tahun 2016 atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik menyatakan larangan keras terhadap pendistribusian informasi melalui internet yang mengandung adanya pemerasan atau pengancaman.

G. RANGKUMAN MATERI

1. Media sosial dapat diartikan sebagai sarana berinteraksi antara pengguna dengan berbagi pesan, cerita, pendapat, informasi, baik yang mengandung nilai positif maupun negatif.
2. Media sosial di tangan pengguna yang kurang bijak dapat menjadi sarana penyebaran *hoax*, sarana provokasi, penyebaran konten dan lain sebagainya. Hal-hal yang menyimpang di media sosial seperti ujaran kebencian, *bullying,* pornografi, *hoax,* judi *online*, penipuan, dan kejahatan lainnya sering terjadi saat menggunakan media sosial.

3. Aspek hukum sangat dibutuhkan dalam mengoperasikan media sosial untuk dapat melindungi penggunanya dari kejahatan-kejahatan di media sosial. Dikarenakan banyaknya kejahatan atau tindakan menyimpang yang terjadi di media sosial, pemerintah mengeluarkan tindakan dengan memberlakukan undang-undang nomor 19 tahun 2016 atas undang-undang nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik atau yang secara umum dikenal dengan sebutan UU ITE.
4. Undang-undang Informasi dan Transaksi Elektronik (UU ITE) hadir untuk membatasi perilaku pengguna media sosial yang menyimpang dan tidak beretika dan melanggar norma-norma hukum. Selain menyebabkan terjadinya perubahan sosial di masyarakat, perkembangan media sosial di sisi lain juga menyebabkan terjadinya perubahan hukum secara signifikan.

TUGAS DAN EVALUASI

1. Apa yang dimaksud dengan media sosial? Sebutkan jenis-jenisnya!
2. Bagaimana peran media sosial dalam investigasi?
3. Apa aspek hukum media sosial?
4. Apa saja kejahatan yang terjadi di media sosial?
5. Sebutkan kejahatan apa yang diatur dalam UU ITE?

DAFTAR PUSTAKA

Al Hadi, Y., & Rinaldi, K. (2023). Fear Of Crime Penjual Tanaman Hias Di Era Pandemi Covid-19(Studi Pada Wilayah Hukum Polres Pangkalan Kerinci. *SEIKAT Jurnal Ilmu Sosial, Politik dan Hukum, 2 No.2*, 107-112.

Andina, E. (2010). *Studi Dampak Negatif Facebook Terhadap Remaja Indonesia.* Jakarta: Pusat Pengkajian, Pengolahan Data dan Informasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia.

Angkupi, P. (2014). Kejahatan Melalui Media Sosial Elektronik Di Indonesia Berdasarkan Peraturan Perundang-Undangan Saat Ini. *Jurnal Mikrotik, 2 No.1*.

Buchori, A. (2018). Pentingnya Literasi Digital Untuk Meningkatkan Partisipasi Masyarakat Dalam Sosialisasi Pembangunan Melalui Media Sosial. *Jurnal Ilmu Komunikasi, 4 No.1*.

Cahyono, A. S. (2016). Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat Di Indonesia. *Publiciana, 9 No.1*.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati, N. A. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology (JIEET), 2 No.2*.

Emilsyah, N. (2021). Peran Media Massa Dalam Menghadapi Serbuan Media Online The Role of Mass Media in Facing Online Media Attacks. *Majalah semu ilmiah populer komunikasi massa, 2 No. 1*, 51-64.

Fahrimal, Y. (2018). Netiquette: Etika Jejaring Sosial Generasi Milenial Dalam Media Sosial. *Jurnal Penelitian Pers dan Komunikasi Pembangunan, 22 No.1*, 69:78.

Finklea, K. (2022). Law Enforcement and Technology: Using Social Media. *Congressional Research Service*.

Hayati, N. (2021). Media Sosial Dan Kekerasan Berbasis Gender Online Selama Pandemi COVID-19. *Jurnal Hukum, Humaniora, Masyarakat dan Budaya, 1 No.1*, 43-52.

Khatimah, H. (2018). Posisi dan Peran Media Dalam Kehidupan Masyarakat. *Tasamuh, 16 No.1*.

Lubis, F. F., Rinaldi , K., & Mianita, H. (2022). Pola Interaksi Sosial Residivis Narkoba Di Dalam Lembaga Pemasyarakatan (Studi Deskriptif Sosialisasi Kejahatan Residivis Narkoba Di Lapas Kelas II B Tebing TInggi, Sumatera Utara). *Prosiding SENKIM: Seminar Nasional Karya Ilmiah Multidisiplin, 2 No.1*, 176-183.

Nisa, C. U., Disemadi, H. S., & Roisah, K. (2020). Aspek Hukum Tentang Black Campaign Pada Platform Media Sosial Instagram. *Mahkamah: Jurnal Kajian Hukum Islam, 5 No. 1*.

Perdana, A. P., & Yusuf, W. (2020). UU ITE Tentang Efek Media Sosial Terhadap Generasi Milenial (THE ACT ON THE EFFECT OF SOCIAL MEDIA ON THE GENERATION OF MILENIAL). *Jurnal Kelitbangan, 8 No.3*.

Prasetyo, T. (2018). *Pengantar Ilmu Hukum.* Jakarta: Rajawali Pers.

Putri, P. A., & Rinaldi, K. (2022). The problems of Illegal Online Loans based on the Victim's Perspective: A Case Study. *International Journal of Advances in Social and Economics, 4 No.3*, 102-106.

Rinaldi, K., Afrizal, & Maulana, M. (2022). Pendekatan Attachment Sebagai Salah Satu Upaya Pencegahan Juvenile Delinquency. *BHAKTI NAGORI Jurnal Pengabdian Kepada Masyarakat, 2 No.2*.

Rizana, Utama, A. S., & Svinarky, I. (2021). PENGARUH MEDIA SOSIAL TERHADAP DINAMIKA MASYARAKAT DAN LAHIRNYA BENTUK-BENTUK PERBUATAN HUKUM BARU DI MEDIA SOSIAL. *Jurnal Cahaya Keadilan, 9 No.2*.

Rizana, Utama, A. S., & Svinarky, I. (2021). Pengaruh Media Sosial Terhadap Dinamika Masyarakat Dan Lahirnya Bentuk-Bentuk Perbuatan Hukum Baru Di Media Sosial. *Jurnal Cahaya Keadilan, 9 No.2*.

Sumartono. (2017). Konstruksi Makna Media Sosial Bagi Anggota DPRD Kota Padang. *Al-Adalah, 20 No.1*, 23.

Tworek, H., & Leerssen, P. (2019). An analysis of Germany's NetzDG law. *First session of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*.

Ubaidillah, Kurnia, A. D., & Octaviany, R. V. (2022). Kejahatan Cybercrime di Era 4.0. *Prosiding Seminar Nasional Ilmu Ilmu Sosial (SNIIS), 1*.

HUKUM *CYBER*

BAB 3: ASPEK HUKUM DALAM *E-COMMERCE*

Ika Atikah, S.H.I., M.H

UIN Sultan Maulana Hasanuddin Banten

BAB 3

ASPEK HUKUM DALAM *E-COMMERCE*

A. PENDAHULUAN

Sistem transaksi perdagangan di Indonesia selalu mengalami peningkatan signifikan. Kemajuan teknologi telah memberikan kemudahan bagi siapa saja berinteraksi termasuk transaksi dagang yang mempertemukan pelaku usaha dan konsumen yang dikenal dengan perdagangan elektronik (*E-commerce*). Eksistensi *E-Commerce* dalam transaksi jual beli barang dan jasa menjadi lebih efisien waktu dan biaya. Masyarakat yang hendak melakukan transaksi jual-beli dapat dengan mudah mencari barang kemudian membelinya hanya dengan bermodalkan jaringan internet saja. Semisal *marketplace* yang kian banyak bermunculan secara daring Tokopedia, Zalora, Shopee, Lazada, JD.ID, blibli, dan lainnya yang merupakan situs dagang *online* yang menjual beragam jenis barang guna memenuhi kebutuhan sehari-hari masyarakat sebagai konsumen.

Berdasarkan laporan *e-Conomy* SEA, ekonomi digital Indonesia diproyeksikan mencapai *Gross Merchandise Value* (GMV) senilai US$ 77 miliar di tahun 2022. Sektor *ecommerce* di Indonesia menjadi sektor yang mengalami pertumbuhan tercepat kedua setelah Vietnam. *E-commerce* Indonesia diprediksi akan tumbuh dengan *Compounded annual growth rate* (CAGR) yang mana tingkat pertumbuhan per tahun sebesar 17 persen dan nilai GMV mencapai 95 miliar dollar. Layanan transportasi dan pesan antar-makanan diprediksi mencapai GMV 8 miliar dollar di tahun 2022. Layanan digital juga terus mengalami peningkatan dengan CAGR 22 persen menjadi GMV 15 miliar dollar hingga tahun 2025 (Tempo, 2023).

Sepak terjang *e-commerce* Indonesia diawali tahun 1999 yang mana forum KASKUS menjadi pelopor toko *online* di Indonesia yang dibangun oleh Andrew Darwis kemudian Bhinneka.com yang menjadi tempat transaksi dagang *online*. Perkembangan pesat *ecommerce* ditandai dengan ketertarikan masyarakat menggunakan teknologi internet. Pemerintah menyadari potensi dari transaksi dagang elektronik harus merumuskan pengaturan hukum yang memadai seiring bermunculan perusahaan *start-up* di tahun 2005 hingga puncak terjadi di tahun 2015 (Mustajibah & Trilaksana, 2021 : 2).

Dalam arti luas, *electronic commerce* disingkat *E-commerce* adalah pertukaran informasi elektronik antara bisnis dan pelanggan. Hal ini dapat dilakukan melalui internet. Dalam arti sempit, perdagangan elektronik adalah solusi kompleks yang menyediakan teknologi internet. Hal ini berarti bahwa banyak aplikasi dan penyedia layanan internet harus bekerja sama dengan sempurna sinkronisasi sebagai situs e-niaga yang dapat beroperasi. Perdagangan elektronik melibatkan penggunaan jaringan komputer untuk tujuan perdagangan. Transaksi *e-commerce* hingga saat ini belum memiliki pengertian yang sama, dikarenakan pengembangan *e-commerce* yang kian berkembang pesat, sehingga tidak dipungkiri setiap waktu *e-commerce* mengalami perubahan dan terbentuk sistem dagang elektronik baru. Namun, bukan berarti tidak ada pengertian yang seragam yang berakibat pada ketika ada sama sekali definisi *E-Commerce* (Riswandi, 2019 : 3).

Ada beberapa jenis transaksi jual beli daring diantaranya, *Business to business Ecommerce (B2B e-Commerce),* bentuk transaksi dagang yang melibatkan antar pebisnis *corporate* dan *Business to consumer*, transaksi jual-beli daring yang melibatkan pelaku usaha dan konsumen. Namun, secara *factual* model transaksi *e-commerce* memiliki banyak ragam, seperti hanya dari segi sifat *Business to Business*, model seperti ini sering dijumpai di era modern, *Business to Consumer*, yang mana konsumen menjual langsung ke konsumen, dan *Consumer to Business* yang mana individu menjual barang atau jasa kebutuhan organisasi (Riswandi, 2019:4).

Menurut Suyanto, *e-commerce* memiliki kegunaan bagi masyarakat, yang mana *ecommerce* memberikan kemudahan bagi setiap orang untuk bekerja di rumah dan tidak perlu keluar rumah sekadar berbelanja dengan

beberapa barang yang dibeli secara daring dan harga terjangkau murah (Suyanto, 2003: 35). Beragam kemudahan yang diberikan *ecommerce* tidak hanya berdampak positif, namun juga berdampak negatif yang mana muncul di tengah pengguna transaksi jual-beli daring. Dalam melakukan transaksi, perlu dilakukan registrasi oleh konsumen saat pembayaran dengan meng*input* data pribadi yang bersifat rahasia. Dari data tersebut, berpotensi muncul ancaman siber pada *e-commerce* (Rohmah, 2022 : 4).

B. PENGATURAN HUKUM *E-COMMERCE*

Transaksi elektronik semakin penting bagi pemerintah, perusahaan, dan konsumen di sebagian besar dunia. Sementara ketergantungan yang lebih besar pada perdagangan elektronik (*e-commerce*) yang menciptakan peluang signifikan, kurangnya keamanan dan kepercayaan tetap menjadi penghalang penting untuk transaksi semacam itu. Penipuan *online* dan pelanggaran data meningkatkan kekhawatiran yang membutuhkan tanggapan hukum dan peraturan yang memadai untuk meningkatkan perdagangan *domestic* dan lintas batas. Namun, mengadopsi kerangka hukum dan peraturan yang tepat menjadi sulit karena keragaman dan kompleksitas hukum dan peraturan dunia maya serta evolusi teknologi dan pasar yang cepat. Solusi pembayaran baru dan ketergantungan yang semakin besar pada komputasi awam menonjolkan kebutuhan untuk membuat kemajuan di bidang ini. Dengan latar belakang tersebut, masalah hukum utama yang perlu ditangani untuk memfasilitasi transaksi elektronik dan membuat interaksi di internet lebih aman secara umum. Catatan tersebut meninjau secara singkat praktik terbaik yang dipilih dalam mengatasi tantangan umum yang diketahui untuk persiapan dan penegakan hukum dunia maya berdasarkan UNCTAD.

Tindakan kebijakan harus mengatasi kebutuhan akan undang-undang yang kompatibel dan pembangunan kapasitas pemangku kepentingan utama, khususnya aparat penegak hukum. Ada beberapa hal terkait dengan *cybercrime* yang mana terjadi penyalahgunaan penggunaan komputer, *cracking*, membocorkan *password*, *e-banking*, pemanfaatan internet untuk pemerintahan dan kesehatan, masalah HaKI, penyalahgunaan nama domain, dan masalah privasi.

UU ITE atau hukum siber memiliki peran sentral dalam sistem hukum negara secara komprehensif. Dengan kehadiran bentuk hukum baru sebagai akibat pengaruh perkembangan teknologi dan globalisasi pengayaan bidang-bidang hukum yang sifatnya sektoral. Hal ini tentu saja terobosan dalam dinamika hukum yang akan menjadi bagian dari sistem hukum nasional. Subekti menyatakan bahwa sistem termasuk susunan atau tatanan yang teratur, yang mana secara keseluruhan memiliki bagian-bagian yang saling terkait satu sama lain, yang merupakan hasil dari suatu pemikiran guna mencapai tujuan. UU ITE No.11/2008 yang sekarang berubah menjadi UU No.19/2016 dan PP No.80/2019 "Penyelenggaraan Melalui Sistem Elektronik" yang mana pasal 28 ayat 1 UU ITE menyatakan "setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik". Pasal tersebut selaras dengan UU No.8/1999 "Perlindungan Konsumen". UU dibuat oleh pemerintah Indonesia bertujuan agar masyarakat sadar dan mandiri sebagai konsumen untuk memproteksi diri sendiri serta menciptakan sistem perlindungan terhadap konsumen dengan memberikan kepastian hukum dan keterbukaan informasi.

Pasal 28 (1) memberikan proteksi atas hak dan kepentingan konsumen dan penyebaran hoaks. Pasal tersebut agak memiliki kemiripan dengan Pasal 378 KUHP, yang mana perbedaan prinsip dari KUHP yakni "menguntungkan diri" dalam pasal 378 KUHP yang tidak lagi tertulis pada pasal 28 ayat 1 UU ITE. Konsekuensi hukum tentu saja dapat diuntungkan atau tidak bagi pelaku penipuan, tidak menghapus unsur pidana atas perbuatan tersebut dengan ketentuan perbuatan yang terbukti menimbulkan kerugian bagi orang lain.

Dalam pasal 45 A ayat 1 UU ITE No.19/206 "Setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagaimana dimaksud dalam pasal 28 ayat 1 dipidana dengan pidana penjara paling lama 6 bulan dan atau denda paling banyak 1 miliar rupiah".

UU Perlindungan Konsumen pasal 6 juga mengatur hak dan kewajiban penjual transaksi jual-beli *online*. Pasal 7 juga menjelaskan pelaku usaha berkewajiban memperlakukan konsumen *online* dengan ramah dan

memberikan informasi produk dengan benar, jelas, dan jujur. Tidak hanya itu, tidak membedakan pelayanan yang prima secara daring dengan para konsumen, memberikan kepercayaan kepada konsumen dengan menjelaskan mutu produk, menerapkan ganti rugi atas barang yang diterima konsumen tidak sesuai yang disepakati bersama.

PP No.80/2019 menyebutkan bahwa "pedagang wajib memiliki izin usaha dari Kementerian atau lembaga yang sesuai dengan bidang yang dijalankan, termasuk bagi pelaku usaha di *marketplace*". Pelaku usaha juga wajib mengikuti peraturan perundang-undangan yang ada dalam kegiatan transaksi dagang baik konvensional maupun elektronik.

C. KEJAHATAN SIBER (*CYBER*) TRANSAKSI *E-COMMERCE*

Kecanggihan teknologi telah mengubah paradigma tradisional menjadi paradigma modern yang ditandai dengan semakin pesat sistem transaksi dagang yang hanya menggunakan jaringan internet. Informasi menjadi hal yang masuk dalam kategori komoditi utama yang diperjualbelikan sehingga muncul berbagai *network* dan informasi *company* yang memfasilitasi bermacam kebutuhan konsumen. Penggunaan internet yang cepat dan perangkat genggam yang kuat, luar biasa kemajuan teknologi, tetap menjadi faktor utama yang berkontribusi terhadap evolusi teknologi *e-commerce*. Web dan Internet menyediakan media penting untuk memfasilitasi transaksi dan teknologi *e-commerce*.

Internet telah memfasilitasi pertumbuhan penggunaan *e-commerce* sehingga memungkinkan banyak perusahaan mengadopsi berbagai model *e-commerce*. *E-commerce* menawarkan banyak peluang bisnis dari kecil dan usaha skala menengah hingga skala besar. Bisnis percaya bahwa penggunaan *e-commerce* menawarkan banyak peluang dan keuntungan bagi pelaku usaha (Apau & Koranteng, 2019:229). Akibat dari perkembangan teknologi yang kian canggih menjadi titik rawan dalam *security device* dalam sistem komputer. Kelemahan daripada sistem yang digunakan merupakan suatu lembaga yang seringkali disalahgunakan oleh pihak ketiga guna kepentingan pribadi.

Dr. Debarati Halder dan Dr. K. Jaishankar mendefinisikan *cybercrime* sebagai tindak pidana yang dilakukan terhadap orang pribadi atau kelompok orang dengan motif *criminal* untuk secara sengaja merusak

reputasi korban atau penyebab kerugian fisik atau mental atau kerugian kepada korban secara langsung atau tidak langsung, menggunakan jaringan telekomunikasi modern seperti internet (*chat room*, email, ponsel sms) (Saroha, 2014: 254). Kamus oxford mendefinisikan istilah kejahatan dunia maya sebagai pidana kegiatan yang dilakukan melalui komputer atau internet. Kejahatan dunia maya dapat dikatakan sebagai spesies yang genusnya adalah kejahatan konvensional, dan di mana komputer adalah objek atau subjek perbuatan yang merupakan kejahatan. Kejahatan dunia maya berarti setiap tindak pidana atau tindak pidana lainnya difasilitasi oleh atau melibatkan penggunaan komunikasi elektronik atau sistem informasi termasuk perangkat apa pun.

Profesor S.T. Viswanathan memberikan tiga definisi dalam bukunya "*The Indian Cyber Law with Cyber*" sebagai berikut:

1. Setiap tindakan *illegal* dimana komputer adalah alat atau objek kejahatan yaitu setiap kejahatan, cara atau tujuan adalah untuk mempengaruhi fungsi sebuah komputer.
2. Setiap insiden terkait dengan teknologi komputer dimana korban menderita kerugian dan pelaku dengan sengaja membuat atau bisa membuat keuntungan sendiri.
3. Penyalahgunaan komputer dianggap *illegal*, tidak etis atau perilaku tidak sah yang berkaitan dengan pemrosesan dan transisi data otomatis (Viswanathan, 2022:81).

Kejahatan adalah fenomena yang berkorelasi secara sosial. Tidak peduli berapa banyak setiap orang mencoba, namun setiap orang tidak dapat terhindari dari kejahatan dunia maya. Penting untuk memverifikasi semua faktor yang mempengaruhi dan berkontribusi terhadap kejahatan. Struktur sosial ekonomi dan politik masyarakat perlu dipahami kejahatan dan jalan lain yang dapat mengekang hal yang sama. Pencegahan dan langkah-langkah korektif diadopsi oleh mesin untuk mengendalikan kejahatan dan perilaku nakal dalam masyarakat juga dipertimbangkan sementara mempelajari sifat dan ruang lingkup kejahatan.

Kejahatan *cyber* telah menjadi perhatian utama di seluruh dunia dikarenakan fakta bahwa banyak perusahaan kehilangan miliar dollar setiap tahun dalam bisnis yang hilang, aset yang dicuri, dan reputasi yang

rusak akibat kejahatan *cyber*. *Cyber Crime* istilah dalam kejahatan komputer. Beberapa sarjana menyatakan istilah "*Computer Misuse*", "*Computer Abuse*", "*Computer Fraud*", "*Computer-related crime*", "*Computer-assisted crime*", atau "*Computer crime".* Namun, para sarjana saat itu lebih mengenal istilah "*computer crime*" karena memiliki makna luas dan digunakan secara internasional (Suhariyanto, 2013 : 9).

Menurut beberapa sarjana mendefinisikan secara luas *Comer* memberikan pengertian kejahatan komputer sebagai "Setiap perbuatan yang dilakukan dengan iktikad buruk guna tujuan keuangan yang melibatkan komputer". *The British Law Commission* "*computer fraud*" sebagai "manipulasi komputer dengan cara apapun yang dilakukan dengan iktikad buruk untuk memperoleh uang, barang atau keuntungan lain atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain. Menurut Mandell "*Computer Crime*" terbagi menjadi dua yakni:

1. Penggunaan komputer untuk melaksanakan perbuatan penipuan, pencurian atau menyembunyikan guna memperoleh keuntungan bisnis/kekayaan pribadi.
2. Ancaman terhadap komputer itu sendiri, semisal pencurian perangkat lunak, pemerasan, dan sabotase (Publitbang MA, 2004 : 10).

Departemen Kriminal Amerika merumuskan "*computer crime*" secara sempit, yaitu "setiap perbuatan melawan hukum dimana pengetahuan komputer diperlukan untuk pelaksanaan, penyidikan atau penuntutan". *Organization of European Community Development* merumuskan "*computer-related crime*" sebagai "*Any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Sedangkan Ulirch Sieber mendefinisikan kejahatan komputer adalah "penipuan dengan manipulasi komputer, spionase komputer dan pembajakan perangkat, sabotase komputer, pencurian waktu kerja komputer, memasuki sistem DP tanpa hak dan *hacking*, dan komputer sebagai alat untuk melakukan kejahatan tradisional" (Puslitbang MA, 2004: 11).

Ada beberapa klasifikasi "*Cybercrime*" sebagai berikut:

1. ***Cyberpiracy*** merupakan penggunaan teknologi komputer guna mencetak ulang *software* atau informasi dan mendistribusikan informasi atau *software* melalui jaringan komputer.
2. ***Cybertrespass*** yaitu penggunaan teknologi komputer guna meningkatkan akses pada sistem komputer dalam sebuah organisasi atau individu dan *website* yang diproteksi dengan *password*.
3. ***Cybervandalism*** adalah penggunaan teknologi komputer guna membuat program yang mengganggu proses transmisi informasi elektronik dan menghancurkan data di komputer (Riswandi, 2019 : 11).

Saat ini, efek *cybercrime* terorganisir telah dirasakan di seluruh dunia melalui *e-Commerce* dan sektor keuangan. Dimana akun pribadi dan layanan keuangan diakses oleh lebih banyak orang dari komputer, penyedia layanan dan penggunanya telah menjadi tujuan utama penipuan *online*. Gartner menunjukkan bahwa lebih dari 50% serangan *online* ditargetkan pada pengguna *e-Commerce* dan layanan keuangan. Hal ini memastikan bahwa orang masih menjadi mata rantai terlemah dalam rantai keamanan dan mengharapkan penipuan rekayasa sosial kriminal seperti *Phishing* dan *Distributed Denial of Service* yang telah mencapai tingkat kelicikan dan prevalensi baru. Dikarenakan industri keamanan gagal menciptakan solusi yang manjur untuk masalah ini, penipuan lebih inventif dan lebih baru menipu orang setiap hari untuk menangkap informasi pribadi dan keuangan.

Banyak peneliti telah mempelajari pengaruh *cybercrime* pada transaksi *e-commerce* dari perspektif yang berbeda. Henson meneliti sejauh mana rasa takut viktimisasi kejahatan dunia maya dan risiko yang dirasakan memengaruhi niat pelanggan untuk membeli menggunakan *platform* e-niaga. Menggunakan data yang dikumpulkan dari mahasiswa Universitas Cincinnati, penelitian tersebut menemukan bahwa sebagian besar responden penelitian merasa khawatir tentang ketakutan menjadi korban kejahatan dunia maya. Ketakutan tersebut mempengaruhi perilaku orang-orang menuju transisi *e-commerce.* Rofiq melakukan hal serupa investasi empiris efek penipuan *cyber* dan kepercayaan dengan pembelian *online* minat konsumen Indonesia. Menggunakan teori *Planned Behavior*,

hasil penelitian menunjukkan bahwa persepsi penipuan *cyber* memiliki efek negatif pada transaksi *e-commerce*. Studi lebih lanjut menunjukkan bahwa persepsi kejahatan dunia maya tidak hanya lazim di negara berkembang. Sebuah studi yang dilakukan oleh Bohme dan Moore menemukan bahwa persepsi kejahatan dunia maya mempengaruhi niat warga Eropa terlibat dalam transaksi jual-beli *online*, perbankan *online*, dan *platform* transaksi elektronik lainnya. Di sisi lain, orang yang belum pernah mendengar apapun tentang kejahatan dunia maya lebih bersedia menggunakan *online* dan teknologi elektronik untuk transaksi (Apau & Koranteng, 2019:231).

Cybercrime dilakukan oleh para penipu atau tindakan sengaja pengguna internet dan memanfaatkan ketersediaan dan kemudahan penggunaan internet. Hal ini menghadirkan ancaman integritas yang serius, kualitas dan keamanan sebagian besar organisasi sistem informasi dikompromikan. Dengan demikian, pengembangan mekanisme keamanan yang efektif menjadi sebuah prioritas. Kejahatan dunia maya melibatkan penggunaan sumber daya komputer untuk melakukan tindakan ilegal.

Ada beberapa model penipuan transaksi *e-commerce* sebagai berikut:

1. ***Phising*** merupakan perbuatan curang yang dilakukan dengan cara, *cybercrime* akan mengirimkan *file* via email berisikan *link* digital palsu. *Cybercrime* akan meyakinkan korban bahwa *link* tersebut asli milik perusahaan *e-commerce*, sehingga korban percaya dan mengisi biodata diri pada *link* yang tersedia. Teknik ini yang paling sering dipraktikkan dalam tindak kejahatan.
2. ***Pharming*** yakni perbuatan *cybercrime* dengan teknik mengelabui korban dengan menginstruksikan dari situs web asli ke situs palsu.
3. ***Pretexting*** adalah praktik kejahatan dengan meminta data pribadi korban mengatasnamakan perusahaan *e-commerce*.
4. ***Quid Pro Quo*** yaitu tindakan curang dengan bermodus hadiah uang *cash* atau barang berharga dengan syarat korban diwajibkan memberitahukan data pribadi.
5. **Menghubungi korban** adalah praktik kejahatan ini yang paling banyak terjadi dan berhasil membohongi korban. Caranya dengan menghubungi korban melalui telepon atau whatsapp secara langsung, kemudian mengakui dari perusahaan *e-commerce* dan akan

memberikan hadiah dengan syarat memberitahukan nomor rekening korban (Silalahi dkk, 2022 : 231).

Penipuan dalam *e-commerce* sering dijumpai termasuk di Indonesia. Tercatat YLKI mendata pengaduan *e-commerce* kategori 3 besar selama 5 tahun terakhir. Uang sudah diberikan kepada penjual, namun barang yang diterima oleh konsumen tidaklah sampai diterima. BPKN (Badan Perlindungan Konsumen Nasional) menerima pengaduan masyarakat 1.136 pada periode 2017-Februari 2023 (cnbc Indonesia). Kebocoran data *e-commerce* di Indonesia juga terjadi pada Tokopedia Mei 2022 sebanyak 91 juta data pengguna bocor dan dijual ke darkweb dengan harga 5.000 dollar kapan saja bebas unduh melalui internet (kompasiana). Indonesia mengalami serangan *cybercrime* terbanyak dengan Vietnam sebagai sasaran *hacker* Bernama ShinyHunters mengklaim 73,2 juta data dari 10 perusahaan digital. Akibat meningkat transaksi *e-commerce* baik selama pandemi dan *post*-pandemi, kejahatan siber terus meningkat di tanah air. Di tahun 2018, berdasarkan data *Global Cybersecurity Indeks* (GCI), Indonesia masuk peringkat ke-9 dalam perbuatan kejahatan dunia maya secara regional. Keamanan data yang dimiliki oleh beberapa perusahaan *e-commerce* dan digital di Indonesia dinilai masih minim yang berakibat kebocoran data terus terulang (Kompasiana).

Banyak faktor yang melatarbelakangi konsumen menjadi korban kejahatan *ecommerce*, yaitu:

1. **Pengetahuan konsumen yang minim**. Konsumen dituntut terus meningkatkan pemahaman tentang kegiatan transaksi perdagangan elektronik. Edukasi berupa sosialisasi dari pemerintah dan lembaga terkait menjadi suatu keharusan dilakukan guna masyarakat semakin paham penggunaan transaksi dagang *online* dan terhindar dari tindak kejahatan siber.
2. **Kebocoran data konsumen**. Kehati-hatian pengguna sebagai konsumen atas data pribadi dengan tidak memberikan data kepada siapapun. Begitu juga perusahaan *ecommerce* untuk meningkatkan sistem keamanan agar tidak mudah di bobol oleh pihak tidak bertanggung jawab.

3. **Konsumen tergiur hadiah palsu.** Tidak langsung percaya apa yang disampaikan oleh si penipu dengan akan memberikan hadiah yang menjanjikan kepada konsumen. Tingkat kecurigaan dan kehati-hatian konsumen sangat berguna dengan mencari tahu terlebih dahulu sistem pemberian hadiah yang benar kepada konsumen.
4. **Sistem keamanan dan kurang tegas kebijakan pemerintah.** Kebocoran data pada aplikasi perusahaan *marketplace* Tokopedia, potret nyata sistem keamanan *ecommerce* Indonesia masih belum aman. Sistem kebijakan yang longgar mengakibatkan para *cybercrime* dengan mudah mencuri data pengguna (Silalahi, 2022:230).

Guna terhindar dari penipuan *cybercrime*, ada beberapa hal yang dapat dilakukan oleh konsumen sebagai berikut:

1. Pilih platform *e-commerce* resmi yang telah terdaftar dan diawasi oleh OJK.
2. Perlu perhatikan dengan detil kode verifikasi terceklis benar.
3. Tidak membagikan kode verifikasi bersifat rahasia.
4. Setiap informasi dan proses transaksi wajib dibaca secara keseluruhan dan teliti oleh konsumen.
5. Mengedepankan iktikad baik saat transaksi *online*.
6. Membayar sesuai total belanja pada aplikasi.
7. Bijak dan hati-hati dalam merespon kasus penipuan.
8. Meng*update* pengetahuan berita modus siber terbaru.
9. Tidak langsung percaya dan teliti atas hadiah gratis yang ditawari oleh si penipu.
10. Mengutamakan kehati-hatian saat transaksi daring (Silalahi, 2022: 233).

D. RANGKUMAN MATERI

Sepak terjang *e-commerce* Indonesia diawali tahun 1999 yang mana forum KASKUS menjadi pelopor toko *online* di Indonesia yang dibangun oleh Andrew Darwis kemudian Bhinneka.com yang menjadi tempat transaksi dagang *online*. Perkembangan pesat *ecommerce* ditandai dengan ketertarikan masyarakat menggunakan teknologi internet. Pemerintah menyadari potensi dari transaksi dagang elektronik harus merumuskan

pengaturan hukum yang memadai seiring bermunculan perusahaan *start-up* di tahun 2005 hingga puncak terjadi di tahun 2015 (Mustajibah & Trilaksana, 2021 : 2).

Dalam arti luas, *electronic commerce* disingkat *E-commerce* adalah pertukaran informasi elektronik antara bisnis dan pelanggan. Hal ini dapat dilakukan melalui internet.

Dalam arti sempit, perdagangan elektronik adalah solusi kompleks yang menyediakan teknologi internet. Hal ini berarti bahwa banyak aplikasi dan penyedia layanan internet harus bekerja sama dengan sempurna sinkronisasi sebagai situs e-niaga yang dapat beroperasi. Perdagangan elektronik melibatkan penggunaan jaringan komputer untuk tujuan perdagangan. Transaksi *e-commerce* hingga saat ini belum memiliki pengertian yang sama, dikarenakan pengembangan *e-commerce* yang kian berkembang pesat, sehingga tidak dipungkiri setiap waktu *e-commerce* mengalami perubahan dan terbentuk sistem dagang elektronik baru. Namun, bukan berarti tidak ada pengertian yang seragam yang berakibat pada ketika ada sama sekali definisi *E-Commerce* (Riswandi, 2019 : 3).

Ada beberapa jenis transaksi jual beli daring diantaranya, *Business to business Ecommerce (B2B e-Commerce),* bentuk transaksi dagang yang melibatkan antar pebisnis *corporate* dan *Business to consumer*, transaksi jual-beli daring yang melibatkan pelaku usaha dan konsumen. Namun, secara *factual* model transaksi *e-commerce* memiliki banyak ragam, seperti hanya dari segi sifat *Business to Business*, model seperti ini sering dijumpai di era modern, *Business to Consumer*, yang mana konsumen menjual langsung ke konsumen, dan *Consumer to Business* yang mana individu menjual barang atau jasa kebutuhan organisasi (Riswandi, 2019:4).

UU ITE atau hukum siber memiliki peran sentral dalam sistem hukum negara secara komprehensif. Dengan kehadiran bentuk hukum baru sebagai akibat pengaruh perkembangan teknologi dan globalisasi pengayaan bidang-bidang hukum yang sifatnya sektoral. Hal ini tentu saja terobosan dalam dinamika hukum yang akan menjadi bagian dari sistem hukum nasional. Subekti menyatakan bahwa sistem termasuk susunan atau tatanan yang teratur, yang mana secara keseluruhan memiliki bagian-bagian yang saling terkait satu sama lain, yang merupakan hasil dari suatu pemikiran guna mencapai tujuan. UU ITE No.11/2008 yang sekarang

berubah menjadi UU No.19/2016 dan PP No.80/2019 “Penyelenggaraan Melalui Sistem Elektronik” yang mana pasal 28 ayat 1 UU ITE menyatakan “setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”. Pasal tersebut selaras dengan UU No.8/1999 “Perlindungan Konsumen”. UU dibuat oleh pemerintah Indonesia bertujuan agar masyarakat sadar dan mandiri sebagai konsumen untuk memproteksi diri sendiri serta menciptakan sistem perlindungan terhadap konsumen dengan memberikan kepastian hukum dan keterbukaan informasi.

Kejahatan adalah fenomena yang berkorelasi secara sosial. Tidak peduli berapa banyak setiap orang mencoba, namun setiap orang tidak dapat terhindari dari kejahatan dunia maya. Penting untuk memverifikasi semua faktor yang mempengaruhi dan berkontribusi terhadap kejahatan. Struktur sosial ekonomi dan politik masyarakat perlu dipahami kejahatan dan jalan lain yang dapat mengekang hal yang sama. pencegahan dan langkah-langkah korektif diadopsi oleh mesin untuk mengendalikan kejahatan dan perilaku nakal dalam masyarakat juga dipertimbangkan sementara mempelajari sifat dan ruang lingkup kejahatan.

Kejahatan *cyber* telah menjadi perhatian utama di seluruh dunia dikarenakan fakta bahwa banyak perusahaan kehilangan miliar dollar setiap tahun dalam bisnis yang hilang, aset yang dicuri, dan reputasi yang rusak akibat kejahatan *cyber*. *Cyber Crime* istilah dalam kejahatan komputer. Beberapa sarjana menyatakan istilah “*Computer Misuse*”, “*Computer Abuse*”, “*Computer Fraud*”, “*Computer-related crime*”, “*Computer-assisted crime*”, atau “*Computer crime”.* Namun, para sarjana saat itu lebih mengenal istilah “*computer crime*” karena memiliki makna luas dan digunakan secara internasional (Suhariyanto, 2013 : 9).

Ada beberapa model penipuan transaksi *e-commerce* sebagai berikut:

1. ***Phising*** merupakan perbuatan curang yang dilakukan dengan cara, *cybercrime* akan mengirimkan *file* via email berisikan *link* digital palsu. *Cybercrime* akan meyakinkan korban bahwa *link* tersebut asli milik perusahaan *e-commerce*, sehingga korban percaya dan mengisi biodata diri pada *link* yang tersedia. Teknik ini yang paling sering dipraktikkan dalam tindak kejahatan.

2. ***Pharming*** yakni perbuatan *cybercrime* dengan teknik mengelabui korban dengan menginstruksikan dari situs web asli ke situs palsu.
3. ***Pretexting*** adalah praktik kejahatan dengan meminta data pribadi korban mengatasnamakan perusahaan *e-commerce*.
4. ***Quid Pro Quo*** yaitu tindakan curang dengan bermodus hadiah uang *cash* atau barang berharga dengan syarat korban diwajibkan memberitahukan data pribadi.
5. **Menghubungi korban** adalah praktik kejahatan ini yang paling banyak terjadi dan berhasil membohongi korban. Caranya dengan menghubungi korban melalui telepon atau whatsapp secara langsung, kemudian mengakui dari perusahaan *e-commerce* dan akan memberikan hadiah dengan syarat memberitahukan nomor rekening korban (Silalahi dkk, 2022 : 231).

Guna terhindar dari penipuan *cybercrime*, ada beberapa hal yang dapat dilakukan oleh konsumen sebagai berikut:

1. Pilih *platform e-commerce* resmi yang telah terdaftar dan diawasi oleh OJK.
2. Perlu perhatikan dengan detil kode verifikasi terceklis benar.
3. Tidak membagikan kode verifikasi bersifat rahasia.
4. Setiap informasi dan proses transaksi wajib dibaca secara keseluruhan dan teliti oleh konsumen.
5. Mengedepankan iktikad baik saat transaksi *online*.
6. Membayar sesuai total belanja pada aplikasi.
7. Bijak dan hati-hati dalam merespon kasus penipuan.
8. Meng*update* pengetahuan berita modus siber terbaru.
9. Tidak langsung percaya dan teliti atas hadiah gratis yang ditawari oleh si penipu.
10. Mengutamakan kehati-hatian saat transaksi daring (Silalahi, 2022: 233).

TUGAS DAN EVALUASI

Jawablah soal di bawah ini dengan benar.

1. Bagaimana perkembangan *e-commerce* di Indonesia? Jelaskan?
2. Apa yang dimaksud dengan *cybercrime* dalam transaksi *e-commerce*? Jelaskan?
3. Bagaimana pemerintah Indonesia melindungi kegiatan transaksi *e-commerce* dari kejahatan siber? Jelaskan?
4. Sebutkan dan jelaskan model penipuan transaksi *e-commerce*?
5. Apa saja yang harus dilakukan agar terhindar dari penipuan kejahatan siber dalam transaksi *e-commerce*? Jelaskan?

DAFTAR PUSTAKA

Apau, Richard & Koranteng, Felix Nti. (2019). Impact of Cybercrime and Trust on the Use of Ecommerce Technologies : An Application of the Theory of Planned Behavior. International Journal of Cyber Criminology – ISSN: 0974–2891 July – December 2019. Vol. 13(2): 228–254. DOI: 10.5281/zenodo.3697886

Bestari, Novina Putri. (2023). Korban Penipuan E-Commerce RI makin Banyak, Cek Data Terbaru!. https://www.cnbcindonesia.com/tech/20230302140853-37-418315/korban-penipuan-ecommerce-ri-makin-banyak-cek-data-terbaru

Kompasiana. (2022). Cybercrime Kian Meningkat, Puluhan Juta Data E-Commerce Bocor di Internet. https://www.kompasiana.com/berlianarani/627be5128d947a295d47bc02/cybercri me-kian-meningkat-puluhan-juta-data-e-commerce-bocor-di-internet

Mustajibah, Tutik & Trilaksana, Agus. (2021). Dinamika E-Commerce di Indonesia Tahun 1999- 2015. Jurnal Avatara e-journal Pendidikan Sejarah. Vol. 10 No.3. https://ejournal.unesa.ac.id/index.php/avatara/article/view/40965

Puslitbang Hukum dan Peradilan Mahkamah Agung Ri. (2004). *Naskah Akademis Kejahatan Internet (Cyber Crimes)*. https://pagresik.go.id/images/NASKAH_AKADEMIS_MARI/01.-Kejahatan-Internet-Cyber- Crimes.pdf

Riswandi, Dedi. (2019). *Transaksi Online (E-Commerce) : Peluang dan Tantangan Dalam Perspektif Ekonomi Islam*. Jurnal Econetica. Vol. 1 No.1

Rohmah, Ratni Nur. 2022. Upaya Membangun Kesadaran Keamanan Siber pada Konsumen Ecommerce di Indonesia. Cendekia Niaga Journal of Trade Development and Studies. Vol.6 No.1. https://jurnal.kemendag.go.id/JCN/article/view/629

Saleh, Houssam et.al. (2017). *The Impact of Cyber Crime on E-Commerce*. International Journal of Intelligent Computing and Information Science. Vo. 1 No. 3. https://www.researchgate.net/publication/332419249_THE_IMPACT_OF_CYBER_CRIME_ON_E-COMMERCE

Saroha, Rashmi. (2014). Profiling a Cyber Criminal. International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 253-258. http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

Silalahi, Purnama Ramadani dkk. (2022). Analisis Keamanan Transaksi E-Commerce dalam Mencegah Penipuan Online. Profit: Jurnal Manajemen, Bisnis dan Akuntansi. Vo.1 No.4 h.224-235. https://journal.unimaramni. ac.id/index.php/profit/article/view/481/405

Suhariyanto, Budi. (2013). *Tindak Pidana Teknologi Informasi (cybercrime)*. Jakarta. PT. RajaGrafindo Persada.

Suyanto, M. (2003). Strategi Periklanan pada E-Commerce Perusahaan Top Dunia. Yogyakarta: penerbit Andi.

Tempo.Co. 2023. Bank Indonesia Proyeksikan Transaksi Uang Elektronik Mencapai Rp.495 Triliun. https://bisnis.tempo.co/read/1723295/bank-indonesia-proyeksikantransaksi-uang-elektronik-mencapai-rp-495-triliun

Viswanathan, Suresh T. (2022). The Indian Cyber Law With The Information Technology Act, 2000. New Delhi. Bharat Law House Pvt.Ltd. 3rd Edition

HUKUM *CYBER*

BAB 4: PERLINDUNGAN KEKAYAAN INTELEKTUAL DI DUNIA MAYA

La Ode Ali Mustafa, S.H., M.H

Fakultas Hukum Univ. Dayanu Ikhsanuddin Baubau

BAB 4

PERLINDUNGAN KEKAYAAN INTELEKTUAL DI DUNIA MAYA

A. PENDAHULUAN

Hak Kekayaan Intelektual (HaKI), merupakan hak eksklusif yang diberikan negara kepada seseorang, sekelompok orang, maupun lembaga untuk memegang kuasa dalam menggunakan dan mendapatkan manfaat dari kekayaan intelektual yang dimiliki atau diciptakan. Istilah HAKI merupakan terjemahan dari *Intellectual Property Right* (IPR), sebagaimana diatur dalam undang-undang Nomor 7 Tahun 1994 tentang pengesahan WTO (*Agreement Establishing The World Trade Organization*). Pengertian *Intellectual Property Right* sendiri adalah pemahaman mengenai hak atas kekayaan yang timbul dari kemampuan intelektual manusia, yang mempunyai hubungan dengan hak seseorang secara pribadi yaitu hak asasi manusia (*human right*) (Tomi Suryo, 2010;1). Jadi HaKI pada umumnya berhubungan dengan perlindungan penerapan ide dan informasi yang memiliki nilai jual. HakI merupakan kekayaan pribadi yang dapat dimiliki dan diperlakukan sama dengan bentuk-bentuk kekayaan lainnya.

Secara umum dapat dikatakan bahwa hak kekayaan intelektual yang merupakan terjemahan dari *Intelectual Property Right* sebenarnya adalah keberadaan hak-hak yang lahir atas perwujudan kreasi intelektual manusia yang mencakup rasa, karsa, dan cipta manusia. Jika dikaji lebih lanjut, sepatutnya yang dinamakan hasil intelektual juga tidak akan terlepas atau terkait erat dengan kebudayaan karena jika pembicaraan intelektual

cenderung melakukan pendekatan kepada individu manusianya, kebudayaan lebih menekankan kepada unsur kolektif masyarakatnya.

Secara garis besar, berdasarkan konvensi International yang menjadi induknya, Hak atas Kekayaan Intelektual (HAKI) dapat dikategorikan dalam dua lingkup besar, yakni Hak Cipta dan Hak-hak yang berkenan dengan Hak Cipta (*copyright* & *related rights*) yang berinduk kepada Konvensi Berne (*Berne Convention* 1886) tentang *Protektion for Literary And Artistic Works*, dan Hak Kekayaan Industrial (Industrial Property) yang berinduk kepada Konvensi Paris (*Paris Convention 1883*) yang melindungi hak-hak industrial meliputi: Paten, Merek, Desain Industri, Rahasia dagang, *Topography* Sirkit Listrik Terpadu dsbnya. (Edmon Makarim, 2005;285)

Karya cipta berwujud dalam bahasan bidang kekayaan intelektual yang dapat didaftarkan untuk memperoleh perlindungan hukum, yaitu seperti karya kesusastraan, artistik, ilmu pengetahuan (*scientific*), pertunjukan, kaset, penyiaran audio visual, penemuan ilmiah, desain industri, paten, merek dagang, nama usaha, dan lain sebagainya. Jadi pada prinsipnya HKI merupakan suatu hak kekayaan yang berada dalam ruang lingkup kehidupan manusia di bidang teknologi, ilmu pengetahuan, maupun seni dan sastra, sehingga pemilikannya bukan terhadap barangnya melainkan terhadap hasil kemampuan intelektual manusianya dan tentu harus berwujud. Pemerintah mempunyai kewajiban untuk melindungi secara hukum dari ide, gagasan dan informasi yang mempunyai nilai komersial atau nilai ekonomi yang telah dihasilkan oleh seseorang maupun kelompok tersebut. Hak kekayaan Intelektual (HKI) memberikan hak monopoli kepada pemilik hak dengan tetap menjunjung tinggi pembatasan-pembatasan yang mungkin diberlakukan berdasarkan peraturan perundang-undangan yang berlaku.

Secara filosofis tampaknya ada hal yang sangat esensial membedakan antara rezim hak cipta dengan rezim Hak Milik Industrial meskipun dalam perkembangannya seakan akan kedua bidang ini telah menjadi satu pembahasannya dalam TRIPs karena satu aspek dalam perdagangan.

Pada rezim hak cipta perlindungan terhadap karya-karya keilmuan dan kesusastraan tampaknya lebih mengarah kepada terbukanya ekspresi dari seseorang dalam menghasilkan suatu karya intelektual itu sendiri sehingga ia tidak mengarah kepada kepentingan industrinya, melainkan kepada

perlindungan kepentingan hukum pribadi dengan titik berat pada hak moral dan hak ekonomi. Edmon Makarim (2005;285) menyatakan agak kontroversi memang pendapat tersebut diatas karena kebanyakan orang mengatakan bahwa hak ekonomi dalam konteks ini sama dengan kepentingan *industry* terhadap suatu karya intelektual. Lebih lanjut Edmon Makarim, (2005;286) mengatakan hal ini sebenarnya jauh berbeda karena tidak selalu suatu kepentingan ekonomi dapat diartikan sama dengan kepentingan *industry*

Lebih lanjut, Edmon mengatakan sebagaimana yang telah diuraikan dalam bab terdahulu' "sehubungan dengan perkembangan teknologi digital, semua kreasi intelektual yang semula dibuat diatas kertas kemudian akan berubah wujud sebagai suatu informasi digital yang direpresentasikan dalam signal digital 0 dan 1 baik yang berbentuk teks, angka, garis, gambar, warna, maupun semua jenis karakter-karakter informasi lainnya

Seiring perkembangan teknologi orisinalitas suatu karya tidak lagi hanya dalam media kertas saja karena seseorang dapat saja menuangkan kreasi intelektualnya dalam bentuk digital atau elektronik secara langsung bukan dalam bentuk media yang konvensional terlebih dahulu sehingga sepatutnya para ahli hukum harus dapat membedakan yang mana isinya dan yang mana medianya. Yang perlu dipahami adalah bahwa informasi elektronik digital tersebut dapat dibedakan dalam dua hal yakni informasi yang hanya merupakan suatu himpunan data dan/atau desain informasi tertentu saja (contoh *database* dan data *massages*) dari program *computer*

Karya cipta berwujud dalam bahasan bidang kekayaan intelektual yang dapat didaftarkan untuk memperoleh perlindungan hukum, yaitu seperti karya kesusastraan, artistik, ilmu pengetahuan (*scientific*), pertunjukan, kaset, penyiaran audio visual, penemuan ilmiah, desain industri, paten, merek dagang, nama usaha, dan lain sebagainya. Jadi pada prinsipnya HKI merupakan suatu hak kekayaan yang berada dalam ruang lingkup kehidupan manusia di bidang teknologi, ilmu pengetahuan, maupun seni dan sastra, sehingga pemilikannya bukan terhadap barangnya melainkan terhadap hasil kemampuan intelektual manusianya dan tentu harus berwujud. Pemerintah mempunyai kewajiban untuk melindungi secara

hukum dari ide, gagasan dan informasi yang mempunyai nilai komersial atau nilai ekonomi yang telah dihasilkan oleh seseorang maupun kelompok tersebut. Hak kekayaan Intelektual (HKI) memberikan hak monopoli kepada pemilik hak dengan tetap menjunjung tinggi pembatasan-pembatasan yang mungkin diberlakukan berdasarkan peraturan perundang-undangan yang berlaku

Direktorat Jenderal Hak Kekayaan Intelektual Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia di dalam buku panduan HKI menjelaskan bahwa Hak Kekayaan Intelektual atau yang disingkat HKI atau akronim HaKI, adalah padanan kata yang biasa digunakan untuk Intellectual Property Rights (IPR), yakni hak yang timbul bagi hasil olah pikir otak yang menghasilkan suatu produk atau proses yang berguna untuk manusia. Pada intinya HKI adalah hak untuk untuk menikmati secara ekonomis hasil dari suatu kreativitas intelektual. Objek yang diatur dalam HKI adalah karya-karya yang timbul atau lahir karena kemampuan intelektual manusia (Edmon Makarim, 2005;286)

Istilah Hak Kekayaan Intelektual sebagai hak milik intelektual dan hak tak berwujud, pengertian Hak Kekayaan Intelektual merujuk pada hubungan proses berpikir manusia yang rasional bahwa kenyataan itu membutuhkan sebuah usaha.

Kekayaan Intelektual adalah hak yang dimiliki di bidang ilmu pengetahuan, seni, sastra, teknologi, bisnis dan industri sebagai hasil kreasi atau inovasi dari intelektualnya. Eddy Damian (1999;44) berpendapat bahwa Kekayaan Intelektual yang timbul dari kemampuan intelektual seseorang adalah bentuk perwujudan *alter ego* (refleksi kepribadiannya) atau kualitas rasa, karsa, dan cipta nalarnya. Pada umumnya, Kekayaan Intelektual merupakan hasil pemecahan atas masalah yang dihadapi oleh seseorang, yang sesuai dengan kodratnya akan terdorong untuk berpikir secara kreatif guna memecahkan suatu masalah yang dialaminya. Kreativitas tersebut selanjutnya memicu daya cipta untuk menghasilkan karya intelektual. (Direktorat Jenderal Kekayaan Intelektual, 2004; 5.) (diakses pada tanggal 24 Mei 2023)

RINCIAN PEMBAHASAN MATERI

B. RUANG LINGKUP HAK KEKAYAAN INTELEKTUAL

Di dalam ketentuan Pasal 2 Ayat 8 Konvensi Pendirian WIPO yang cakupan Hak Kekayaan Intelektual didefinisikan sebagai berikut: (Muhammad Akham Subroto dan Suprapedi, 2008; 15)

"Intellectual property shall incude the rights relating to:

a. *Literary, artistic and scientific works,*
b. *Performance of performing artists, phonograms, and broadcastas,*
c. *Inventions in all fields of human endeavour,*
d. *Scientific discoveries,*
e. *Industrial designs,*
f. *Trademarks, service marks, and commercial names and designations,*
g. *Protection against unfair competition,*
h. *And all other rights resulting from intel*

Secara umum, Hak Kekayaan Intelektual terbagi menjadi 2 (dua) bagian, yaitu: (Sahat Maruli T Situmeang", 2020;74)

a. Hak Cipta (*copyright*)

Perkembangan teknologi informasi dan komunikasi telah menjadi salah satu variabel dalam Undang-Undang tentang Hak Cipta ini, mengingat teknologi informasi dan komunikasi di satu sisi memiliki peran strategis dalam pengembangan Hak Cipta, tetapi di sisi lain juga menjadi alat untuk pelanggaran hukum di bidang ini. Pengaturan yang proporsional sangat diperlukan, agar fungsi positif dapat dioptimalkan dan dampak negatifnya dapat diminimalkan

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat

Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta: Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan

diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan

Pencipta, adalah seorang atau beberapa orang yang secara bersama-sama yang atas inspirasinya melahirkan suatu ciptaan berdasarkan kemampuan pikiran, imajinasi, kecekatan, keterampilan, dan keahlian yang dituangkan dalam bentuk yang khas dan bersifat pribadi.

Hak cipta adalah hak eksklusif bagi pencipta atau penerima hak untuk mengumumkan atau memperbanyak ciptaannya atau memberi izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan perundang-undangan yang berlaku. (Buku Panduan Hak Kekayaan Intelektual 2006;1)

- Perlindungan Hak Cipta.

Berdasarkan sistem perlindungan atas ciptaan menurut pendapat Ahmad M Ramli, 2004;72 -81) terkait perspektif *Cyber Law* dapat diuraikan hal-hal sebagai berikut;

a) Subyek Perlindungan

Pencipta adalah seorang atau beberapa orang yang secara sendiri-sendiri atau bersama-sama menghasilkan suatu ciptaan yang bersifat khas dan pribadi (Undang-Undang RI Nomor 28 Tahun 2014, Pasal 1 Angka 2. Kecuali terbukti sebaliknya, yang dianggap sebagai Pencipta, yaitu Orang yang namanya: a. disebut dalam Ciptaan; b. dinyatakan sebagai Pencipta pada suatu Ciptaan; c. disebutkan dalam surat pencatatan Ciptaan; dan/atau d. tercantum dalam daftar umum Ciptaan sebagai Pencipta

Dalam perspektif *Cyber Law*, pencipta atau pemegang hak cipta yaitu pihak yang melakukan *up load* (unggah) dan atau namanya dicantumkan dalam ciptaan yang diunggah tersebut, kecuali dibuktikan lain.

b) Obyek Perlindungan

Ciptaan yang dilindungi meliputi Ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra. Perincian secara lengkap tentang obyek hak cipta dapat dilihat dari ketentuan Pasal 40 Ayat (1) UUHC. Ciptaan berupa terjemahan, tafsir, saduran, bunga rampai, basis data, adaptasi, aransemen, modifikasi dan karya lain dari hasil transformasi dilindungi sebagai Ciptaan tersendiri dengan tidak mengurangi Hak Cipta atas Ciptaan asli. Pelindungan sebagaimana dimaksud, termasuk pelindungan

terhadap Ciptaan yang tidak atau belum dilakukan Pengumuman tetapi sudah diwujudkan dalam bentuk nyata yang memungkinkan Penggandaan Ciptaan tersebut. Dalam perspektif *Cyber Law*, maka ciptaan-ciptaan yang diunggah termasuk obyek yang dilindungi

c) Stelsel Pendaftaran

Pendaftaran Ciptaan dan produk Hak Terkait bukan merupakan syarat untuk mendapatkan Hak Cipta dan Hak Terkait. Ketentuan ini menjelaskan bahwa Hak Cipta menganut stelsel deklaratif,artinya pendaftaran tidak merupakan kewajiban, pemegang hak adalah yang menggunakan terlebih dahulu (*first to use*). Penerapan stelsel deklaratif dalam perspektif *Cyber* Law sangat bermanfaat untuk internet yang perlu serba praktis dan tanpa birokrasi yang berbelit

d) Jangka Waktu

UU Hak Cipta Tahun 2014 mengatur secara tegas masa berlakunya hak moral dan hak ekonomi. Masa berlakunya hak moral tercantum dalam Pasal 57 yang berbunyi:

(1) Hak moral Pencipta sebagaimana dimaksud dalam Pasal 5 Ayat (1) huruf a, huruf b, dan huruf e berlaku tanpa batas waktu.
(2) Hak moral Pencipta sebagaimana dimaksud dalam Pasal 5 Ayat (1) huruf c dan huruf d berlaku selama berlangsungnya jangka waktu Hak Cipta atas Ciptaan yang bersangkutan.

Dalam perspektif *Cyber Law* seharusnya mendapat pelindungan yang sama dalam media internet tetapi jangka waktu lima puluh tahun untuk pelindungan komputer agak berlebihan mengingat program komputer sangat cepat berubah (Ahmad M Ramli,2004; 81)

e) Pembatasan Hak Cipta

Pembatasan Hak Cipta sebagaimana diatur dalam Pasal 43 dimaksudkan sebagai Perbuatan yang tidak dianggap sebagai pelanggaran Hak Cipta meliputi:

1) Pengumuman, Pendistribusian, komunikasi, dan/atau Penggandaan lambang negara dan lagu kebangsaan menurut sifatnya yang asli;

2) Pengumuman, Pendistribusian,Komunikasi, dan/atau Penggandaan segala sesuatu yang dilaksanakan oleh atau atas nama pemerintah, kecuali dinyatakan dilindungi oleh peraturan perundang-undangan, pernyataan pada Ciptaan tersebut, atau ketika terhadap Ciptaan tersebut dilakukan Pengumuman, Pendistribusian, Komunikasi, dan/ atau Penggandaan;
3) Pengambilan berita aktual, baik seluruhnya maupun sebagian dari kantor berita, Lembaga Penyiaran, dan surat kabar atau sumber sejenis lainnya dengan ketentuan sumbernya harus disebutkan secara lengkap; atau
4) Pembuatan dan penyebarluasan konten Hak Cipta melalui media teknologi informasi dan komunikasi yang bersifat tidak komersial dan/atau menguntungkan Pencipta atau pihak terkait, atau Pencipta tersebut menyatakan tidak keberatan atas pembuatan dan penyebarluasan tersebut.
5) Penggandaan, Pengumuman, dan/atau Pendistribusian Potret Presiden, Wakil Presiden, mantan Presiden, mantan Wakil Presiden, Pahlawan Nasional, pimpinan lembaga negara, pimpinan kementerian/lembaga pemerintah *non* kementerian, dan/atau kepala daerah dengan memperhatikan martabat dan kewajaran sesuai dengan ketentuan peraturan perundang-undangan. Dalam perspektif *Cyber Law*, terdapat undang-undang yang terkait dengan ketentuan ini yaitu Pasal 27 UU ITE

f) Kepentingan pendidikan & penelitian, keamanan, hiburan.

Penggunaan, pengambilan, Penggandaan, dan/atau pengubahan suatu Ciptaan dan/atau produk Hak Terkait secara seluruh atau sebagian yang substansial tidak dianggap sebagai pelanggaran Hak Cipta jika sumbernya disebutkan atau dicantumkan secara lengkap untuk keperluan:

1) Pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah dengan tidak merugikan kepentingan yang wajar dari Pencipta atau Pemegang Hak Cipta;
2) Keamanan serta penyelenggaraan pemerintahan, legislatif, dan peradilan;

3) Ceramah yang hanya untuk tujuan pendidikan dan ilmu pengetahuan; atau
4) Pertunjukan atau pementasan yang tidak dipungut bayaran dengan ketentuan tidak merugikan kepentingan yang wajar dari Pencipta.

Perlindungan terhadap suatu ciptaan timbul secara otomatis sejak ciptaan itu diwujudkan dalam bentuk nyata. Pendaftaran ciptaan tidak merupakan suatu kewajiban untuk mendapatkan hak cipta. Namun demikian, pencipta maupun pemegang hak cipta yang mendaftarkan ciptaannya akan mendapat surat pendaftaran ciptaan yang dapat dijadikan sebagai alat bukti awal di Pengadilan apabila timbul sengketa di kemudian hari terhadap ciptaan tersebut

Perlindungan terhadap karya cipta diberikan terhadap hasil karya dibidang ilmu pengetahuan, seni dan sastra. Hal tersebut mencakup karya-karya buku, program *computer*, *pamphlet*, perwajahan, karya tulis, ceramah, pidato, kuliah, dan ciptaan lain yang sejenis.dll.

Perlindungan terhadap suatu ciptaan timbul secara otomatis sejak ciptaan itu diwujudkan dalam bentuk nyata. Pendaftaran ciptaan tidak merupakan suatu kewajiban untuk mendapatkan hak cipta. Namun demikian, pencipta maupun pemegang hak cipta yang mendaftarkan ciptaannya akan mendapat surat pendaftaran ciptaan yang dapat dijadikan sebagai alat bukti awal di pengadilan apabila timbul sengketa di kemudian hari terhadap ciptaan tersebut

Hak cipta memberikan jangka waktu perlindungan terhadap hasil karya atau ciptaan pencipta tersebut selama hidup pencipta dan akan terus berlangsung hingga lima puluh tahun setelah pencipta meninggal dunia.

Hasil karya atau ciptaan itu haruslah memenuhi minimum suatu kriteria orisinal atau asli, khusus dan merupakan hasil kreativitas. Kata orisinal disini bukan berarti suatu ciptaan tersebut harus baru atau unik, tetapi ciptaan tersebut haruslah berasal dari pemiliknya dan bukan tiruan serta bersifat khusus yang merupakan hasil kreativitas si pencipta.

Perlindungan hak cipta tidak diberikan kepada ide atau gagasan, karena karya cipta harus memiliki bentuk yang khas, bersifat pribadi dan menunjukkan keaslian sebagai ciptaan yang lahir berdasarkan kemampuan,

kreativitas atau keahlian, sehingga ciptaan itu dapat dilihat, dibaca atau didengar

b. Hak Milik Perindustrian, yang terdiri dari:

1) Paten (*Patent*)
   Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 14 Tahun 2001 tentang Paten: Paten adalah hak eksklusif yang diberikan negara kepada inventor atas hasil invensinya di bidang teknologi, yang untuk selama waktu tertentu melaksanakan sendiri invensinya tersebut atau memberikan persetujuannya kepada pihak lain untuk melaksanakannya.
2) Merek (*Trademark*)
   Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis:yang dimaksud dengan Merek adalah tanda yang dapat ditampilkan secara grafis berupa gambar, logo, nama, kata, huruf, angka susunan warna, dalam bentuk 2 (dua) dimensi dan/atau 3 (tiga) dimensi, suara, hologram, atau kombinasi dari 2 (dua) atau lebih unsur tersebut untuk membedakan barang dan/atau jasa yang diproduksi oleh orang atau badan hukum dalam kegiatan perdagangan barang dan/atau jasa.‖
3) Desain Industri (*Industrial Design*)
   Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 31 Tahun 2000 tentang Desain Industri: yang dimaksud dengan Desain industri adalah suatu kreasi tentang bentuk, konfigurasi, atau komposisi garis atau warna, atau berbentuk tiga dimensi atau dua dimensi yang memberikan kesan estetis dan dapat diwujudkan dalam pola tiga dimensi atau dua dimensi serta dapat dipakai untuk menghasilkan suatu produk, barang komoditas industri, atau kerajinan tangan.
4) Desain Tata Letak Sirkuit Terpadu
   Berdasarkan Pasal 1 Angka 1 dan 2 Undang-Undang Nomor 32 Tahun 2000 Tentang Desain Tata Letak Sirkuit Terpadu: yang dimaksud dengan Sirkuit terpadu adalah suatu produk dalam bentuk jadi atau setengah jadi, yang di dalamnya terdapat berbagai elemen, dan sekurang-kurangnya satu dari elemen tersebut adalah elemen aktif, yang sebagian atau seluruhnya saling berkaitan serta dibentuk secara

terpadu di dalam sebuah bahan semi konduktor yang dimaksudkan untuk menghasilkan fungsi elektronik

5) Perlindungan Varietas Tanaman
   Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 29 Tahun 2000 tentang Perlindungan Varietas Tanaman: yang dimaksud dengan Perlindungan Varietas Tanaman yang selanjutnya disingkat PVT adalah suatu perlindungan khusus yang diberikan negara, yang dalam hal ini diwakili oleh Pemerintah dan pelaksanaannya dilakukan oleh Kantor Perlindungan Varietas Tanaman, terhadap Varietas Tanaman yang dihasilkan oleh pemulia tanaman melalui kegiatan pemuliaan tanaman
6) Rahasia Dagang
   Menurut Pasal 1 Angka 1 Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang: yang dimaksud dengan Rahasia dagang adalah informasi yang tidak diketahui oleh umum di bidang teknologi dan/atau bisnis, mempunyai nilai ekonomi karena berguna dalam kegiatan usaha, dan dijaga kerahasiaannya oleh pemilik Rahasia Dagang

Disamping ruang lingkup tersebut diatas Hak Kekayaan Intelektual mencakup didalamnya yaitu hak milik dalam lingkup kehidupan manusia seperti teknologi, ilmu pengetahuan, ataupun sebuah seni dan juga sastra. Kepemilikan Hak Kekayaan Intelektual bukan tertetak pada sebuah barang yang dihasilkan melainkan terhadap hasil intelektual berupa ide atau pemikiran yang memiliki kekhasan.

Menurut W.R. Cornish, (Muhammad Djumhana R. Djubaedillah, 1997; 17) milik intelektual melindungi pemakaian ide dan informasi yang mempunyai nilai komersial atau nilai ekonomi.

Hak Kekayaan Intelektual baru ada jika kemampuan intelektual manusia itu membentuk sesuatu, baik itu yang bisa dilihat, didengar, dibaca, maupun digunakan dengan praktis

Dari uraian di atas maka dapat diketahui bahwa bentuk nyata dari karya intelektual tersebut bisa di bidang tata teknologi, ilmu pengetahuan ataupun seni dan sastra. Sebagai suatu hak milik yang timbul dari karya, karsa, cipta manusia atau dapat pula dikatakan sebagai hak yang timbul karena lahir dari kemampuan intelektualitas manusia, maka harus diakui

bahwa yang telah menciptakan tersebut boleh menguasainya untuk tujuan yang menguntungkannya. Kreasi sebagai milik berdasarkan postulat hak milik dalam arti seluas-luasnya yang juga meliputi milik yang tidak berwujud. Esensi terpenting dari setiap bagian Hak Kekayaan Intelektual yaitu adanya suatu ciptaan tertentu (*creation*).

Hak Kekayaan Intelektual, sebagai bagian dari hukum benda (hukum kekayaan), maka pada prinsipnya adalah pemiliknya bebas dalam berbuat apa saja sesuai dengan kehendaknya dan memberikan isi yang dikehendakinya sendiri pada hubungan hukumnya. Hanya di dalam perkembangan selanjutnya kebebasan itu mengalami perubahan. Misalnya terkait dengan adanya suatu pembatasan berupa adanya lisensi wajib, pengambilalihan oleh negara, ataupun kreasi dan penciptaan tidak boleh bertentangan dengan kesusilaan dan ketertiban umum (Sahat Maruli T. Situmeang,2020;78)

C. PENGATURAN PERATURAN PERUNDANG-UNDANGAN DAN KONVENSI-KONVENSI *INTERNATIONAL*

Pada saat ini Indonesia telah memiliki perangkat peraturan perundang-undangan di bidang hak kekayaan intelektual yang cukup memadai dan tidak bertentangan dengan ketentuan sebagaimana yang dipersyaratkan dalam Persetujuan TRIPS. Peraturan perundang-undangan dimaksud mencakup (Direktorat Jenderal Industri Kecil Menengah Departemen Perindustrian Republik Indonesia) " kebijakan pemerintah dalam Perlindungan haki dan liberalisasi perdagangan jasa profesi di bidang hukum."

a) Undang-undang No. 12 Tahun 1997 tentang Perubahan Undang-undang No. 6 Tahun 1982 tentang Hak Cipta sebagaimana telah diubah dengan Undang-undang No. 7 tahun 1987 (UU Hak Cipta); dalam waktu dekat, Undang-undang ini akan direvisi untuk mengakomodasikan perkembangan mutakhir dibidang hak cipta;
b) Undang-undang No. 29 Tahun 2000 tentang Perlindungan Varietas Tanaman;
c) Undang-undang No. 30 Tahun 2000 tentang Rahasia Dagang;
d) Undang-undang No. 31 Tahun 2000 tentang Desain Industri;

e) Undang-undang No. 32 Tahun 2000 tentang Desain Tata Letak Sirkuit Terpadu;
f) Undang-undang No. 14 Tahun 2001 tentang Paten (UU Paten); dan
g) Undang-undang No. 15 Tahun 2001 tentang Merek

a. Pengaturan Hukum Hak Kekayaan Intelektual dalam Hukum Internasional

Ketentuan hukum mengenai Hak Kekayaan Intelektual untuk pertama kalinya dilakukan di Venesia, yakni aturan Paten yang mulai berlaku pada tahun 1470. Upaya harmonisasi (penyelarasan aturan secara internasional) tentang Hak Kekayaan Intelektual pertama kali terjadi pada tahun 1883 dengan lahirnya Paris *Convention* (Haris Munandar dan Sally Sitanggang, 2008;.6)

Berikut ini berbagai instrumen hukum internasional yang mengatur tentang Hak Kekayaan Intelektual. Sejalan dengan perubahan berbagai undang-undang tersebut di atas, Indonesia juga telah meratifikasi 7 konvensi internasional di bidang hak kekayaan intelektual, yaitu sebagai berikut:

1) *Convention Establishing The World Intellectual Property Organization* (WIPO) diadakan di Stockholm tahun 1967, yang kemudian diratifikasi Indonesia melalui Keputusan Presiden Nomor 24 Tahun 1979 yang telah dirubah dengan Keputusan Presiden Nomor 15 Tahun 1997
2) *Paris Convention for The Protection of Industrial Property Rights* (*Paris Convention*) di bidang hak milik perindustrian ditandatangani di Paris pada tanggal 20 Maret 1883. Konvensi ini diratifikasi dengan Keputusan Presiden Nomor 15 Tahun 1997.
3) *Berne Convention for The Protection of Literary and Artistic Works* (*Berne Convention*) di bidang Hak Cipta, ditandatangani di Berne, 9 September 1986. Indonesia meratifikasi dengan dengan Keputusan Presiden Nomor 18 Tahun 1997.
4) *Agreement on Trade Related Aspects of Intellectual Property Rights* (TRIPs) yang mulai berlaku pada tanggal 1 Januari 1995.
5) *Agreement Establishing World Trade Organization* (WTO) yang diratifikasi dengan Undang-Undang Nomor 7 Tahun 1994.

6) *Trademark Law Treaty*, mengatur perlindungan terhadap Merek, disahkan di Genewa pada tanggal 27 Oktober 1997, diratifikasi Indonesia melalui Keputusan Presiden Nomor 17 Tahun 1997.
7) *Patent Cooperation Treaty* (PCT), yaitu perjanjian kerjasama di bidang Paten. Indonesia meratifikasinya dengan Keputusan Presiden Nomor 16 Tahun 1997.

b. Pengaturan Hukum Hak Kekayaan Intelektual dalam Hukum Positif di Indonesia

Sejarah lahirnya peraturan mengenai Hak Kekayaan Intelektual di Indonesia di mulai pada tahun 1953, dimana ada suatu Rancangan peraturan perundang-undangan di bidang Hak Kekayaan Intelektual yang memuat mengenai Paten dan kemudian pemerintah Indonesia melalui Menteri Kehakiman Republik Indonesia menerbitkan surat edaran Nomor: J. S. 5/41 tanggal 12 Agustus 1954 dan Nomor J.G. 1/2/17 tanggal 29 Oktober 1953 tentang Pendaftaran Sementara Paten, Kemudian pada tahun 1989 awal mula disahkannya Undang-Undang Nomor 6 Tahun 1989 tentang Paten, kemudian dilakukan amandemen pada tahun 1997 yang di ubah menjadi Undang-Undang Nomor 13 Tahun 1997 Tentang Paten, hal inilah yang menjadi tonggak lahirnya peraturan hukum nasional yang terkait dengan Hak Kekayaan Intelektual

Setelah mengalami beberapa perkembangan, maka peraturan perundang-undangan yang terkait dengan Hak Kekayaan Intelektual adalah sebagai berikut

1) Undang-Undang Nomor 29 Tahun 2000 tentang Perlindungan Varietas Tanaman;
2) Undang-Undang Nomor 30 Tahun 2000 tentang Rahasia Dagang;
3) Undang-Undang Nomor 31 Tahun 2000 tentang Desain Industri;
4) Undang-Undang Nomor 32 Tahun 2000 tentang Desain Tata Letak Sirkuit Terpadu;
5) Undang-Undang Nomor 14 Tahun 2001 tentang Paten;
6) Undang-Undang Nomor 8 Tahun 2014 tentang Hak Cipta;
7) Undang-Undang Nomor 20 Tahun 2016 tentang Merek dan Indikasi Geografis.

D. PERLINDUNGAN HAK KEKAYAAN INTELEKTUAL DALAM *CYBER LAW*

Negara hukum mempunyai beberapa ciri, antara lain adanya perlindungan Hak Asasi manusia, yaitu: ”Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia” (Undang-Undang Dasar Republik Indonesia Amandemen ke 4, Pasal 28C)

Pan Panhuys, *International Organization and Integration: A Collection of the Text odf Document Relating to the United Nation, its Related Agencies and Regional International, Cornelis van Vollenhoven, Leyden and the Europe Institute*, 1968, *page* 249 dalam Sudjana, “sistem perlindungan atas ciptaan berdasarkan undang-undang nomor 28 tahun 2014 tentang hak cipta dalam perspektif *cyber law*” Jurnal, hal 5 diakses pada tanggal 24 Mei 2023 . Perlindungan Kekayaan Intelektual secara universal tercantum dalam Pasal 27 *Declaration of Human Rights* (10 Desember 1948) berbunyi

a. *Everyone has the right freely to participate in the cultural life of community, to enjoy the arts and to share in scientific advancement and its benefits.*
b. *Everyone has the right to protection of moral and material interest resulting from any scientific, literary or artistic production of which he is the author*

Salah satu keterkaitan teknologi informasi yang saat ini menjadi perhatian adalah pengaruhnya terhadap eksistensi Hak Atas Kekayaan Intelektual (HAKI), di samping terhadap bidang-bidang lain seperti transaksi bisnis (elektronik), kegiatan *e-government*, dan lain-lain Kasus-kasus terkait dengan pelanggaran Hak Cipta dan Merek melalui sarana internet dan media komunikasi lainnya adalah contoh yang marak terjadi saat ini. Di samping itu pelanggaran hukum dalam transaksi elektronik juga merupakan fenomena yang sangat mengkhawatirkan mengingat tindakan *carding, hacking, cracking*, dan *cybersquating* telah menjadi bagian dari aktivitas internet yang telah menjadikan Indonesia disorot dunia *International*. *Cyber Crime* dilakukan oleh subjek yang menggunakan

sarana teknologi canggih dan sulit dilacak keberadaannya bahkan seringkali dilakukan dari luar teritori Indonesia atau sebaliknya, Sehingga menjadi persoalan yang seringkali sulit terpecahkan. (Sudjana,hal 10)

Dalam *Cyber Law*, Hak Kekayaan Intelektual memiliki kedudukan yang sangat khusus mengingat kegiatan dalam *cyber crime* sangat lekat dengan pemanfaatan teknologi informasi berbasis pada perlindungan rezim hukum Hak Cipta, Merek, Paten, Rahasia Dagang, Desain Industri dll. Seiring dengan perkembangan zaman yang ditandai dengan lahirnya aktivitas virtual dan internet, hukum mengenai Hak Kekayaan Intelektual mendapatkan tantangan baru. Permasalahan yang timbul saat ini mengenai perlindungan terhadap program *computer*, dan objek hak cipta lainnya yang ada dalam aktivitas siber.

Perlindungan Hak Kekayaan Intelektual dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang Informasi dan Transaksi Elektronik atau Undang Undang nomor 11 tahun 2008 atau UU ITE adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum.

Berikut ini adalah pasal pasal dari UU ITE yang mengatur terkait perlindungan hukum Hak Kekayaan Intelektual, diantaranya diatur dalam Bab VI Nama Domain, Hak Kekayaan Intelektual, Dan Perlindungan Hak Pribadi sebagai berikut:

Pasal 23 (1) Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama. (2) Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain. (3) Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud

Dalam penjelasan Pasal tersebut berbunyi: Pasal 23 Ayat (1) Nama Domain berupa alamat atau jati diri penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang perolehannya didasarkan pada prinsip pendaftar pertama (*first come first serve*). Prinsip pendaftar pertama berbeda antara ketentuan dalam Nama Domain dan dalam bidang hak

kekayaan intelektual karena tidak diperlukan pemeriksaan substantif, seperti pemeriksaan dalam pendaftaran merek dan paten. Ayat (2) Yang dimaksud dengan “melanggar hak Orang lain”, misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan nama sejenisnya yang pada intinya merugikan Orang lain. Ayat (3) Yang dimaksud dengan “penggunaan Nama Domain secara tanpa hak” adalah pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya, atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan konsumen.

Pasal 24 (1) Pengelola Nama Domain adalah Pemerintah dan/atau masyarakat. (2) Dalam hal terjadi perselisihan pengelolaan Nama Domain oleh masyarakat, Pemerintah berhak mengambil alih sementara pengelolaan Nama Domain yang diperselisihkan. (3) Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan. (4) Ketentuan lebih lanjut mengenai pengelolaan Nama Domain sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 25 berbunyi Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Dalam penjelasan Pasal 25 disebutkan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan

Pasal 26 (1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Dalam penjelasan Pasal 26 Ayat (1) berbunyi "Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*).

Hak pribadi mengandung pengertian sebagai berikut:

1) Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
2) Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
3) Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

Undang-undang Informasi dan Transaksi Elektronik (ITE) mengatur peraturan dan sangsi atas pelanggaran terhadap HKI yang salah satunya adalah hak cipta dengan perlindungan hak pribadi dan perlindungan terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual.

Perlindungan berdasarkan UU Nomor 19 tahun 2016 tentang ITE Pasal 40 (1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan peraturan perundang-undangan. (2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan peraturan perundang-undangan. (2a) Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan. (2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.

Nico Kansil, (Sudjana, hal 6) menjelaskan teori yang mendasari perlindungan hukum terhadap Kekayaan Intelektual yaitu:

1) Teori *Reward*, bahwa pencipta di bidang ilmu pengetahuan, seni dan sastra, serta penemu di bidang teknologi baru yang mengandung langkah inovatif serta dapat diterapkan dalam industri, diberikan suatu penghargaan dan pengakuan serta perlindungan atas keberhasilan upayanya dalam melahirkan ciptaan baru itu
2) Teori *Recovery*, bahwa atas usaha dari pencipta dan penemu yang telah mengeluarkan tenaga, pikiran, waktu dan biaya yang tidak sedikit jumlahnya, kepadanya diberikan hak eksklusif untuk mengeksploitasi KI guna meraih kembali yang telah dikeluarkannya;
3) Teori *Incentif*, bahwa insentif diberikan untuk merangsang kreativitas dan upaya menciptakan karya-karya baru di bidang teknologi;
4) Teori *Public Benefit*, bahwa Kekayaan Intelektual merupakan suatu alat untuk meraih dan mengembangkan ekonomi

Dalam undang undang hak cipta dengan jelas melarang setiap perbuatan yang bertentangan peraturan perundang-undangan

Setiap Orang dilarang melakukan Pengumuman, Pendistribusian, atau Komunikasi Ciptaan yang bertentangan dengan moral, agama, kesusilaan, ketertiban umum, atau pertahanan dan keamanan negara. (Undang-Undang Nomor 11 Tahun 2008, Pasal 50.)

Dalam perspektif *Cyber Law*, terdapat undang-undang yang terkait dengan ketentuan ini yaitu Pasal 27 UU ITE , yang berbunyi:

1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

4) Setiap Orang 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.

E. RANGKUMAN MATERI

Secara umum, Hak Kekayaan Intelektual terbagi menjadi 2 (dua) bagian, yaitu:

1. Hak Cipta (*copyright*)

Berdasarkan Pasal 1 angka 1 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta: Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan

2. Hak Milik Perindustrian, yang terdiri dari:

a. Paten (*Patent*)
b. Merek (*Trademark*)
c. Desain Industri (*Industrial Design*)
d. Desain Tata Letak Sirkuit Terpadu
e. Perlindungan Varietas Tanaman
f. Rahasia Dagang

Mengenai Pengaturan Haki Indonesia juga telah meratifikasi 7 konvensi internasional di bidang hak kekayaan intelektual, yaitu sebagai berikut:

1) *Convention Establishing The World Intellectual Property Organization* (WIPO) diadakan di Stockholm tahun 1967,
2) *Paris Convention for The Protection of Industrial Property Rights* (*Paris Convention* 20 Maret 1883)
3) *Berne Convention for The Protection of Literary and Artistic Works* (*Berne Convention* 9 September 1986.)
4) *Agreement on Trade Related Aspects of Intellectual Property Rights* (TRIPs1 Januari 1995.)
5) *Agreement Establishing World Trade Organization* (WTO)
6) *Trademark Law Treaty*, Genewa, 27 Oktober 1997,

7) *Patent Cooperation Treaty* (PCT).

Secara umum perlindungan HAKI di Dunia Maya dapat ditemukan dalam Amandemen UUD RI 1945 Negara hukum mempunyai beberapa ciri, antara lain adanya perlindungan Hak Asasi manusia, yaitu: ”Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia” (Undang-Undang Dasar Republik Indonesia Amandemen ke 4, Pasal 28C)

Perlindungan Hak Kekayaan Intelektual dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Bab VI Nama Domain, Hak Kekayaan Intelektual, Dan Perlindungan Hak Pribadi, Pasal 25 berbunyi Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Dalam penjelasan Pasal 25 disebutkan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan

TUGAS DAN EVALUASI

1. Apa yang dimaksud dengan Hak Kekayaan Intelektual
2. Sebutkan dua jenis HKI secara umum
3. Sebutkan peraturan hukum yang mengatur HKI baik Internasional dan sumber HKI dalam hukum Nasional Indonesia
4. Bagaimana Perlindungan HKI dalam dunia maya menurut *system* Hukum Nasional Indonesia
5. Mengapa HKI perlu dilindungi dengan peraturan perundang-undangan

DAFTAR PUSTAKA

Ahmad M Ramli, Cyber Law dan HAKI Dalam Sistem Hukum Indonesia, Refika Aditama, Bandung, 2004.

Danrivanto Budhijanto,2019. Cyber Law dan Revolusi Industri 4.0 Bandung, LogosPublishing

David I Bainbridge, *Computers and The Law,* Pitman Publishing, first edition, London, 1990.

Dikdik M.Arief Mansur,dan Elisatris Gultom, Cyber Law (Aspek Hukum teknologi Informasi) Rafika Aditama, Bandung, 2009 Cet 2

Direktorat Jenderal Hak Kekayaan Intelektual, 2013,Buku Panduan Hak Kekayaan Intelektual

Eddy Damian, Hukum Hak Cipta Menurut Beberapa Konvensi Internasional, Undang-Undang Hak Cipta 1997 dan Perlindungan Terhadap Buku serta Perjanjian , Alumni, Bandung, 1999.

Edmon Makarim, Pengantar Hukum telematikan, PT Raja Grafindo Persada, Jakarta, 2005

Haris Munandar dan Sally Sitanggang, 2008, Mengenal Hak Kekayaan Intelektual, Hak Cipta, Paten,Merek, dan Seluk-Beluknya, Erlangga,Jakarta

Hilary Pearson dan Clifford Miller, Commercial Exploitation of Intellectual Property, Blackstone Limited, London, 1990,

Ibrahim Fikma Edrisy. Pengantar Hukum Cyber, Sai Wawai Publishing, Lampung, 2019

John F William, A Manager's Guide to Patent, Trade Marks & Copyright, Kogan Page, first edition, London, 1986.

Locke, *Two Treatises of Government,* edited and introduced by Peter Laslett, 1988

Muhammad Akham Subroto dan Suprapedi, Pengenalan Hak Kekayaan Intelektual, Indeks, Jakarta, 2008,

Muhammad Djumhana & R. Djubaedillah, 1997, Hak Milik Intelektual (Sejarah, Teori dan Prakteknya di Indonesia), Bandung, Citra Aditya Bakti,

Nico Kansil, Perlindungan Hukum terhadap Kekayaan Intelektual , Makalah pada Seminar Nasional KI, UNDIP Semarang, tanggal 27 April 1993.(dalam Sudjana hal 6

Pan Panhuys, *International Organization and Integration: A Collection of the Text of Document Relating to the United Nation, its Related Agencies and Regional International*, Cornelis van Vollenhoven, Leyden and the Europe Institute, 1968.

Ranti Fauza Mayana, Perlindungan Desain Industri Di Indonesia dalam Era Perdagangan Bebas, Grasinsdo, Jakarta, 2004

Sahat Maruli T Situmeang" Cyeber Law,Cakra, Bandung, 2020

Sudjana, sistem perlindungan atas ciptaan berdasarkan undang-undang nomor 28 tahun 2014 tentang hak cipta dalam perspektif cyber law Jurnal, hal 5) diakses pada tanggal 24 Mei 2023

Tim Lindsey, dkk, Hak Kekayaan Intelektual Suatu Pengantar,Bandung, PT Alumni, 2013.

Tomi Suryo, Hak Kekayaan Intelektual (HKI) di Era Globalisasi, Sebuah Kajian Kontemporer, Graha Ilmu, Yogyakarta, 2010

HUKUM *CYBER*

BAB 5: KEBIJAKAN DAN REGULASI HUKUM *CYBER*

Dr. Margie Gladies Sopacua, S.H., M.H

Fakultas Hukum Universitas Pattimura

BAB 5

KEBIJAKAN DAN REGULASI HUKUM *CYBER*

A. PENDAHULUAN

Salah satu perkembangan teknologi yang sering digunakan dan dibutuhkan semua kalangan masyarakat adalah komputer. Dengan komputer seseorang dapat dengan mudah menyelesaikan pekerjaan, tetapi dengan adanya komputer seseorang menggunakannya pada hal-hal yang baik atau hal-hal yang buruk. Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user)* atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer (Agus, 2016)

Teknologi informasi diyakini membawa keuntungan dan kepentingan yang besar bagi negara-negara di dunia. Setidaknya ada 2 (dua) hal yang menjadikan teknologi informasi dianggap penting dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi itu, seperti komputer, modem, sarana untuk membangun jaringan internet dan sebagainya. Kedua, memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya (Raharjo, 2002).Perkembangan globalisasi dan teknologi informasi telah membawa perubahan besar dalam kehidupan

manusia. Teknologi Informasi menjadikan hubungan komunikasi antar manusia dan antar bangsa semakin mudah dan cepat tanpa dipengaruhi oleh ruang dan waktu. Globalisasi adalah suatu proses perubahan dinamika lingkungan global sebagai kelanjutan dari situasi yang pernah ada sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan saling ketergantungan, pengaburan terhadap batas-batas negara (*borderless*) (Scholte, 2017). Globalisasi telah menjadi pendorong terciptanya era perkembangan teknologi informasi. Kecepatan perkembangan teknologi informasi ini telah menyebar di seluruh negara-negara di dunia, mulai dari negara-negara maju seperti di daratan Eropa dan Amerika sampai ke negara-negara berkembang seperti di sebagian daratan Asia, Afrika, serta Amerika Latin telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing. Teknologi informasi memiliki kedudukan atau peran sangat penting dalam suatu negara, sehingga perkembangan teknologi mendapat tempat yang penting bagi kemajuan dan perkembangan negara yang bersangkutan (Wahyu Beny Mukti Setiyawan, 2020)

Walaupun demikian perkembangan teknologi informasi ibarat kata seperti pedang bermata dua, di satu sisi membawa dampak positif dan di sisi lain membawa dampak negatif. Perkembangan teknologi informasi telah mengakibatkan perubahan perilaku pada masyarakat. Selain itu, perkembangan teknologi informasi menjadikan dunia seakan tanpa batas (*borderless*) (Suhariyanto, 2013). *Cyber space* juga menjadi salah satu sumber dari berbagai ancaman kedaulatan suatu negara. Ancaman tersebut dapat bersumber dari pemerintahan, individu maupun pengusaha yang bertujuan memperoleh keuntungan sendiri. Dunia saat ini tidak lagi memandang militer sebagai satu-satunya potensi ancaman, melainkan mulai menaruh perhatian terhadap ancaman yang bersifat *non* militer, yakni salah satunya ancaman *cyber*. *Cyber space* dapat menjadi ancaman bagi suatu negara karena dapat digunakan untuk mencuri informasi, propaganda, provokasi, maupun serangan terhadap informasi di berbagai bidang seperti data perbankan, jaringan militer maupun sistem pertahanan negara. Tanpa adanya penguasaan atau pengawasan terhadap *cyber space* sangat mungkin terjadinya gangguan stabilitas keamanan dan pertahanan suatu Negara (Wahyu Beny Mukti Setiyawan, 2020)

"Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum *cyber*. Istilah "hukum *cyber*" diartikan dari kata *cyber law*. Saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. istilah lain yang digunakan adalah hukum dunia maya (*virtual word law*), hukum teknologi informasi (*law of information technology*)". "Istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual atau maya. Kemudian setelah itu, muncul istilah baru dari kejahatan komputer yaitu *Cyber crime*. *Cyber Crime* merupakan perkembangan dari *computer crime"*. "*Cyber crime* dan *cyber law* dimana kejahatan ini sudah melanggar hukum pidana. Dengan adanya kasus yang terjadi di dunia maya tersebut, telah banyak menjatuhkan korban, bukan hanya pada kalangan remaja namun disemua usia. Hal tersebut mengharuskan satuan kepolisian untuk segera bertindak dalam menangani kasus *cyber crime* (kejahatan dunia maya) yang cakupan kejahatannya sangat luas bahkan tidak terbatas" (Agus, 2016).

Secara umum yang dimaksud dengan kejahatan komputer atau kejahatan di dunia maya (*Cyber crime*) adalah: "upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa izin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut. "Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. "Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer *independen* atau *device.* Kejahatan yang berhubungan dengan komputer merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan peralatan komputer. Kejahatan tersebut dibedakan menjadi dua kategori yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *Cyber crime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer,

sedangkan *cyber crime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana *computer* (Sumarwani, 2014).

"Cyber crime sebagai suatu masalah bukanlah hal yang mudah untuk diselesaikan. Hal ini dikarenakan *cyber crime* sebagai suatu jenis kejahatan merupakan suatu tindakan yang dilakukan di dalam dunia yang tidak mengenal batas wilayah hukum dan kejahatan tersebut dapat terjadi tanpa perlu adanya suatu interaksi langsung antara pelaku dengan korbannya. Sehingga dapat dikatakan, bahwa ketika suatu kejahatan *cybe*r terjadi, maka semua orang dari berbagai negara yang dapat masuk ke dalam dunia *cyber* dapat terlibat di dalamnya, entah itu sebagai pelaku (secara langsung atau tidak langsung), korban, ataupun hanya sebagai saksi. Di Indonesia, masalah dari *cyber crime* juga bisa dikatakan mulai diperhatikan sebagai suatu masalah yang serius. Dengan masuknya Indonesia ke dalam era globalisasi, khususnya dalam hal hubungannya dengan dunia *cyber*, berbagai bidang kehidupan masyarakat Indonesia mulai mendapatkan pengaruh dari dunia *cyber* tersebut. Oleh karenanya tidaklah mengherankan bila mulai bermunculan kasus-kasus kejahatan yang berhubungan pula dengan dunia *cyber* tersebut. (Guntara, 2017).

Berdasarkan pengertian tentang *cyber crime* diatas maka dapat di dipahami bahwa *cyber crime* merupaka*n* salah satu bentuk kejahatan di bidang teknologi, dimana kejahatan atau tindak pidana tersebut dilakukan tanpa batas antara ruang dan waktu kejahatan atau tindak pidana itu terjadi.

B. KEBIJAKAN DAN REGULASI HUKUM *CYBER*

Perkembangan teknologi di bidang komputer dewasa ini melanda hampir seluruh belahan dunia, yang diakibatkan oleh pertumbuhan ekonomi yang tinggi di dunia dan menyebabkan perkembangan dalam dunia bisnis sudah makin mengglobal. Atas dasar tersebut, seiring dengan pesatnya perkembangan dibidang teknologi informatika, telah merubah paradigma dengan hadirnya *cyber space*, yang merupakan imbas dari jaringan komputer global, termasuk di dalamnya jaringan internet (Priyatno, 2018).

Pelaku *cyber* merupakan orang-orang yang mempunyai pengetahuan, keunggulan, kemahiran dan kecerdasan yang mampu dalam bidang komputer. Pelaku *cyber* biasanya menguasai dan mengerti bagaimana memprogramkan komputer secara canggih dan ahli, serta pelaku *cyber* dapat menganalisa cara kerja sistem yang terdapat pada *computer* tersebut dan pandai menganalisis sistem komputer yang ada dan kemudian para pelaku *cyber* melaksanakan tindak kejahatan tersebut.

Proses penyidikan kejahatan *cyber crime* sama dengan proses penyidikan kejahatan konvensional lainnya. Bedanya hanya dari segi proses penangkapan pelaku kejahatan beserta koordinasi dengan pihak-pihak tertentu. Terlihat bahwa penanganan tindak kejahatan *cyber crime* sedikit rumit dibandingkan kejahatan konvensional, sebab terlebih dahulu harus berkoordinasi dengan beberapa pihak tertentu untuk mendapatkan kepastian bahwa hal tersebut benar-benar merupakan tindak kejahatan pidana atau bukan. Sementara dalam menetapkan tersangka kejahatan *cyber crime*, memiliki tingkat kesulitan yang lebih rendah dibanding kejahatan konvensional, dengan melihat barang bukti berupa nomor *handphone* atau alamat sosial media yang dimiliki pelaku dan tentunya dengan barang bukti tersebut maka akan tertuju secara langsung kepada pihak yang melakukan tindakan kejahatan (Agus, 2016)

Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk (Gultom, 2005), antara lain:

1. "***Unauthorized Acces Computer System and Service***. Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya;"
2. "***Illegal Contents***. Merupakan kejahatan dengan menggunakan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum;"

3. "***Data Forgery***. Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet;"
4. "***Cyber Espionage***. Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran;"
5. "***Cyber Sabotage and Extortion***. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet; dan"
6. "***Offense Against Intellectual Property*.** Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contoh, peniruan tampilan pada web *page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan informasi rahasia dagang orang lain dan sebagainya."

Jenis-Jenis Kejahatan yang masuk ke dalam Tindak Pidana *cyber* (Ersya, 2017) diantaranya;

1. ***Cyber-Terorism***
   National Police Agency of Japan (NPA) mendefinisikan *Cyber Terrorism* sebagai *electronic attack through computer networks againt critical infrastructures that have potential critical effect on social and economic activites of the nation*
2. ***Cyber-Pornography***
   Penyebarluasan *obscene materials* termasuk *porno-graphy*, *indecent exposure*, dan *child pornography*
3. ***Cyber-Harassment***
   Pelecehan seksual melalui e-mail, *website*, atau *chatt* program;
4. ***Cyber-Stalking***
   Crimes of stalking melalui penggunaan komputer dan internet
5. ***Cyber Squatting***
   Diartikan sebagai mendapatkan, memperjualbelikan, atau menggunakan suatu nama domain dengan itikad tidak baik

6. ***Hacking***
   Penggunaan *Programming abilities* dengan maksud yang bertentangan dengan hukum;
7. ***Carding ("credit-card fraud")***
   Melibatkan berbagai macam aktivitas yang melibatkan kartu kredit, *Carding* muncul ketika seseorang yang bukan pemilik akun kartu kredit menggunakan kartu kredit tersebut secara melawan hukum;
8. ***Government and freelance spying*** **termasuk** ***corporateespionage***; dan ***Organized crime***
   Menggunakan internet untuk memfasilitasi kegiatan ilegal mereka (*smugling*, jual beli senjata, narkotika)
9. ***Academic cheating*** **dan** ***sicentific miscoduct*** untuk melakukan tindak pidana *plagiarism*

Kebijakan Regulasi dan Hukum *Cyber* dalam hukum Pidana Terhadap kejahatan Teknologi Informasi pada saat ini adalah Kebijakan dalam bentuk upaya untuk menyelamatkan dan menjaga berbagai informasi yang memerlukan suatu analisa yang memadai, berkaitan dengan segi filosofis, sosiologis, dan yuridis. Teknologi informasi dewasa ini sangat penting serta mempunya dampak terhadap kegiatan manusia oleh sebab itu itu diperlukan aturan-aturan khusus melalui pembentukan perundang-undangan yang bisa menanggulangi tindak pidana di bidang informasi dan teknologi .

"Barda Nawawi Arief menyatakan bahwa kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal *(criminal policy*) dengan menggunakan sarana hukum pidana (*penal*), dan oleh karena itu termasuk bagian dari "kebijakan hukum pidana" (*penal policy*), khususnya kebijakan formulasinya". Selanjutnya menurut Barda Nawawi Arief "kebijakan kriminalisasi bukan sekedar kebijakan menetapkan atau merumuskan atau memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan

formulasi atau legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu" (Arief, 2003).

Kebijakan kriminal digunakan sebagai salah satu alternatif dalam menyelesaikan kebijakan sosial. Penanggulangan masalah sosial dilakukan dengan penegakan hukum yang menjadi respon atas kejahatan yang dilakukan oleh masyarakat. Sebagai suatu respon atas kejahatan, kebijakan kriminal tersebut memiliki keterbatasan dalam menanggulangi kejahatan yang demikian luas dan kompleks, oleh sebab itu penanggulangan kejahatan dilakukan dengan sarana *penal* (penggunaan hukum pidana) dan diimbangi dengan sarana *non penal* (Arief, 2005). Dalam menanggulangi *cyber crime* maka diperlukan upaya komprehensif baik melalui hukum pidana maupun melalui saluran hukum pidana. Pencegahan dan penanggulangan kejahatan dilakukan dengan pendekatan integral antara kebijakan *penal* dengan kebijakan *non penal*. Kebijakan *penal* memiliki beberapa keterbatasan dan kelemahan yakni bersifat fragmatis, individualitik (*offender oriented*), lebih bersifat represif dan harus didukung dengan infrastruktur yang memerlukan biaya tinggi. Dengan demikian maka penanggulangan kejahatan lebih baik dilakukan dengan menggunakan kebijakan *non penal* yang bersifat *preventif* (Hatta, 2010).

"Kebijakan hukum pidana merupakan terjemahan langsung dari istilah *penal policy*, namun adakalanya istilah *penal policy* ini diterjemahkan pula dengan politik hukum pidana. Istilah *penal policy* ini mempunyai pengertian yang sama dengan istilah *criminal law policy* dan *strafrechtspolitiek* sehingga kedua istilah ini juga diterjemahkan dengan politik hukum pidana atau kebijakan hukum pidana, akan tetapi dari penjelasan sebelumnya bahwa istilah kebijakan diambil dari istilah *policy* dalam bahasa Inggris atau *Politiek* dalam bahasa Belanda" (Arief, 1996). "Kebijakan hukum pidana merupakan bagian dari politik kriminal, kebijakan sanksi/hukuman, kebijakan yudisial melalui sistem peradilan pidana, adanya penegakan hukum dan administrasi kebijakan pidana yang pada dasarnya merupakan upaya yang rasional untuk mencapai Kebijakan Sosial yakni tercapainya kesejahteraan sosial dan perlindungan kepada masyarakat yang tidak terlepas dari kebijakan legislasi yang mengkaji, merencanakan dan membuat produk-produk peraturan perundang-

undangan melalui proses penyusunan sehingga melahirkan kebijakan hukum yang yang diterima oleh masyarakat. Peraturan perundang-undangan yang berlaku mempunyai fungsi yaitu fungsi mengekspresikan nilai-nilai dan fungsi *instrument*" (Muladi, 2002)

Kita dapat melihat dari pengertian diatas bahwa kebijakan dalam menanggulangi kejahatan *cyber crime* dapat dilakukan dengan dua tahapan atau dua cara diantaranya yaitu

1. Kebijakan *Penal* dan;
2. Kebijakan *Non Penal*

Usaha untuk menanggulangi kejahatan, politik kriminal (Arief, 2002) dapat dijabarkan dalam berbagai bentuk, antara lain:

1. Penerapan hukum pidana (*criminal law application*);
2. Pencegahan tanpa pidana (*prevention without punishment*);dan
3. Mempengaruhi pandangan masyarakat mengenai kejahatan dan pemidanaan lewat *mass media* (*influencing views of society on crime andpunishment*)

Dua masalah sentral dalam kebijakan kriminal dengan menggunakan sarana *penal* (hukum pidana) ialah masalah penentuan (Arief, 2002):

1. Perbuatan apa yang seharusnya dijadikan tindak pidana, dan;
2. Sanksi apa yang sebaiknya digunakan atau dikenakan kepada si pelanggar.

Untuk menetapkan suatu perbuatan sebagai tindak kriminal, (Arief, 1996) maka perlu memperhatikan kriteria umum sebagai berikut:

1. Apakah perbuatan itu tidak disukai atau dibenci oleh masyarakat karena merugikan, atau dapat merugikan, mendatangkan korban atau dapat mendatangkan korban;
2. Apakah biaya mengkriminalisasi seimbang dengan hasilnya yang akan dicapai, artinya *cost* pembuatan undang-undang, pengawasan dan penegakan hukum, serta beban yang dipikul oleh korban, pelaku kejahatan itu sendiri harus seimbang dengan situasi tertib hukum yang akan dicapai

3. Apakah akan makin menambah beban aparat penegak hukum yang tidak seimbang atau nyata-nyata tidak dapat diemban oleh kemampuan yang dimilikinya; dan
4. Apakah perbuatan itu menghambat atau menghalangi cita-cita bangsa, sehingga merupakan bahaya bagi keseluruhan masyarakat

Politik hukum pidana dalam penanggulangan *cyber crime* melalui sarana *penal* perlu diimbangi dengan kebijakan *non penal*. Kebijakan *non penal* yang dapat dilakukan (Bunga, 2019) adalah sebagai berikut:

a. Menyusun kebijakan di luar hukum pidana yang mendukung upaya pencegahan *cyber crime*, seperti melalui kebijakan anti-kebencian, kebijakan anti-*bullying* dan kebijakan berinternet sehat melalui sistem pendidikan
b. Melakukan sosialisasi terhadap potensi kejahatan di dunia maya dengan mengedukasi masyarakat pengguna internet untuk tidak mencantumkan identitas pribadi, bertransaksi di tempat dengan fasilitas internet yang aman dan sebagainya
c. Membangun kerjasama dengan pihak swasta untuk membangun sistem keamanan di dunia maya; dan
d. Membentuk jaringan kelembagaan dalam mencegah *cybe crime* baik dalam tataran nasional maupun dalam tingkat internasional. Kerjasama internasional dalam penanggulangan *cyber crime* sangat diperlukan mengingat *cyber crime* merupakan kejahatan transnasional yang terorganisir

Regulasi Khusus di Bidang Teknologi Informasi dalam hukum *Cyber*, diantaranya yaitu

1. Ratifikasi Konvensi Dewan Eropa Tentang *Convention on Cyber Crime, Budhapest*, Hongaria 2001 oleh Indonesia

Dewan Eropa adalah salah satu organisasi supranasional di Eropa. Pada tahun 1985 dibentuk komite ahli *Europe Committee on Crime Problems* untuk mempertimbangkan berbagai masalah hukum yang ditimbulkan oleh kejahatan komputer. Konvensi Dewan Eropa tahun 2001 saat ini merupakan regulasi pertama yang mengatur tindak pidana siber dan menjadi pedoman dalam regulasi tindak pidana *cyber* dalam hukum

nasional. Oleh karena itu, Indonesia sebagai negara yang belum meratifikasi konvensi tersebut untuk kedepannya perlu adanya peratifikasian terhadap konvensi Dewan Eropa tahun 2001 ini. Alasannya ialah untuk memperkuat landasan hukum serta memperkuat berlakunya Undang-undang khusus tindak pidana siber terhadap pelaku kejahatan yang berada di luar negara Indonesia. Tentunya, ratifikasi ini nantinya harus sesuai dengan prosedur yang berlaku baik itu menurut hukum internasional (Konvensi Wina 1969) maupun menurut hukum nasional (pasal 11 UUD NKRI 1945) (Wahyu Beny Mukti Setiyawan, 2020)

2. Undang-undang tentang kejahatan *cyber*

Seiring dengan perkembangan zaman, dan dalam mengatur *cyber space* dan *cyber crime* telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam "Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas "Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi. Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di *cyber space*. Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang-Undang "Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan "Setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia" (Sari, 2021).

Disahkannya "UU ITE pada 21 April 2008 merupakan hukum *cyber* pertama di Indonesia yang pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mencegah terjadinya kejahatan berbasis teknologi informasi

serta melindungi masyarakat pengguna jasa yang menggunakan teknologi informasi dan komunikasi. UU ini terdiri dari 54 pasal yang terbagi menjadi 13 bab. Ketentuan yang mengatur rumusan terkait kriminalisasi perbuatan yang dikategorisasikan sebagai tindak pidana siber terdapat dalam Bab VII tentang Perbuatan yang Dilarang Pasal 27 sampai dengan Pasal 37 beserta sanksi pidananya dalam Bab XI tentang Ketentuan Pidana Pasal 45 sampai dengan Pasal 52". (Putra, 2014)

"Pasal 5 ayat (1) sampai dengan ayat (3)" menyatakan secara tegas bahwa penguatan tentang alat bukti elektronik ini sebagai alat bukti yang sah (Wahyu Beny Mukti Setiyawan, 2020) diantaranya;

a. "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah";
b. "Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia" dan
c. "Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini".

UU ITE ini lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, tidak lebih. Padahal siapa pun tahu bahwa dunia *cyber* (*cyber word*) lebih luas dari sekedar transaksi elektronik. Ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum termasuk dalam Undang-undang ITE seperti kelalaian atau khilaf. Undang-Undang ITE ini juga tidak mengatur kapan kadaluwarsa perbuatan pidana kejahatan *hacking* (Pahajow, 2016).

Maka dengan itu dalam hal melakukan pencegahan serta penanggulangan kejahatan *cybe*r, pemerintah Indonesia sudah mengundangkan suatu undang-undang. "Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik". Undang-undang tersebut merupakan dasar hukum untuk penanganan tindak pidana *cyber crime.*

C. RANGKUMAN MATERI

Perkembangan teknologi yang sering digunakan dan dibutuhkan semua kalangan masyarakat adalah komputer. Dengan komputer seseorang dapat dengan mudah menyelesaikan pekerjaan, tetapi dengan adanya komputer seseorang menggunakannya pada hal-hal yang baik atau hal-hal yang buruk. Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan, mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Kebijakan Regulasi dan Hukum *Cyber* dalam hukum Pidana Terhadap kejahatan Teknologi Informasi pada saat ini adalah Kebijakan dalam bentuk upaya untuk menyelamatkan dan menjaga berbagai informasi yang memerlukan suatu analisa yang memadai, berkaitan dengan segi filosofis, sosiologis, dan yuridis. Teknologi informasi dewasa ini sangat penting serta mempunya dampak terhadap kegiatan manusia oleh sebab itu itu diperlukan aturan-aturan khusus melalui pembentukan perundang-undangan yang bisa menanggulangi tindak pidana di bidang informasi dan teknologi. Dalam menanggulangi kejahatan *cyber crime* dapat dilakukan dengan dua tahapan atau dua cara diantaranya yaitu Kebijakan *Penal* dan; Kebijakan *Non Penal*. Regulasi Khusus di Bidang Teknologi Informasi dalam hukum *Cyber*, diantaranya yaitu

1. Ratifikasi Konvensi Dewan Eropa Tentang *Convention on Cyber Crime, Budhapest*, Hongaria 2001 oleh Indonesia. Dewan Eropa adalah salah satu organisasi supranasional di Eropa. Pada tahun 1985 dibentuk komite ahli *Europe Committee on Crime Problems* untuk mempertimbangkan berbagai masalah hukum yang ditimbulkan oleh kejahatan komputer. Konvensi Dewan Eropa tahun 2001 saat ini merupakan regulasi pertama yang mengatur tindak pidana siber dan menjadi pedoman dalam regulasi tindak pidana *cyber* dalam hukum nasional. Oleh karena itu, Indonesia sebagai negara yang belum meratifikasi konvensi tersebut untuk kedepannya perlu adanya peratifikasian terhadap konvensi Dewan Eropa tahun 2001 ini. Alasannya ialah untuk memperkuat landasan hukum serta memperkuat berlakunya Undang-undang khusus tindak pidana siber

terhadap pelaku kejahatan yang berada di luar negara Indonesia. Tentunya, ratifikasi ini nantinya harus sesuai dengan prosedur yang berlaku baik itu menurut hukum internasional (Konvensi Wina 1969) maupun menurut hukum nasional (pasal 11 UUD NKRI 1945) (Wahyu Beny Mukti Setiyawan, 2020)

2. Undang-undang tentang kejahatan *cyber*.
   Seiring dengan perkembangan zaman, dan dalam mengatur *cyber space* dan *cyber crime* telah terbit peraturan yang khusus mengatur tentang tindak pidana teknologi informasi yang tercantum dalam "Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas "Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE ini diharapkan dapat menjadi kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi. Secara sosiologis, masyarakat memang membutuhkan suatu peraturan tentang regulasi hukum yang konkrit tentang teknologi informasi yang sebelum dikeluarkannya UU ITE, peraturan yang ada hanya sebatas berhubungan dengan teknologi informasi, belum menjelaskan dengan secara langsung dan lebih konkrit. Dengan adanya UU ITE dimaksudkan untuk mengatur berbagai aktivitas masyarakat saat berinteraksi di *cyber space*. Selain memenuhi syarat sosiologis, UU ITE juga telah memenuhi syarat secara filosofis. Secara filosofis, lahirnya UU ITE ini didasarkan pada amanat yang terkandung dalam Pasal 28F Undang- Undang "Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan "Setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia" (Sari, 2021).

TUGAS DAN EVALUASI

1. Apakah yang dimaksud dengan *cyber crime* menurut Agus?
2. Menurut Gultom terdapat Beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini sebutkanlah!
3. Terdapat 10 jenis kejahatan yang masuk ke dalam Tindak Pidana *cyber* menurut Ersya, sebutkan dan jelaskan 5 kejahatan tersebut!
4. Politik hukum pidana dalam penanggulangan *cyber crime* melalui sarana *penal* perlu diimbangi dengan kebijakan *non penal*. Kebijakan *non penal* yang dapat dilakukan menurut pendapat Bunga terdapat 4 jelaskanlah!
5. Ada dua langkah Regulasi Khusus di Bidang Teknologi Informasi dalam hukum *Cyber*. Jelaskanlah dua langkah tersebut!

DAFTAR PUSTAKA

Agus, A. A. (2016). Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Supremasi*, *11*(1), 26. https://doi.org/https://doi.org/10.26858/supremasi.v11i1.3023

Arief, B. N. (1996). *Bunga Rampai Kebijakan Hukum Pidana*. PT. Citra Aditya Bakti.

Arief, B. N. (2002). *Bunga Rapai Kebijakan Hukum Pidana*. Citra Aditya Bakti.

Arief, B. N. (2003). *Kapita Selekta Hukum Pidana*. PT.Citra Aditya Bakti.

Arief, B. N. (2005). *Pembaharuan Hukum Pidana; Dalam Perpekstif Kajian Perbandingan*. Citra Aditya Bakti.

Bunga, D. (2019). Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. *Jurnal Legislasi Indonesia*, *16*(1), 1–15.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civil Education*, *1*(1), 60. https://doi.org/https://doi.org/10.24036/8851412020171112

Gultom, D. M. A. M. & E. (2005). *Cyber Law (Aspek Hukum Teknologi Informasi)*. PT. Refika Aditama.

Guntara, B. (2017). Legitimasi Penyebaran Informasi Yang Memiliki Muatan Penghinaan Dan/Atau Pencemaran Nama Baik Dalam Pasal 310 Kuhp Dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, *4*(2), 242.

Hatta. (2010). *Kebijakan Politik Kriminal; Penegakan Hukum dalam Rangka Penanggulan Kejahatan*. Pustaka Pelajar.

Muladi. (2002). *Kapita Selekta Hukum Sistem Peradilan Pidana*. Universitas Diponegoro.

Pahajow, A. A. J. (2016). Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia. *Jurnal Lex Crimen*, *5*(2), 97.

Priyatno, D. (2018). *Bunga Rampai Pembaharuan Hukum Pidana Indonesia*. Pustaka Reka Cipta.

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime Dalam Hukum Nasiona. *Jurnal Ilmu Hukum*, *5*(2), 105.

Raharjo, A. (2002). *Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknolog* (Cetakan I). PT Citra Aditya Bakti.

Sari, U. I. P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Mimbar Jurnal Hukum*, *2*(1).

Scholte, J. A. (2017). Globalization: A Critical Introduction, (London: Palgrave, 2000). Dalam Ineu Rahmawati, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan Dan Bela Negara*, *7*(2), 52.

Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (CyberCrime)*. PT Raja Grafindo Persada.

Sumarwani, S. (2014). Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum Volume*, *1*(3), 288.

Wahyu Beny Mukti Setiyawan, E. C. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal USM Law Review*, *3*(2), 272–295.

HUKUM *CYBER*

BAB 6: ASPEK HUKUM DALAM PENYEDIAAN LAYANAN INTERNET

Dr. Nanda Dwi Rizkia, S.H., M.H., M.Kn., M.A

Sekolah Tinggi Ilmu Hukum Dharma Andigha

BAB 6

ASPEK HUKUM DALAM PENYEDIAAN LAYANAN INTERNET

A. LATAR BELAKANG

Dalam berbisnis diperlukan produk yang berkualitas untuk dipasarkan sehingga dapat menguntungkan bagi perusahaan, hal ini sesuai dengan yang dikatakan Griffin dan Ebert bahwa definisi bisnis adalah suatu kegiatan menyediakan barang atau jasa yang dibutuhkan oleh pelanggan untuk mendapatkan laba. Pada era globalisasi ini, produk dan jasa yang bersaing dalam satu pasar semakin banyak dan beragam. Sehingga terjadilah persaingan antarprodusen untuk dapat memenuhi kebutuhan pelanggan serta memberikan kepuasan kepada pelanggan secara maksimal, karena pada dasarnya tujuan dari suatu bisnis salah satunya adalah untuk menciptakan rasa puas pada pelanggan. Salah satu tindakan untuk memuaskan pelanggan adalah dengan cara memberikan pelayanan kepada pelanggan dengan sebaik-baiknya. Terdapat beberapa hal yang dapat memberikan kepuasan pelanggan, menurut Kotler yaitu nilai total pelanggan yang terdiri dari nilai produk, nilai pelayanan, nilai personal, nilai *image* atau citra, dan total biaya pelanggan yang terdiri dari biaya moneter, biaya waktu, biaya tenaga, dan biaya pikiran. Jika perusahaan memberikan pelayanan yang baik kepada pelanggannya, maka akan menciptakan kepuasan bagi pelanggannya. Setelah pelanggan merasa puas dengan produk atau jasa yang diterimanya, pelanggan akan menilai

pelayanan yang telah diberikan oleh perusahaan tersebut dengan pelayanan di perusahaan lainnya.[1]

Apabila pelanggan merasa benar-benar puas, mereka akan melakukan pembelian ulang serta merekomendasikan produk tersebut kepada orang lain agar membeli di tempat yang sama. Oleh karena itu menurut Tjiptono (2015) perusahaan harus memiliki pelayanan yang prima untuk memuaskan pelanggan sehingga kesan yang baik akan tercipta dan tentunya akan menguntungkan bagi perusahaan kelak. Pelayanan berkualitas yang diberikan oleh perusahaan diperlukan untuk menarik keputusan pembelian dan mencapai tingkat kepuasan pelanggan. Peningkatan kualitas pelayanan yang dilakukan secara terus-menerus merupakan salah satu strategi yang dapat menguntungkan perusahaan penyedia jasa atau barang dan pelanggannya. Sehingga dari hal tersebut, dibutuhkan peningkatan teknik untuk menganalisis tingkat kepuasan pelanggan yang dapat dijadikan sebagai tolok ukur perusahaan dalam mengetahui kepuasan pelanggannya berada pada level yang mana. Kualitas pelayanan yang diberikan oleh perusahaan penyedia layanan atau barang, dapat menciptakan suatu persepsi positif dari pelanggan terhadap perusahaan penyedia jasa dan menghasilkan suatu kepuasan serta loyalitas dari pelanggan. PT Telekomunikasi Indonesia yang berfokus pada bidang *Telecommunication, Information, Media, Edutainment*, dan *Service* yang disingkat menjadi (*TIMES*) menyiapkan produk seperti Indihome dan Wifi.ID untuk memfasilitasi masyarakat digital. Pertumbuhan pengguna internet yang meningkat dari tahun 1998 sampai tahun 2017 pada gambar 1 mengharuskan PT Telekomunikasi Indonesia membuat produk yang menggunakan internet sebagai sarana berbagi informasi. Produk tersebut adalah Indihome yang diluncurkan pada tahun 2015 untuk menghadapi persaingan di dunia bisnis yang semakin meningkat.[2]

[1] Ayu Marluthy, Peran Kualitas Pelayanan Penyedia Internet Terhadap Kepuasan Pelanggan, Jurnal Riset Bisnis dan Investasi Vol. 5, No. 1, April 2019, hlm.2460-8211

[2] Yusuf Ilham, Analisis Pengaruh Kualitas Jaringan, Kualitas Pelayanan, Kualitats Informasi, Keamanan dan Privasi Penyedia Layanan Internet Terhadap Kepuasan Anggaran dan Dampak Pada Niat Pembeli Ulang, Diponegoro Journal of Managemen, Vol.9, No.4, 2020, hlm, 3

Tabel 1. *Market Share* Penyedia Internet Tahun 2016-2018

Merk	Market Share (%)			Kenaikan
	2016	2017	2018	(%)
Indihome	48,1%	50,3%	42,1%	6%
Biznet.Net	-	2,1%	6,4%	4,3%
First Media/ FastNet	18,6%	17,3%	22,4%	3,8%
Telkomnet Instant	4,7%	-	-	0%

Sumber: Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)

Gambar 1. Pertumbuhan Pengguna Internet di Indonesia

Produk Indihome meliputi layanan *tripleplay* (3P) yaitu paket layanan komunikasi dan data seperti telepon rumah (*Voice*), internet (*Internet on Fiber* atau *High Speed Internet*), dan layanan televisi interaktif (*Usee TV Cable*, IPTV). Berdasarkan data yang diperoleh dari www.topbrand-award.com tentang *market share* Indihome selama tiga tahun terakhir menunjukkan pelanggan yang memilih untuk menggunakan produk Indihome terlihat fluktuatif atau tidak stabil yaitu naik turun, hal ini dapat dilihat pada tabel 1 bahwa dari 48,1% tahun 2016 sempat naik menjadi 50,3% tahun 2017 tetapi pada tahun 2018 mengalami penurunan menjadi 42,1%. Sedangkan dibandingkan dengan pesaingnya yang lain seperti (*First Media*/FastNet, Biznet dan Telkomnet Instan) Indihome menguasai pangsa pasar layanan data dan TV berbayar selama tiga tahun terakhir. Data tersebut dapat memberitahukan bahwa secara umum Indihome belum bisa memenuhi harapan pelanggannya, karena penggunanya yang relatif naik turun dalam tiga tahun terakhir. Selain itu, pelanggan sering mengeluhkan kurangnya informasi yang disampaikan PT Telekomunikasi

Indonesia mengenai jumlah tagihan yang harus dibayarkan, sedangkan pelanggan yang baru saja berlangganan satu atau dua bulan sudah meminta untuk dicabut karena sering terjadi gangguan. Keluhan tersebut dapat dibuktikan pada gambar 2.[3]

Sumber: Twitter @TelkomCare

Gambar 2. Keluhan Pelanggan Indihome

PT Telekomunikasi Indonesia menyediakan Grapari Plasa Telkom untuk memenuhi kewajibannya melayani pelanggan yang memiliki keluhan atas salah satu produknya yaitu Indihome. Namun banyak keluhan yang disampaikan pelanggan seperti Indihome yang sering mengalami gangguan dan proses penanganan gangguannya pun membutuhkan waktu lama sehingga pelanggan banyak meminta cabut layanannya. Permintaan cabut Indihome yang sudah berlangganan tentunya akan merugikan perusahaan karena dari sisi pendapatan pun akan berkurang. Demi tercapainya kualitas pelayanan yang baik dan dapat memuaskan pelanggan sehingga mengurangi permintaan cabut, PT Telekomunikasi Indonesia Divisi Regional III Jawa Barat menyediakan pelayanan di Grapari Plasa Telkom Group yang ada di Jawa barat. Terdapat

[3] Alma, B. *Manajemen Pemasaran dan Pemasaran Jasa.* Bandung: CV. Alfabeta. 2004, hlm.21

11 Grapari Plasa Telkom Group yang tersebar di beberapa tempat di Jawa Barat seperti di Setiabudi, Supratman, Supratman, Rajawali, Cimahi, Karawang, Cirebon, Tasikmalaya, Sukabumi, Kuningan, dan Indramayu. Kesebelas plasa tersebut menangani pelayanan pasang baru, laporan gangguan, laporan keluhan, layanan informasi, pemintaan perubahan layanan, permintaan cabut, informasi tagihan, pembayaran di kasir, dan layanan *quick service* yang membutuhkan penanganan secara cepat atas keluhan yang disampaikan pelanggan. Grapari Plasa Supratman melayani informasi mengenai produk Indihome khususnya, pembayaran tagihan Indihome, menangani keluhan pelanggan mengenai gangguan serta melayani permintaan cabut Indihome dengan alasan seperti pindah alamat. Kualitas pelayanan yang diberikan PT Telekomunikasi Indonesia di Grapari Plasa Supratman sebaiknya dievaluasi agar dapat mengetahui sejauh mana pelanggan merasa puas. Dengan demikian, Grapari Plasa Supratman dapat meningkatkan kepuasan pelanggan atas kualitas layanan Indihome yang diberikan kepada pelanggan Indihome dan mengurangi permintaan cabut seperti yang diharapkan perusahaan.[4]

B. PENYEDIA LAYANAN INTERNET

Penyedia jasa layanan internet atau sering dikenal sebagai *Internet Service Provider* (ISP) adalah sebuah perusahaan dimana menawarkan sebuah jasa layanan kepada masyarakat supaya dapat tersambung atau terhubung dengan internet. Dengan adanya perusahaan penyedia jasa layanan internet tersebut, kita dapat terhubung ke internet dimana kita cukup menghubungkan ISP melalui modem atau yang sering didengar dengan kata Wi-Fi dengan komputer atau pc atau *gadget*. PIJI suatu singkatan dari Penyelenggara Jasa Internet atau nama lain dari ISP tersebut biasanya perusahaan-perusahaan telepon yang mana sebagai penyelenggara jasa internet tersebut. ISP sendiri memiliki jaringan secara domestik maupun secara internasional sehingga pelanggan dapat terhubung ke jaringan internet global. Hubungan tersebut biasanya dibagi menjadi dua kategori yaitu model *Dial-Up* dan juga jalur lebar. Hubungan

[4] Bobanto, W. Analisis Kualitas Layanan Jaringan Internet (Studi Kasus PT. Kawanua Internetindo Manado). Analisis Kualitas Layanan Jaringan Internet (Studi Kasus PT. Kawanua Internetindo Manado).2014, hlm.112

dial-up saat ini banyak yang ditawarkan secara gratis atau dengan harga yang murah serta dapat menggunakan kabel telepon biasa. Hubungan jalur lebar dapat berupa *non*-kabel, ISDN, kabel modem, DSL atau satelit. *Broadband* dibandingkan modem memiliki kecepatan yang lebih cepat biasanya namun biayanya juga lebih mahal. Beberapa ISP yang saat ini cukup banyak penggunanya antara lain IndiHome, Biznet, MNC Play Media, First Media, dan lain sebagainya. Biznet adalah sebuah operator telekomunikasi *fixed-line* dan operator multimedia di Indonesia yang menyediakan berupa layanan jaringan, layanan internet, pusat data, serta layanan *hosting* dan *cloud computing*. Biznet didirikan pada tahun 2000 dengan fokus pasar pada dunia korporat. Biznet juga memiliki dan mengoperasikan jaringan serat optik mutakhir dengan pusat data terbesar di Indonesia dan juga telah menyediakan layanan premium dengan performa jaringan yang cepat dan handal. IndiHOME atau kepanjangan dari Indonesia Digital HOME adalah salat satu produk layanan dari PT. Telkom Indonesia, dimana layanan tersebut berupa paket layanan komunikasi dan data seperti telepon rumah, internet, dan layanan televisi interaktif atau yang disebut sebagai Usee TV.[5]

Jadi IndiHOME tersebut bukan hanya layanan internet saja melainkan tiga layanan dalam satu paket. Produk IndiHOME tersebut diluncurkan untuk menggantikan paket internet *Speedy* yang dulu juga sebagai salah satu produk dari PT. Telkom Indonesia. Produk IndiHOME tersebut resmi diluncurkan oleh PT. Telkom Indonesia pada tahun 2015 dimana produk IndiHOME ini juga sebagai salah satu program dari proyek utama PT. Telkom. MNC *Play* atau sebelumnya bernama MNC *Play* Media adalah sebuah stasiun televisi kabel dan penyedia jasa internet berbasis serat optik milik perusahaan MNC Media. MNC *Play* tersebut didirikan pada bulan Januari tahun 2013 dibawah naungan MNC Kabel Mediacom yang merupakan bagian dari grup Media Nusantara Citra. MNC *Play* memiliki koneksi internet super cepat pertama di Indonesia yang memiliki kecepatan hingga 1000 Mbpsi dengan didukung jaringan berkapasitas 10 Gbps. PT. First Media Tbk yang mana sebelumnya bernama PT. *Broadband* Multimedia Tbk adalah suatu perusahaan publik di Indonesia yang

[5]Budi Sutedjo Dharma Oetomo, Perspektif eCommerce, Yogyakarta, Andi, 2001, hlm.19

terdaftar di BEI. *Broadband* Multimedia didirikan pada tahun 1994 dan mengganti namanya pada tahun 16 Juni 2007 menjadi First Media serta meluncurkan merek baru sebadai pentedia layanan "*Triple Play*". Perusahaan tersebut menyediakan jasa layanan internet pita lebar, televisi kabel dan komunikasi dan yang diperkenalkan sebagai "*Triple Play*".[6]

Tabel 1 TOP BRAND AWARD Dalam Kategori Penyedia Layanan Internet Tahun 2016-2019 Di Indonesia

	INTERNET SERVICE PROVIDER				
BRAND	**TBI 2016**	**TBI 2017**	**TBI 2018%**	**TBI 2019**	
Indihome	48.1%	50.3%	42.1%	39.8%	**TOP**
First Media/FastNet	18.6%	17.3%	22.4%	29.9%	**TOP**
Telkomnet Instant	4.7%	2.1%	6.4%	8.9%	

Sumber: Top Brand Award, 2019.

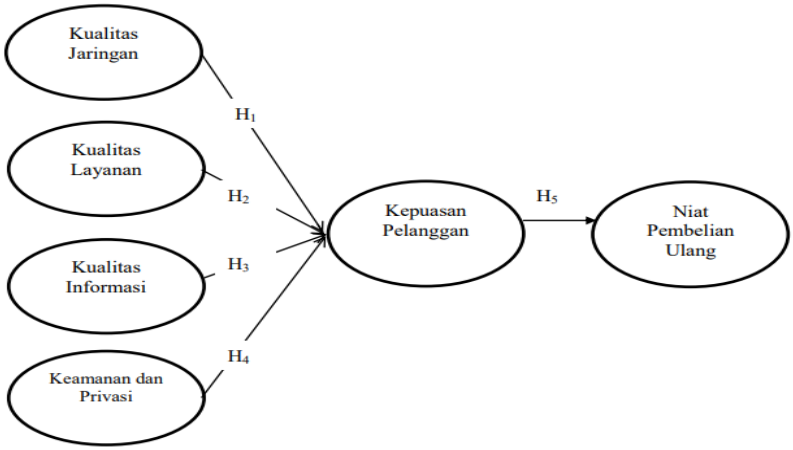
Berdasarkan Tabel 2 dapat disimpulkan bahwa para penyedia layanan internet masih perlu melakukan evaluasi dan peningkatan kepuasan pelanggan yang nantinya diharapkan dapat memenuhi kebutuhan konsumen dan mempengaruhi pelanggan untuk melakukan pembelian ulang pada penyedia layanan internet tersebut. Terdapat beberapa faktor yang dapat mempengaruhi kepuasan pelanggan agar dapat menumbuhkan niat pembelian ulang. Salah satunya yaitu suatu keadaan dimana seseorang merasa bahwa menggunakan layanan internet akan meningkatkan kinerja pekerjaannya.

Tabel 3 Data Keluhan Pengguna Jasa Penyedia Layanan Internet

No.	Masalah	Keterangan
1	Kualitas jaringan	Koneksi internet tidak lancar
2	Kualitas layanan	Pelayanan yang tidak sesuai harapan pelanggan
3	Kualitas informasi	Informasi yang diberikan tidak relevan
4	Keamanan dan privasi	Data konsumen disebarkan tanpa izin

[6] Ishaq, Dasar-Dasar Ilmu Hukum, Jakarta, Sinar Frafika, 2008, hlm.112

Berdasarkan tabel 3 di atas merupakan keluhan atau masalah-masalah yang ada dalam jasa penyedia layanan internet. Dengan adanya data di atas, para jasa penyedia layanan internet dapat melihat dari keluhan atau masalah-masalah yang ada agar dapat meningkatkan kualitas maupun melakukan perubahan. Tujuan dari penelitian ini adalah untuk menganalisis seberapa besar pengaruh faktor-faktor pada variabel yang diteliti terhadap kepuasan pelanggan serta dampak pada niat pembelian ulang.



Dimensi yang disebut sebagai "kualitas jaringan" telah diusulkan sebagai pendorong kualitas layanan keseluruhan di pasar layanan internet perumahan. Dimensi ini, yang terkait dengan kinerja layanan inti, memperhitungkan keandalan dalam industri layanan ini. Dalam industri telekomunikasi, kualitas jaringan mencakup kualitas dan kekuatan sinyal jaringan jumlah kesalahan, kecepatan mengunduh dan mengunggah. Ini berarti bahwa setiap terobosan dalam konektivitas internet dapat menyebabkan adanya kepuasan pelanggan. H1: Kualitas Jaringan berpengaruh positif terhadap kepuasan pelanggan pada penggunaan Jasa Penyedia Layanan Internet. Kualitas memberikan suatu dorongan kepada pelanggan untuk menjalin ikatan hubungan yang kuat dengan perusahaan. Dalam jangka panjang, ikatan seperti ini memungkinkan perusahaan untuk memahami dengan seksama harapan pelanggan serta kebutuhan mereka sehingga perusahaan dapat meningkatkan kepuasan pelanggan dengan

cara memaksimalkan pengalaman pelanggan yang menyenangkan dan meminimalkan atau meniadakan pengalaman pelanggan yang kurang menyenangkan. H2: Kualitas Layanan berpengaruh positif terhadap kepuasan pelanggan pada penggunaan Jasa Penyedia Layanan Internet.[7]

C. KUALITAS LAYANAN JASA AKSES INTERNET DI INDONESIA

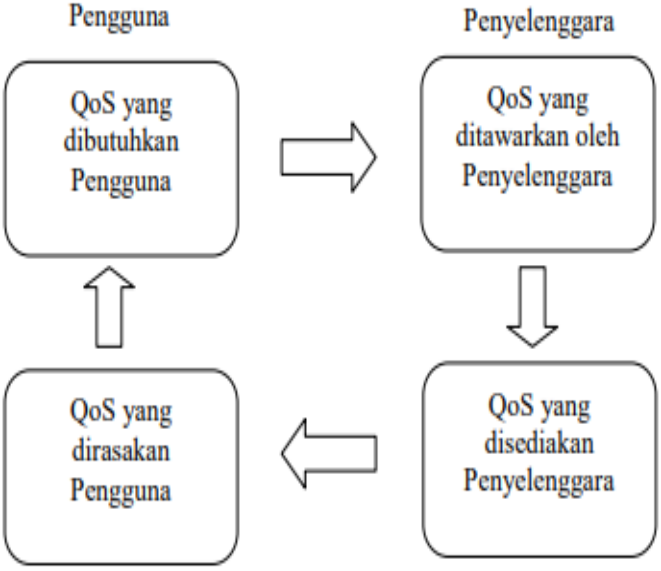
Jasa akses internet merupakan kegiatan penyediaan pelayanan dan penyelenggaraan telekomunikasi berbasis Internet Protokol yang dapat dimanfaatkan masyarakat untuk mengakses jaringan internet dengan menggunakan jaringan telekomunikasi. Berdasarkan Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi, diketahui bahwa bentuk penyelenggaraan telekomunikasi di Indonesia dapat dibedakan seperti pada Tabel 1. Menurut data Ditjen SDPPI, pada tahun 2011 terdapat 210 penyelenggara jasa akses internet (ISP) dan 49 jasa interkoneksi internet (NAP).

Tabel 4 Penyelenggaraan Telekomunikasi Di Indonesia

Jaringan telekomunikasi	Jaringan tetap	Jartap lokal
		Jartap SLJJ
		Jartap SLI
		Jartap tertutup
		Jartap mobilitas terbatas*
	Jaringan bergerak	Terestrial
		Seluler
		Satelit
Jasa telekomunikasi	Jasa teleponi dasar	
	Jasa nilai tambah teleponi	
	Jasa multimedia	Jasa akses internet (ISP)
		Jasa interkoneksi internet (NAP)
		Jasa internet teleponi
		Jasa sistem komunikasi data
Telekomunikasi khusus		

[7] Richardus Eko Indrajit, E-Commerce: Kiat dan Strategi Bisnis Di Dunia Maya, PT. Elex Media Komputindo, Jakarta, 2001, hlm.29

Kualitas layanan (*Quality of Service*) dalam hal jasa akses internet mengacu pada kemampuan dalam menjamin pengiriman arus data penting atau kumpulan dari berbagai kriteria performansi yang menentukan tingkat kepuasan penggunaan suatu layanan (Kamarullah, 2009). Menurut International Telecommunication Union (ITU), organisasi standarisasi telekomunikasi dunia, QoS didefinisikan sebagai "efek kolektif kinerja pelayanan yang menentukan tingkat kepuasan pengguna". Dengan demikian, untuk mendapatkan kepuasan pengguna internet, kriteria performansi layanan jasa akses internet tidak hanya dipengaruhi oleh kinerja jaringan semata, namun juga kinerja layanan dari penyedia jasa. Sejalan dengan hasil penelitian sebelumnya, penelitian ini akan melihat indikator Kinerja Layanan dan Kinerja Jaringan yang mempengaruhi tingkat kepuasan pengguna terhadap kualitas layanan jasa akses internet. Menurut ITU, QoS dapat dilihat dari 4 sudut pandang seperti terlihat pada Gambar 2.[8]



Gambar 2 Sudut pandang kualitas layanan (Sumber: Handbook QoS ITU)

[8] Abdul Halim Barkatullah dan Teguh Prasetyo, Bisnis E-Commerce: Studi Sistem Keamanan dan Hukum di Indonesia, Pustaka Pelajar, Yogyakarta, 2005

Tujuan akhir dari QoS adalah memberikan layanan jaringan (*network service*) yang lebih baik dan terencana dengan parameter-parameter tertentu (Ningsih dkk., 2004). Menurut Michael H. Desroches (2012) beragam parameter yang menunjukkan kinerja jaringan akses internet, seperti parameter *packet loss, throughput*, dan *latency. Packet loss* merupakan persentase rasio paket yang dikirim dari satu titik, titik A, dalam jaringan yang tidak mencapai tujuan yang dimaksud, titik B, dengan jumlah paket dikirim melalui interval waktu tertentu. Sementara *latency/delay* didefinisikan sebagai waktu yang dibutuhkan untuk sebuah paket untuk mencapai tujuan, karena adanya antrian yang panjang, atau mengambil rute yang lain untuk menghindari kemacetan. *Delay* dapat dicari dengan membagi antara panjang paket (L, *packet length* (bit/s)) dibagi dengan *link bandwith* (R, *link bandwith* (bit/s)). *Throughput* adalah kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan *bandwidth*. Nilai *throughput* didapat dari rasio jumlah data yang dikirim dengan waktu pengiriman data. Selain ketiga parameter tersebut, parameter lain yang menggambarkan kualitas jaringan tersebut yaitu utilisasi *bandwidth* dan ketersediaan jaringan (*network availability*). *Availability* menunjukkan sejauh mana suatu jaringan akses beroperasi dan tidak dalam keadaan kegagalan (*down*) setiap titik waktu, nilainya didapat dari [(*Total Operational minutes - Total minutes of service downtime*) / *Total operational minutes*] x 100% Level trafik yang dapat disediakan oleh penyedia kepada pengguna dipengaruhi oleh teknologi akses yang digunakan oleh pengguna. Teknologi jasa akses internet terbagi atas 3 kategori, sebagai berikut:[9]

1. *Leased line* yaitu sambungan berupa saluran telepon atau kabel fiber optik yang didirikan diantara pengguna dan penyelenggara jasa. Umumnya, *leased line* digunakan ketika terdapat kebutuhan komunikasi data jarak jauh yang harus dilakukan secara terus-menerus untuk menghubungkan satu lokasi ke lokasi lainnya. *Leased line* memiliki beberapa tingkatan tarif yang bergantung kepada lebar jalur data (*bandwidth*) yang mampu dikirimkan melalui *leased line* tersebut. Internet berkecepatan tinggi biasanya menggunakan saluran ini.

[9] Ahmad M Ramli, Cyber Law dan Haki dalam Sistem Hukum Indonesia, PT. Refika. 2004, hlm.12

2. *Dial-Up* merupakan layanan yang memberikan kemudahan kepada pelanggan untuk dapat mengakses internet menggunakan saluran telepon tetap atau telepon bergerak, dengan akses yang mendukung hingga 64 Kbps. Layanan ini memberikan kemudahan akses internet dimanapun berada.
3. Jasa akses *broadband* adalah layanan pita lebar yang mempunyai kapasitas *downstream* lebih dari 256 kbps, dengan media kabel ataupun nirkabel terrestrial. Berdasarkan karakteristik teknologi berbasis kabel dan teknologi nirkabel, dapat dibandingkan antara komunikasi *broadband* kabel dan *wireless*/nirkabel.

Selain pilihan teknologi akses, level trafik yang diberikan penyedia jasa juga dipengaruhi oleh pilihan paket/tarif dan *bandwidth* yang dilanggan. Ada 3 (tiga) macam pilihan paket yang biasanya disediakan, yaitu sistem kuota (*quota based*), sistem waktu pemakaian (*time based*), maupun tak terbatas (*unlimited*). Dengan sistem kuota artinya penggunaan internet dihitung berdasarkan besarnya data yang diakses (*upload* & *download*), sementara sistem *time based tariff* dihitung berdasarkan waktu pemakaian (misalnya 100 rupiah per menit), sedangkan sistem *unlimited* tidak dibatasi kuota dan waktu pemakaian. Banyak faktor yang mempengaruhi kualitas akses internet. Diantaranya kecenderungan penggunaan internet yang terus naik, sementara perbandingan jumlah pengguna dan penyelenggara jasa internet kurang seimbang. Selain itu terjadinya stagnansi dari jumlah *bandwidth* yang ada, sedangkan jumlah pengguna terus meningkat. Gejala lain menunjukkan adanya indikasi *bandwidth Throttling* (pengaturan besar-kecil "keran" *bandwith* secara sistematis) yang tentu melanggar prinsip *neutral network*. Kecepatan akses internet yang dirasakan oleh pengguna juga dapat dipengaruhi oleh hal-hal teknis lainnya selain pilihan paket dan teknologi akses yang digunakan, seperti: pilihan komputer, sistem komputer, dan aplikasi *browser*; kualitas sinyal saat mengakses secara *wireless*; jumlah pengguna yang mengakses satu server pada saat bersamaan; maupun letak server internet yang diakses. Keragaman faktor pengaruh tersebut menyebabkan penentuan dan pengukuran QoS internet seringkali ambigu dan diperdebatkan. Namun, para ahli menyimpulkan bahwa pengukuran dan

pencapaian QoS internet memungkinkan untuk dilakukan, namun dengan kompromi tertentu sebab tidak ada solusi yang sempurna. Bahkan, dapat dikatakan bahwa layanan yang ditawarkan sering kali tidak sesuai ekspektasi karena sejauh ini tidak ada jaminan dalam internet. Yang dapat dilakukan adalah menyediakan level trafik sebaik mungkin (*best effort*) dengan konsisten untuk pelanggan dan aplikasi yang berbeda. Kinerja jaringan yang terukur melalui QoS merupakan sistem arsitektur *end to end* dan bukan merupakan sebuah *feature* yang dimiliki oleh jaringan.[10]

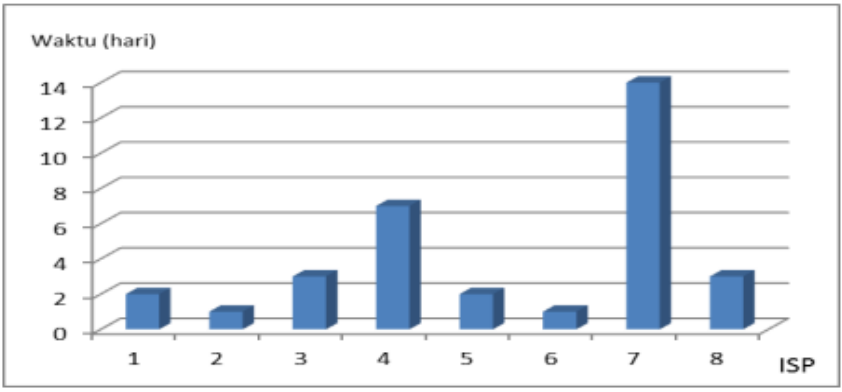
1. Kinerja Layanan

Parameter kinerja layanan akan dilihat dari indikator pemenuhan aktivasi pelanggan baru, pemulihan layanan, dan penanganan keluhan pelanggan seperti ditunjukkan pada data dibawah ini. Namun, dari tabulasi laporan 14 (empat belas) ISP sampel, hanya 6-8 ISP saja yang memberikan informasi lengkap tentang parameter kinerja layanan. Dari Tabel 2 terlihat kinerja layanan yang disediakan oleh penyelenggara dalam hal pemenuhan permohonan pelanggan untuk pasang baru koneksi internet terindikasi kurang maksimal. Data laporan dari 6 (enam) operator menunjukkan bahwa dalam kurun waktu 24 jam, baru dua operator yang mampu menyelesaikan sebagian besar permohonan pasang baru, dengan persentase sebesar 70% dan 80%. Sementara dalam kurun waktu 48 jam, hanya dua operator yang mampu menyelesaikan 90%-97,41% permohonan pasang baru pelanggan. Dua operator lainnya hanya mampu menangani 20%-50% permohonan pasang baru pelanggan dalam kurun waktu 2 hari. Bahkan, ada operator yang membutuhkan waktu sampai dengan 7 hari untuk menyelesaikan 100% permohonan pasang baru. Ada pula yang membutuhkan waktu lebih dari 7 hari, terlihat dari persentase permohonan yang berhasil diselesaikan dalam waktu 7 hari kurang dari 100%. Indikasi yang sama terlihat dari rata-rata waktu aktivasi pelanggan baru seperti ditunjukkan pada Gambar 3. Dari data laporan 8 (delapan) operator diketahui bahwa ada dua operator yang mengakui bahwa rata-rata waktu yang dibutuhkan untuk aktivasi pelanggan baru lebih dari 3 hari, yaitu 7 hari dan 14 hari. Hal ini tentu merugikan masyarakat yang perlu menunggu waktu lama untuk berlangganan internet. Dan pihak operator

[10] Endang Purwaningsih, Hukum Bisnis, Bab 4 –Transaksi E-Commerce, Ghalia Indonesia. 2010, hlm.21

perlu meningkatkan kinerjanya, terlebih jika pemerintah ingin menetapkan standar pemenuhan permohonan pasang baru selambat-lambatnya 3 (tiga) hari kerja terhitung sejak permohonan diterima. Menanggapi hal tersebut, menurut Bapak Benyamin Naibaho dari APJII ((28/06/2013), waktu yang dibutuhkan untuk instalasi pemasangan jaringan baru berbeda antara akses *wireless*, VSAT, maupun fiber optik. Tempat tinggal pelanggan pemohon pasang baru juga mempengaruhi waktu instalasi yang dibutuhkan, daerah diluar Jakarta membutuhkan waktu instalasi yang lebih lama dibanding Jakarta.[11]

ISP	Persentase permohonan pasang baru selesai dlm 24 jam	Persentase permohonan pasang baru selesai dlm 48 jam	Persentase permohonan pasang baru selesai dlm 7 hari
1	0%	97,41%	100%
2	0%	0%	100%
3	70%	90%	100%
4	80%	90%	100%
5	0%	20%	80%
6	0%	50%	100%



Gambar 3 Rata-rata waktu aktivasi pelanggan baru (sumber: data diolah)

[11] Lia Sautunninda, Jual Beli melalui Internet (E-Commerce) kajian menurut buku III KUH Perdata dan Undang-Undang informasi dan Elektronik, Fakultas Hukum Universitas Syiah Kuala, 2008, hlm,112

ISP	Persentase pemulihan layanan selesai dlm 24 jam	Persentase pemulihan layanan selesai dlm 48 jam
1	100%	100%
2	100%	100%
3	90%	100%
4	99%	100%
5	100%	100%
6	95%	100%

Sumber: data LKO 2011, diolah

Sumber: data LKO 2011, diolah Jika melihat data pada Tabel 3 dapat diketahui kinerja 6 (enam) operator penyelenggara jasa internet dalam hal mengatasi kerusakan jaringan atau memulihkan layanan. Dapat dikatakan bahwa dari aspek pemulihan layanan, kinerja operator tersebut terindikasi baik. Dalam kurun waktu 24 jam, persentase pemulihan layanan yang mampu diselesaikan mencapai lebih dari 90%, dan dalam waktu 48 jam, 100% permohonan pemulihan layanan pelanggan mampu diselesaikan. Jika dibandingkan dengan usulan pengaturan kualitas layanan yang disiapkan pemerintah, yaitu standar pemulihan layanan selambat-lambatnya 48 (empat puluh delapan) jam terhitung sejak waktu permohonan pemulihan layanan diterima, maka dari gambaran diatas dapat dikatakan bahwa dalam hal kinerja layanan, para penyelenggara jasa dapat memenuhi kriteria yang tersebut.

Tabel 4 Rata-Rata Waktu Untuk Mengatasi Keluhan Pelanggan

ISP	Rata-rata waktu untuk mengatasi keluhan pelanggan	Rata-rata waktu untuk memperbaiki kerusakan di pelanggan
1	30 menit	5 jam
2	1.5-2 menit	maks 1 hari
3	1 hari	1 hari
4	5 menit	120 menit
5	30 menit	60 menit
6	15 menit	60 menit
7	15 menit	30 menit
8	15 menit	60 menit

Sumber: data LKO 2011, diolah

Sejalan dengan data pada tabel sebelumnya, data pada Tabel 4 menunjukkan lebih detail rata-rata waktu yang dibutuhkan 8 (delapan) operator untuk memperbaiki kerusakan pelanggan (*Mean Time to Recovery*). Diketahui bahwa rata-rata waktu yang dibutuhkan berkisar antara 30 menit hingga maksimal 1 hari. Sementara rata-rata waktu untuk mengatasi keluhan pelanggan, artinya kecepatan *service agent* pihak operator untuk merespon keluhan pelanggan (*Mean Time to Response*), berkisar antara 5 menit hingga 1 hari. Kecepatan respon ini dipengaruhi oleh ragam keluhan pelanggan, serta media komunikasi yang dipakai, apakah melalui telepon, e-mail, atau surat tertulis. Menurut Bapak Benyamin Naibaho dari APJII ((28/06/2013), *Mean Time to Recovery* dipengaruhi pula oleh letak daerah layanan, misalnya untuk kerusakan di daerah Jakarta, operator membutuhkan waktu pemulihan layanan maksimum 6 jam, sementara untuk daerah diluar Jakarta, waktu yang dibutuhkan maksimum 24 jam. Artinya letak daerah layanan perlu dipertimbangkan untuk *men-set* batas maksimal *Mean Time to Recovery*. Demikian juga dengan *Mean Time to Response*, waktu untuk merespon keluhan pelanggan melalui telepon harusnya berkisar antara 5-15 menit.[12]

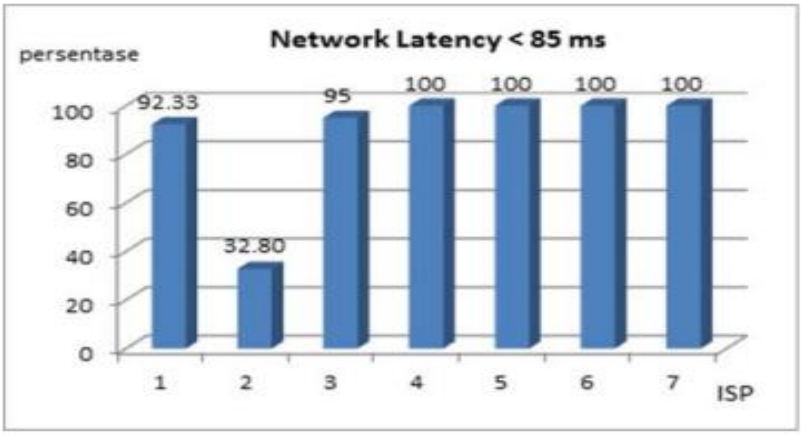
Artinya dalam waktu kurang dari 15 menit, keluhan pelanggan harus dijawab, walaupun belum sampai pada perbaikan, setidaknya telah diinvestigasi masalah yang terjadi. Sementara, respon keluhan pelanggan yang disampaikan melalui e-mail dapat dilayani dalam 30 menit, maksimal 24 jam sudah dijawab. Disamping *Mean Time to Recovery* dan *Mean Time to Response* yang bergantung pada kinerja *service agent* operator, sebenarnya yang paling penting adalah masalah *downtime performance* jaringan yang ditunjukkan oleh indikator *availability* (ketersediaan jaringan). Hal ini akan terlihat pada data Gambar 6 di bawah ini. Selain itu, menurutnya, kinerja layanan operator juga dipengaruhi oleh skala perusahaan, apakah kelas kecil, atau kelas besar. Untuk operator kelas besar, parameter yang wajib dimiliki seperti 24 jam x 7 hari *technical support center*, nomor pengaduan nasional yang dapat diakses 24 jam, dan *backup* sistem. Sehingga menurutnya, standar kualitas bagi operator,

[12] Onno W.Purbo, Aang Arif Wahyudi, Mengenal eCommerce, Jakarta, Elex Media Komputindo, 2001, hlm.17

ada parameter wajib dan ada parameter pengukuran/pengujian, ada parameter masalah layanan dan ada pula parameter masalah jaringan.

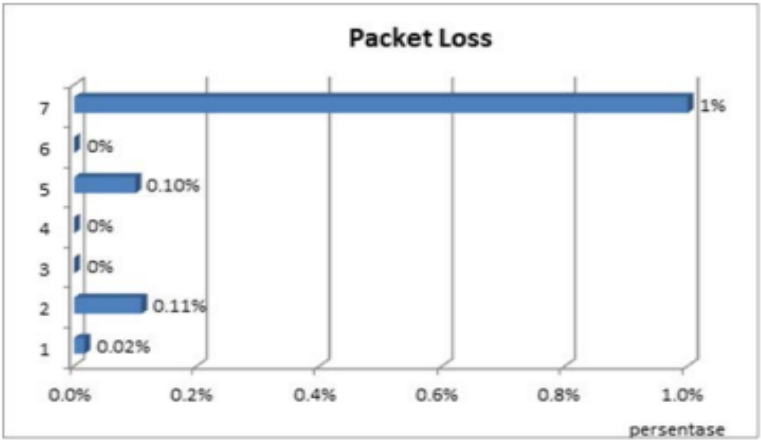
2. Kinerja Jaringan

Parameter kinerja jaringan akan dilihat dari indikator *Network latency*, utilisasi *bandwidth, throughput, packet loss*, ketersediaan layanan (*availability*), serta rata-rata waktu *downtime server* per bulan, seperti ditunjukkan pada data dibawah ini. Namun, dari tabulasi laporan 14 (empat belas) ISP sampel, hanya 7 (tujuh) ISP saja yang memberikan informasi lengkap tentang parameter kinerja jaringan.



Gambar 4. Network Latency < 85 ms (sumber : data diolah)

Dalam hal kinerja jaringan yang ditunjukkan oleh data pada Gambar 4 tentang *network latency* kurang dari 85 *milisecond* (ms), terlihat bahwa dari data laporan 7 (tujuh) ISP, 6 diantaranya telah memiliki kinerja baik, yang ditandai dengan lebih dari 90% performansi jaringan yang mampu disediakan memiliki toleransi *latency/delay* maksimal 85 *milisecond* (ms). Namun, tampak pula kinerja rendah dari satu operator dimana lebih dari 60% performansi jaringan sering mengalami *delay* lebih dari 85 *milisecond* (ms).



Dari data pada Gambar 5 tentang *packet loss* terlihat bahwa kinerja jaringan dari 7 (tujuh) ISP sudah baik, dimana semuanya menunjukkan performansi *packet loss* kurang dari 1%. Mengacu pada standar *international* versi TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*) seperti terlihat pada Tabel 5, maka data kinerja jaringan diatas yaitu *network latency* < 85 ms masuk dalam kategori 'sangat bagus'. Demikian juga untuk parameter *packet loss*, kinerja jaringan yang disediakan oleh penyelenggara jasa masuk dalam kategori 'sangat bagus.[13]

D. ASPEK HUKUM PENYEDIA LAYANAN INTERNET

Perkembangan dunia dewasa ini, khususnya kegiatan finansial, produksi, investasi dan perdagangan, mengalami perubahan yang sangat besar karena revolusi teknologi komunikasi dan informasi. Kini hampir setiap orang menggunakan alat-alat teknologi komunikasi dan informasi untuk menikmati keuntungan dan kemudahan melalui teknologi tersebut. Hal ini disebabkan oleh setiap negara yang berbeda sumber daya manusia,

[13] Emyana Ruth, Deskripsi Kualitas Layanan Jasa Akses Internet di Indonesia dari Sudut Pandang Penyelenggara Description of Internet Quality of Services (Qos) in Indonesia From the Providers' Point of View, Buletin Pos dan Telekomunikasi, Vol.11 No.2 Juni 2013, hlm.137-146

alam, iklim, letak geografis, sosial budaya dan perekonomiannya, sehingga produksi dan konsumsi masyarakatnya berbeda pula penggerakannya. Namun terkadang produksi suatu negara dipengaruhi keunggulan-keunggulan sumber daya manusia dan keunggulan teknologi. Hal ini menimbulkan hubungan perdagangan antarnegara untuk saling memenuhi kebutuhan dengan keunggulan masing-masing. Pada perkembangannya saat ini banyak kita temui jenis operator yang mewarnai jaringan telekomunikasi seluler berbasis GSM, yakni Telkomsel Indonesia Satelit, Tbk (Indosat), PT Telkomsel, Tbk (Telkomsel), PT. Exelcomindo Pratama (XL), Three, Hepi, Axis, Fren, Smart dan lainnya. Berbagai macam perusahaan *provider* mulai menggencarkan diferensiasi harga dari tarif hemat antar sesama pengguna. Sejalan dengan cepatnya perkembangan bidang teknologi, perusahaan semakin dipacu untuk menggunakan teknologi yang maju untuk tetap *survive* dan memenangkan persaingan yang semakin meningkat. Dampak pada aspek persaingan dalam memasarkan penggunaannya, sehingga menimbulkan kompetisi yang semakin tajam. Globalisasi ekonomi juga membuat perubahan menjadi konstan, pesat, radikal, serentak, dan *pervasive*. Perkembangan perekonomian dunia juga berkembang sangat pesat dan cepat akibat arus globalisasi dan perdagangan bebas juga disebabkan oleh kemajuan teknologi, telekomunikasi dan informasi telah memperluas ruang transaksi barang dan jasa yang ditawarkan menjadi lebih bervariasi, baik barang dan jasa produksi dalam negeri maupun produksi luar negeri. Kemajuan tersebut telah menghadirkan banyaknya fasilitas telekomunikasi dan canggihnya produk teknologi informasi yang mampu mengintegrasikan semua media informasi untuk mempermudah segala kegiatan manusia sehari-hari. Kecanggihan teknologi ini dapat diketahui dari teknologi informasi yang memudahkan orang untuk dapat mengetahui sesuatu hanya dengan melalui komputer yaitu menggunakan sarana internet. [14]

Tidak hanya untuk mengetahui informasi tetapi internet ini juga sudah menjadi sedemikian pentingnya karena membawa berbagai dampak pada berbagai segi kehidupan, yaitu pendidikan, kesehatan (*telemedicine*),

[14] Zahrotunnimah, Zahrotunnimah; Yunus, Nur Rohim; Susilowati, Ida. "Rekonstruksi Teori Komunikasi Politik Dalam Membangun Persepsi Publik," dalam Jurnal Staatsrecht: Indonesian Constitutional Law Journal, Volume 2, Nomor 2 (2018).

perdagangan (*e-commerce*) bahkan telah ada pula sektor pemerintahan yaitu *e-government*. Pelaksanaan *e-commerce* sebagai aplikasi banyak dilakukan oleh perusahaan *provider* yang membuat *Application Service Provider* (ASP) yang biasanya menjadi sarana utama bagi pelaku usaha di bidang ini. ASP menyediakan *disk space* untuk disewa pengusaha untuk menawarkan produksinya. *Disk space* tersebut tidak dapat dipergunakan tanpa dilengkapi dengan program tertentu (dalam bentuk *software*) sehingga *space* tersebut menjadi *website*. Pemilik ASP biasanya menyewakan *space* yang dimilikinya kepada perusahaan-perusahaan tertentu yang selanjutnya akan menggunakannya sebagai *website*-nya. Perusahaan yang menyewa *space* dimaksud kemudian mengisinya dengan perangkat lunak yang dapat diakses oleh para calon pembeli. Dari *website* tersebut maka perusahaan dimaksud menawarkan barang produksinya. Pelaksanaan penggunaan internet yang diakses melalui internet *service provider* untuk perdagangan elektronik (*e-commerce*) menawarkan model transaksi bisnis yang praktis, cepat, mudah dan murah di seluruh dunia sejak akhir abad 20. Sinergi komputer dan sistem telekomunikasi menciptakan manfaat baru berupa kemudahan, ketepatan, dan kecepatan miliaran transaksi per detik di seluruh dunia. Kinerja transaksi komersial semakin meningkat melalui *e-commerce* yang memiliki 3 (tiga) keunggulan khusus yakni "*accuracy, speed, and efficiency*". Hal ini dipastikan pelaksanaannya oleh perusahaan *provider* yaitu seperti Telkomsel, Indosat, dan lain-lain. Oleh karena itu transaksi para pihak ini juga didasarkan pada asas utamanya yaitu asas kebebasan berkontrak. Asas kebebasan berkontrak merupakan refleksi dari perkembangan paham pasar bebas yang dipelopori oleh Adam Smith. Penggunaan layanan internet, khususnya jaringan seluler yang berkembang dengan pesat saat ini memberikan kepuasan tersendiri bagi pengguna seluler pendukung layanan internet.

Dengan berkembangnya jaringan seluler juga memberikan peluang bagi para perusahaan *provider* untuk bersaing dalam membangun sebuah Internet Service *Provider* (ISP). Berbagai layanan yang dapat ditawarkan sehingga melahirkan kompetitor-kompetitor baru yang menyebabkan kian turunnya nilai pendapatan perusahaan per-konsumen (*Average Revenue Per User*). Dengan adanya hal ini, tidak diragukan lagi para penyedia

layanan tersebut dituntut dapat berupaya kreatif dan inovatif. Untuk dapat menjaga kelayakan layanan internet, penyedia *Internet Service Provider* (ISP) diupayakan dapat menyediakan *Quality of Service* (QoS) yang bagus pada trafik jaringannya. Dengan menyediakan *Quality of Service* (QoS) tersebut pada pelaksanaannya membutuhkan tolak ukur terhadap performansi jaringan seluler yang digunakan dengan beragam parameter jaringan, dengan standar yang dianggap berkualitas. Pada revolusi industri 4.0, banyak faktor yang dapat mempengaruhi kualitas jaringan (*network quality*) bagi penyedia *Internet Service Provider* (ISP). Salah satunya adalah turunnya nilai *throughput* dan menaikkan nilai *delay*, sehingga menurunkan kualitas layanan internet. Banyaknya *provider* (ISP) dapat menyebabkan meningkatkan besarnya *delay* jaringan dari banyaknya paket data yang menunggu atau mengantri untuk dapat dikirimkan. Banyaknya bangunan ataupun gedung dan dimana pemukiman tempat yang mengakses layanan internet juga dapat menyebabkan terganggunya proses propagasi gelombang atau yang biasa disebut redaman propagasi. Redaman propagasi menyebabkan adanya paket data yang hilang (*packet loss*) pada saat pentransmisian yang sangat berpengaruh terhadap besarnya nilai *throughput*. Peran perusahaan *provider* dalam menghadapi revolusi industri 4.0 pada pelaksanaan *e-commerce* di Indonesia juga patut diperhatikan. Hal ini dikarenakan perubahan dinamika laju pergerakan yang semula tersentralisasi bahwa manusia sebagai subyek yang vital dalam tumbuh dan berkembangnya denyut nadi perekonomian telah mengalami pergeseran secara perlahan, tapi pasti tergantikan oleh otomatisasi mekanis dan digitalisasi teknologi dalam menggerakkan roda perekonomian. Dasar perubahan ini sebenarnya adalah pemenuhan hasrat keinginan pemenuhan kebutuhan manusia secara cepat dan berkualitas. Revolusi Industri telah mengubah cara kerja manusia dari penggunaan manual menjadi otomatisasi atau digitalisasi.[15]

Inovasi menjadi kunci eksistensi dari perubahan itu sendiri. Selain itu perusahaan *provider* dalam kompetisi global harus mempersiapkan mental dan *skill* yang mempunyai keunggulan persaingan (*competitive advantage*)

[15] Joshua Sitompul. Cyberspace, Cybercrimes, Cyberlaw. Jakarta: Tatanusa, 2012. hlm.28

dari lainnya. Dalam perkembangan revolusi industri 4.0 patut memberikan kepastian hukum yang tepat dalam penggunaannya karena gelombang internet tersebut dapat saling bertabrakan dan bermasalah sehingga hal layanan ISP tidak terlaksana dengan baik di masyarakat sehingga pelaksanaan perdagangan *ecommerce* dapat dilakukan dengan baik untuk perkembangan perekonomian tersebut.

E. REVOLUSI INDUSTRI 4.0

Dengan lahirnya teknologi digital saat ini pada revolusi industri 4.0 berdampak terhadap kehidupan manusia diseluruh dunia. Revolusi industri 4.0 semua proses dilakukan secara sistem otomatisasi didalam semua proses aktivitasi, dimana perkembangan teknologi internet semakin berkembang tidak hanya menghubungkan manusia seluruh dunia namun juga menjadi suatu basis bagi proses transaksi perdagangan dan transportasi secara *online* yang dilaksanakan perusahaan *provider*. Hal ini tampak dalam teknologi yang semakin berkembang banyak sekali munculnya bisnis transportasi *online* seperti Go-Jek, Uber dan Grab, dimana menunjukkan integrasi aktivitas manusia dengan teknologi informasi, sehingga mengakibatkan pertumbuhan ekonomi semakin meningkat. Di era revolusi industri 4.0 transportasi yang bersifat konvensional tidak pernah diprediksi bahwa model ini transportasi konvensional ini yang dahulu banyak digunakan oleh masyarakat untuk kepentingan mobilitas manusia, namun pada era revolusi industri 4.0 model transportasi konvensional ini sudah sedikit digunakan oleh masyarakat, dimana dapat terlihat antara taksi konvensional versi taksi *online* atau ojek pangkalan dengan ojek *online*, dengan perkembangan teknologi yang semakin berkembang secara pesat model transportasi konvensional model transportasi yang memanfaatkan dengan sistem aplikasi berbasis internet menjadi alat transportasi yang dimanfaatkan masyarakat untuk kepentingan mobilitas manusia, dampaknya publik menjadi lebih mudah mendapatkan layanan transportasi dan bahkan dengan harga yang sangat terjangkau. Selain transportasi yang memanfaatkan teknologi informasi dengan memanfaatkan sistem aplikasi berbasis internet menjadi model transportasi yang dipilih oleh masyarakat, tidak sebatas sebagai transportasi *online* namun berkembang menjadi

bisnis layanan (*online delivery order*), teknologi *online* yang telah membawa perubahan besar terhadap perubahan ekonomi. Di era revolusi industri 4.0 akan lebih cepat dalam perkembangan produk dan menciptakan konsumen yang beragam dan berdampak terhadap harga relatif murah, perubahan pada era ini tidak hanya pada perubahan cara atau strategi dalam proses pemasaran pada aspek fundamental. Namun perkembangan teknologi yang sudah dipakai para masyarakat, juga didasarkan pada Undang-Undang Nomor 11 Tahun 2008 tentang Informatika dan Transaksi Elektronik. Perkembangan teknologi informasi telah berhasil menciptakan infrastruktur informasi baru, tersedianya layanan akses data internet yang memberikan efisiensi, alternatif ruang dan pilihan yang tanpa batas kepada penggunanya untuk melakukan banyak kegiatan diantaranya bisnis. [16]

Daya tarik ini yang menjadikan banyak pengguna transaksi bisnis konvensional kemudian beralih menggunakan sistem elektronik (*e-commerce*). Istilah "Revolusi Industri" diperkenalkan oleh Friedrich Engels dan Louis-Auguste Blanqui di pertengahan abad ke-19. Revolusi industri ini pun sedang berjalan dari masa ke masa. Dekade terakhir ini sudah dapat disebut memasuki fase ke empat 4.0. Perubahan fase ke fase memberi perbedaan artikulatif pada sisi kegunaannya. Fase pertama (1.0) bertempuh pada penemuan mesin yang menitikberatkan (*stressing*) pada mekanisasi produksi. Fase kedua (2.0) sudah beranjak pada etape produksi massal yang terintegrasi dengan *quality control* dan standarisasi. Fase ketiga (3.0) memasuki tahapan keseragaman secara massal yang bertumpu pada integrasi komputerisasi. Fase keempat (4.0) telah menghadirkan digitalisasi dan otomatisasi perpaduan internet dengan manufaktur. Pelaku industri bagi perusahaan adalah sebagai entitas organisasi yang membuat atau menyediakan barang atau jasa bagi konsumen. Oleh karena itu perusahaan *provider* dalam melaksanakan tetap mendasarkan bisnis umumnya dibentuk untuk menghasilkan keuntungan (*profit oriented*) dan meningkatkan kemakmuran bagi pemiliknya (*self interest*). Secara sederhana dapat disimpulkan visi industri bagi pelaku industri adalah visi mereka yang terlembaga dan teroganisasi

[16] Satjipto Rahardjo. Hukum dan Perubahan Sosial: Suatu Tinjauan Teoritis Serta Pengalaman-Pengalaman di Indonesia. Bandung: Alumni, 1983.hlm.38

dalam perusahaan untuk meraih keuntungan sebesar-besarnya. Melayani konsumen pada hakikatnya melayani kepentingan/tujuannya sendiri. Implikasi dari tata kerja industri ini menyasar semua orang baik yang terlibat proses produksi sampai pengguna akhir (konsumen). Pilihannya hanya tinggal dua menjadi pemain dengan segala risiko (*risk taker*) atau pemakai dengan menerima risiko (*risk maker*). Industri merupakan kegiatan ekonomi yang mengolah bahan mentah menjadi barang jadi atau barang setengah jadi. Lingkup skala perindustrian terdapat berbagai jangkauan yakni industri kecil, sedang, besar, dan industri rumah tangga. Berapapun dimensi industri adalah tempat penciptaan lapangan kerja. Efek kesempatan kerja yang diciptakan sama besar dengan yang dihasilkan, sehingga akan mempunyai dampak pertumbuhan ekonomi. Berdirinya sebuah industri akan mempunyai *multi player affect* bagi tumbuh dan berkembangnya laju perekonomian dan kesejahteraan masyarakat sekitar. Industri memegang peranan penting bagi pembangunan ekonomi di semua sektor kehidupan, dan tanggung jawab pemerintah atau pemilik industri adalah pemerataan pertumbuhan sebuah industri. Hal ini dikarenakan industri mampu memberikan manfaat (*benefit*) sebagai berikut: pertama Industri memberikan lapangan kerja dimana ia didirikan. Kedua, Industri memberikan tambahan pendapatan tidak saja bagi pekerja atau kepala keluarga, tapi bagi anggota keluarga lain.

Ketiga, pada beberapa hal industri mampu memproduksi barang-barang keperluan penduduk setempat dan daerah secara lebih efisien atau lebih murah. Peran industri yang begitu besar diatas dan menyangkut hajat hidup masyarakat dapat disebut sebagai modal sosial. Namun apabila modal sosial tersebut dikelola pada perspektif pemilik modal yang selalu bertumpu pada *profit oriented* dengan cara efisiensi pekerja dan itu secara perlahan menghilangkan makna modal sosial, maka sesungguhnya revolusi industri pada fase berapapun akan berujung pada revolusi sosial yang menyebabkan kekacauan (*chaos*) sebuah pemerintahan. Disinilah urgensinya sinergisitas revolusi industri 4.0 sebagai kebutuhan dengan revolusi mental yang menekankan aspek pemberdayaan masyarakat. Revolusi industri yang mengedepankan tata nilai pertumbuhan ekonomi masyarakat melalui pemberdayaan akan mampu membangun kerukunan dan kerjasama yang sinergi guna berkembangnya ekonomi masyarakat.

Seperti halnya pendapat Boourdeou yang menyatakan bahwa modal ekonomi bukanlah modal dari segala modal. Tapi membangun mental/ karakter (*character building*) suatu masyarakat adalah potensi ekonomi yang mampu mengalir dalam struktur sosial, sehingga dapat dijadikan dasar untuk bergerak bagi revolusi industri tersebut ke arah kemanfaatan. Secara obyektif tidak dapat dipungkiri bahwa revolusi industri terkini menyimpan beragam keuntungan dan tantangan besar yang harus dihadapi bagi setiap entitas diri yang terlibat didalamnya. Khususnya soal ekonomi bagi suatu bangsa dan negara. Salah satu keuntungan yang diperoleh adalah menemukan peluang baru namun juga diikuti oleh tantangan baru. Disisi lain, keadaan tersebut memunculkan kompetisi yang makin ketat baik antar sesama individu atau perusahaan dalam negeri maupun dengan perusahaan asing. Kompetisi ini justru semakin meningkatkan kualitas internal maupun eksternal setiap individu atau perusahaan. Revolusi industri juga memunculkan ekonomi berbasis teknologi atau yang lebih dikenal dengan ekonomi digital. Pada era ini potensi Indonesia lebih besar kepada dunia. Indonesia merupakan empat negara besar dengan jumlah penduduk sekitar 260 juta penduduk yang terdiri dari multikultural dan terbagi pada daerah kepulauan yang terpisah jarak, ruang dan waktu. Jumlah penduduk yang besar ini dan mayoritas penduduknya ada pada rentang usia 15-64 tahun, dimana usia tersebut disebut usia produktif (Indonesia-*invesment*).[17]

Besarnya angka usia produktif ini dapat dikatakan sebagai bonus demografi. Secara sederhana bonus demografi dapat diartikan sebagai peluang (*window of oppurtunity*) yang dinikmati suatu negara akibat dari besarnya proporsi penduduk produktif. Bonus demografi juga mendorong pertumbuhan ekonomi dan pendapatan perkapita. Struktur penduduk yang didominasi usia produktif berpotensi meningkatkan tabungan dan meminimalkan konsumsi. Berdasarkan data Menteri Keuangan Sri Mulyani sudah lebih 85 juta penduduk Indonesia menggunakan jaringan internet. Disinilah Indonesia mempunyai peluang dalam *e-commerce* dan pengembang ekonomi digital. Pelbagai inovasi berbasis ekonomi digital telah lahir dan terus berkembang diantaranya Go-Jek, Buka Lapak,

[17] Abdul Halim Barkatulla, Perlindungan Hukum Bagi Konsumen Dalam Transaksi ECommerce Lintas Negara di Indonesia, Pasca Sarjana UII Yogyakarta, 2009, hlm.118

Tokopedia dan lainnya berbagai *start up* yang terus tumbuh dan berkembang mengatasi masalah yang ada di masyarakat secara digital. Teknologi digital akan menciptakan 3,7 juta pekerjaan baru dalam 7 tahun mendatang dan mayoritas bergerak pada sektor jasa. Tantangannya adalah peningkatan keahlian diri yang harus ditingkatkan dengan cara yang tepat pula dan kemauan untuk melakukan inovasi secara berkelanjutan. Industri kreatif kini telah menjelma menjadi kekuatan baru menjadi sektor gemilang dalam penopang perekonomian Indonesia. Pelaku usaha ini mengerti cara memahami dengan selalu inovatif dan adaptif terhadap permintaan minat, perubahan selera pasar. Sehingga mampu menciptakan peluang kerja secara massal ditengah ancaman putus hubungan kerja secara massal pula. Kunci keberhasilan memasuki revolusi industri 4.0 adalah revolusi mental demi perbaikan karakter bangsa. Revolusi mental adalah gerakan bersama menyadarkan diri betapa pentingnya meningkatkan kompetensi diri melalui pendidikan dan meningkatkan potensi diri melalui pelatihan. Pendidikan dan pelatihan terhadap setiap disiplin ilmu menjadi dapat mengantarkan bangsa Indonesia sukses memasuki era strategis. Perusahaan *provider* dalam meningkatkan layanan ISP tersebut juga mendasarkan pada peraturan Undang-Undang Nomor 11 Tahun 2008 tentang Informatika dan Transaksi Elektronik. Selain itu diperlukan kepastian hukum perusahaan *provider* dalam jaringan internetnya yang digunakan para pihak, bila melaksanakan pemesanan transportasi maupun perdagangan *e-commerce* tersebut. Oleh karena itu persaingan usaha antara perusahaan *provider* dalam memasarkan *simcard* untuk penggunaan internet patut berlangsung secara sehat dan kepastian jaringan internet antara semua layanan ISP jugalah harus berlangsung dengan baik agar masyarakat dapat menggunakannya.

F. PERATURAN PERUNDANG-UNDANGAN NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Salah satu bentuk implementasi dari yurisdiksi untuk menetapkan hukum (*yuridiction to enforce*) terhadap tindak pidana siber berdasarkan hukum pidana Indonesia adalah salah satu pembentukan Undang-undang ITE. Undang-undang ITE merupakan Undang-undang yang dibentuk khusus

untuk mengatur berbagai aktivitas manusia dibidang teknologi informasi dan komunikasi termasuk beberapa tindak pidana yang dikategorikan tindak pidana siber. Namun demikian berdasarkan luas lingkup dan kategorisasi tindak pidana siber, disamping UU ITE peraturan perundang-undangan lainnya juga secara eksplisit atau implisit mengatur tindak pidana siber. Kriminalisasi tindak pidana siber dalam peraturan perundang-undangan Indonesia tersebut memiliki implikasi terhadap upaya pemberantas tindak pidana siber di Indonesia khususnya dan dunia pada umumnya. Undang-undang Nomor 11 Tahun 2008 tentang ITE yang disahkan pada tanggal 21 April 2008 dinilai telah cukup mampu mengatur permasalahan-permasalahan hukum dari sistem *Internet banking* sebagai salah satu layanan perbankan yang merupakan wujud perkembangan teknologi informasi. Kendala seperti aspek teknologi dan aspek hukum bukan lagi menjadi faktor penghambat perkembangan *Internet banking* di Indonesia, meskipun dalam pasal-pasal Undang-undang ITE tidak ada pasal-pasal yang spesifik mengatur mengenai Internet Banking itu sendiri, akan tetapi terdapat pasal-pasal yang mengatur mengenai transaksi dengan media Internet. Setiap penyelenggara sistem elektronik diwajibkan untuk menyediakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya.[18]

Undang-undang ITE juga mengatur bahwa sepanjang tidak ditentukan lain oleh Undang-undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut yaitu:

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut.
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik.

[18] Dikdik M.Arief Mansur, Elisatris Gultom: Cyber Law Aspek hukum Teknologi Informasi, PT Refika Aditama , Bandung, 2009, hlm.16

4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik.
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau produk.

Selain itu juga perlindungan hukum yang diberikan oleh Undang-undang ITE dalam hal perlindungan data pribadi, berhubungan dengan hak pribadi nasabah (privasi), menurut Pasal 26 menyatakan bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Perkembangan teknologi informasi saat ini memungkinkan bahwa keamanan privasi data pribadi nasabah yang menggunakan layanan perbankan melalui media internet kurang terjamin. Hal ini dikarenakan masih banyak kelemahan dalam mengantisipasi berbagai pelanggaran atau penyalahgunaan dari media internet yang berdampak kerugian berbagai pihak. Ada juga beberapa pengaturan perbuatan yang dilarang dan dikenai sanksi pidana, yaitu sebagai berikut:

1. Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah)
2. Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah). Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).
3. Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 31 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800. Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana penjara paling lama 8 (delapan) tahun

dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah)000.000,00 (delapan ratus juta rupiah)

4. Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 31 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

G. UNDANG-UNDANG NOMOR 36 TAHUN 1999 TENTANG TELEKOMUNIKASI

Dalam hal perlindungan hukum atas data pribadi nasabah terdapat pada ketentuan Pasal 22 Undang-undang Telekomunikasi yang menyatakan bahwa:

Setiap orang yang dilarang melakukan perbuatan tanpa hak, dan tidak sah, atau memanipulasi: [19]

1. Akses ke jaringan telekomunikasi, dan/atau
2. Akses ke jasa telekomunikasi, dan/atau
3. Akses ke jaringan telekomunikasi khusus.

Ketentuan ini apabila dianalogikan pada masalah perlindungan data pribadi nasabah dalam penyelenggaraan layanan *internet banking* terasa ada perbedaan dari objek data atau informasi yang dilindungi dimana ketentuan ini lebih menitikberatkan pada data yang ada dalam jaringan dan data yang sedang ditransfer. Ketentuan pidana terhadap para pihak yang melakukan pelanggaran atas ketentuan Pasal 22 Undang-undang Telekomunikasi tersebut terdapat dalam Pasal 50 menyatakan bahwa: Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam pasal 22, dipidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah). Beberapa ketentuan perundang-undangan diatas dapat diberlakukan pada berbagai macam kasus mengenai data pribadi nasabah dan hak nasabah apabila mengalami kerugian dalam layanan Internet Banking namun hal tersebut tergantung kepada jenis kasusnya. Ketentuan perundang-undangan perbankan tidak dapat diberlakukan pada kasus (*Typosquatting*) yang

[19] Renouw, Dian Mega Erianti, Perlindungan E-Commerce, Yayasan Taman Pustaka, Jakarta. 2017, hlm.28

merugikan nasabah, karena dalam hal ini keterangan atau data nasabah yang bocor tidak melibatkan pihak-pihak yang terkait dalam lembaga perbankan tersebut. Data nasabah yang sampai kepada pihak lain tersebut disebabkan kekurang hati-hatian nasabah yang dimanfaatkan si pelaku tindak kejahatan dengan membuat situs plesetan yang hampir sama. Berdasarkan uraian keseluruhan perlindungan hukum atas data pribadi nasabah dalam penyelenggara Internet Banking tersebut diatas yang dilakukan melalui cara *self regulation* dan *government regulation* maka dapat ditarik kesimpulan bahwa upaya perlindungan hukum telah dilakukan namun belum mencerminkan asas keseimbangan. Sampai saat ini belum ada ketentuan khusus atau aturan yang mencerminkan suatu hak dan kewajiban yang seimbang antara penyelenggara Internet Banking dan nasabah sendiri.[20]

H. RANGKUMAN MATERI

Perkembangan teknologi khususnya dalam bidang internet telah membuka peluang baru bagi pelaku usaha dalam memasarkan produknya kepada calon pembeli. Dengan memanfaatkan perkembangan dalam bidang teknologi informasi ini pelaku usaha tidak perlu membuka tempat usaha baru untuk memperluas jangkauan pasarnya, Pelaku Usaha hanya perlu membuat suatu *website* mengenai barang-barang yang akan mereka tawarkan kepada calon pembeli, dan juga sebuah Sistem Elektronik yang dapat digunakan sebagai alat bukti bahwa telah terjadi kesepakatan diantara pelaku usaha dengan pembeli mengenai barang, harga, dll. Namun karena seringkali media *eCommerce* ini disalahgunakan oleh para pihak yang beritikad buruk dan tidak bertanggung jawab, maka pemerintah mengeluarkan Undang-Undang Nomor 11 tahun 2008. Dengan adanya Undang-Undang ini maka segala bentuk penyalahgunaan media *eCommerce* dapat dikurangi asalkan pelaku usaha dan konsumen melaksanakan dengan baik hal-hal yang diatur oleh Undang-Undang ini. Jadi, agar setiap perbuatan ekonomi melalui media *eCommerce* ini dapat berjalan dengan lancar dan aman, maka pelaku usaha dan konsumen

[20] Sjahputra, Iman, Perlindungan Konsumen dalam Transaksi Elektronik, Alumni, Bandung. 2010, hlm.31

harus mematuhi segala peraturan yang ada yang diatur dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

TUGAS DAN EVALUASI

1. Apa yang di maksud dengan penyedia layanan internet?
2. Bagaimana aspek hukum penyedia layanan internet di Indonesia?

DAFTAR PUSTAKA

Abdul Halim Barkatulla, Perlindungan Hukum Bagi Konsumen Dalam Transaksi ECommerce Lintas Negara di Indonesia, Pasca Sarjana UII Yogyakarta, 2009

Abdul Halim Barkatullah dan Teguh Prasetyo, Bisnis E-Commerce: Studi Sistem Keamanan dan Hukum di Indonesia, Pustaka Pelajar, Yogyakarta, 2005

Ahmad M Ramli, Cyber Law dan Haki dalam Sistem Hukum Indonesia, PT. Refika. 2004

Alma, B. *Manajemen Pemasaran dan Pemasaran Jasa.* Bandung: CV. Alfabeta. 2004

Ayu Marluthy, Peran Kualitas Pelayanan Penyedia Internet Terhadap Kepuasan Pelanggan, Jurnal Riset Bisnis dan Investasi Vol. 5, No. 1, April 2019,

Bobanto, W. Analisis Kualitas Layanan Jaringan Internet (Studi Kasus PT. Kawanua Internetindo Manado). Analisis Kualitas Layanan Jaringan Internet (Studi Kasus PT. Kawanua Internetindo Manado).2014,

Budi Sutedjo Dharma Oetomo, Perspektif eCommerce, Yogyakarta, Andi, 2001

Dikdik M.Arief Mansur, Elisatris Gultom: Cyber Law Aspek hukum Teknologi Informasi, PT Refika Aditama , Bandung, 2009

Emyana Ruth, Deskripsi Kualitas Layanan Jasa Akses Internet di Indonesia dari Sudut Pandang Penyelenggara Description of Internet Quality of Services (Qos) in Indonesia From the Providers' Point of View, Buletin Pos dan Telekomunikasi, Vol.11 No.2 Juni 2013

Endang Purwaningsih, Hukum Bisnis, Bab 4 –Transaksi E-Commerce, Ghalia Indonesia. 2010

Ishaq, Dasar-Dasar Ilmu Hukum, Jakarta, Sinar Frafika, 2008

Joshua Sitompul. Cyberspace, Cybercrimes, Cyberlaw. Jakarta: Tatanusa, 2012

Lia Sautunninda, Jual Beli melalui Internet (E-Commerce) kajian menurut buku III KUH Perdata dan Undang-Undang informasi dan Elektronik, Fakultas Hukum Universitas Syiah Kuala, 2008

Onno W.Purbo, Aang Arif Wahyudi, Mengenal eCommerce, Jakarta, Elex Media Komputindo, 2001

Renouw, Dian Mega Erianti, Perlindungan E-Commerce, Yayasan Taman Pustaka, Jakarta. 2017

Richardus Eko Indrajit, E-Commerce: Kiat dan Strategi Bisnis Di Dunia Maya, PT. Elex Media Komputindo, Jakarta, 2001

Satjipto Rahardjo. Hukum dan Perubahan Sosial: Suatu Tinjauan Teoritis Serta Pengalaman-Pengalaman di Indonesia. Bandung: Alumni, 1983

Sjahputra, Iman, Perlindungan Konsumen dalam Transaksi Elektronik, Alumni, Bandung. 2010

Yusuf Ilham, Analisis Pengaruh Kualitas Jaringan, Kualitas Pelayanan, Kualitats Informasi, Keamanan dan Privasi Penyedia Layanan Internet Terhadap Kepuasan Anggaran dan Dampak Pada Niat Pembeli Ulang, Diponegoro Journal of Managemen, Vol.9, No.4, 2020

Zahrotunnimah, Zahrotunnimah; Yunus, Nur Rohim; Susilowati, Ida. "Rekonstruksi Teori Komunikasi Politik Dalam Membangun Persepsi Publik," dalam Jurnal Staatsrecht: Indonesian Constitutional Law Journal, Volume 2, Nomor 2 (2018)

HUKUM *CYBER*

BAB 7: ASPEK HUKUM INTERNASIONAL DALAM DUNIA MAYA

Judy Marria Saimima, S.H., M.H

Fakultas Hukum, Universitas Pattimura

BAB 7

ASPEK HUKUM INTERNASIONAL DALAM DUNIA MAYA

A. PENDAHULUAN

Perkembangan teknologi telah memberikan dampak besar pada hukum internasional yang mengatur aktivitas siber lintas negara. Konsep batasan wilayah geografis negara tidak lagi menjadi faktor utama dalam mengatur subjek dan objek hukum internasional. Perubahan yang cepat dalam teknologi dan norma-norma baru yang muncul sebagai respons terhadap perubahan tersebut telah menciptakan hukum baru yang terkait dengan aktivitas siber. Kejahatan siber memiliki karakteristik yang berbeda dengan kejahatan konvensional, di mana pelakunya dapat dengan mudah melintasi batas negara dan sulit untuk dideteksi.

Tantangan utama dalam mengatur kejahatan siber adalah sifat globalnya. Kejahatan ini tidak terbatas pada satu wilayah geografis tertentu, melainkan dapat terjadi di mana saja di dunia. Hal ini membuat penegakan hukum menjadi lebih rumit, karena hukum yang berlaku di suatu negara tidak selalu berlaku di negara lain. Kerjasama internasional menjadi penting dalam mengatasi kejahatan siber.

PEMBAHASAN MATERI

B. ASPEK HUKUM INTERNASIONAL DALAM DUNIA MAYA

Perkembangan teknologi telah membawa dampak signifikan pada aspek hukum internasional yang mengatur aktivitas siber yang melintasi batas negara. Deteritorialisasi hukum internasional menjadi fenomena yang semakin nyata, di mana konsep batasan wilayah geografis negara

tidak lagi menjadi faktor utama dalam mengatur subjek dan objek hukum internasional. Perubahan yang cepat dalam teknologi dan norma-norma yang muncul sebagai respons terhadap perubahan tersebut telah menciptakan hukum baru yang berkaitan dengan aktivitas siber. Aktivitas siber memiliki karakteristik yang berbeda dengan kejahatan konvensional, di mana pelakunya dapat dengan mudah melintasi batas negara dan sulit untuk dideteksi.

Salah satu tantangan utama dalam mengatur kejahatan siber adalah sifat globalnya. Kejahatan ini tidak terbatas pada satu wilayah geografis tertentu, melainkan dapat terjadi di mana saja di dunia. Hal ini menjadikan penegakan hukum menjadi lebih rumit, karena hukum yang berlaku di suatu negara tidak selalu berlaku di negara lain. Dalam hal ini, kerjasama internasional menjadi krusial untuk mengatasi kejahatan siber, di mana negara-negara perlu bekerja sama dalam pertukaran informasi dan ekstradisi pelaku kejahatan tersebut. Selain itu, kejahatan siber juga memiliki sifat yang sulit untuk diamati secara langsung. Tidak seperti kejahatan konvensional yang sering kali menimbulkan kekacauan yang terlihat, kejahatan siber dapat dilakukan secara tersembunyi dan sulit terdeteksi. Pelaku kejahatan siber dapat menghindari identifikasi dengan menggunakan alat dan teknik yang canggih, seperti jaringan anonim dan teknik enkripsi. Hal ini mempersulit upaya penegakan hukum dalam menindak pelaku kejahatan siber.

Selain tantangan dalam penegakan hukum, fenomena deteritorialisasi kedaulatan juga muncul dalam konteks aktivitas siber. Kedaulatan suatu negara, yang sebelumnya terkait erat dengan batasan wilayah geografis, menjadi kabur karena aktivitas siber tidak mengenal batas-batas negara. Ini berarti bahwa pelaku kejahatan siber dapat melakukan serangan dari negara lain dan menghindari tanggung jawab hukum dari negara tempat mereka beroperasi. Fenomena ini memicu perdebatan tentang kewenangan negara dalam mengatur dan menegakkan hukum terkait aktivitas siber. Dalam rangka mengatasi tantangan ini, komunitas internasional telah berupaya untuk menciptakan kerangka kerja hukum yang lebih luas untuk mengatur aktivitas siber. Beberapa negara telah mengadopsi peraturan dan undang-undang yang khusus mengatur kejahatan siber, sementara organisasi internasional seperti PBB dan Uni

Eropa telah menciptakan kerangka kerja hukum yang bersifat global untuk mengatasi masalah ini.

Secara keseluruhan, aspek hukum internasional dalam dunia maya berkaitan dengan regulasi dan hukum yang mengatur aktivitas siber telah menghadapi perubahan dan tantangan yang signifikan. Deteritorialisasi hukum internasional, kejahatan siber yang bersifat global, serta fenomena deteritorialisasi kedaulatan adalah beberapa isu utama yang perlu diatasi dalam mengatur dan menegakkan hukum terkait aktivitas siber di era internet ini.

Teknologi dan hukum merupakan dua unsur yang saling mempengaruhi dan keduanya juga mempengaruhi masyarakat. Pada dasarnya, teknologi diciptakan untuk memenuhi suatu kebutuhan tertentu manusia. Di lain pihak, hukum merupakan batasan bagi masyarakat dalam bertingkah laku dan terhadap pelanggarannya dikenakan sanksi yang memaksa oleh negara. Hukum diperlukan untuk menciptakan ketertiban dalam masyarakat dan memberikan keadilan. Ketertiban dan keadilan dicapai dengan menjaga kepentingan tertentu, baik individu maupun masyarakat. Di dalam masyarakat terjadi dinamika dan di dalam masyarakat pula muncul kejahatan. Teknologi dan masyarakat bersifat dinamis karena terus berkembang, demikian juga kejahatan. Hukum harus merespon perkembangan teknologi dan kejahatan berbasis teknologi (Sitompul, 2012).

Istilah *Cyber Crime* pertama kali dikenalkan oleh William Gibson (1982) yang tertulis dalam novelnya dengan judul Neuromancer pada tahun 1984. Dalam novelnya terdapat istilah *'cyber space'* yang digambarkan dengan dunia maya yang terkoneksi dengan aktivitas komputer dan istilah *'cyber crime'* digambarkan dengan tindak kejahatan yang bertempat di dunia maya tersebut dan mengancam keamanan(D, 2007). Indra Safitri berpendapat bahwa *Cyber Crime* adalah kejahatan yang berkaitan dengan penggunaan teknologi informasi sebagai media dan mencari celah keamanan sebuah sistem yang diakses oleh pengguna internet (Wahid, 2005). Dalam perkembangannya, *cyber crime* berkembang secara pesat dengan modus yang beragam. *Cyber* diartikan sebagai "dunia maya" yang menjadi media kejahatan itu berlangsung (Baker, 2003).

Sudut pandang hukum internasional, dunia maya atau internet diatur oleh berbagai peraturan dan aturan internasional yang mengatur kejahatan dunia maya. Salah satu perjanjian internasional yang relevan adalah Konvensi tentang Kejahatan Dunia Maya, yang bertujuan untuk melindungi masyarakat dari kejahatan di dunia maya dengan tingkat kejahatan yang serupa dengan kejahatan konvensional. Selain itu, prinsip bahwa hukum internasional berlaku juga di dunia maya telah diterima oleh masyarakat internasional.

Namun, menginterpretasikan konsep hukum internasional yang sudah mapan, seperti kedaulatan, penanggulangan, atau perbuatan curang (*perfidy*), dalam konteks dunia maya dapat menjadi tantangan yang signifikan. Kehadiran teknologi dan fenomena baru dalam dunia maya seringkali melampaui batas-batas yang telah ditetapkan oleh hukum internasional yang ada. Oleh karena itu, diperlukan modernisasi hukum pidana nasional dan proses hukum acara yang sesuai dengan konvensi internasional yang terkait dengan kejahatan dunia maya. Tujuannya adalah untuk memastikan bahwa negara-negara memiliki kerangka hukum yang efektif untuk menghadapi dan menangani kejahatan di dunia maya.

Hukum siber, juga dikenal sebagai *cyberlaw*, merupakan aspek hukum yang mencakup semua hal yang terkait dengan individu atau subjek hukum yang terlibat dalam pemanfaatan teknologi informasi. Hal ini mencakup masalah seperti keamanan siber, privasi data, kejahatan siber, hak kekayaan intelektual, dan peraturan penggunaan internet. Hukum siber berfungsi sebagai kerangka hukum yang mengatur dan mengatur berbagai aspek dalam lingkup aktivitas siber di dunia maya. Dalam rangka menjaga ketertiban dan keamanan dalam dunia maya yang semakin kompleks, penting untuk terus memperbarui dan mengembangkan hukum internasional serta hukum nasional yang relevan dengan dunia maya. Kolaborasi antara negara-negara dalam bentuk kerjasama internasional juga penting untuk mengatasi tantangan yang dihadapi dalam mengatur aktivitas siber dan menegakkan hukum di dunia maya yang terhubung secara global.

Pada tahun 1980-an khususnya Negara-negara di Eropa dan Amerika Utara mulai melakukan kriminalisasi terhadap perbuatan baru seiring dengan penggunaan teknologi komputer dalam melakukan tindak pidana

konvensional. Pada tahun 1990-an beberapa Negara di berbagai belahan dunia sudah mulai mengatur tindak pidana siber seperti memasuki sistem komputer secara *illegal*, merusak data dalam sistem komputer dan menyebarkan virus. Pelaku tindak pidana siber mempunyai kemampuan dan kesempatan untuk melakukan tindak pidana dari suatu Negara yang akan mengakibatkan kerugian terhadap seseorang di beberapa tempat di Negara lain. Untuk menghadapi ancaman tindak pidana siber beberapa organisasi internasional telah melakukan kajian-kajian dan pertemuan-pertemuan ilmiah yang membahas tindak pidana siber, kerjasama internasional untuk mendorong pembentukan hukum internasional tentang tindak pidana siber. Beberapa organisasi internasional yang telah melakukan usaha-usaha tersebut antara lain:

a. *Organisation for Economic Co-operation and Development* (OECD)

Usaha internasional pertama dalam memerangi tindak pidana penyalahgunaan komputer dilakukan oleh OECD antara tahun 1983dan tahun 1985. Pada tahun 1985 negara-negara anggota OEDC direkomendasikan mempertimbangkan untuk melakukan kriminalisasi terhadap kejahatan dengan penyalahgunaan komputer dan mengaturnya dalam hukum pidana nasional. Tahun 1986 OECD mengeluarkan laporan tentang *Computer-Related-Crime: Analysis of Legal Policy*. Berdasarkan hasil kajian tersebut OECD menganjurkan beberapa perbuatan untuk dikriminalisasi dalam hukum pidana nasional, yaitu : 1) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/ program komputer dengan maksud untuk melakukan transfer dana atau sesuatu yang bernilai lainnya secara *illegal*. 2) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/program komputer dengan maksud untuk melakukan pemalsuan. 3) Memasukan, mengubah, menghapus, dan/atau menyembunyikan data komputer/ program komputer dengan maksud untuk mengganggu sistem komputer atau sistem telekomunikasi lainnya. 4) Pelanggaran hak eksklusif atas program komputer yang dilindungi yang dilakukan dengan sengaja untuk kepentingan komersial. 5) Mengakses atau mengintersep sistem komputer/telekomunikasi tanpa seizin pihak yang bertanggung jawab atas sistem tersebut baik dengan cara pelanggaran atas sistem pengamanan, atau untuk tujuan maksud jahat lain. Usaha lain yang dilakukan OECD

adalah kontribusinya mengenai pedoman tentang kebijakan keamanan komputer internasional yang saat ini menjadi *Guidelines for the Security of Information System and Networks*.

b. *United Nations* (UN)

Perserikatan Bangsa-Bangsa (PBB) melakukan *monitoring* terhadap *Computer related crime*, dimulai pada tahun 1990 dengan *Eight UN Congress on the Prevention of Crime and Treatment of Offender*. Dalam resolusi kongres PBB tersebut Negara-negara dihimbau untuk mengintensifkan usaha-usaha memerangi *computer related crime* dengan melakukan tindakan-tindakan berikut: 1) Modernisasi hukum pidana materiil dan hukum acara pidana nasional untuk menjamin dan memadai dalam menindak tindak pidana siber. 2) Meningkatkan upaya-upaya pengamanan komputer dan upaya-upaya preventif, dengan memperhitungkan masalah-masalah terkait perlindungan privasi, penghormatan hak asasi manusia dan kebebasan-kebebasan fundamental serta setiap mekanisme pengaturan penggunaan/pemanfaatan komputer. 3) Mengadopsi upaya-upaya agar masyarakat, aparat pengadilan dan penegak hukum peka terhadap masalah *computer-related crimes* dan pentingnya mencegah tindak pidana tersebut. 4) Mengadopsi pelatihan-pelatihan yang memadai untuk hakim, pejabat dan aparat yang bertanggung jawab atas pencegahan, penyidikan, penuntutan dan pengadilan mengenai tindak pidana ekonomi dan *computer-related crimes* 5) Mengelaborasi -- dalam kolaborasi dengan organisasi-organisasi yang berkepentingan—*rules of ethics* dalam penggunaan komputer 5 dan mengajarkannya sebagai bagian dari kurikulum dan *training* informatika. 6) Mengadopsi kebijakan-kebijakan untuk korban *computer-related crimes* yang konsisten dengan *United Nations Declarartion of Basic Principles of Justice for Victims of Crime and Abuse of Power*, termasuk pengembalian aset yang diperoleh dari kejahatan, dan upaya-upaya mendorong korban agar mau melaporkan kejahatan kepada penguasa yang berwenang.

c. *The Group of Eight* (G8)

G8 adalah kelompok Negara-negara *industry* yang terdiri dari Kanada, Jerman, Perancis, Itali, Jepang, Inggris, Amerika Serikat, dan Rusia. Menurut G8 setidaknya ada 2 bentuk ancaman dari perkembangan *high-tech crime*/tindak pidana teknologi tinggi yaitu; (1) para pelaku kejahatan yang canggih menjadikan komputer dan sistem telekomunikasi sebagai target untuk memperoleh atau mengalihkan informasi yang berharga tanpa izin dan mencoba mengganggu sistem-sistem perdagangan penting dan sistem-sistem *public* lainnya, (2) para pelaku kejahatan termasuk kelompok dari anggota kejahatan terorganisir dan para teroris, menggunakan teknologi baru ini sebagai alat kejahatan tradisional yang merupakan ancaman terhadap keamanan umum. G8 menyetujui 10 prinsip memerangi *high-tech crimes* tersebut adalah: 1) Tidak boleh ada tempat berlindung bagi mereka yang menyalahgunakan teknologi informasi. 2) Penyidikan dan penuntutan atas pelaku kejahatan *high-tech* internasional harus dilaksanakan dengan berkoordinasi dengan seluruh Negara yang berkepentingan, terlepas dari wilayah hukum mana kerugian ditimbulkan. 3) Aparat penegak hukum harus terlatih dan diperlengkapi/ dipersiapkan untuk menangani kejahatan *high-tech*. 4) Sistem hukum harus melindungi kerahasiaan, keutuhan dan ketersediaan data dan sistem dari kerusakan yang diakibatkan oleh adanya perbuatan melawan hukum dan menjamin adanya penghukuman terhadap penyalahgunaan serius. 5) Sistem hukum harus memungkinkan pengamanan data elektronik dan akses yang cepat terhadap data elektronik, yang kerap sangat penting bagi keberhasilan investigasi kejahatan. 6) Rezim bantuan timbal balik harus dapat menjamin perolehan dan pertukaran alat bukti yang cepat dalam kasus yang melibatkan kejahatan *high-tech* internasional. 7) Akses elektronik lintas batas oleh penegak hukum terhadap informasi yang dapat diakses oleh umum tidak memerlukan pengesahan/izin dari Negara dimana data itu diperoleh atau berada. 8) Harus dikembangkan dan diterapkan standar *forensic* untuk memperoleh dan mensahkan data elektronik dalam proses investigasi dan penuntutan. 9) Sistem informasi dan telekomunikasi harus dirancang untuk membantu pencegahan dan mengetahui penyalahgunaan jaringan, dan juga harus dapat digunakan menelusuri dan menemukan para penjahat dan mengumpulkan alat bukti.

10) Kegiatan dibidang ini harus dikoordinasikan dengan kegiatan dalam for a internasional lainnya yang relevan untuk memastikan tidak adanya upaya yang tumpang tindih.

d. *Council of Erope* (CoE)

Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapun di Dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber. *Convention on Cyber Crime* 2001 merupakan puncak dari usaha-usaha yang telah dimulai lebih dari 20 tahun lalu oleh OECD, kemudian juga dilakukan PBB dan organisasi internasional lainnya yang telah mengkaji dan menyelenggarakan berbagai penemuan internasional dalam menghadapi perkembangan tindak pidana siber. *Convention on Cyber Crime* 2001 merupakan regulasi internasional pertama yang mengatur tindak pidana Siber dan menjadi pedoman dalam regulasi tindak pidana siber dalam hukum nasional. *Convention on Cyber Crime* 2001 terdiri dari 48 Pasal dan dibagi dalam 4 bab, ketentuan yang berkaitan dengan kriminalisasi tindak pidana siber adalah Bab II Hukum Pidana Materil Bagian 1 hukum pidana materil (Pasal2-Pasal 13) mengatur ketentuan-ketentuan tentang hukum pidana materiil, kriminalisasi, dan ketentuan lainnya yang berkaitan dengan tindak pidana siber. Tindak pidana siber terdapat 9 jenis tindak pidana siber yang dikelompokkan dalam empat kategori tindak pidana, yaitu: 1) Kelompok pertama: tindak pidana terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan data (*availability*) data dan sistem komputer terdiri dari: *illegal access* (pasal 2), *illegal interception* (pasal 3), data *interference* (pasal 4), *system interference* (pasal 5), dan *misuse of device* (pasal 6). 2) Kelompok kedua: tindak pidana yang berkaitan dengan komputer, terdiri dari pemalsuan yang berkaitan dengan komputer (*computer related forgery* (pasal 7)), dan penipuan yang berkaitan dengan komputer (*computer related fraud* (pasal 8)). 3) Kelompok ketiga: tindak pidana yang berkaitan dengan konten yang berisi ketentuan tentang tindak pidana yang berkaitan dengan pornografi anak (*offens related to child pornography* (pasal 9)). 4) Kelompok keempat: tindak pidana yang

berkaitan dengan pelanggaran hak cipta dan hak-hak terkait (pasal 10). Disamping empat kelompok tindak pidana siber, dalam Bab I hukum pidana materil juga mengatur kewajiban tambahan dan sanksi terdiri dari: 1) Pasal 11, perbuatan yang dikriminalisasi adalah dengan sengaja (1) membantu atau menghasut, (2) mencoba untuk melakukan tindak pidana yang diatur dalam Pasal 2-Pasal 10. 2) Pasal 12, mengatur tentang badan-badan hukum dapat diminta pertanggungjawaban atas tindak pidana yang telah ditetapkan sesuai dengan konvensi ini, yang dilakukan untuk keuntungan mereka oleh orang perseorangan, baik secara individual, maupun sebagai bagian dari organ badan hukum, yang memegang posisi pimpinan didalamnya berdasarkan: a) Kuasa perwakilan badan hukum tersebut, b) Wewenang untuk mengambil keputusan atas nama badan hukum tersebut, c) Wewenang untuk mengendalikan dalam badan hukum tersebut. 3) Pasal 13, mengatur mengenai adanya jaminan bahwa tindak pidana dari pasal 2-pasal 10 dipidana dengan sanksi yang efektif, proporsional, dan *dissuasive*, termasuk sanksi pidana perampasan kemerdekaan untuk orang atau sanksi *non-penal* atau tindakan, termasuk juga sanksi pidana denda untuk badan hukum.

Munculnya kejahatan baru yang bersifat transnasional dan dalam bentuk tindakan-tindakan yang dilakukan dalam dunia maya telah menyadarkan masyarakat Internasional tentang perlunya perangkat Hukum Internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *cybercrime*. *Instrument* Hukum Internasional *public* yang mengatur kejahatan siber adalah Konvensi tentang Kejahatan Siber (*Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh Negara manapun di Dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber. Konvensi ini dibentuk dengan pertimbangan-pertimbangan (dalam pembukaan EU *Convention On Cyber Crime*) antara lain sebagai berikut: 1) Masyarakat internasional menyadari perlunya kerjasama antar Negara dan *industry* dalam memerangi kejahatan siber dan adanya kepentingan untuk melindungi kepentingan yang sah di dalam penggunaan serta pengembangan teknologi informasi. 2) Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk

melakukan perbuatan *criminal*. Dengan demikian perlunya adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan *domestic* melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat. 3) Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegak hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Konvenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik dan Sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi dan pendapat. Konvensi ini telah disepakati oleh Masyarakat Uni Eropa sebagai Konvensi yang terbuka untuk diaksesi oleh Negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan *instrument* Hukum Internasional dalam mengatasi kejahatan siber, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi (Situmeang, 2020).

Konvensi tentang Kejahatan Dunia Maya merupakan sebuah perjanjian internasional yang memberikan perlindungan terhadap kejahatan dunia maya dengan tingkat kejahatan yang sebanding dengan kejahatan konvensional. Konvensi ini menjadi konvensi pertama yang secara khusus mengatur tentang kejahatan di dunia maya dan dapat diadopsi oleh negara-negara di seluruh dunia yang memiliki komitmen untuk melawan kejahatan dunia maya.

Konvensi ini mencakup berbagai aspek terkait dengan kejahatan dunia maya, antara lain:

1. Kejahatan melalui internet dan jaringan komputer: Konvensi ini mengatur berbagai jenis kejahatan yang dilakukan melalui internet dan jaringan komputer, seperti akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat.
2. Pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer: Konvensi ini juga mengatur pelanggaran terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer. Hal ini termasuk akses ilegal, intersepsi ilegal, gangguan data, gangguan sistem, dan penyalahgunaan perangkat.

3. Pembentukan kebijakan kriminal: Konvensi ini juga mencakup pembentukan kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari kejahatan dunia maya. Negara-negara diharapkan untuk mengadopsi undang-undang dan kebijakan yang efektif dalam menangani kejahatan dunia maya serta untuk melakukan kerjasama internasional dalam hal ini.
4. Kewenangan Majelis Eropa: Konvensi ini mulai berlaku pada tahun 2001 dan kewenangan atas penetapan isi perjanjian diberikan kepada Majelis Eropa. Pada awalnya, Konvensi tentang Kejahatan Dunia Maya hanya berlaku bagi negara-negara di Eropa. Namun, kemudian konvensi ini terbuka untuk aksesi dan ratifikasi oleh negara-negara di seluruh dunia yang ingin berkomitmen dalam melawan kejahatan dunia maya.

Konvensi ini merupakan perjanjian internasional pertama mengenai kejahatan yang dilakukan melalui Internet dan jaringan komputer lainnya, terutama yang berhubungan dengan pelanggaran hak cipta, penipuan terkait komputer, pornografi anak, dan pelanggaran keamanan jaringan. Konvensi ini juga berisi serangkaian wewenang dan prosedur seperti penggeledahan jaringan komputer dan penyadapan. Tujuan utamanya, sebagaimana tercantum dalam mukadimah, adalah untuk mengupayakan kebijakan kriminal bersama yang ditujukan untuk melindungi masyarakat dari kejahatan dunia maya, terutama dengan mengadopsi undang-undang yang sesuai dan membina kerja sama internasional. Dengan adanya Konvensi tentang Kejahatan Dunia Maya, diharapkan bahwa negara-negara dapat bekerja sama dalam menghadapi tantangan dan mengatasi kejahatan di dunia maya. Konvensi ini menjadi dasar hukum internasional yang penting dalam upaya melindungi masyarakat dan mempromosikan keamanan dalam lingkungan digital.

Digitalisasi memberikan dampak baik dan buruk kepada Indonesia karena kondisi penduduk yang padat dan mendapatkan bonus demografi pada tahun 2030-2035. Dampak baik dari lajunya perkembangan era 5.0 ini ialah menjadikan masyarakat dan pemerintah Indonesia serta pihak swasta untuk menyesuaikan perkembangan teknologi dan informasi digital. Sedangkan dampak buruk dari era 5.0 adalah meningkatnya ancaman

kejahatan siber atau *cyber crime* dengan sasaran perseorangan bahkan suatu negara melalui dunia maya. (Mustameer, 2022).

Di tengah meningkatnya penetrasi internet yang luas, kita harus menyadari bahwa adanya potensi terjadinya kejahatan di dunia maya. Internet, yang sering disebut sebagai dunia maya atau *cyberspace*, telah memberikan kesempatan bagi kejahatan siber atau *cyber crime* untuk berkembang dengan lebih kompleks dibandingkan dengan kejahatan komputer tradisional. Namun, kita perlu memahami bahwa dampak negatif ini sebagian besar disebabkan oleh penggunaan internet yang tidak bijak.

Kejahatan siber telah mencakup berbagai tindakan yang merugikan. Praktik penyebaran virus yang merusak komputer telah menjadi ancaman global, dengan banyak perusahaan, lembaga keuangan, dan individu yang mengalami kerugian finansial yang signifikan. Bahkan, serangkaian insiden peretasan telah mengungkapkan kerentanan data keamanan nasional yang diakses oleh pihak yang tidak berwenang. Selain itu, berbagai kejahatan lainnya juga dilakukan melalui internet, seperti penyebaran konten pornografi anak, penyerangan privasi individu, perdagangan barang ilegal, serta kehadiran situs-situs yang mengganggu ketenteraman masyarakat.

Namun, kita tidak boleh melupakan bahwa internet juga membawa banyak manfaat bagi kehidupan kita. Percepatan komunikasi, kemudahan akses informasi, dan inovasi teknologi adalah beberapa contoh dampak positif yang telah kita nikmati berkat internet. Oleh karena itu, penting bagi kita untuk memanfaatkan internet dengan bijak dan bertanggung jawab.

Pemerintah dan lembaga terkait juga memiliki peran penting dalam melawan kejahatan siber. Mereka harus mengembangkan kebijakan dan sistem keamanan yang efektif, serta meningkatkan kesadaran masyarakat tentang ancaman dan tindakan pencegahan terhadap kejahatan di dunia maya. Hanya dengan kerjasama dan upaya bersama, kita dapat menjaga internet sebagai lingkungan yang aman dan produktif bagi semua pengguna.

Salah satu contoh kejahatan siber yang sering terjadi adalah penyebaran virus yang merusak komputer di seluruh dunia. Praktik ini telah menyebabkan kerugian finansial yang besar bagi bank-bank dan lembaga keuangan. Bahkan, negara-negara maju seperti Amerika Serikat dan Inggris serta beberapa negara lainnya telah mengungkapkan kasus peretasan data keamanan nasional, di mana orang-orang yang tidak berkepentingan mengakses dan mengunduh informasi yang sensitif.

Tidak hanya itu, kejahatan lainnya juga dapat terjadi melalui media internet. Contohnya, penyebaran konten pornografi anak yang merusak dan melanggar hak privasi individu, perdagangan barang ilegal, serta keberadaan situs-situs yang mengganggu ketenteraman masyarakat. Internet juga memberikan kesempatan bagi mereka yang gemar berjudi untuk melakukannya secara daring, baik dari rumah maupun kantor.

Namun, penting untuk diingat bahwa kejahatan di dunia maya tidak mewakili seluruh aspek internet. Internet juga telah memberikan manfaat yang besar bagi masyarakat, seperti mempercepat komunikasi, mempermudah akses informasi, dan memfasilitasi perkembangan teknologi. Oleh karena itu, sangat penting bagi pengguna internet untuk menggunakan teknologi ini dengan bijak dan bertanggung jawab, serta untuk pemerintah dan lembaga terkait untuk mengembangkan kebijakan dan sistem keamanan yang efektif dalam melawan kejahatan siber (Nugraha, 2021).

Dalam sistem hukum pidana, kriminalisasi merupakan proses di mana pemerintah atau otoritas yang berwenang menetapkan tindakan-tindakan tertentu sebagai kejahatan yang dapat dihukum. Dalam konteks Indonesia, kejahatan siber termasuk dalam kategori tindak pidana khusus, meskipun beberapa unsurnya dapat sejalan dengan pasal-pasal yang ada dalam Kitab Undang-Undang Hukum Pidana (KUHP). Namun, kejahatan siber ini dilakukan dengan menggunakan metode-metode baru atau modus operandi yang belum terdokumentasi secara rinci dalam hukum yang ada. Oleh karena itu, untuk melawan kejahatan ini, diperlukan instrumen hukum yang lebih canggih dan terperinci.

Dalam upaya memerangi kejahatan siber, pemerintah Indonesia telah melakukan berbagai upaya untuk mengkriminalisasi tindakan-tindakan tersebut. Undang-Undang dan peraturan-peraturan yang lebih spesifik

telah diberlakukan guna menangani kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan terkait perlindungan data pribadi. Instrumen hukum ini dirancang untuk memberikan kerangka kerja yang jelas dalam menangani berbagai bentuk kejahatan siber, termasuk penipuan daring, penyebaran konten ilegal, peretasan, dan pelanggaran privasi.

Namun, dengan laju perkembangan teknologi yang terus berubah, tantangan dalam melawan kejahatan siber juga semakin kompleks. Kejahatan siber sering kali melibatkan pelaku yang tersembunyi di balik jaringan yang sulit dilacak, serta penggunaan teknik canggih untuk menyembunyikan jejak digital. Oleh karena itu, penegakan hukum dan penanganan kejahatan siber memerlukan kolaborasi antara pemerintah, lembaga penegak hukum, dan sektor swasta. Selain itu, peningkatan kesadaran masyarakat tentang ancaman kejahatan siber juga menjadi faktor penting dalam upaya pencegahan dan perlindungan.

Dalam konteks ini, penting bagi sistem hukum Indonesia untuk terus beradaptasi dan mengembangkan instrumen hukum yang lebih jelimet dan responsif terhadap perkembangan teknologi serta kejahatan siber. Diperlukan upaya yang berkelanjutan untuk memastikan bahwa hukum dapat efektif dalam menghadapi tantangan yang terus berkembang di dunia maya (Ersya, 2017). Formulasi kejahatan di dunia maya dapat dilihat pada pengaturan tindakan tersebut dalam undang-undang. Dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur sejumlah perbuatan yang dilarang yang menjadi tindakan *cybercrime.*

Sebelum Undang-Undang Informasi dan Transaksi Elektronik (UU-ITE) diberlakukan, pengadilan dalam mengadili kejahatan dunia maya atau *cybercrime* menggunakan ketentuan yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan undang-undang lain yang mengatur tindak pidana di luar KUHP. Kejahatan siber pada saat itu dianggap sebagai variasi dari kejahatan komputer atau kejahatan konvensional lainnya yang dapat diterapkan dengan analogi hukum yang ada. Misalnya, tindakan peretasan atau pencurian data melalui internet dapat dijerat dengan

pasal-pasal dalam KUHP yang terkait dengan peretasan komputer atau pencurian. Namun, karena modus operandi kejahatan siber yang berbeda dan menggunakan teknologi informasi, ada kebutuhan untuk memperkuat dan mengklarifikasi hukum yang mengatur kejahatan di dunia maya.

Dalam konteks ini, pengenalan UU-ITE pada tahun 2008 di Indonesia merupakan langkah penting dalam memperbarui dan menyempurnakan kerangka hukum yang mengatur *cybercrime*. UU-ITE memberikan landasan hukum yang lebih spesifik dan komprehensif dalam menghadapi tantangan kejahatan siber. Undang-undang ini mengatur berbagai tindakan yang melibatkan penggunaan teknologi informasi, seperti penipuan daring, pencemaran nama baik, penghinaan melalui media sosial, penyebaran konten ilegal, dan banyak lagi. Dengan adanya UU-ITE, pengadilan memiliki landasan hukum yang jelas dan lebih tepat dalam mengadili tindak pidana di dunia maya. Undang-undang ini memperkuat perlindungan terhadap korban kejahatan siber, mengatur sanksi yang sesuai untuk pelaku, dan memberikan dasar bagi penegakan hukum yang lebih efektif dalam lingkungan digital(Bunga, 2019).

Namun, terus berkembangnya teknologi dan tindak kejahatan siber yang semakin kompleks menuntut adanya evaluasi dan penyempurnaan hukum yang berkelanjutan. Penting bagi pemerintah dan lembaga terkait untuk terus memantau perkembangan kejahatan siber dan menyesuaikan kerangka hukum agar tetap relevan dan efektif dalam menghadapi tantangan masa depan di dunia maya. Ketentuan yang digunakan untuk menangani *cybercrime* dalam KUHP adalah tentang pemalsuan (pasal 263-276), pencurian (pasal 362-372), penipuan (pasal 378-395), perusakan barang (pasal 407-412). Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* yaitu:

a) **Pasal 362 KUHP** yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card* generator di Internet untuk melakukan transaksi di *ecommerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank

ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

b) **Pasal 378 KUHP** dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

c) **Pasal 335 KUHP** dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.

d) **Pasal 311 KUHP** dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

e) **Pasal 303 KUHP** dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.

f) **Pasal 282 KUHP** dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang terlarang atau *illegal*.

g) **Pasal 282 dan 311 KUHP** dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet, misalnya kasus-kasus video porno para mahasiswa, pekerja atau pejabat publik.

h) **Pasal 378 dan 262 KUHP** dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
i) **Pasal 406 KUHP** dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

Undang-Undang ITE adalah ketentuan hukum yang mengatur perbuatan hukum dalam dunia maya. Undang-undang ini berlaku bagi siapa pun yang melakukan tindakan yang memiliki akibat hukum dan merugikan kepentingan negara Indonesia, baik di dalam maupun di luar wilayah hukum Indonesia. UU ITE adalah hukum siber pertama di Indonesia dan memiliki tujuan utama untuk memberikan kepastian hukum bagi masyarakat dalam melakukan transaksi elektronik, mendorong pertumbuhan ekonomi, mencegah kejahatan berbasis teknologi informasi dan komunikasi, serta melindungi pengguna jasa teknologi informasi dan komunikasi. Undang-undang ini mencerminkan kesadaran akan pentingnya perlindungan data pribadi, keamanan informasi, dan tata kelola teknologi informasi yang bertanggung jawab. Namun, UU ITE perlu terus dievaluasi dan diperbarui sesuai dengan perkembangan teknologi dan tantangan masa depan agar tetap relevan dan efektif dalam menghadapi perubahan yang terjadi dalam dunia maya.

Beberapa materi perbuatan yang dilarang (*cybercrimes*) yang diatur dalam UU ITE, antara lain (Situmeang, 2020):

1. Perbuatan yang dikriminalisasi dalam Pasal 27 meliputi, dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan atau membuat informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dapat diakses, memiliki muatan perjudian dapat diakses, memiliki muatan penghinaan dan/atau pencemaran nama baik dapat diakses, memiliki muatan pemerasan atau pengancaman dapat diakses.
2. Pasal 28 Perbuatan yang dikriminalisasi dalam pasal 28 meliputi perbuatan yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen

dalam transaksi elektronik dan dengan sengaja dan tanpa hak menyebarkan informasi untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan SARA.

3. Perbuatan yang dikriminalisasi dalam pasal 29 adalah dengan sengaja serta tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang didalamnya memuat ancaman berupa kekerasan atau menakuti yang ditujukan kepada pribadi atau seseorang.
4. Perbuatan yang dikriminalisasi dalam pasal 30 meliputi, dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik atau dokumen elektronik, dan dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
5. Perbuatan yang dikriminalisasi dalam pasal 31 meliputi, yaitu dengan sengaja dan tanpa hak atau melawan hukum melakukan penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer atau sistem elektronik tertentu milik orang lain dan dengan melakukan penyadapan suatu transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik dari, ke dan didalam suatu komputer atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, penghilangan, atau penghentian informasi elektronik atau dokumen elektronik yang sedang di transmisikan.
6. Perbuatan yang dikriminalisasi dalam pasal 32 sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik atau dokumen elektronik milik orang lain atau milik publik dan yang tidak berhak.
7. Perbuatan yang dikriminalisasi dalam pasal 33 adalah dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

8. Perbuatan yang dikriminalisasi dalam pasal 34 adalah dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki, perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33, Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33.
9. Perbuatan yang dikriminalisasi dalam pasal 35 adalah dengan sengaja dan tanpa hak atau melawan hukum, melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.
10. Perbuatan yang dikriminalisasi dalam pasal 36 adalah dengan sengaja dan tanpa hak atau melawan hukum perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang dapat mengakibatkan kerugian bagi orang lain.
11. Ketentuan pasal 37 tidak mengatur perbuatan yang dilarang tetapi mengatur mengenai yurisdiksi atas perbuatan yang dilakukan di luar wilayah Indonesia terhadap sasaran atau objek yang ada di wilayah Indonesia.

Dalam Undang-Undang ITE, terdapat rumusan perbuatan yang dianggap sebagai tindak pidana siber yang dikriminalisasi. Rumusan tersebut mencakup unsur-unsur seperti "dengan sengaja" dan "tanpa hak". Beberapa pasal dalam UU ITE juga menggunakan alternatif rumusan "melawan hukum" sebagai pengganti unsur "tanpa hak", seperti yang terdapat dalam Pasal 30 hingga Pasal 36. Penggunaan kata "dengan sengaja" menunjukkan bahwa tindak pidana siber sebagaimana diatur dalam UU ITE akan dikenai sanksi pidana jika dilakukan dengan sengaja. Artinya, niat pelaku untuk melakukan perbuatan tersebut menjadi faktor penting dalam penentuan pidana. Namun, perbuatan yang dilakukan

secara tidak sengaja atau tanpa disengaja bukan merupakan tindak pidana dan tidak akan dikenai sanksi pidana. Hal ini menunjukkan bahwa UU ITE mendasarkan penegakan hukum pada unsur kesengajaan pelaku dalam melakukan tindak pidana siber. Tujuan dari pendekatan ini adalah untuk membedakan antara perbuatan yang dilakukan secara sengaja dengan kelalaian atau kebetulan yang tidak dimaksudkan sebagai tindak pidana. Dalam hal ini, kehadiran unsur "dengan sengaja" memberikan landasan hukum yang jelas dalam menentukan pertanggungjawaban pidana terhadap pelaku tindak pidana siber. Selain itu, hal ini juga membantu dalam menjaga keseimbangan antara perlindungan terhadap masyarakat dari kejahatan siber dan kebebasan individu dalam menggunakan teknologi informasi dan komunikasi. Namun, perlu diingat bahwa interpretasi dan penerapan unsur-unsur ini tetap menjadi tugas pengadilan dan lembaga penegak hukum yang berwenang. Dalam praktiknya, kasus-kasus tindak pidana siber akan dinilai berdasarkan fakta dan bukti yang ada serta melalui proses hukum yang berlaku (Situmeang, 2020).

C. RANGKUMAN MATERI

Perkembangan teknologi telah membawa dampak signifikan pada aspek hukum internasional yang mengatur aktivitas siber yang melintasi batas negara. Dalam era digital ini, batasan wilayah geografis negara tidak lagi menjadi faktor utama dalam mengatur subjek dan objek hukum internasional. Aktivitas siber memiliki karakteristik yang berbeda dengan kejahatan konvensional, di mana pelakunya dapat dengan mudah melintasi batas negara dan sulit untuk dideteksi. Kejahatan ini tidak terbatas pada satu wilayah geografis tertentu, melainkan dapat terjadi di mana saja di dunia. Hal ini menjadikan penegakan hukum menjadi lebih rumit, karena hukum yang berlaku di suatu negara tidak selalu berlaku di negara lain. Dalam hal ini, kerjasama internasional menjadi krusial untuk mengatasi kejahatan siber, di mana negara-negara perlu bekerja sama dalam pertukaran informasi dan ekstradisi pelaku kejahatan tersebut. Selain itu, kejahatan siber juga sulit untuk diamati secara langsung dan pelaku kejahatan dapat menghindari identifikasi dengan menggunakan alat dan teknik yang canggih. Selain tantangan dalam penegakan hukum,

fenomena deteritorialisasi kedaulatan juga muncul dalam konteks aktivitas siber. Aktivitas siber tidak mengenal batas-batas negara, sehingga pelaku kejahatan siber dapat melakukan serangan dari negara lain dan menghindari tanggung jawab hukum dari negara tempat mereka beroperasi. Fenomena ini memicu perdebatan tentang kewenangan negara dalam mengatur dan menegakkan hukum terkait aktivitas siber. Dalam rangka mengatasi tantangan ini, komunitas internasional telah berupaya untuk menciptakan kerangka kerja hukum yang lebih luas untuk mengatur aktivitas siber. Beberapa negara telah mengadopsi peraturan dan undang-undang khusus yang mengatur kejahatan siber, sementara organisasi internasional seperti PBB dan Uni Eropa telah menciptakan kerangka kerja hukum yang bersifat global untuk mengatasi masalah ini. Konvensi tentang Kejahatan Dunia Maya atau *Convention on Cyber Crime* tahun 2001 menjadi perjanjian internasional yang relevan dalam mengatur kejahatan dunia maya. Konvensi ini bertujuan untuk melindungi masyarakat dari kejahatan di dunia maya dengan tingkat kejahatan yang sebanding dengan kejahatan konvensional. Konvensi ini memberikan landasan hukum yang jelas dan komprehensif dalam menghadapi tantangan kejahatan siber.

Dalam konteks Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) tahun 2008 merupakan instrumen hukum yang spesifik dalam mengatur kejahatan siber. Undang-undang ini mengatur berbagai tindakan yang melibatkan penggunaan teknologi informasi, seperti penipuan daring, pencemaran nama baik, dan penyebaran konten ilegal. Namun, dengan perkembangan teknologi dan kejahatan siber yang terus berubah, diperlukan upaya yang berkelanjutan dalam mengembangkan dan menyempurnakan kerangka hukum yang mengatur kejahatan di dunia maya. Pemerintah dan lembaga terkait harus terus memantau perkembangan kejahatan siber dan menyesuaikan hukum agar tetap relevan dan efektif dalam menghadapi tantangan masa depan di dunia maya.

TUGAS DAN EVALUASI

1. Bagaimana aspek hukum internasional dalam dunia maya berperan dalam mengatur dan menegakkan hukum terkait aktivitas siber?
2. Bagaimana peran organisasi internasional seperti PBB dan Uni Eropa dalam menciptakan kerangka kerja hukum global untuk mengatasi kejahatan siber?
3. Bagaimana pasal-pasal dalam KUHP dapat diterapkan dalam kasus-kasus kejahatan siber seperti *carding*, penipuan, pemerasan, pencemaran nama baik, dan lainnya?
4. Apa tujuan utama dari Undang-Undang ITE dan mengapa perlindungan data pribadi, keamanan informasi, dan tata kelola teknologi informasi menjadi fokus dalam undang-undang ini?
5. Mengapa penting bagi pemerintah dan lembaga terkait untuk melakukan evaluasi dan penyempurnaan hukum secara berkelanjutan terkait dengan kejahatan siber?

DAFTAR PUSTAKA

Baker, C. D. (2003). Tolerance of International Espionage: A Functional Approach. *American University International Law Review*, *19*(5), 12.

Bunga, D. (2019). POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME. *Jurnal LEGISLASI INDONESIA*, *16*(1), 1–15.

D, W. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Moraland Civic Education*, *1*(1), 50–62.

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. *Jurnal Yustika (Media Hukum Dan Keadilan)*, *25*(1), 40–53.

Nugraha, R. (2021). PERSPEKTIF HUKUM INDONESIA (CYBERLAW) PENANGANAN KASUS CYBER DI INDONESIA. *Jurnal Ilmiah Hukum Dirgantara*, *11*(2), 44–56. https://doi.org/https://doi.org/10.35968/jihd.v11i2.767

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. Tatanusa. https://balitbangsdm.kominfo.go.id/perpustakaan/index.php?p=show_detail&id=1377

Situmeang, S. M. T. (2020). *Cyber Law*. Cakra.

Wahid, A. (2005). *Kejahatan Mayantara (Cyber Crime)*. RefikaAditama.

HUKUM *CYBER*

BAB 8: KEBEBASAN BERBICARA DAN HUKUM *CYBER*

Dr. Yanti Amelia Lewerissa, S.H., M.H

Fakultas Hukum Universitas Pattimura

BAB 8

KEBEBASAN BERBICARA DAN HUKUM *CYBER*

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah merubah dan mempengaruhi seluruh aspek kehidupan manusia. Kemajuan teknologi informasi dan komunikasi selain memberikan kontribusi bagi peningkatan kesejahteraan dan kemajuan peradaban manusia, tetapi dapat juga menjadi sarana melakukan perbuatan melawan hukum (Ahmad M Ramli dkk, 2005). Muncullah perilaku-perilaku menyimpang dengan memanfaatkan teknologi canggih sebagai alat untuk melakukan kejahatan. Salah satunya adalah kebebasan berbicara yang dapat menimbulkan perbuatan anti sosial bahkan melawan hukum seperti ujaran kebencian dan pencemaran nama baik dengan memanfaatkan kemajuan teknologi informasi dan komunikasi.

Kebebasan berbicara merupakan hak setiap individu. Kebebasan berbicara individu sebagai hak dalam berkomunikasi, berekspresi dan mengeluarkan pendapat, melalui media cetak tentunya berbeda dengan kebebasan berbicara dengan menggunakan media elektronik/internet. Kebebasan berbicara melalui media cetak tetap disunting atau diedit ulang oleh dewan editor dan dewan redaksi sebelum aspirasi/pendapat/ide/ gagasan atau substansi yang kita bicarakan tersampaikan kepada orang lain ketika membacanya. Namun, berbeda dengan kebebasan berbicara melalui media elektronik/internet. Tidak ada dewan editor ataupun dewan redaksi untuk menyunting atau mengedit apa pun yang akan kita

sampaikan kepada orang lain yang sama-sama menggunakan media elektronik/internet tersebut.

Kebebasan berbicara melalui media internet yang berbeda jika menggunakan sarana media cetak, dapat menimbulkan terjadinya perdebatan opini yang biasanya muncul karena adanya perbedaan pandangan, kebiasaan, kultur, dan lainnya. Perdebatan akan dimulai ataupun diakhiri dengan komentar yang menyakiti, vulgar, atau hal lain yang tidak relevan. Kebebasan berbicara melalui media internet yang sering digunakan oleh masyarakat adalah penggunaan media sosial. Kenetralan dan kebebasan berpendapat dalam media sosial dapat menjadi senjata bermata dua untuk penggunanya (Shelma mayolaika dkk, 2021). Sehingga kadangkala hal inilah yang memunculkan kejahatan di dunia maya. Inilah yang dikenal sebagai *cyber crime*. Bentuk *cyber crime* yang berkaitan dengan kebebasan berbicara adalah ujaran kebencian dan pencemaran nama baik.

Tanpa adanya hukum dan etika yang ketat dalam bermedia sosial, pengguna media sosial dapat melakukan apa pun, termasuk melakukan hal yang tidak baik dan merugikan orang lain. Untuk itu penanggulangan dan penegakan hukum terhadap *cyber crime* sangat dibutuhkan untuk menjadi payung hukum dalam menyelesaikan berbagai persoalan yang muncul akibat penggunaan kecanggihan teknologi informasi dan komunikasi. Inilah yang disebut sebagai hukum *cyber* atau *cyber law*. Dengan demikian dalam penulisan ini, materi yang akan dibahas adalah kebebasan berbicara dalam media sosial dan hukum *cyber* yang ada untuk mengatur kebebasan berbicara pada media sosial.

PEMBAHASAN MATERI

B. KEBEBASAN BERBICARA

Kebebasan berbicara, mengeluarkan pendapat dan berekspresi, menjadi perhatian internasional dan diatur dalam *instrument* internasional seperti pada Pasal 19 Deklarasi Universal Hak Asasi Manusia (DUHAM) yang menyebutkan bahwa: “Setiap orang berhak atas kebebasan mempunyai dan mengeluarkan pendapat dan berekspresi; dalam hal ini termasuk kebebasan menganut pendapat tanpa mendapat gangguan, dan untuk mencari, menerima dan menyampaikan keterangan-keterangan dan

pendapat dengan cara apa pun dan dengan tidak memandang batas-batas". Pembatasan kebebasan ini, diatur dalam Pasal 29 DUHAM, "yang ditetapkan undang-undang yang tujuannya semata-mata untuk menjamin pengakuan serta penghormatan yang tepat terhadap hak-hak dan kebebasan-kebebasan orang lain, dan untuk memenuhi syarat-syarat yang adil dalam hal kesusilaan, ketertiban, dan kesejahteraan umum dalam suatu masyarakat yang demokratis".

Jaminan kebebasan berbicara/berpendapat dan berekspresi sebagaimana diatur dalam Pasal 19 DUHAM, juga sejalan dengan Pasal 19 Kovenan Internasional Hak-Hak Sipil dan Politik (ICCPR) yang menyebutkan bahwa: 1. Setiap orang berhak untuk berpendapat tanpa campur tangan. 2. Setiap orang berhak atas kebebasan untuk menyatakan pendapat, hak ini termasuk kebebasan untuk mencari, menerima dan memberikan informasi dan pemikiran apa pun, terlepas dari pembatasan-pembatasan secara lisan, tertulis, atau dalam bentuk cetakan, karya seni atau melalui media lain sesuai dengan pilihannya. 3. Pelaksanaan hak-hak yang dicantumkan dalam Ayat 2 pasal ini menimbulkan kewajiban dan tanggung jawab khusus. Oleh karenanya dapat dikenai pembatasan tertentu, tetapi hal ini hanya dapat dilakukan sesuai dengan hukum dan sepanjang diperlukan untuk: a. Menghormati hak atau nama baik orang lain; b. Melindungi keamanan nasional atau ketertiban umum atau kesehatan atau moral umum.

Pembatasan jaminan kebebasan yang diatur dalam Pasal 19 Konvensi Internasional Hak-Hak Sipil dan Politik, telah diatur dalam ayat 3 bahwa kebebasan tersebut harus menghormati hak atau nama baik orang lain, melindungi kepentingan nasional atau ketertiban umum atau kesehatan atau moral umum. Dari kedua *instrument* internasional di atas, terlihat bahwa kebebasan berbicara, berpendapat dan berekspresi tetap diberikan pembatasan.

Indonesia sebagai salah satu negara yang menganut paham demokrasi, menjamin kebebasan berbicara, mengeluarkan pendapat dan berekspresi setiap warga negaranya. Jaminan kebebasan berbicara dan berekspresi merupakan hak setiap warga negara harus dijaga dan dilindungi sebagaimana diatur dalam Pasal 28 F UUD 1945. Hak berkomunikasi dan memperoleh informasi, hak untuk mencari, memperoleh, memiliki,

menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia, termasuk menggunakan media sosial sebagai sarana berbicara dan berekspresi. Namun, hak bebas berbicara dan berekspresi tersebut, tetap dibatasi dengan kewajibannya sebagai warga negara yang tetap harus menjaga ketenteraman dan keamanan hidup berbangsa dan bernegara. Sejumlah hak yang melekat padanya, tetap harus dibatasi guna melindungi kepentingan/hak individu lainnya. Pembatasan kebebasan pendapat dalam KUHP dapat dilihat pada: (1) Pasal 207, 208, 209 mengenai penghinaan terhadap penguasa dan badan usaha umum; (2) Pasal 310, 311, 315, 316, penyerangan atau pencemaran kehormatan atau nama baik seseorang dengan tulisan; (3) Pasal 317, fitnah, pemberitahuan palsu, pengaduan palsu: (4) pencemaran nama baik orang mati.

Kebebasan berpendapat dan berekspresi sangat penting dalam kehidupan berdemokrasi, karena: (1) kebebasan berekspresi "penting sebagai cara untuk menjamin pemenuhan diri seseorang" dan juga untuk mencapai potensi maksimal seseorang; (2) untuk pencarian kebenaran dan kemajuan pengetahuan atau dengan kata lain, "seseorang yang mencari pengetahuan dan kebenaran harus mendengar semua sisi pertanyaan, mempertimbangkan seluruh alternatif, menguji penilaiannya dengan menghadapkan penilaian tersebut kepada pandangan yang berlawanan, serta memanfaatkan berbagai pemikiran yang berbeda seoptimal mungkin; (3) kebebasan berekspresi penting agar orang dapat berpartisipasi dalam proses pengambilan keputusan, khususnya di arena politik; dan (4) kebebasan berekspresi memungkinkan masyarakat (dan negara) untuk mencapai stabilitas dan adaptasi/kemampuan beradaptasi (Marwandianto dan Hilmi , 2020).

Kebebasan berbicara, berpendapat dan berekspresi dalam kemajuan teknologi informasi dan komunikasi, maka media sosial dapat menjadi sarana untuk menyalurkan kebebasan berbicara dan berekspresi. Media sosial memungkinkan informasi apapun tersebar secara luas di internet tanpa menyaring apakah konten tersebut baik atau buruk. Konten yang baik akan bermanfaat bagi penggunanya, sebaliknya konten buruk akan merugikan (Rachman, Ryan, *et al.,* 2021).

Media sosial terbagi menjadi 6 jenis, yaitu jejaring sosial, forum, blog, wiki, konten, dan dunia virtual (Kaplan dan Haenlein, 2010). Dari 6 jenis media sosial di atas, yang sering digunakan oleh masyarakat luas adalah Jejaring sosial, blog dan konten. Jejaring sosial adalah sarana bagi pengguna untuk berinteraksi, berkomunikasi, dan bertukar informasi secara *online*. Sedangkan Blog adalah sarana bagi pengguna untuk menyampaikan buah pikirannya secara bebas dalam sebuah situs *online* yang biasanya milik pribadi atau milik bersama (institusi atau komunitas). Selanjutnya Konten adalah hasil karya dari para pembuat yang ingin menyampaikan pikiran dan pendapatnya melalui media yang bisa berbentuk tertulis, lisan, maupun video. Pada tiga jenis jejaring sosial ini, setiap pengguna yang sudah registrasi dan memenuhi syarat usia yang ditentukan dapat dengan bebas menyampaikan pendapatnya asalkan tidak melanggar peraturan-peraturan yang sudah ditetapkan masing-masing media sosial.

Kebebasan berbicara dan berekspresi dalam konteks media sosial tidak hanya berkaitan dengan kebebasan berekspresi, tetapi juga kebebasan atas konektivitas dan kebebasan berpendapat, termasuk kebebasan pers yang berlaku dalam ekosistem jurnalisme digital, ketika menggunakan media digital sebagai sarana berpendapat dan berekspresi. Walaupun media digital merupakan perkembangan dari media konvensional dalam arti fisik, namun media digital tidak terlepas dari manusia sebagai pembangun atau kreator dari media itu sendiri. Hal ini berarti bahwa dalam perkembangan teknologi informasi dan komunikasi di era digitalisasi masih membutuhkan aspek manusia dan pemikirannya yang merupakan pembangunnya (Mufti Nurlatifah, 2020). Manusia sebagai pencipta ekosistem dari media digital tidak terlepas dari sistem sosial, ekonomi, dan politik masyarakat, sehingga akan memberi pengaruh atau berdampak pada isi atau muatan yang ditampilkan dalam media digital tersebut. Untuk itu perlu adanya pembatasan dalam kebebasan berbicara, berpendapat dan berekspresi.

Pembatasan kebebasan berekspresi ini bukan dalam rangka membelenggu hak individu atas kebebasan. Namun memberikan ruang konsekuensi, bahwa dalam setiap kebebasan berekspresi terdapat tanggung jawab sosial. Menurut Laporan Kebebasan Berekspresi PBB

tahun 1998, jaminan atas kebebasan berekspresi ini memiliki pembatasan pada tiga aspek. Pertama, pembatasan dilakukan secara prediktabilitas dan transparansi. Hal ini dilakukan dengan menggunakan hukum yang dapat diakses oleh semua orang. Kedua, pembatasan dilakukan dengan tujuan melindungi hak dan reputasi orang lain serta melindungi keamanan nasional serta ketertiban umum. Ketiga, pembatasan dilakukan dengan prinsip kepentingan dan prinsip proporsionalitas. Pembatasan dilakukan dan harus dibuktikan bahwa hal tersebut dilakukan dengan seminimal mungkin.

C. HUKUM *CYBER*

Dunia maya sebagai lingkungan yang memberikan kesempatan bagi siapa pun untuk berbicara, berekspresi dan menyuarakan ide/pendapat/ gagasannya membutuhkan "aturan main" agar ekspresi diri melalui kebebasan berbicara tidak merugikan atau mengganggu orang lain. Ancaman penyalahgunaan internet ketika diperhadapkan dengan kebebasan berbicara melalui media sosial, seperti adanya ujaran kebencian dan pencemaran nama baik, tentunya membutuhkan seperangkat aturan yang dapat menjadi "rambu-rambu" mengatasi aksi kriminal di dunia maya. Walaupun untuk menciptakan aturan hukum yang ideal sangatlah sulit, karena definisi ideal dapat menimbulkan penafsiran yang berbeda-beda di kalangan penegak hukum (Magdalena dan Setiyadi, 2007).

Kejahatan atau tindak kriminal merupakan perilaku anti sosial yang akan senantiasa ada sepanjang masih ada masyarakat. Tidak ada masyarakat yang sepi dari kejahatan. Menurut Saparinah Sadli, perilaku menyimpang itu merupakan suatu ancaman nyata atau ancaman terhadap norma-norma sosial yang mendasari kehidupan dan keteraturan sosial, dapat menimbulkan ketegangan individu maupun ketegangan sosial, dan merupakan ancaman riil atau potensial bagi keberlangsungan ketertiban sosial (Muladi dan Barda, 2010). Hukum merupakan komponen sistem sosial yang dianggap lebih efektif menyelesaikan problem sosial berupa kejahatan di masyarakat. Keberadaan hukum dalam masyarakat adalah untuk mengatur kepentingan-kepentingan yang timbul dalam pergaulan masyarakat, dimana kepentingan-kepentingan tersebut bisa bertentangan

antara satu dengan yang lain. Untuk itu hukum "hadir" agar lalu lintas kepentingan-kepentingan tersebut tidak saling bertentangan (Budi Suharitanyo, 2013). Demikian pula hukum dibutuhkan dalam mengatur lalu lintas kepentingan setiap individu dalam hal kebebasan berbicara dengan memanfaatkan kecanggihan teknologi informasi dan komunikasi seperti kebebasan berbicara di media sosial, sehingga dapat meminimalisir terjadinya aksi kejahatan ujaran kebencian dan pencemaran nama baik.

Konten yang memuat ujaran kebencian sengaja dibuat oleh oknum tertentu yang bertujuan untuk menghasut dan memprovokasi orang tertentu untuk melakukan kebencian dan kekerasan serta diskriminasi terhadap tokoh agama atau politik tertentu. Tujuan utamanya menciptakan intoleransi dan konflik sosial (Lewerissa, 2018). Sedangkan konten yang memuat pencemaran nama baik bertujuan untuk menyerang kehormatan atau nama baik seseorang (Ali, 2010).

Pengaturan ujaran kebencian dalam UU ITE (merujuk pada Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik), diatur dalam Pasal 28 ayat (2) jo Pasal 45 A ayat (2). Pasal 28 ayat (2) mengatur tentang perbuatan yang dilarang dan Pasal 45 A ayat (2) mengatur tentang ketentuan pidananya. Adapun Pasal 28 ayat (2) berbunyi: "Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antargolongan (SARA)". Sedangkan Pasal 45 A ayat (2) berbunyi: "Setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) Tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu miliar rupiah)".

Kedua pasal dalam UU ITE ini, kemudian diganti dan direformulasi menjadi Pasal 243 ayat (1) jo ayat (2) KUHP baru (merujuk pada Undang-Undang No 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana). Bunyi Pasal 243 ayat (1) KUHP baru: "Setiap orang yang menyiarkan, mempertunjukkan, atau menempelkan tulisan atau gambar sehingga

terlihat oleh umum atau memperdengarkan rekaman sehingga terdengar oleh umum atau menyebarluaskan dengan sarana teknologi informasi, yang berisi pernyataan perasaan permusuhan dengan maksud agar isinya diketahui atau lebih diketahui oleh umum, terhadap satu atau beberapa golongan atau kelompok penduduk Indonesia berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik yang berakibat timbulnya kekerasan terhadap orang atau barang, dipidana dengan pidana penjara paling lama 4 (empat) Tahun atau pidana denda paling banyak kategori IV. Sedangkan bunyi Pasal 243 ayat (2) KUHP baru: " Jika setiap orang sebagai mana dimaksud pada ayat (1) melakukan tindak pidana tersebut dalam menjalankan profesinya dan pada waktu itu belum lewat 2 (dua) tahun sejak adanya putusan pemidanaan yang telah memperoleh kekuatan hukum tetap karena melakukan tindak pidana yang sama, pelaku dapat dijatuhi pidana tambahan berupa pencabutan hak sebagaimana dimaksud dalam Pasal 86 huruf f".

Pasal 86 huruf f mengatur tentang pidana tambahan berupa pencabutan hak untuk menjalankan profesi tertentu. Pengaturan ujaran kebencian dalam KUHP baru memiliki beberapa perbedaan jika dibandingkan pengaturan sebelumnya dalam UU ITE. Dalam KUHP baru, norma atau muatan materinya lebih luas jika dibandingkan pengaturannya dalam UU ITE, sanksi pidana dalam KUHP baru lebih ringan dibandingkan sanksi pidana yang diatur dalam UU ITE. Selain itu dalam KUHP baru terdapat pidana tambahan berupa pencabutan hak untuk menjalankan profesi tertentu, yang mana sanksi berupa pidana tambahan ini, tidak terdapat pada UU ITE.

Pengaturan pencemaran nama baik dalam UU ITE pada Pasal 27 ayat (3) yang mengatur terkait perbuatan yang dilarang jo Pasal 45 ayat (3) yang mengatur ancaman pidananya (sanksi pidana). bunyi Pasal 27 ayat (3): "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/ atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Sedangkan Pasal 45 ayat (3) berbunyi: "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 penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) Tahun dan/atau denda paling banyak 750.000.000,- (tujuh ratus lima puluh juta rupiah).

Kedua pasal dalam UU ITE ini, kemudian direformulasi dalam KUHP baru Pasal 433 ayat (1), (2) dan (3). Bunyi Pasal 433 ayat (1): "Setiap orang yang dengan lisan menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum, dipidana karena pencemaran, dengan pidana penjara paling lama 9 (Sembilan) Bulan atau pidana denda paling banyak kategori II". Bunyi Pasal 433 ayat (2): "Jika perbuatan sebagaimana dimaksud pada ayat (1) dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan, atau ditempelkan di tempat umum, dipidana karena pencemaran tertulis, dengan pidana penjara paling lama 1 (satu) tahun 6 (enam) Bulan atau pidana denda paling banyak kategori III". Bunyi Pasal 433 ayat (3): "Perbuatan sebagaimana dimaksud pada Pasal 433 ayat (1) dan ayat (2) tidak dipidana jika dilakukan untuk kepentingan umum atau karena terpaksa membela diri".

Ketentuan pada Pasal 441 ayat (1) KUHP baru mengatur tentang pemberatan pidana terhadap tindak pidana pencemaran nama baik yang dilakukan melalui sarana teknologi informasi seperti platform digital. Bunyi Pasal 441 ayat (1): "Ketentuan pidana sebagaimana dimaksud dalam Pasal 433 sampai dengan Pasal 439 dapat ditambah 1/3 (satu per tiga) jika dilakukan dengan sarana teknologi informasi".

Perbedaan mendasar pengaturan pencemaran nama baik dalam UU ITE dan dalam KUHP baru adalah: penafsiran tindak pidana pencemaran nama baik dalam KUHP baru menjadi lebih jelas, melindungi orang yang tidak bermaksud kontennya diketahui oleh umum misalnya postingan yang bersifat japri atau *direct message*, ada alasan tidak dipidana jika perbuatan tersebut dilakukan demi kepentingan umum dan terpaksa membela diri, adanya pemberatan pidana sebagaimana diatur dalam Pasal 441 dan pidana tambahan yang diatur dalam Pasal 442 KUHP baru (Ahmad M Ramli, 2023). Demikianlah materi terkait kebebasan berbicara dan hukum *cyber* yang menjelaskan tentang hak setiap orang untuk berbicara

dan mengutarakan pendapatnya terkhusus ketika menggunakan media digital, maka hukum *cyber* hadir untuk memberikan rambu-rambu bagaimana berbicara yang baik sehingga tidak menimbulkan konflik apalagi kejahatan *cyber*.

D. RANGKUMAN MATERI

Kebebasan berbicara, mengeluarkan pendapat dan berekspresi adalah hak setiap individu. Bagi Indonesia sebagai negara yang menganut prinsip demokrasi, kebebasan berbicara, berpendapat dan ekspresi merupakan hak setiap warga negara sebagaimana telah diatur dalam Pasal 28 F UUD 1945. Namun kebebasan berbicara, berpendapat dan berekspresi haruslah dibatasi dengan menghormati dan menghargai kepentingan warga negara yang lain serta menjaga keamanan dan ketenteraman hidup berbangsa dan bernegara.

Kebebasan berbicara melalui media sosial sebagai bentuk kemajuan teknologi informasi dan komunikasi, tetap harus dibatasi dengan rambu-rambu menghormati hak orang lain dan tidak membahayakan kepentingan umum. Untuk itu, dalam dunia maya, dibutuhkan aturan yang memberikan batasan serta pedoman bagi kebebasan berbicara, berpendapat dan berekspresi dalam dunia maya, sehingga tidak menimbulkan kejahatan dunia maya atau *cyber crime*. Dengan demikian hukum *cyber* dibutuhkan untuk mengatur kebebasan berbicara dengan menggunakan sarana media internet.

TUGAS DAN EVALUASI

1. Jelaskan *instrument* hukum internasional dan hukum nasional yang memberikan kebebasan berbicara, berpendapat dan berekspresi ?
2. Jelaskan batasan-batasan hukum internasional dan hukum nasional terhadap kebebasan berbicara, berpendapat dan berekspresi baik melalui media konvensional maupun media digital ?
3. Jelaskan pendapat saudara mengapa kebebasan berbicara, berpendapat dan berekspresi perlu dibatasi ?
4. Mengapa ujaran kebencian dan pencemaran nama baik menjadi bentuk kejahatan di dunia maya atau *cyber crime* ?
5. Jelaskan bagaimana pengaturan tindak pidana ujaran kebencian dan pencemaran nama baik dalam UU ITE dan KUHP baru ?

DAFTAR PUSTAKA

Ahmad M Ramli, Pager Gunung, Indra Apriadi, Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik, Departemen Komunikasi dan Informatika RI, Jakarta, 2005, Hal 1

Ahmad M Ramli, Pasal Ujaran Kebencian UU ITE yang Dicabut dan Penggantinya di UU KUHP, https://nasional.kompas.com/read/2023/03/01/13285951/, Maret 2023

Budi Suharitanyo, Tindak Pidana Teknologi Informasi (cyber crime) Urgensi Pengaturan dan Celah Hukumnya, Raja Grafindo Persada, Jakarta, 2013, Hal 22-23

Kaplan, Andreas M; Michael Haenlein, Users of the world, unite the challenges and opportunities of social media, Businness Horizons 53 (1), Hal 59-68

Mahrus Ali, Pencemaran nama baik melalui sarana Informasi dan Transasi Elektronik (kajian Putusan MK No 2/ PUU-VII/2009), 2010, Hal 143

Marwandianto dan Hilmi Ardani Nasution, Hak Atas Kebebasan Berpendapat dan Berekspresi Dalam Koridor Penerapan Pasal 310 dan 311 KUHP (The Rights to Freedom of Opinion and Expression in The Corridor od Article 310 and 311 KUHP), Jurnal HAM, Vol 11 No 1 Tahun 2020, Hal 2

Merry Magdalena dan Maswigrantoro Roes Setiyadi, Cyber Law ? Tidak perlu Takut, CV ANDI, Yogjakarta, 2007, Hal 116

Mufti Nurlatifah, Persimpangan Kebebasan Berekspresi dan Tanggung Jawab Sosial pada Regulasi Jurnalisme Digital di Indonesia , Jurnal IPTEK-KOM, Vol. 22 No. 1, Juni 2020, Hal 77 – 93

Muladi dan Barda Nawawi Arief, Teori-teori dan Kebijakan Hukum Pidana, Edisi revisi, Alumni, Bandung, 2010, Hal 93

Rachman F, Ryan T, Kabatiah M, Batubara A, Pratama F, F Nurgiansah, T. H, Pelaksanaan Kurikulum PPKn pada Kondisi Khusus Pandemic Covid-19, Jurnal Basicedu, Vo. 5 No 6 Tahun 2021, hal 5682-5691

Shelma Mayolaika, Valerie Victoria Effendy, Christian Delvin, & Mohammad Aqila Hanif, Pengaruh kebebasan Berpendapat Di Sosial Media Terhadap Perrubahan Etika dan Norma Remaja Indonesia, Jurnal Kewarganegaraan Vol. 5 No. 2 Desember, 2021, Hal 831

Yanti Amelia Lewerissa, Criminal policy of Hate Speech in Social Media Against The Religious Dignity of Society in The Digital Century, ASSEHR Vol 187, Atlantis Press, 2018, Hal 71-76

HUKUM *CYBER*

BAB 9: PENGATURAN INTERNET DAN KEAMANAN NASIONAL

Fahririn, S.H., M.H

Universitas Sahid

BAB 9

PENGATURAN INTERNET DAN KEAMANAN NASIONAL

A. PENDAHULUAN

Perkembangan internet dari tahun ke tahun telah mengubah cara kita hidup, berkomunikasi, dan berinteraksi dengan dunia di sekitar kita. Berikut adalah ringkasan tentang perkembangan internet dari tahun ke tahun dan dampaknya secara umum:

Awal 1990-an: Pada awal 1990-an, internet mulai menjadi lebih populer di kalangan masyarakat umum. *World Wide Web* (WWW) diperkenalkan oleh Tim *Berners-Lee* pada tahun 1991, yang mengubah internet menjadi *platform* untuk mengakses informasi dan berbagi konten.

Dampak: Kemunculan WWW memungkinkan pertukaran informasi yang lebih mudah dan cepat di seluruh dunia. Ini membuka pintu bagi akses ke pengetahuan, perdagangan elektronik, dan komunikasi global yang lebih luas. Pertengahan 1990-an: Pada pertengahan 1990-an, munculnya layanan email, *chatting*, dan forum *online* semakin mempopulerkan penggunaan internet. Teknologi modem *dial-up* digunakan secara luas. Dampak: Komunikasi *online* menjadi lebih mudah dan cepat. Masyarakat dapat berinteraksi melalui email, *chatting*, dan forum untuk berbagi ide, informasi, dan pengalaman.

Akhir 1990-an: Pada akhir 1990-an, munculnya layanan jejaring sosial seperti *Friendster* dan *Myspace* membuka jalan bagi interaksi sosial *online* yang lebih luas.

Dampak: Jejaring sosial memungkinkan orang untuk terhubung dengan teman, keluarga, dan orang-orang dengan minat yang sama. Ini memfasilitasi pembentukan komunitas *online* dan berbagi konten secara lebih terbuka. Awal 2000-an: Pada awal 2000-an, munculnya layanan seperti Google, Wikipedia, dan YouTube mengubah cara kita mencari informasi, mendapatkan pengetahuan, dan mengakses konten multimedia.

Dampak: Akses ke informasi menjadi lebih mudah dan cepat. Orang-orang dapat mencari berbagai topik, mendapatkan pengetahuan, dan mengakses video, musik, dan konten multimedia dengan mudah.

Pertengahan hingga akhir 2000-an: Perkembangan teknologi *broadband*, komputasi awan, dan perangkat *mobile* seperti *smartphone* memperluas akses internet ke lebih banyak orang di seluruh dunia. Dampak: Kemampuan untuk terhubung dengan internet menjadi lebih cepat, lebih stabil, dan lebih mudah diakses. Masyarakat dapat mengakses internet di mana saja dan kapan saja melalui perangkat *mobile*, membuka pintu bagi berbagai layanan dan aplikasi yang inovatif. Tahun 2010-an hingga saat ini: Perkembangan internet selama dekade terakhir ini ditandai oleh kehadiran media sosial seperti Facebook, Twitter, dan Instagram, serta peningkatan adopsi teknologi *Internet of Things* (IoT) dan kecerdasan buatan (AI).

B. PERKEMBANGAN DAN PENGERTIAN INTERNET

Perkembangan internet saat ini telah mencapai tingkat yang sangat maju dan terus berkembang dengan pesat. Perkembangan internet saat ini telah mencapai tingkat yang sangat maju dan terus berkembang dengan pesat. Hal ini disebabkan oleh beberapa faktor utama. Pertama, kemajuan teknologi dan infrastruktur dalam bidang komunikasi dan jaringan telah memungkinkan pengembangan infrastruktur yang kuat untuk mendukung pertumbuhan internet. Teknologi nirkabel seperti 4G dan 5G, serta jaringan serat optik yang canggih, memberikan kecepatan dan kapasitas yang diperlukan untuk mentransfer data dengan cepat dan efisien. Permintaan akan konektivitas internet yang lebih cepat dan akses yang lebih mudah semakin meningkat di kalangan masyarakat.

Selain itu, inovasi terus muncul dalam pengembangan aplikasi dan layanan internet. Perusahaan dan pengembang berlomba-lomba untuk menciptakan solusi yang lebih baik, lebih efisien, dan lebih mudah digunakan. Hal ini menghasilkan peningkatan fitur, fungsionalitas, dan pengalaman pengguna yang lebih baik. Internet juga telah menghubungkan orang-orang dari berbagai belahan dunia, menghapuskan batasan geografis dan memungkinkan pertukaran informasi yang lebih cepat dan luas. Dukungan pemerintah dan investasi juga memainkan peran penting dalam memfasilitasi perkembangan internet. Banyak pemerintah dan lembaga swasta mengakui pentingnya perkembangan internet dan berinvestasi dalam infrastruktur dan teknologi yang diperlukan. Langkah-langkah ini termasuk pengembangan kebijakan progresif, alokasi sumber daya yang cukup, dan mendorong inovasi dan penelitian di bidang teknologi internet.

Semua faktor ini saling berhubungan dan saling mempengaruhi, menciptakan lingkungan yang kondusif bagi perkembangan internet yang maju dan pesat.

Berikut ini adalah beberapa perkembangan teknologi internet saat ini:

1. Internet Kecepatan Tinggi
   Teknologi *broadband* dan jaringan serat optik telah menghadirkan internet kecepatan tinggi yang memungkinkan transfer data yang lebih cepat dan akses yang lebih lancar.
2. Internet Nirkabel
   Kemajuan dalam teknologi nirkabel telah menghasilkan konektivitas internet yang lebih mudah dan lebih luas melalui Wi-Fi, 4G, dan 5G. Ini memungkinkan akses internet yang cepat dan stabil di berbagai perangkat seperti *smartphone*, tablet, dan perangkat pintar.
3. *Internet of Things* (IoT)
   IoT mengacu pada jaringan perangkat terhubung yang dapat saling berkomunikasi dan berbagi data melalui internet. Ini mencakup perangkat seperti sensor pintar, peralatan rumah tangga terhubung, kendaraan otonom, dan banyak lagi. IoT telah membuka jalan bagi solusi yang inovatif dalam berbagai bidang, termasuk rumah pintar, kesehatan, transportasi, dan industri.

4. *Cloud Computing*
   Layanan *cloud computing* memungkinkan penyimpanan dan akses data melalui internet. Ini memberikan kemampuan untuk menyimpan, mengelola, dan mengakses data dari berbagai perangkat secara fleksibel, serta menyediakan layanan seperti komputasi awan, penyimpanan data, dan pengolahan data di awan.
5. Kecerdasan Buatan (*Artificial Intelligence*, AI)
   Kemajuan dalam AI telah mempengaruhi perkembangan internet dengan cara yang signifikan. AI digunakan dalam berbagai aplikasi internet, termasuk pengenalan suara dan gambar, *chatbot*, personalisasi konten, dan rekomendasi produk.

Secara teknis, internet adalah jaringan komputer yang terdiri dari berbagai perangkat seperti komputer, *server, router*, dan perangkat jaringan lainnya yang terhubung melalui berbagai teknologi seperti kabel serat optik, kabel tembaga, nirkabel, dan satelit. Kata "internet" sendiri berasal dari bahasa Inggris dan merupakan singkatan dari "*Interconnected Network*". Istilah ini digunakan oleh Vinton Cerf dan Bob Kahn pada tahun 1974 dalam konteks pengembangan protokol TCP/IP. Istilah "internet" kemudian menjadi istilah yang umum digunakan untuk merujuk pada jaringan komputer global yang kita kenal saat ini, termasuk dalam bahasa Indonesia.

C. DAMPAK NEGATIF DAN BENTUK KEJAHATAN AKIBAT PERKEMBANGAN INTERNET

Selain memiliki manfaat yang banyak, internet juga memiliki dampak *negative*. Berikut adalah beberapa masalah atau dampak *negative* yang muncul:

1. Keamanan Data:

a. Ancaman keamanan siber
   Dengan semakin banyaknya aktivitas *online*, risiko terhadap serangan siber dan pencurian data meningkat. Peretasan, *malware, phishing*, dan serangan lainnya dapat mengakibatkan kerugian finansial dan pencurian informasi pribadi.

b. Pelanggaran privasi
Banyak *platform online* mengumpulkan data pengguna untuk tujuan pemasaran atau analisis. Hal ini menimbulkan kekhawatiran tentang pelanggaran privasi dan penggunaan data pribadi tanpa izin.

2. Kecanduan Internet:

a. Gangguan keseimbangan kehidupan
Kecanduan internet dapat menyebabkan gangguan dalam kehidupan sehari-hari, termasuk penurunan produktivitas, isolasi sosial, dan masalah kesehatan mental dan fisik.

b. Ketergantungan pada media sosial
Penggunaan berlebihan media sosial dapat menyebabkan kecemasan sosial, depresi, dan perasaan tidak puas terhadap kehidupan pribadi.

3. Kesenjangan Digital:

a. Aksesibilitas terbatas
Tidak semua orang memiliki akses yang setara ke internet dan teknologi terkait. Kesenjangan digital terjadi antara mereka yang memiliki akses yang luas dan fasilitas teknologi yang memadai dengan mereka yang tidak.

b. Ketimpangan informasi
Orang-orang yang tidak memiliki akses internet atau tidak terampil dalam penggunaan teknologi dapat tertinggal dalam akses terhadap informasi penting, peluang pendidikan, dan kebutuhan ekonomi.

Perkembangan internet telah membuka pintu bagi berbagai bentuk kejahatan baru. Berikut adalah beberapa contoh kejahatan yang sering terjadi di era digital:

1. Penipuan *Online*
Kejahatan penipuan *online* melibatkan manipulasi, penipuan, atau penyalahgunaan informasi secara elektronik. Ini termasuk penipuan melalui email, situs web palsu, atau aplikasi perpesanan. Contohnya adalah penipuan investasi, penipuan jual beli *online*, atau penipuan melalui *phishing*.

2. Serangan Siber
   Serangan siber melibatkan upaya yang tidak sah untuk mengakses, merusak, atau menghancurkan sistem komputer, jaringan, atau perangkat elektronik lainnya. Contoh serangan siber termasuk serangan virus komputer, serangan DDoS (*Distributed Denial of Service*), dan pencurian data.
3. Kejahatan Seksual *Online*
   Internet juga digunakan oleh pelaku kejahatan seksual untuk menyebarkan, memperoleh, atau memperdagangkan materi pornografi anak, menyebarkan pelecehan seksual *online*, atau melakukan penipuan romansa.
4. Penyebaran Konten Ilegal
   Internet memungkinkan penyebaran konten ilegal seperti pornografi anak, materi teroris, atau konten yang melanggar hak cipta.
5. *Cyberbullying*
   Cyberbullying terjadi ketika seseorang diserang, dilecehkan, atau diintimidasi secara *online* melalui pesan, komentar, atau media sosial. Ini dapat memiliki dampak serius pada kesehatan mental dan emosional korban.
6. Identitas Palsu
   Internet juga digunakan untuk menciptakan identitas palsu atau mengambil alih identitas orang lain dengan tujuan penipuan, pelecehan, atau tindakan kriminal lainnya.
7. Kejahatan Keuangan *Online*
   Ini meliputi pencurian identitas, pencurian informasi kartu kredit, dan penipuan keuangan lainnya yang dilakukan melalui internet.

D. PENGATURAN INTERNET

Berikut adalah poin penting yang harus kita pahami tentang pengaturan internet, khususnya yang ada di negara Indonesia.

Undang-Undang ITE (Informasi dan Transaksi Elektronik):

Undang-undang (UU) No. 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE) Merupakan undang-undang yang mengatur kegiatan di dunia maya di Indonesia, termasuk sanksi pidana dan perdata terkait pelanggaran

melalui internet. Undang-Undang ITE (Informasi dan Transaksi Elektronik) merupakan kerangka hukum utama di Indonesia yang mengatur berbagai aspek kegiatan di dunia maya atau internet. Undang-Undang ini diberlakukan untuk melindungi kepentingan masyarakat, menjaga keamanan, ketertiban, dan ketenteraman dalam penggunaan teknologi informasi dan transaksi elektronik. Berikut ini adalah beberapa poin penting yang perlu dipahami tentang Undang-Undang ITE:

1. Ruang Lingkup
   Undang-Undang ITE mencakup berbagai aspek seperti transaksi elektronik, komunikasi elektronik, perlindungan informasi elektronik, dan tindakan-tindakan pidana yang terkait dengan penggunaan teknologi informasi.
2. Definisi dan Ketentuan
   Undang-Undang ITE menguraikan definisi dari berbagai istilah yang terkait dengan teknologi informasi dan transaksi elektronik. Hal ini membantu dalam penafsiran dan implementasi hukum tersebut.
3. Transaksi Elektronik
   Undang-Undang ITE mengatur tentang legalitas dan validitas transaksi elektronik, termasuk pengakuan hukum terhadap dokumen elektronik, tanda tangan elektronik, dan penerimaan surat elektronik sebagai bukti.
4. Kebijakan Keamanan dan Privasi
   Undang-Undang ITE mewajibkan pihak yang melakukan kegiatan di dunia maya untuk menjaga keamanan dan privasi data pribadi yang diperoleh atau diolah. Hal ini menekankan perlindungan terhadap informasi pribadi dan mengatur tanggung jawab pengguna dan penyedia layanan terkait dengan pengelolaan data.
5. Pelanggaran dan Sanksi
   Undang-Undang ITE menetapkan berbagai tindakan yang dianggap melanggar hukum, seperti penyebaran konten negatif, penghinaan, penipuan, atau serangan siber. Sanksi pidana dan perdata yang berlaku untuk pelanggaran tersebut diatur dalam undang-undang ini.
6. Tanggung Jawab *Platform*
   Undang-Undang ITE mengatur tanggung jawab penyelenggara sistem elektronik atau *platform* terkait dengan konten yang diunggah oleh

pengguna. Penyelenggara *platform* diharuskan untuk melakukan tindakan yang wajar dalam mengelola dan menyaring konten ilegal atau berbahaya.

7. Proses Penyelidikan dan Penyidikan
   Undang-Undang ITE juga mencakup ketentuan mengenai proses penyelidikan dan penyidikan terkait tindak pidana yang dilakukan melalui teknologi informasi. Hal ini melibatkan proses penuntutan, pengumpulan bukti elektronik, serta koordinasi antara lembaga penegak hukum dan penyelenggara sistem elektronik.

Undang-Undang ITE terus mengalami perkembangan dan penyesuaian sesuai dengan perkembangan teknologi dan kebutuhan masyarakat. Penting untuk mengikuti perubahan terkini dalam undang-undang ini guna memahami hak dan kewajiban terkait dengan penggunaan internet di Indonesia

Sesuai dengan Undang-Undang ITE, terdapat sanksi pidana dan perdata yang dapat diberikan kepada pelanggaran yang dilakukan melalui internet. Berikut ini adalah penjelasan lebih lanjut mengenai sanksi-sanksi tersebut:

1. Sanksi Pidana
   a. Pasal-pasal yang mengatur tindakan pidana di dalam Undang-Undang ITE mencakup berbagai pelanggaran seperti pencurian identitas, penyebaran konten negatif, penghinaan, pencemaran nama baik, penipuan *online*, serangan siber, dan tindakan kriminal lainnya yang dilakukan melalui internet.
   b. Sanksi pidana yang dapat diberikan meliputi hukuman penjara, denda, atau kombinasi dari keduanya, tergantung pada tingkat pelanggaran dan kerugian yang ditimbulkan.
   c. Sanksi pidana juga dapat diberikan kepada penyelenggara sistem elektronik atau *platform* yang tidak mematuhi kewajiban mereka dalam mengelola konten atau tidak memberikan kerja sama dalam proses penyidikan.

2. Sanksi Perdata
    a. Selain sanksi pidana, Undang-Undang ITE juga menyediakan sanksi perdata bagi pelanggaran yang dilakukan melalui internet. Sanksi ini berkaitan dengan tuntutan ganti rugi atau kompensasi atas kerugian yang ditimbulkan akibat pelanggaran tersebut.
    b. Seseorang atau perusahaan yang mengalami kerugian akibat pelanggaran yang dilakukan melalui internet dapat mengajukan tuntutan perdata untuk mendapatkan penggantian kerugian yang telah diderita.

Perlu dicatat bahwa sanksi pidana dan perdata yang diberikan bergantung pada tingkat pelanggaran, kerugian yang ditimbulkan, serta pertimbangan lain yang relevan. Penerapan sanksi tersebut dilakukan melalui proses hukum yang melibatkan penyidikan, persidangan, dan putusan pengadilan yang berwenang.

Penting untuk mematuhi Undang-Undang ITE dan menghindari pelanggaran hukum dalam penggunaan internet. Mengetahui dan memahami ketentuan hukum ini dapat membantu masyarakat dan mahasiswa dalam menjaga keamanan dan bertindak secara bertanggung jawab dalam beraktivitas di dunia maya.

Beberapa poin penting dalam Undang-Undang ITE yang berhubungan dengan privasi, keamanan data, dan hak cipta:

1. Privasi dan Perlindungan Data Pribadi:
    a. Undang-Undang ITE menegaskan perlindungan terhadap privasi dan data pribadi individu yang diperoleh atau diolah melalui teknologi informasi.
    b. Penyelenggara sistem elektronik atau *platform* wajib menjaga kerahasiaan informasi pribadi yang diperoleh atau diolah dalam pengelolaan sistem mereka.
    c. Individu memiliki hak untuk mengetahui penggunaan data pribadi mereka serta dapat mengajukan permintaan penghapusan, perbaikan, atau pemblokiran data tersebut jika dibutuhkan.

2. Keamanan Data dan Sistem:
    a. Undang-Undang ITE mengatur bahwa penyelenggara sistem elektronik atau platform wajib melindungi data dan sistem dari akses, penggunaan, dan perubahan yang tidak sah.
    b. Penyelenggara sistem elektronik diharuskan melaksanakan tindakan keamanan yang wajar sesuai dengan standar teknis yang berlaku.
    c. Pelanggaran terhadap keamanan data atau sistem yang mengakibatkan kerugian dapat menimbulkan sanksi pidana atau perdata bagi pelaku.
3. Hak Cipta dan Konten Digital:
    a. Undang-Undang ITE melindungi hak cipta atas karya-karya yang dilindungi undang-undang, termasuk dalam bentuk digital.
    b. Penyebaran, penggandaan, atau pemutaran karya yang dilindungi hak cipta melalui internet tanpa izin dari pemegang hak cipta dapat dikenai sanksi pidana atau perdata.
    c. Penyedia *platform* atau penyelenggara sistem elektronik juga memiliki tanggung jawab untuk mencegah penyebaran konten yang melanggar hak cipta atau menghapus konten tersebut setelah adanya laporan yang sah.
4. Kejahatan Siber:
    a. Undang-Undang ITE mencakup ketentuan yang mengatur tindakan pidana terkait kejahatan siber seperti peretasan, pencurian data elektronik, penipuan *online*, dan serangan terhadap keamanan sistem elektronik.
    b. Pelaku kejahatan siber dapat dikenai sanksi pidana sesuai dengan tingkat pelanggaran dan kerugian yang ditimbulkan.

Poin-poin di atas merupakan beberapa aspek penting yang terkait dengan privasi, keamanan data, dan hak cipta dalam Undang-Undang ITE. Memahami ketentuan-ketentuan ini penting untuk melindungi hak-hak individu dan mencegah pelanggaran dalam penggunaan teknologi informasi dan transaksi elektronik di Indonesia.

E. PERLINDUNGAN DATA PRIBADI YANG DIATUR OLEH UNDANG-UNDANG NOMOR 11 TAHUN 2020

Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, yang juga dikenal sebagai Omnibus Law, mengatur Perlindungan Data Pribadi di Indonesia. Undang-Undang ini memiliki beberapa poin penting yang berhubungan dengan perlindungan data pribadi, meskipun tidak secara spesifik fokus pada aspek tersebut. Berikut adalah penjelasan mengenai poin-poin utama yang berkaitan dengan perlindungan data pribadi dalam Undang-Undang tersebut:

1. Definisi Data Pribadi
   Undang-Undang Cipta Kerja mengakui pentingnya perlindungan data pribadi dan memberikan definisi yang luas tentang apa yang dianggap sebagai "data pribadi." Definisi ini mencakup informasi yang dapat mengidentifikasi individu, baik langsung maupun tidak langsung.
2. Persetujuan Pemilik Data
   Undang-Undang ini menegaskan bahwa penggunaan data pribadi harus didasarkan pada persetujuan dari pemilik data. Penyelenggara sistem elektronik atau pihak yang memproses data harus memperoleh persetujuan yang jelas dan tegas sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi tersebut.
3. Pengumpulan, Penggunaan, dan Pengungkapan Data Pribadi
   Undang-Undang Cipta Kerja mewajibkan pihak yang mengumpulkan data pribadi untuk menjaga kerahasiaan, keutuhan, dan keamanan data tersebut. Penggunaan dan pengungkapan data pribadi hanya boleh dilakukan sesuai dengan tujuan yang dijelaskan dalam persetujuan pemilik data atau jika diizinkan oleh hukum.
4. Kewajiban Penyelenggara Sistem Elektronik
   Undang-Undang ini menetapkan kewajiban bagi penyelenggara sistem elektronik untuk melindungi data pribadi yang mereka kelola. Mereka harus mengimplementasikan langkah-langkah keamanan dan tindakan yang wajar untuk mencegah akses, penggunaan, dan perubahan data pribadi oleh pihak yang tidak berwenang.

5. Pemindahan Data Pribadi ke Luar Negeri
   Undang-Undang Cipta Kerja mengatur bahwa pemindahan data pribadi ke luar negeri harus memenuhi persyaratan tertentu, termasuk memastikan bahwa negara tujuan memiliki tingkat perlindungan data yang memadai.
6. Hak Pemilik Data
   Undang-Undang ini memberikan hak kepada pemilik data untuk mengakses, memperbaiki, dan menghapus data pribadi mereka yang dikumpulkan atau diolah oleh pihak lain. Pemilik data juga memiliki hak untuk membatasi atau menghentikan penggunaan data pribadi mereka dalam situasi tertentu.

Meskipun Undang-Undang Cipta Kerja mencakup beberapa aspek perlindungan data pribadi, secara umum undang-undang ini lebih fokus pada reformasi hukum untuk mendorong investasi dan pertumbuhan ekonomi di Indonesia. Untuk aspek perlindungan data pribadi yang lebih spesifik, terdapat undang-undang terpisah yang relevan, seperti Rancangan Undang-Undang Perlindungan Data Pribadi yang saat ini masih dalam proses pembahasan di Indonesia.

Dampak perkembangan internet juga berbanding lurus dengan perkembangan penggunaan media sosial dan *platform* digital lainnya. Beberapa perusahaan dan masyarakat bersaing dalam membuat konten digital sebagai bentuk promosi digital atau khususnya dibidang digital kreatif. Tetapi ada beberapa konten digital yang mengabaikan aturan-aturan yang berlaku. Peraturan mengenai konten digital yang meliputi larangan atas penyebaran konten negatif, berbahaya, atau melanggar hukum.

Peraturan mengenai konten digital adalah aturan yang mengatur penyebaran konten di ruang digital dengan tujuan menjaga keamanan, integritas, dan kepatuhan terhadap hukum di lingkungan digital. Peraturan ini bertujuan untuk melarang penyebaran konten negatif, berbahaya, atau melanggar hukum. Meskipun persyaratan dan batasan yang diberlakukan dapat bervariasi antara negara dan yurisdiksi, terdapat beberapa prinsip umum yang sering diadopsi dalam peraturan mengenai konten digital.

Berikut ini adalah beberapa aspek yang sering diatur dalam peraturan tersebut:

1. Larangan atas Konten Negatif
   Peraturan mengenai konten digital biasanya melarang penyebaran konten yang dianggap negatif, seperti konten yang mengandung kebencian, penghinaan, diskriminasi, atau ancaman terhadap individu atau kelompok tertentu. Tujuannya adalah untuk mencegah penyebaran konten yang merugikan atau merugikan orang lain.
2. Larangan atas Konten Berbahaya
   Peraturan tersebut juga melarang penyebaran konten yang dianggap berbahaya, seperti konten yang mengandung kekerasan, pornografi anak, anjuran bunuh diri, atau penyebaran informasi yang dapat merusak kesehatan atau keamanan masyarakat.
3. Pelanggaran Hak Kekayaan Intelektual
   Peraturan mengenai konten digital juga melarang penyebaran konten yang melanggar hak kekayaan intelektual, termasuk pelanggaran hak cipta, merek dagang, atau paten. Konten seperti reproduksi tidak sah, pembajakan, atau penyebaran barang palsu dapat dilarang dan dikenai sanksi.
4. Perlindungan Anak
   Peraturan ini juga memberikan perlindungan khusus terhadap anak-anak dengan melarang penyebaran konten yang merugikan atau melanggar hak-hak anak, seperti konten pornografi anak, eksploitasi anak, atau kekerasan terhadap anak.
5. Penyebaran Informasi yang Melanggar Hukum
   Peraturan ini melarang penyebaran konten yang melanggar hukum, termasuk penyebaran informasi palsu atau hoaks, fitnah, atau konten yang melibatkan tindakan kriminal, seperti penyebaran narkoba, perdagangan manusia, atau kegiatan teroris.

Peraturan mengenai konten digital dapat bervariasi dari negara ke negara, dan penerapan serta sanksi yang diberlakukan juga berbeda-beda. Penting bagi individu dan perusahaan untuk memahami peraturan yang berlaku dalam yurisdiksi mereka dan mematuhi persyaratan tersebut guna menjaga integritas dan keamanan di ruang digital.

F. MEKANISME PELAPORAN DAN PENANGANAN KONTEN ILEGAL ATAU BERBAHAYA DI *PLATFORM DIGITAL*

Di Indonesia, terdapat mekanisme pelaporan dan penanganan konten ilegal atau berbahaya di *platform* digital yang diatur oleh Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika (Permendikbud) Nomor 5 Tahun 2020 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE).

Berikut adalah langkah-langkah umum dalam mekanisme pelaporan dan penanganan konten ilegal atau berbahaya di *platform digital* di Indonesia:

1. Pelaporan Konten: Jika pengguna menemukan konten yang dianggap ilegal atau berbahaya, mereka dapat melaporkannya kepada penyedia platform atau ke pihak berwenang. Biasanya, platform menyediakan mekanisme pelaporan di dalam platform mereka sendiri, seperti tombol "Laporkan Konten" atau formulir pelaporan yang dapat diakses pengguna.
2. Identifikasi dan Verifikasi: Setelah menerima laporan, penyedia platform akan mengidentifikasi dan memverifikasi konten yang dilaporkan. Mereka akan mengevaluasi apakah konten tersebut melanggar hukum atau kebijakan yang telah ditetapkan.
3. Tindakan Penanganan: Jika konten dikonfirmasi melanggar hukum atau kebijakan, penyedia platform akan mengambil tindakan yang sesuai. Tindakan tersebut dapat berupa penghapusan konten, penonaktifan akun pengguna yang melanggar, atau tindakan lain yang dianggap perlu untuk menangani konten tersebut.
4. Kerja Sama dengan Pihak Berwenang: Jika konten ilegal melibatkan tindak pidana yang lebih serius, penyedia platform dapat bekerja sama dengan pihak berwenang, seperti Kepolisian atau Kementerian Komunikasi dan Informatika, untuk melakukan tindakan lebih lanjut sesuai dengan hukum yang berlaku.

Selain itu, di Indonesia terdapat juga beberapa lembaga yang berperan dalam penanganan konten ilegal atau berbahaya, seperti Badan Reserse Kriminal (Bareskrim) Polri, Badan Siber dan Sandi Negara (BSSN),

dan Komisi Penyiaran Indonesia (KPI). Lembaga-lembaga ini bertugas untuk memantau, mengawasi, dan mengatasi masalah terkait konten ilegal atau berbahaya di platform digital.

Perlu dicatat bahwa setiap platform digital mungkin memiliki mekanisme dan prosedur yang sedikit berbeda dalam penanganan konten ilegal atau berbahaya. Oleh karena itu, penting bagi pengguna untuk mengacu pada pedoman dan kebijakan yang ditetapkan oleh masing-masing *platform* yang mereka gunakan.

Di Indonesia, pengaturan mengenai *e-government, e-commerce*, dan transaksi elektronik diatur oleh beberapa undang-undang dan peraturan. Berikut adalah pengaturan yang relevan dalam konteks tersebut:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
   Undang-undang ini menjadi dasar hukum yang mengatur transaksi elektronik di Indonesia. UU ITE mengatur penggunaan informasi elektronik, tanda tangan elektronik, dan keamanan transaksi elektronik.
2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Amandemen)
   Undang-undang ini merupakan amandemen dari UU ITE yang mencakup aspek perlindungan data pribadi dan hak-hak individu dalam konteks transaksi elektronik.
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik
   Undang-undang ini mengatur penggunaan teknologi informasi dalam penyelenggaraan pelayanan publik (*e-government*). Undang-undang ini mendorong penerapan teknologi informasi dalam proses administrasi pemerintahan dan memberikan akses elektronik yang mudah kepada masyarakat untuk mendapatkan layanan publik.
4. Peraturan Bank Indonesia Nomor 18/40/PBI/2016 tentang Penyelenggaraan Sistem Pembayaran
   Peraturan ini mengatur tentang penyelenggaraan sistem pembayaran elektronik di Indonesia. Peraturan ini menetapkan standar keamanan

dan ketentuan yang harus dipatuhi oleh penyelenggara jasa sistem pembayaran elektronik.

5. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik
   Peraturan ini mengatur *e-commerce* di Indonesia. Peraturan ini mencakup persyaratan dan kewajiban bagi pelaku usaha *e-commerce*, perlindungan konsumen, ketentuan mengenai penawaran, transaksi, dan penyelesaian sengketa dalam perdagangan melalui sistem elektronik.
6. Peraturan Kementerian Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
   Peraturan ini mengatur perlindungan data pribadi dalam konteks transaksi elektronik. Peraturan ini menetapkan persyaratan dan prosedur pengelolaan dan perlindungan data pribadi yang harus dipatuhi oleh penyelenggara sistem elektronik dan pengguna data pribadi.

Pengaturan-pengaturan tersebut bertujuan untuk menciptakan kerangka hukum yang jelas dan mengatur praktik yang aman dalam *e-government, e-commerce*, dan transaksi elektronik di Indonesia. Hal ini memberikan perlindungan kepada pengguna, mengatur tata cara bertransaksi secara elektronik, dan mendorong pertumbuhan sektor digital di negara ini.

G. PERAN DAN UPAYA PEMERINTAH DALAM PENGATURAN INTERNET

Peran pemerintah Indonesia dalam pengaturan internet melibatkan beberapa aspek yang penting untuk dipahami. Berikut adalah beberapa hal yang perlu diketahui:

1. Kebijakan Regulasi
   Pemerintah Indonesia memiliki peran utama dalam merumuskan dan menerapkan kebijakan regulasi terkait pengaturan internet. Ini termasuk undang-undang, peraturan, dan keputusan yang mengatur berbagai aspek penggunaan internet, seperti privasi data, keamanan *online*, hak cipta, dan isu-isu lainnya.

2. Komisi Penyiaran Indonesia (KPI)
   KPI adalah lembaga yang bertugas mengawasi dan mengatur konten di media penyiaran, termasuk internet. Mereka bertanggung jawab memastikan bahwa konten yang disiarkan melalui internet mematuhi standar moral, etika, dan hukum yang berlaku di Indonesia.
3. Kementerian Komunikasi dan Informatika (Kominfo)
   Kementerian Komunikasi dan Informatika adalah lembaga pemerintah yang memiliki peran penting dalam pengaturan internet di Indonesia. Mereka bertanggung jawab mengembangkan kebijakan dan regulasi terkait telekomunikasi, informasi, dan teknologi di negara ini. Kominfo juga mengawasi keamanan siber, perlindungan data pribadi, serta pengaturan konten di internet.
4. Blokir Konten
   Pemerintah Indonesia memiliki kebijakan untuk memblokir akses ke konten yang dianggap melanggar hukum, seperti konten pornografi, perjudian *online*, penyebaran hoaks, dan konten yang dianggap mengancam keamanan nasional. Blokir konten dilakukan oleh Kominfo berdasarkan dasar hukum yang berlaku di Indonesia.
5. Perlindungan Data Pribadi: Pemerintah Indonesia juga mengatur perlindungan data pribadi pengguna internet. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur mengenai perlindungan data pribadi serta tindakan yang melanggar privasi *online*.
6. Pengawasan dan Penegakan Hukum
   Pemerintah Indonesia memiliki kewenangan untuk mengawasi dan menegakkan hukum terkait kejahatan yang dilakukan melalui internet, seperti penyebaran konten ilegal, penipuan *online*, atau serangan siber. Penegakan hukum dilakukan oleh berbagai lembaga, seperti kepolisian dan lembaga penegak hukum lainnya.
7. Program Digitalisasi
   Pemerintah Indonesia juga memiliki peran dalam mendorong dan memfasilitasi program digitalisasi di negara ini. Mereka mendorong pengembangan infrastruktur digital, akses internet yang merata, serta pemanfaatan teknologi informasi dan komunikasi (TIK) untuk meningkatkan efisiensi dan pelayanan publik.

Penting untuk diingat bahwa pengaturan internet terus berubah seiring perkembangan teknologi dan perubahan kebutuhan masyarakat. Oleh karena itu, peran pemerintah dalam pengaturan internet juga akan terus berkembang untuk menghadapi tantangan baru yang muncul.

H. KEAMANAN NASIONAL TERHADAP DAMPAK PERKEMBANGAN INTERNET

Keamanan nasional Indonesia memiliki dampak yang signifikan terhadap perkembangan internet. Pemerintah Indonesia mengambil langkah-langkah untuk menjaga keamanan nasional dalam konteks penggunaan dan perkembangan internet dengan cara berikut:

1. Keamanan Siber: Pemerintah Indonesia mengakui pentingnya keamanan siber dalam era digital. Untuk melindungi keamanan nasional, pemerintah telah membentuk Badan Siber dan Sandi Negara (BSSN) yang bertanggung jawab atas keamanan siber negara. BSSN berperan dalam mendeteksi, mencegah, dan menanggulangi ancaman siber terhadap infrastruktur kritis dan kepentingan nasional.
2. Regulasi dan Kebijakan: Pemerintah Indonesia telah mengeluarkan berbagai regulasi dan kebijakan yang mengatur aspek keamanan internet. Undang-Undang ITE, misalnya, mencakup ketentuan tentang kejahatan siber dan ancaman terhadap keamanan nasional. Regulasi dan kebijakan lainnya, seperti Peraturan Pemerintah tentang Keamanan dan Perlindungan Data Pribadi, juga menetapkan langkah-langkah untuk melindungi data dan informasi sensitif.
3. Kolaborasi Internasional: Indonesia menjalin kerja sama dengan negara-negara lain untuk memerangi ancaman siber yang melintasi batas. Kerja sama ini melibatkan pertukaran informasi, pelatihan, dan koordinasi untuk menjaga keamanan nasional di dunia maya.
4. Perlindungan Infrastruktur Kritis: Pemerintah Indonesia memprioritaskan perlindungan infrastruktur kritis dari serangan siber. Infrastruktur kritis, seperti sistem telekomunikasi, transportasi, energi, dan keuangan, dianggap sebagai aset penting yang perlu dilindungi dengan menjaga keamanan jaringan dan sistem komputer yang terkait.

5. *Awareness* dan Pendidikan: Pemerintah juga melakukan upaya kesadaran dan pendidikan kepada masyarakat tentang keamanan siber. Ini melibatkan kampanye kesadaran tentang ancaman siber, praktik keamanan yang baik, dan langkah-langkah yang harus diambil untuk melindungi diri mereka sendiri dan informasi pribadi mereka di dunia digital.
6. Penegakan Hukum: Pemerintah Indonesia melakukan penegakan hukum terhadap pelaku kejahatan siber. Pihak berwenang seperti kepolisian dan BSSN berperan dalam menyelidiki, menangkap, dan mengadili pelaku kejahatan siber.
7. Peran Swasta: Pemerintah bekerja sama dengan sektor swasta, termasuk penyedia layanan internet dan perusahaan teknologi, untuk membangun kerjasama dan memperkuat keamanan jaringan dan sistem mereka. Ini melibatkan pelaporan dan respons terhadap insiden keamanan serta pelatihan untuk meningkatkan kesadaran keamanan di kalangan perusahaan dan organisasi.

I. RANGKUMAN MATERI

Perkembangan internet saat ini telah mencapai tingkat yang sangat maju dan terus berkembang dengan pesat. Perkembangan internet saat ini telah mencapai tingkat yang sangat maju dan terus berkembang dengan pesat. Perkembangan internet telah membuka pintu bagi berbagai bentuk kejahatan baru. Berikut adalah beberapa contoh kejahatan yang sering terjadi di era digital, seperti Penipuan *Online*, Serangan Siber, Kejahatan Seksual *Online*, Penyebaran Konten Ilegal, *Cyberbullying*. Identitas Palsu.

Undang-undang (UU) No. 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE) Merupakan undang-undang yang mengatur kegiatan di dunia maya di Indonesia, termasuk sanksi pidana dan perdata terkait pelanggaran melalui internet. Undang-Undang ITE (Informasi dan Transaksi Elektronik) merupakan kerangka hukum utama di Indonesia yang mengatur berbagai aspek kegiatan di dunia maya atau internet. Undang-Undang ini diberlakukan untuk melindungi kepentingan masyarakat, menjaga

keamanan, ketertiban, dan ketenteraman dalam penggunaan teknologi informasi dan transaksi elektronik.

Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja, yang juga dikenal sebagai Omnibus Law, mengatur Perlindungan Data Pribadi di Indonesia. Undang-Undang ini memiliki beberapa poin penting yang berhubungan dengan perlindungan data pribadi, meskipun tidak secara spesifik fokus pada aspek tersebut. Dampak perkembangan internet juga berbanding lurus dengan perkembangan penggunaan media sosial dan platform digital lainnya. Beberapa perusahaan dan masyarakat bersaing dalam membuat konten digital sebagai bentuk promosi digital atau khususnya dibidang digital kreatif. Tetapi ada beberapa konten digital yang mengabaikan aturan-aturan yang berlaku. Peraturan mengenai konten digital yang meliputi larangan atas penyebaran konten negatif, berbahaya, atau melanggar hukum.

Peraturan mengenai konten digital adalah aturan yang mengatur penyebaran konten di ruang digital dengan tujuan menjaga keamanan, integritas, dan kepatuhan terhadap hukum di lingkungan digital. Peraturan ini bertujuan untuk melarang penyebaran konten negatif, berbahaya, atau melanggar hukum. Meskipun persyaratan dan batasan yang diberlakukan dapat bervariasi antara negara dan yurisdiksi, terdapat beberapa prinsip umum yang sering diadopsi dalam peraturan mengenai konten digital.

Keamanan nasional Indonesia memiliki dampak yang signifikan terhadap perkembangan internet. Pemerintah Indonesia mengambil langkah-langkah untuk menjaga keamanan nasional dalam konteks penggunaan dan perkembangan internet dengan cara, meningkatkan Keamanan Siber: Pemerintah Indonesia mengakui pentingnya keamanan siber dalam era digital. Untuk melindungi keamanan nasional, pemerintah telah membentuk Badan Siber dan Sandi Negara (BSSN) yang bertanggung jawab atas keamanan siber negara. BSSN berperan dalam mendeteksi, mencegah, dan menanggulangi ancaman siber terhadap infrastruktur kritis dan kepentingan nasional serta Regulasi dan Kebijakan: Pemerintah Indonesia telah mengeluarkan berbagai regulasi dan kebijakan yang mengatur aspek keamanan internet. Undang-Undang ITE, misalnya, mencakup ketentuan tentang kejahatan siber dan ancaman terhadap keamanan nasional. Regulasi dan kebijakan lainnya, seperti Peraturan

Pemerintah tentang Keamanan dan Perlindungan Data Pribadi, juga menetapkan langkah-langkah untuk melindungi data dan informasi sensitif.

TUGAS DAN EVALUASI

1. Jelaskan perkembangan Internet dan dampak akibat dari perkembangan internet!
2. Sebutkan aturan-aturan yang mengatur tentang dunia maya atau kejahatan pada *cyber*
3. Jelaskan bagaimana Mekanisme pelaporan dan penanganan konten ilegal atau berbahaya di *platform digital*.
4. Bagaimana upaya pemerintah dalam mengatur dampak *negative* dari perkembangan internet
5. Sebutkan langkah-langkah pemerintah untuk menjaga keamanan nasional dalam konteks penggunaan dan perkembangan internet

DAFTAR PUSTAKA

Ahmad M. Ramli. (2006). *Cyber law dan HAKI dalam sistem hukum Indonesia*. Bandung: PT Refika Aditama

Allan. (2005). *Pengertian Internet dan Asal Usul dari Kata Internet*. Surabaya: Penerbit Indah

Dikdik M. Arief Mansu. (2005). *Cyber Law, Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Rosadi, Sinta Dewi. (2015). *CYBER LAW Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional.* Bandung: PT Refika Aditama

Solove, dan Rotenberg. (2006*). Information and Privacy Law.* New York: Aspen Publication.

----------(2009). Cyberlaw Aspek Hukum Teknologi Informasi, cet-2. Bandung: Refika Aditama.

HUKUM *CYBER*

BAB 10: KEBIJAKAN PRIVASI DAN PERLINDUNGAN DATA

Dr. Betsy A Kapugu, S.H., M.H

Fakultas Hukum Unsrat Manado

BAB 10

KEBIJAKAN PRIVASI DAN PERLINDUNGAN DATA

A. PENDAHULUAN

Setiap orang pasti memiliki data pribadi. Data pribadi merupakan sesuatu yang melekat pada setiap orang. Data pribadi merupakan sesuatu yang bersifat sensitif. Data pribadi adalah sesuatu yang harus dilindungi karena sejatinya merupakan hak privasi setiap orang. Hak privasi adalah hak konstitusional warga negara yang telah diatur dalam Undang-Undang Dasar Negara republik Indonesia Tahun 1945. Hak konstitusional adalah kewajiban dari suatu negara terhadap warga negaranya. Tujuan dan fokus penelitian ini adalah menemukan hakikat dari perlindungan hukum data pribadi sebagai hak privasi dan bentuk perlindungan hukum data pribadi sebagai hak privasi di Indonesia. Hasil dari penelitian ini adalah hakikat dari perlindungan hukum data pribadi sebagai hak privasi adalah hak konstitusional warga negara.

Setiap warga negara memiliki hak konstitusional, yaitu hak yang dijamin oleh Undang- Undang. Dengan adanya hak konstitusional tersebut, maka negara memiliki kewajiban konstitusional, yaitu melindungi seluruh warga negara. Kewajiban konstitusional negara ini telah tertuang dalam Pembukaan Alinea Ke-4 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDRI 1945) yang menyatakan bahwa negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasar kemerdekaan, perdamaian dunia serta keadilan sosial.

Hak konstitusional yang diatur dalam UUDRI 1945 mencakup 40 hak warga negara. Salah satunya adalah hak atas perlindungan diri pribadi. Hak tersebut diatur pada Pasal 28 G Ayat (1) dengan garis besar bahwa warga negara berhak atas perlindungan diri pribadi, keluarga,kehormatan, martabat dan harta benda yang di bawah kekuasaannya. Pada pasal tersebut, mengasumsikan hak pribadi adalah hak milik. Tetapi, dengan berkembangnya teknologi informasi dan komunikasi harusnya hak pribadi tidak hanya diartikan sebagai hak milik. Hak pribadi seharusnya juga sebagai hak privasi. Hak privasi bersifat lebih sensitif yang dapat mewakili hak pribadi tersebut. Hak pribadi merupakan hal yang sensitif yang berkaitan dengan data pribadi atau identitas seseorang.

Perkembangan teknologi informasi dan komunikasi yang melaju dengan pesat telah menimbulkan berbagai peluang dan tantangan. Salah satu bidang yang dipengaruhi oleh perkembangan teknologi informasi adalah terjadinya interaksi yang aktif antara individu dengan pihak penyedia jasa informasi. Berbagai sektor kehidupan telah memanfaatkan sistem informasi, seperti bidang perdagangan *(e-commerce),* transportasi, industri, pariwisata, bidang pemerintahan *(e-government)* dan industri keuangan *(e-payment)*. Cakupan dan sistem teknologi informasi meliputi pengumpulan *(collect),* penyimpanan *(store),* pemroses, produksi dan pengiriman, dari dan ke industri atau masyarakat secara cepat dan efektif (Sinta Dewi, 2015: 165).

PEMBAHASAN

B. KEBIJAKAN PRIVASI DAN PERLINDUNGAN DATA

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Dalam perkembangan ekonomi yang modern seperti sekarang ini, informasi termasuk juga data pribadi, merupakan aset yang sangat berharga karena memiliki nilai ekonomi yang tinggi sehingga banyak dimanfaatkan oleh kalangan bisnis. Keadaan ini dikenal dengan istilah *digital dossier*, yaitu pengumpulan informasi tentang seseorang dalam jumlah yang banyak dengan menggunakan teknologi digital yang diawali sejak awal tahun 1970 dengan menggunakan komputer hingga sekarang dengan menggunakan internet. Salah satu perkembangan teknologi

informasi adalah revolusi di bidang teknologi komputer yang dapat menyimpan data dalam jumlah yang besar yang dinamakan *cloud computing* atau komputasi awan, yang merupakan gabungan pemanfaatan teknologi komputer ('komputasi') dan pengembangan berbasis internet ('awan').

Cloud computing adalah teknologi yang menggunakan internet dan *server* pusat yang jauh untuk menjaga atau mengelola data pelanggan. *Cloud computing* membantu konsumen dan pebisnis untuk menggunakan aplikasi tanpa melakukan instalasi, mengakses *file* pribadi mereka di manapun dengan menggunakan akses internet. Teknologi ini memungkinkan efisiensi dengan memusatkan penyimpanan, pemrosesan dan memori data (ACLU, 2010: 1-4). Disamping itu, kelebihan *cloud computing* yang lain adalah ia dapat meningkatkan produktivitas bisnis pelanggan sehingga pelanggan tidak perlu lagi mengeluarkan investasi dan biaya untuk membangun pusat data. Selain itu, pemanfaatan *cloud computing* dapat dilakukan secara cepat dan mudah dan memiliki mobilitas yang sangat tinggi karena dapat diakses melalui internet (ACLU, 2010: 1-4).

Berdasarkan penelitian yang telah dilakukan oleh para ahli menunjukkan bahwa pada tahun 2014, bisnis *cloud computing* telah mencapai nilai 60 juta hingga 80 juta dolar Amerika Serikat atau sekitar 10% dari pemasaran industri informasi dan teknologi secara keseluruhan (Paolo Balboni, 2010: 1-3). Hal ini menunjukkan bahwa bisnis *cloud computing* menjadi salah satu bisnis yang menjanjikan di masa sekarang dan yang akan datang. Beberapa perusahaan yang menggunakan teknologi *cloud computing* diantaranya adalah yahoo email dan google email. Di Indonesia, salah satu perusahaan yang bergerak di bidang telekomunikasi yang telah menggunakan *cloud computing* adalah PT. Telkom sebagai pemain utama di bidang layanan data *center*. *Cloud computing* yang dikelola PT. Telkom telah dimanfaatkan untuk berbagai sektor industri seperti pertanian, pendidikan, kesehatan, keuangan dan perbankan, hotel, transportasi, dan pertambangan.

Perkembangan teknologi telah memberikan dampak yang signifikan terhadap kehidupan sosial. Teknologi menawarkan banyak fasilitas terutama berkontribusi terhadap kecepatan konektivitas internet. Secara

bersamaan, aksesibilitas terhadap kemajuan teknologi menimbulkan pertanyaan tentang hak individu untuk mempertahankan kerahasiaannya untuk beberapa informasi. Penyebaran informasi yang mudah dan cepat melalui teknologi menciptakan ancaman terhadap privasi dengan memberikan peluang besar bagi pihak yang memiliki akses ke informasi pribadi tersebut. Sebagai suatu bentuk inovasi, teknologi informasi sekarang ini telah mampu melakukan pengumpulan, penyimpanan, pembagian dan penganalisaan data di mana hal tersebut tidak dapat dibayangkan sebelumnya, sehingga hak privasi telah berkembang untuk merumuskan hak untuk melindungi data pribadi, sebagaimana dinyatakan dalam Pasal 17 *Human Rights Committee General Commnt No. 16 on the Rights to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation.*

Konsep perlindungan data menginsyaratkan bahwa individu memiliki hak untuk menentukan apakah ia akan bergabung dengan masyarakat kemudian akan membagi atau bertukar data pribadi diantara mereka serta hak untuk menentukan syarat-syarat apakah yang harus dipenuhi untuk melakukan hal tersebut. Hukum perlindungan data secara umum juga mencakup langkah-langkah pengamanan perlindungan dari keamanan data pribadi dan memperbolehkan penggunaannya oleh orang lain sepanjang sesuai dengan syarat yang ditentukan. Konsep hak privasi menjadi populer pada tahun 1890 ketika Samuel Warren dan Louis Brandeis menulis esai berjudul, "*The Right to Privacy*," yang diterbitkan oleh Harvard *Law Review*. Mereka mengusulkan pengakuan hak individu "*right to be let alone*" dan juga berpendapat bahwa hak ini harus dilindungi oleh hukum yang ada sebagai bagian dari masalah hak asasi manusia. Dengan demikian, konsep hak privasi telah diakui akan tetapi masih sulit untuk didefinisikan. Privasi, sebagai bagian dari hak asasi manusia, mengidentifikasi perlindungan data pribadi sebagai hak yang penting (Sinta Dewi, 2009: 23). Hak privasi melalui perlindungan data bukan hanya penting namun juga merupakan elemen kunci bagi kebebasan dan harga diri individu. Perlindungan data menjadi pendorong kuat bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan seksual. Hak untuk menentukan nasib sendiri, kebebasan

berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia.

Perlindungan data juga merupakan hak asasi manusia yang fundamental. Sejumlah negara telah mengakui perlindungan data sebagai hak konstitusional atau dalam bentuk *'habeas data'* yakni hak seseorang untuk mendapatkan pengamanan terhadap data yang dimilikinya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya. Portugal adalah salah satu contoh negara yang telah mengakui perlindungan data sebagai hak konstitusional, yaitu di Pasal 35 Undang-Undang Dasar miliknya. Selain itu, Armenia, Filipina, Timor-Leste, Colombia dan Argentina adalah negara-negara dengan perbedaan sejarah dan budaya yang juga telah mengakui peran perlindungan data dalam memfasilitasi proses demokrasi dan telah menjamin perlindungan data privasi di dalam konstitusi mereka. ASEAN *Human Rights Declaration* yang baru saja diadopsi negara-negara ASEAN juga secara jelas mengakui hak atas data privasi (Pasal 21). Dewasa ini, setidaknya ada lebih dari 75 negara telah banyak negara yang undang-undangnya mengatur perlindungan data (Graham Greenleaf, 2011).

Beberapa negara memiliki hukum khusus yang melindungi privasi dan data pribadi bagi warga negaranya. Hal ini terutama telah terwujud di negara-negara Eropa dan Amerika Serikat, dimana terdapat hukum yang khusus melindungi privasi dan data pribadi. Namun demikian, konsep privasi yang terdapat di Eropa dan Amerika Serikat memiliki perbedaan karakteristik. Amerika Serikat tidak memiliki regulasi tunggal untuk melindungi privasi dan data yang dapat diterapkan secara khusus. Sementara di Uni Eropa, karena merupakan kawasan terintegrasi, maka perlindungan privasi dan data pribadi diatur oleh kebijakan yang bersifat supranasional dalam bentuk *the EU Data Protection Directive.*

Sementara itu, konsep dasar perlindungan data pribadi pertama kali muncul sekitar tahun 1960. Selanjutnya tahun 1970, Jerman adalah negara pertama yang memberlakukan peraturan tentang perlindungan data yang kemudian diikuti oleh hukum nasional Swedia pada tahun 1973,Amerika Serikat pada tahun 1974, dan Perancis pada tahun 1978. Konsep perlindungan data sering diperlakukan sebagai bagian dari perlindungan privasi, seperti aturan memberikan perlindungan untuk data pribadi.

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi, dan gagasan itu sendiri dapat diterapkan sebagai kategori yang lebih luas dari privasi. Melihat perlindungan data sebagai bagian dari privasi adalah konsisten dengan pemahaman bahwa privasi sebagai bentuk kerahasiaan, atau hak terhadap pengungkapan maupun penutupan informasi, atau hak untuk membatasi akses individu, atau kontrol informasi yang berkaitan dengan diri seseorang. Namun, terdapat perbedaan penting dalam hal ruang lingkup, tujuan, dan isi dari perlindungan privasi dan data.

Perlindungan data secara eksplisit melindungi nilai-nilai yang bukan inti dari privasi seperti syarat untuk pengolahan secara adil, persetujuan, legitimasi, dan *non*-diskriminasi. Ekspresi dari konsep perlindungan data erat kaitannya dengan hak untuk menghormati kehidupan pribadi dan keluarga. Pengaturan perlindungan data merupakan kunci dari permasalahan bisnis dan ekonomi di bidang bisnis informasi intensif di era modern sekarang ini. Praktek bisnis modern saat ini seringkali melibatkan manipulasi data seperti segmentasi data pelanggan, termasuk penambangan data dan pemetikan data, menciptakan profil pelanggan, pengkonsolidasian pengolahan data global, dan proses bisnis lainnya.

Indonesia sebagai salah satu negara berkembang memiliki jumlah pengguna teknologi dan sistem komunikasi modern yang sangat besar. Namun hingga kini Indonesia belum memiliki hukum yang secara spesifik mengatur mengenai perlindungan privasi dan data. Dengan meningkatnya pemanfaatan teknologi, urgensi untuk mengatasi permasalahan hukum yang terkait dengan perlindungan privasi dan data menjadi meningkat. Hal ini disebabkan karena seringkali hukum yang sudah ada tidak dapat bekerja secara efektif dalam mengikuti perkembangan teknologi. Hukum seringkali berjalan lebih lambat dibandingkan dengan perkembangan masyarakatnya, termasuk juga perkembangan teknologi. Kekosongan hukum ini tentu saja membawa implikasi terhadap perlindungan privasi dan data pribadi. Sebagai anggota dari *Asia-Pacific Economic Cooperation (APEC)* dan juga sebagai negara calon anggota *the Organization for Economic Co-operation and Development* (OECD), Indonesia membutuhkan pengaturan terkait perlindungan privasi dan data pribadi ini sehingga diharapkan aturan ini dapat memecahkan masalah-masalah

yang timbul karena adanya penyalahgunaan pengelolaan data pribadi. Pengaturan perlindungan data pribadi harus dipertimbangkan sebagai salah satu bidang yang paling penting yang dibutuhkan oleh Indonesia. Ini merupakan isu yang penting dalam komunitas modern karena perlindungan data pribadi akan mempengaruhi cara berkomunikasi. Pertumbuhan teknologi memberikan berbagai kesempatan untuk mengumpulkan, menganalisa, dan menyebarkan informasi dengan berbagai cara, oleh sebab itu, masalah perlindungan hukum privasi atas data pribadi menjadi sesuatu hal yang urgen untuk dipikirkan.

Memperhatikan perkembangan internasional dalam pengaturan data privasi, baik yang telah dilakukan oleh banyak negara di dunia maupun oleh organisasi-organisasi internasional, maka Indonesia harus segera mengambil Langkah-langkah untuk beradaptasi dengan perkembangan global tersebut. Indonesia harus segera membentuk suatu sistem hukum yang dapat menjamin kepastian hukum namun tetap memperhatikan kesiapan masyarakat dalam menghadapi nilai-nilai baru (Lili Rasjidi, I.B Wyasa Putra, 2003: 187). Nilai baru yang dimaksud di sini adalah kemajuan teknologi yang menghendaki adanya perlindungan privasi atas data pribadi pengguna khususnya dalam menghadapi perkembangan industri. Hingga saat ini, Indonesia belum memiliki pengaturan khusus mengenai privasi atas data pribadi. Oleh sebab itu, diperlukan pengaturan hal ini dalam bentuk undang-undang yang secara khusus mengatur perlindungan privasi atas data pribadi, baik yang dilakukan melalui media biasa maupun elektronik (Sinta Dewi, 2009: 51). Selain itu, pembentukan sistem hukum teknologi informasi sangat diperlukan untuk mendorong terjadinya koordinasi dengan undang-undang terkait lainnya dan terciptanya harmonisasi baik dengan prinsip-prinsip internasional maupun dengan pengaturan di negara lain. Jadi penyusunan undang-undang dapat mengakomodasi beberapa kepentingan: pertama, melindungi privasi masyarakat atas informasi pribadi, kedua, memperlancar hubungan perdagangan internasional khususnya *e-commerce* dengan mengikuti standar pengaturan internasional dengan menyesuaikan dengan keadaan masyarakat Indonesia.

Menurut Lawrence M. Friedman, sistem hukum yang baik akan tercipta melalui beberapa unsur yaitu: (1) struktur; (2) substansi; dan (3) budaya hukum (Lawrence M. Friedman, tahun: 5-19). Pengertian struktur adalah sistem pengadilan. Khusus di dalam membentuk sistem hukum teknologi informasi, perlu dipersiapkan sampai sejauh mana pengadilan di Indonesia dapat menyelesaikan kasus pelanggaran privasi, khususnya yang dilakukan dalam lalu lintas *e-commerce*. Pengadilan memerlukan suatu pemahaman yang mendalam mengenai pelanggaran privasi dalam *e-commerce*. Kemampuan dan kemauan para aparat penegak hukum (hakim, jaksa dan polisi) diperlukan agar memahami apa itu pelanggaran privasi khususnya dalam kaitan dengan *e-commerce*. Hakim dan penegak hukum lainnya harus mampu menyelesaikan kasus-kasus yang muncul sebagai akibat terjadinya perubahan kondisi sosial masyarakat tersebut. Pada akhirnya, dengan adanya struktur yang memadai, diharapkan dapat memberikan kontribusi terhadap pembentukan hukum yang responsif. Hukum responsif adalah hukum yang dapat mengakomodasi dan mengikuti perubahan zaman terutama dalam hal ini berkaitan dengan hukum teknologi informasi yang selalu cepat berubah.

Teknologi informasi telah mengubah pola hidup masyarakat dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung dengan signifikan, Perkembangan teknologi informasi dan potensi ekonomi digital yang cukup besar juga diiringi oleh beberapa dampak negatif antara lain ancaman terhadap hak atas privasi dan data diri warga negara. Hak atas privasi atau *privacy right* merupakan salah satu hak dalam *fundamental right*. Penggunaan teknologi internet yang meluas di dunia merupakan faktor substansi yang memberikan kontribusi atas meningkatnya pemrosesan data. Hal tersebut tidak diragukan bahwa internet menjadikan pertukaran informasi antar individu lebih mudah dan dan lebih masif.

Setiap negara yang memfasilitasi kehidupan bernegara dengan penggunaan sistem elektronik dan internet yang maju, secara tidak langsung perkembangan *cyber law* di dalamnya turut maju. *Cyber law* erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan

dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya.

Ruang lingkup *cyber law* meliputi hak cipta, hak merek, pencemaran nama baik, penistaan, penghinaan, *hacking*, transaksi elektronik, pengaturan sumber daya internet, keamanan pribadi, kehati-hatian, kejahatan IT, pembuktian, penyelidikan, pencurian lewat internet, perlindungan konsumen dan pemanfaatan internet dalam keseharian. Karena erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana maka *cyber law* menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan elektronik yang termasuk juga di dalamnya kejahatan pencucian uang dan kejahatan terorisme.

Kehadiran *cyber law* di Indonesia sudah diinisiasi sebelum 1999. Di masa itu, *cyber law* adalah perangkat hukum yang menjadi dasar dan peraturan yang menyinggung transaksi elektronik. Pendekatan dengan perangkat hukum ini dimaksudkan agar ada pijakan yang dapat digunakan oleh undang-undang dan peraturan lainnya. Banyaknya berbagai kejahatan dan pelanggaran hukum dalam pemanfaatan teknologi maka dibuat sebuah undang-undang sebagai dasar hukum atas segala kejahatan dan pelanggaran yang terjadi.

Undang-undang yang mengatur mengenai Teknologi Informasi ini di antaranya:

1. UU Hak Cipta No. 19 Tahun 2002 tentang Hak Cipta
2. UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008 tentang Pornografi di Internet, Transaksi di Internet, dan Etika Pengguna Internet.

Cyber law atau UU Informasi dan Transaksi Elektronik (UU ITE) disahkan oleh DPR pada tanggal 25 Maret 2008. UU ITE terdiri dari 13 BAB dan 54 pasal yang mengupas secara jelas aturan bermain di dunia maya dan transaksi yang terjadi di dalamnya.

Secara garis besar terdapat lima pembahasan *cyber law* di setiap negara, yaitu:

1. *Information security*, menyangkut masalah keotentikan pengirim atau penerima dan integritas dari pesan yang mengalir melalui internet, dalam hal ini diatur masalah kerahasiaan dan keabsahan tanda tangan elektronik.
2. *Online transaction* yang meliputi penawaran, jual beli, pembayaran hingga pengiriman barang melalui internet.
3. *Right in electronic information*, mengenai hak cipta dan hak-hak yang muncul bagi pengguna maupun penyedia konten.
4. *Regulation information content*, perangkat hukum yang mengatur sejauh mana konten yang dialirkan melalui internet.
5. *Regulation online contact,* tata krama dalam berkomunikasi dan berbisnis melalui internet termasuk perpajakan, restriksi ekspor-impor kriminalitas dan yurisdiksi hukum.

Sedangkan terkait dengan penentuan hukum yang berlaku, dikenal beberapa asas yang biasa digunakan, di antaranya:

1. *Subjective territoriality*, hal ini menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan yang dilakukan dan penyelesaian tindak pidana dilakukan di negara lain.
2. *Objective territoriality,* menyatakan bahwa hukum yang berlaku adalah hukum akibat sebuah perbuatan terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
3. *Nationality,* menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.
4. *Passive nationality*, menekankan yurisdiksi berdasarkan kewarganegaraan korban.
5. *Protective principle*, menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya yang umumnya digunakan jika korban adalah negara atau pemerintah.
6. *Universality*, asas ini memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus *cyber*. Asas ini menentukan bahwa setiap negara berhak menangkap dan menghukum para pelaku pembajakan, lalu kemudian asas ini diperluas hingga mencakup kejahatan terhadap kemanusiaan dan terus dikembangkan untuk

kejahatan sangat serius berdasarkan perkembangan hukum internasional.

Terdapat tiga pendekatan dalam perlindungan hak privasi warga negara dalam era ekonomi digital ini, pendekatan tersebut antara lain aspek hukum, aspek teknologi dan aspek etika. Khusus untuk penelitian ini, aspek yang digunakan adalah aspek hukum. Penelitian ini juga menggunakan studi komparasi dengan perlindungan terhadap privasi warga negara di Uni Eropa. *European Charter of Human Rights* (ECHR, 2000) dan ASEAN *Human Rights Declaration* (AHRD, 2012) telah mengakui Hak atas perlindungan data pribadi sebagai jenis Hak Asasi Manusia. Hak atas perlindungan data pribadi merupakan suatu hak hasil bentukan dari irisan penggabungan hak atas informasi dan hak atas privasi yang telah melalui evolusi yang panjang sejak diakuinya hak asasi manusia dalam *the Universal Declaration of Human Rights* (UDHR, 1948).

Data pribadi merupakan keterangan yang benar dan nyata yang melekat pada diri seseorang, sehingga dapat mengidentifikasikan orang tersebut. Pentingnya perlindungan data pribadi adalah untuk memastikan bahwa data pribadi seseorang yang terkumpul digunakan sesuai dengan tujuan pengumpulan, sehingga tidak terjadi penyalahgunaan data. Hak perlindungan data pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut *the right to private life*. Konsep kehidupan pribadi berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak perlindungan data pribadi. Privasi memang tidak dicantumkan secara eksplisit di dalam Undang-Undang Dasar 1945. Namun, secara implisit hak atas privasi terkandung di dalam Pasal 28G ayat (1) UUD NRI 1945 sebagai berikut: "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Jaminan terhadap hak atas privasi juga termaktub dalam undang-undang lain yaitu Pasal 29 ayat (1) dan Pasal 30 Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia. Data Pribadi merupakan suatu konsep yang menggambarkan proses atau upaya menggabungkan

pengaturan-pengaturan mengenai privasi dan data pribadi yang tersebar di berbagai instrumen hukum ke dalam satu instrumen hukum tersendiri. Dengan demikian perlindungan privasi dan data pribadi memiliki tempat yang sui generis. Uni Eropa telah memiliki *The European Union DP Directive (Directive)* diperkenalkan tahun 1995 dengan tujuan untuk mengharmonisasi peraturan nasional di antara negara-negara anggota EU. *Directive* tersebut dianggap sebagai satu di antara rezim yang paling kuat. Regulasi terkini di Uni Eropa terkait Hak atas privasi pada data pribadi ada dalam *General Data Protection Regulation* (GDPR).

Di Asia sendiri, beberapa negara telah memiliki regulasi terkait perlindungan hak atas privasi. Hong Kong telah memiliki *Personal Data Privacy Ordinance* of 1995 (PDPO) sebagai peraturan perundang-undangan nasional pertama yang mengatur masalah privasi dan data pribadi data secara komprehensif. Privasi atas data pribadi Malaysia dilindungi melalui *The Personal Data Protection Act* No. 709 of 2010 (PDPA Malaysia). Sedangkan, Privasi dan data pribadi di Singapura dilindungi secara sektoral oleh *The Personal Data Protection Act* No. 26 of 2012 Singapore (PDPA 2012 Singapura).

Indonesia saat ini sedang melalui proses pembahasan perlindungan privasi dan data pribadi karena Indonesia telah memiliki RUU Perlindungan Data Pribadi. Fakta bahwa para ilmuwan tidak tahu aturan yang menentukan bidang permainan mereka sambil mempertahankan bahwa mereka dibatasi oleh mereka adalah masalah. Sebagai permulaan, *ignorantia juris non excusat* ("ketidaktahuan hukum tidak memaafkan"), dan kedua, hukum memiliki kekuatan normatif, aturan seharusnya dipatuhi. Rancangan Undang-Undang tersebut bertujuan untuk menggabungkan pengaturan-pengaturan privasi atas data pribadi yang tersebar, ke dalam suatu undang-undang tersendiri. Perancangan Naskah Akademik sebagai fase awal proses konvergensi tersebut telah dirampungkan pada bulan Oktober 2015. Indonesia cukup tertinggal dalam menyelesaikan isu terkait perlindungan hak atas privasi terutama jika melihat kerangka legislasi dari perlindungan hak atas privasi, baik dari segi waktu maupun variasi perlindungannya.

Perlindungan hukum merupakan salah satu cara terbaik untuk memproteksi suatu subjek hukum dari kesewenangan yang diterapkan. Perlindungan hukum mencangkup secara luas dalam segi tatanan hukumnya. Informasi adalah sumber utama. Di bidang ekonomi, dan memang untuk beberapa waktu sekarang, informasi telah dianggap sebagai barang yang sangat berbeda. Ini diperlukan untuk setiap transaksi (mis., Untuk setiap pembelian di pasar) dan biayanya mahal (setidaknya dalam bentuk biaya pencarian dan waktu). Bahkan, informasi telah menjadi salah satu komponen kunci dari teori ekonomi dan bidang utama penelitian ekonomi. Walaupun perkembangan teknologi informasi dan ekonomi digital sangat pesat namun penelitian terkait hukum dan teknologi secara umum dan perlindungan hak privasi belum terlalu banyak.

Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandheis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul "*The Right to Privacy*" atau hak untuk tidak diganggu. Dalam jurnal tersebut menurut Warren dan Brandheis dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa ada hak seseorang untuk menikmati hidup. Menurut Warren dan Brandeis menyatakan bahwa: "*Privacy is the rught to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition*". Privasi adalah suatu hak setiap orang untuk menikmati hidup dan menuntut privasinya untuk dilindungi.

Alasan hak privasi harus dilindungi adalah; Pertama, dalam membina hubungan dengan orang lain, seseorang harus menutupi sebagian kehidupan pribadinya sehingga dia dapat mempertahankan posisinya pada tingkat tertentu. Kedua, seseorang di dalam kehidupannya memerlukan waktu untuk dapat menyendiri sehingga privasi sangat diperlukan oleh seseorang. Ketiga, privasi adalah hak yang berdiri sendiri dan tidak bergantung kepada hak lain akan tetapi hak ini akan hilang apabila orang tersebut mempublikasikan hal-hal yang bersifat pribadi kepada umum. Keempat, privasi juga termasuk hak seseorang untuk melakukan hubungan domestik termasuk bagaimana seseorang membina perkawinan, membina keluarganya dan orang lain tidak boleh mengetahui hubungan pribadi tersebut. Sehingga kemudian Warren menyebutnya sebagai *the*

right against the word. Kelima, alasan lain mengapa privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai. Kerugiannya dirasakan jauh lebih besar dibandingkan dengan kerugian fisik, karena telah mengganggu kehidupan pribadinya, sehingga bila ada kerugian yang diderita maka pihak korban wajib mendapatkan kompensasi.

Alan Westin memberikan pengertian privasi sebagai "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others* (privasi adalah klaim individu, kelompok, atau institusi untuk menentukan sendiri kapan, bagaimana,dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain). Hak privasi merupakan salah satu hak yang melekat pada diri setiap orang. Hak privasi merupakan martabat setiap orang yang harus dilindungi. Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga. Data pribadi merupakan hal yang sensitif dimiliki setiap orang. Data pribadi menjadi hak privasi seseorang yang wajib dilindungi dari berbagai aspek kehidupan.

Pengertian lain dari "data pribadi" adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia. Memiliki sifat yang sensitif menjadikan data pribadi suatu hal yang menarik bagi orang lain karena banyak sekali kebutuhan kegiatan seseorang yang berkaitan dengan data pribadi seseorang. Data pribadi merupakan suatu aset atau komoditas bernilai ekonomi tinggi. Titik awal dari hukum di Indonesia pasti berasal dari Konstitusi dan peraturan perundang-undangan yang berlaku. UUD 1945 mengatur bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak rasa aman dan perlindungan dari ancaman ketakutan. Dalam UUDNRI 1945 khususnya pada pasal 28 huruf G Ayat (1) menyatakan bahwa "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Konsep

perlindungan data mengisyaratkan bahwa individu memiliki hak untuk menentukan apakah mereka akan membagi atau bertukar data pribadi mereka atau tidak. Selain itu, individu juga memiliki hak untuk menentukan syarat-syarat pelaksanaan pemindahan data pribadi tersebut. Lebih jauh, perlindungan privasi. Hak privasi telah berkembang sehingga dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.

Data Pribadi adalah data pribadi yang memerlukan perlindungan khusus yang terdiri dari data yang berkaitan dengan agama/keyakinan, kesehatan, kondisi fisik dan kondisi mental, kehidupan seksual, data keuangan pribadi, dan data pribadi lainnya yang mungkin dapat membahayakan dan merugikan privasi subjek data. (*Draft* RUU PDP). Data pribadi penduduk yang harus dilindungi:

a. Nomor KK (Kartu Keluarga);
b. NIK (Nomor Induk Kependudukan);
c. Tanggal/bulan/tahun lahir;
d. Keterangan tentang kecacatan fisik dan/atau mental;
e. NIK ibu kandung;
f. NIK ayah; dan
g. Beberapa isi catatan Peristiwa Penting

C. RANGKUMAN MATERI

Dengan dasar hukum tersebut, maka hak privasi terhadap data pribadi harus dilakukan dan perlindungan terhadap data pribadi sebagai hak privasi merupakan Hak Konstitusional warga negara Indonesia. Hak konstitusional adalah kewajiban bagi negara untuk memberikan perlindungan secara hukum untuk aspek kehidupan masyarakat Indonesia. Hak konstitusional harus didapatkan oleh setiap warga negara Indonesia. Hak konstitusional harus memiliki tujuan hukum yaitu kepastian hukum, keadilan hukum dan kemanfaatan hukum. Dengan dasar hukum tersebut juga beberapa peraturan perundang-undangan di Indonesia mengatur secara tersirat mengenai perlindungan data pribadi.

Kewajiban dari penyedia sistem elektronik diatur dalam diatur dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Kemenkoinfo No. 4/2016 sebagai berikut:

a. Melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik yang melakukan Transaksi Elektronik;
b. Memiliki dan melaksanakan kebijakan dan prosedur untuk mengambil tindakan jika terdapat indikasi terjadi pencurian data;
c. Memastikan pengendalian terhadap otorisasi dan hak akses terhadap sistem, *database*, dan aplikasi Transaksi Elektronik;
d. Menyusun dan melaksanakan metode dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Transaksi Elektronik;
e. Memiliki dan melaksanakan standar dan pengendalian atas penggunaan dan perlindungan data jika pihak penyedia jasa memiliki akses terhadap data tersebut;
f. Memiliki rencana keberlangsungan bisnis termasuk rencana kontingensi yang efektif untuk memastikan tersedianya sistem dan jasa Transaksi Elektronik secara berkesinambungan; dan
g. Memiliki prosedur penanganan kejadian tak terduga yang cepat dan tepat untuk mengurangi dampak suatu insiden, penipuan, dan kegagalan Sistem Elektronik.

Selain kewajiban yang secara eksplisit diatur, jika kita membaca Peraturan Pemerintah Nomor 82 Tahun 2012 dan Peraturan Kemenkoinfo No. 4/2016 kita dapat melihat kewajiban lainnya yaitu:

a. Memastikan perjanjian tentang tingkat layanan minimum dan keamanan informasi terhadap layanan teknologi informasi yang digunakan serta keamanan dan fasilitas keamanan komunikasi internal yang diterapkannya
b. Melindungi dan memastikan privasi dan perlindungan data pribadi pengguna
c. Memastikan penggunaan yang sah dan pengungkapan data pribadi
d. Menyediakan pusat data dan pusat pemulihan bencana (untuk Penyedia Sistem Elektronik untuk layanan publik)
e. Memberikan catatan audit tentang semua penyediaan kegiatan *system* elektronik. Memberikan informasi dalam *system* elektronik berdasarkan permintaan yang sah dari penyidik untuk kejahatan tertentu

f. Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang diproses sehingga [Data Pribadi] dapat atau tidak dapat digunakan atau ditampilkan oleh pihak ketiga berdasarkan Persetujuan selama itu terkait dengan tujuan untuk memperoleh dan mengumpulkan Data Pribadi
g. Memberikan akses atau peluang kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadi mereka tanpa mengganggu manajemen sistem Data Pribadi, kecuali jika sebaliknya diatur oleh undang-undang dan peraturan.
h. Menghapus data pribadi jika:
    1) Telah mencapai periode maksimum menyimpan data pribadi (paling singkat lima tahun atau berdasarkan peraturan yang berlaku/peraturan *sectoral* tertentu); atau
    2) Atas permintaan dari Pemilik Data Pribadi, kecuali jika sebaliknya diatur oleh hukum dan peraturan, dan
    3) Memberikan orang yang mudah dihubungi oleh Pemilik Data Pribadi sehubungan dengan Data Pribadi mereka

Di sektor telekomunikasi, Pasal 19 Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.KOMINFO/05/2007 tentang Keamanan dan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet (sebagaimana diamandemen) (MR 26/2007) juga menyediakan bahwa penyedia layanan telekomunikasi bertanggung jawab atas penyimpanan data karena kewajibannya untuk mencatat *file log*-nya setidaknya selama tiga bulan.

Pasal 15 (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan bahwa penyedia Sistem Elektronik harus memberikan pemberitahuan tertulis kepada pemilik data pribadi setelah kegagalannya melindungi data pribadi. Pasal 20 (3) PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik menyatakan bahwa penyedia Sistem Elektronik harus melakukan upaya terbaik untuk melindungi data pribadi dan untuk segera melaporkan kegagalan atau gangguan sistem serius atau gangguan kepada pejabat penegak hukum atau Otoritas Pengawas dan Pengatur sektor terkait. Pasal 25 ayat 2 Peraturan Kemenkoinfo No. 4/2016

Peraturan mengatur bahwa pemberitahuan tertulis kepada Pemilik Data Pribadi diperlukan jika ada kegagalan dalam melindungi kerahasiaan Data Pribadi dalam Sistem Elektronik.

Ketentuan pemberitahuan pelanggaran harus memberikan alasan atau penyebab terjadinya kegagalan dalam melindungi kerahasiaan Data Pribadi. Ini dapat diberikan secara elektronik, jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu pada saat memperoleh dan mengumpulkan Data Pribadi mereka Harus memastikan bahwa pemberitahuan tersebut telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian pada Data Pribadi yang relevan Pemilik, dan Pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi selambat-lambatnya 14 hari setelah kegagalan ditemukan

Di Indonesia, sanksi untuk pelanggaran privasi data ditemukan di bawah undang-undang yang relevan dan pada dasarnya adalah denda. Penjara dapat dijatuhkan dalam kasus yang berat, seperti dalam hal terjadi pelanggaran yang disengaja. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur pelanggaran privasi pada Pasal 30 ayat (1), (2), dan (3).112 Sedangkan sanksi pidana untuk pelanggaran pada Pasal 30 ayat (1), (2), (3) terdapat pada pasal 46 ayat (1), (2), dan (3).

UU ITE dan Amandemen UU ITE memberikan hukuman pidana mulai dari: denda Rp 600 juta hingga Rp 800 juta dan hukuman penjara enam hingga delapan tahun untuk akses tidak sah, denda Rp800 juta dan hukuman penjara 10 tahun karena intersepsi atau penyadapan transmisi. Sedangkan denda Rp2 miliar hingga Rp5 miliar dan 8 hingga 8 tahun. 10 tahun penjara karena perubahan, penambahan, pengurangan, transmisi, gangguan, penghapusan, memindahkan atau menyembunyikan Informasi Elektronik atau Kegagalan Arsip Elektronik untuk mematuhi Reg. 82 dikenai sanksi administratif (yang tidak menghilangkan tanggung jawab perdata dan pidana).

Sanksi administrasi ini adalah dalam bentuk: Peringatan tertulis Denda administratif Pengusiran sementara dari daftar pendaftaran (sebagaimana disyaratkan dalam peraturan) Kegagalan untuk mematuhi PERATURAN KEMENKOINFO NO. 4/2016 Peraturan tunduk pada sanksi administratif

dalam bentuk: Peringatan lisan Peringatan tertulis Pemberhentian sementara kegiatan Pengumuman di situs web *online* Hukum Perbankan Menurut Pasal 47 UU Perbankan, komisaris, direktur atau karyawan bank atau afiliasinya yang dengan sengaja memberikan informasi yang harus dirahasiakan dapat dijatuhi hukuman penjara tidak kurang dari 2 tahun tetapi tidak lebih dari 4 tahun, dan didenda setidaknya Rp4 miliar tetapi tidak lebih dari Rp8 miliar.

TUGAS DAN EVALUASI

1. Kebijakan dan hukum apa yang diterapkan di Indonesia untuk melindungi privasi informasi data pribadi?
2. Kapan kehadiran *cyber law* di Indonesia?
3. Apa saja yang perlu dilindungi dari data pribadi?
4. Berikan beberapa alasan mengapa hak privasi harus dilindungi?
5. Sanksi apa saja yang dikenakan terhadap pelanggaran privasi yang ada di Indonesia?

DAFTAR PUSTAKA

Abdul Raman Saad. 2005. Personal Data & Privacy Protection. Malaysia: Puddingburn Publishing.

Abu Bakar Munir. 2002. Siti Hajar Mohd Yasin, Privacy & Data Protection. Malaysia: Sweet & Maxwell Asia,.

Alan F. Westin (Editor), 1971, Information Technology in a Democracy, Massachusetts: Harvard University Press,

Alan F. Westin,1984, The Origins of Modern Claims to Privacy, dalam buku: Philosophical Dimensions of Privacy: an Anthology (ed. Schoeman, F. D.), Cambridge: Cambridge University Press

Anggraeni, SF, 2018, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum Di Indonesia", *Jurnal Hukum & Pembangunan*, Vol. 48 No. 4, 814 – 825

Aswandi, R, Putri R, Muhammad S, 2020, "Perlindungan Data dan Informasi Pribadi Melalui *Indonesia Data Protection System (IDPS*), *Legislatif*, Vol. 3 No.2, Hal.167-190

Aswandi, R, Putri R, Muhammad S, 2020, "Perlindungan Data dan Informasi Pribadi Melalui *Indonesia Data Protection System (IDPS*), *Legislatif*, Vol. 3 No.2, Hal.167-190

Bambang Pratama, 2018,"*Data Pribadi (Elektronik) Dalam Perspektif Uu-Ite*", https://business- law.binus.ac.id/2018/12/07/data-pribadi-elektronik-dalam-perspektif-uu-ite/.

Banisar, 2000, Privacy & Human Rights, An International Survey of Privacy Laws and Developments. Washington. D.C: Electronic Privacy Information Centre.

Chee, JS, Brian, 2010, dan Curtis, Franklin, Cloud Computing: Technologies and Strategies of the Ubiquitous Data Centre. Florida: CRC Publications.

Christopher (ed), 2013, Cloud Computing Law. United Kingdom: Oxford University Press. Sinta Dewi. 2009. Cyberlaw: Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional. Bandung: Widya Padjadjaran.

Cynthia,H , 2018, “Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia”, *Jurnal HAM*, Vol.9 No.2, Hal 191 – 204

Fanny, P, 2019, “Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum”,*Jatiswara,* Vol.34 No. 3, Hal. 239-249

https://journal.unusia.ac.id/index.php/alwasath/index ISSN 2721-6160 (Online)

https://www.hukumonline.com/berita/a/mengenal-cyber-law-dan-aturannya-lt6239804025ad0/

https://www.its.ac.id/dptsi/wp-content/uploads/sites/8/2019/01/PPT_Pak_Donny.pdf

Journal homepage: https://journal.unusia.ac.id/index.php/alwasath/index ISSN 2721-6160 (Online)

Olga Stepanova dan Alan Charles Raul, 2018, Privacy, Data Protection and Cybersecurity Law Review Fifth EditionLondon: Law Business Research Ltd

Rosadi, SD, 2015, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional*, *Regional dan Nasional*, Refika Aditama, Jakarta,Hal. 23

Sinta Dewi, 2015, Aspek Perlindungan Data Pribadi Menurut Hukum Internasional, Regional dan Nasional,Bandung: Refika Aditama

Syaifudin.A, 2020, “Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan *Financial Technology* Berbasis *Peer to Peer* (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta)”, *Dinamika*, Vol.26 No.4, Hal.408- 421

Woods, M, Jeanne and Lewis, Hope. 2004. Human Rights and the Global Marketplace. New York: Transnational Publishers Inc.

HUKUM *CYBER*

BAB 11: ETIKA DALAM HUKUM *CYBER*

Dr. Irwanto, S.Pd.T., M.T

Universitas Sultan Ageng Tirtayasa

BAB 11

ETIKA DALAM HUKUM *CYBER*

A. PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi (IPTEK) telah memberikan dampak yang sangat positif bagi peradaban umat manusia. Salah satu fenomena abad modern yang sampai saat ini masih terus berkembang dengan pesat adalah *internet*. Pada mulanya jaringan *internet* hanya dapat digunakan oleh lingkungan pendidikan (perguruan tinggi) dan lembaga penelitian. Kemudian tahun 1995, *internet* baru dapat digunakan untuk publik, beberapa tahun kemudian tim *Berners-Lee* mengembangkan aplikasi *Word Wide Web (WWW)* yang memudahkan orang untuk mengakses informasi di internet. Setelah dibukanya internet untuk keperluan publik semakin banyak muncul aplikasi-aplikasi bisnis di *internet* (Budi Raharjo, 2003).

Terutama dalam perkembangan jaringan internet memunculkan dampak negatif, sebagaimana dikemukakan oleh Roy Suryo, seorang pakar teknologi informasi, dalam penelitiannya yang dikutip oleh harian Kompas menyatakan: (Roy Suryo, 2001)

Kejahatan *cyber* (*cyber crime*) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup memperhatikan serta yang dilakukan oleh para *hacker* yang rata-rata anak muda yang keliatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet.

Keunggulan komputer berupa kecepatan dan ketelitiannya dalam menyelesaikan pekerjaan sehingga dapat menekan jumlah tenaga kerja, biaya serta memperkecil kemungkinan melakukan kesalahan,

mengakibatkan masyarakat semakin mengalami ketergantungan kepada komputer. Dampak negatif dapat timbul apabila terjadi kesalahan yang ditimbulkan oleh peralatan komputer yang akan mengakibatkan kerugian besar bagi pemakai (*user*) atau pihak-pihak yang berkepentingan. Kesalahan yang disengaja mengarah kepada penyalahgunaan komputer (Andi Hamzah, 1990). Usaha mewujudkan cita-cita hukum untuk mensejahterakan masyarakat melalui kebijakan hukum pidana tidak merupakan satu-satunya cara yang memiliki peran paling strategis. Dikatakan demikian karena hukum pidana hanya sebagai salah satu dari sarana kontrol masyarakat (sosial). Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan Hukum Siber, yang diambil dari kata *Cyber Law* adalah istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang digunakan adalah Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan hukum Mayantara. Istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbaris virtual.

Istilah hukum siber digunakan dalam tulisan ini dilandasi pemikiran bahwa *cyber* jika diidentikkan dengan *Dunia Maya* akan cukup menghadapi persoalan jika harus membuktikan suatu persoalan yang diasumsikan sebagai "maya", sesuatu yang tidak terlihat dan semu. Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyber space*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya etika, dan ketiga pendekatan hukum (Ahmad M Ramli, 2004). Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak. Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *Cyber Crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas

kekuatan Undang-undang yang telah ada sebelumnya (*asas legalitas*), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal I ayat (1) KUHP:

Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada.

Dari alasan di atas, bagaimana pembuktian-pembuktian dalam *Cyber Crime* cukup sulit dilakukan mengingat, bahwa hukum di Indonesia yang mengatur masalah ini masih banyak cacat hukum yang dapat dimanfaatkan oleh para pelaku *Cyber Crime* untuk lepas dari proses pemidanaan. Bentuk-bentuk *Cyber Crime* pada umumnya yang dikenal dalam masyarakat dibedakan menjadi 3 (tiga) kualifikasi umum, yaitu: (Natalie D Voss, 1994)

a. Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer:
    1. *Illegal access* (akses secara tidak sah terhadap sistem komputer)
    2. *Data interference* (mengganggu data komputer)
    3. *System interference* (mengganggu sistem komputer)
    4. *Illegal interception in the computers, systems and computer networks operation* (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer)
    5. *Data Theft* (mencuri data)
    6. *Data leakage and espionage* (membocorkan data dan memata-matai)
    7. *Misuse of devices* (menyalahgunakan peralatan komputer)
b. Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan:
    1. *Credit card fraud* (penipuan kartu kredit)
    2. *Bank fraud* (penipuan terhadap bank)
    3. *Service Offered fraud* (penipuan melalui penawaran suatu jasa)
    4. *Identity Theft and fraud* (pencurian identitas dan penipuan)
    5. *Computer-related fraud* (penipuan melalui komputer)
    6. *Computer-related forgery* (pemalsuan melalui komputer)

7. *Computer-related betting* (perjudian melalui komputer)
8. *Computer-related Extortion and Threats* (pemerasan dan pengancaman melalui komputer)

c. Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem komputer:
   1. *Child pornography* (pornografi anak)
   2. *Infringements Of Copyright and Related Rights* (pelanggaran terhadap hak cipta dan hak-hak terkait)
   3. *Drug Traffickers* (peredaran narkoba), dan lain-lain.

Kegiatan siber meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lagi untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hokum secara nyata dalam Pasal 5 Undang-undang Nomor 11 Tahun 2008.

Kejahatan *cyber crime* dibagi menjadi 2 kategori, yakni *cyber crime* dalam pengertian sempit dan dalam pengertian luas. *cyber crime* dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan *cyber crime* dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer (Barda Nawawi Arief, 2006). Melihat fakta hukum sebagaimana yang ada pada saat ini, dampak perkembangan ilmu pengetahuan dan teknologi yang telah disalahgunakan sebagai sarana kejahatan ini menjadi teramat penting untuk diantisipasi bagaimana kebijakan hukumnya, sehingga *cyber crime* yang terjadi dapat dilakukan upaya penanggulangannya dengan hukum pidana, termasuk dalam hal ini adalah mengenai sistem pembuktiannya. Dikatakan teramat penting karena dalam penegakan hukum pidana dasar pembenaran seseorang dapat dikatakan bersalah atau tidak melakukan tindak pidana, di samping perbuatannya dapat dipersalahkan atas kekuatan undang-undang yang

telah ada sebelumnya (asas legalitas), juga perbuatan mana didukung oleh kekuatan bukti yang sah dan kepadanya dapat dipertanggungjawabkan (unsur kesalahan). Pemikiran demikian telah sesuai dengan penerapan asas legalitas dalam hukum pidana (KUHP) kita, yakni sebagaimana dirumuskan secara tegas dalam Pasal 1 ayat (1) KUHP *Nullum Delictum Nulla poena sine praevia lege poenali* atau dalam istilah lain dapat dikenal, tiada tindak pidana, tidak ada pidana, tanpa adanya aturan hukum pidana terlebih dahulu (Sudaryono & Natangsa Surbakti, 2005).

RINCIAN PEMBAHASAN MATERI

Media sosial merupakan media yang memanfaatkan internet sebagai sarana untuk para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan suatu konten yang isinya meliputi blog, jejaring sosial, forum, dunia virtual, dan lain sebagainya (Nasrullah, 2015). Pada praktiknya saat ini, media sosial digunakan oleh masyarakat tidak hanya untuk kegiatan interaksi ataupun berbagi konten biasa saja, melainkan juga digunakan untuk kegiatan lainnya seperti bisnis dan pendidikan. Contoh media sosial yang banyak digunakan saat ini adalah *Instagram*, *Facebook*, *Twitter*, *WhatsApp*, *Line*, dan lain sebagainya.

Berkaitan dengan penggunaan media sosial dalam ranah pendidikan, kegiatan tersebut belakangan ini menjadi hal yang lumrah seiring dengan perkembangan zaman dan teknologi informasi. Selain itu, kondisi Pandemi COVID-19 yang terjadi pada awal tahun 2020 hingga saat ini menjadi salah satu faktor lainnya yang mengharuskan sistem pendidikan termasuk di negara Indonesia untuk terus berkembang dan berinovasi. Adapun manfaat daripada penggunaan media sosial dalam kegiatan pendidikan diantaranya ialah: (Vanue, 2021)

1) Media sosial sebagai saluran komunikasi
   Komunikasi yang efektif antara guru dan siswa merupakan aspek utama dan terpenting dalam menjalankan roda pembelajaran. Apabila tidak tersedia forum atau media untuk berkomunikasi antara guru dan siswa, makan kegiatan pengajaran dan pembelajaran akan sulit dilakukan dengan optimal. Demikian kehadiran media sosial menjadi salah satu solusi untuk kelancaran komunikasi.

2) Pembelajaran *Online* yang kreatif
   Pembelajaran *online* atau daring (*E-Learning*) merupakan metode pembelajaran yang dilakukan melalui media elektronik dan aplikasi *online* seperti *Youtube* ataupun *Zoom Meeting.* Melalui media dan aplikasi-aplikasi tersebut, guru dan siswa dapat mengekspresikan langsung pendapat serta pengetahuan yang hendak disampaikan. Selain itu, materi yang disampaikan kerap kali lebih mudah dipahami apabila dapat dilihat sekaligus didengarkan berulang kali.
3) Mempermudah perolehan informasi
   Media sosial untuk kegiatan pendidikan dinilai dapat meningkatkan prestasi akademik siswa dan menambah pengetahuan mereka karena adanya kemudahan untuk mengakses informasi dan melakukan pengumpulan data. Informasi tersebut dapat diperoleh dari berbagai *platform online* yang terkait dengan materi, serta melalui grup-grup belajar yang ada pada media sosial seperti *WhatsApp*, *Line*, dan *Facebook*.

Demikian penggunaan media sosial untuk kegiatan pendidikan merupakan hal yang bermanfaat guna meningkatkan kualitas pembelajaran dan pengajaran terutama di era perkembangan teknologi informasi dan Pandemi COVID-19. Meski begitu, seiring peningkatan tersebut perlu diimbangi juga dengan pemahaman oleh semua kalangan yang beraktivitas secara *online* atau terhubung dengan internet mengenai cara atau ketentuan pada media sosial atau bahkan *cyberspace* dengan baik dan benar. Pemahaman mengenai etika merupakan salah satu hal yang sangat penting guna mewujudkan aktivitas pada *cyberspace* yang baik dan benar. Etika merupakan aturan tidak tertulis yang diakui dan dipatuhi oleh masyarakat. Kemudian etika dijelaskan juga sebagai suatu ilmu yang mengkaji tentang persoalan baik dan buruk berdasarkan akal pikiran manusia (Mawardi, 2012). Secara teoritis etika diketahui terdiri atas beberapa bentuk diantaranya: (Miswardi, Nasfi & Antoni, 2021)

1) Etika Deskriptif
   Etika deskriptif yaitu memberikan gambaran dan ilustrasi tentang tingkah laku manusia ditinjau dari nilai-nilai baik dan buruk serta hal-

hal yang mana yang boleh dilakukan sesuai dengan etis yang dianut oleh masyarakat.

2) Etika Normatif
   Etika Normatif yang membahas dan mengkaji ukuran baik, buruknya tindakan manusia yang biasanya dikelompokkan menjadi sebagai berikut:
   a. Etika umum yang membahas berbagai macam hubungan dengan kondisi manusia untuk bertindak etis dalam mengambil berbagai macam kebijakan berdasarkan teori-teori dan juga prinsip-prinsip moral.
   b. Etika khusus yang terdiri dari:
      1) Etika Sosial yaitu etika yang menekankan tanggung jawab sosial dan hubungan antar sesama manusia dalam aktivitas yang dilakukannya.
      2) Etika Individual yaitu etika yang lebih menekankan kepada kewajiban manusia sebagai pribadi.
      3) Etika Terapan yaitu etika yang diterapkan pada suatu profesi.

Selanjutnya, adapun fungsi dari penerapan etika secara umum dalam kegiatan bermasyarakat diantaranya adalah: (Gramedia, 2021)

1) Memperoleh pandangan atau perspektif kritis yang berhadapan langsung dengan berbagai moral.
2) Guna pandangan atau orientasi etis dalam mengambil suatu sikap yang wajar dalam situasi dan kondisi masyarakat yang majemuk (pluralisme).
3) Guna memperlihatkan suatu keterampilan berpikir jernih dalam berargumentasi secara kritis dan rasional.
4) Berfungsi sebagai pembeda mana yang boleh diubah dan mana yang tidak boleh diubah.
5) Berfungsi menyelidiki suatu konflik atau permasalahan hingga ke akar-akarnya.
6) Berfungsi untuk membantu sebuah konsistensi.
7) Berfungsi untuk menyelesaikan konflik, baik itu konflik moralitas maupun konflik sosial lainnya dengan gagasan yang tersistematis dan kritis.

Demikian hal-hal tersebut memperlihatkan bahwa etika secara umum memiliki beberapa manfaat seperti untuk membedakan antara hal yang baik dan buruk, kemudian menjadikan seseorang memiliki sikap lebih kritis dan rasional, serta dapat membantu untuk berpendapat dan bersikap (menjadi pandangan hidup). Bagi seseorang yang tidak mematuhi etika yang berlaku, ia akan menerima sanksi sosial dari masyarakat tersebut sehingga pemahaman dan penerapan etika dalam kegiatan bermasyarakat sangatlah penting.

Pada praktiknya saat ini, penggunaan media sosial dalam *cyberspace* di Indonesia terus meningkat. Berdasarkan hasil survei dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), diketahui terdapat 210,03 juta pengguna internet di dalam negeri pada periode 2021-2022, jumlah tersebut meningkat 6,78% dibandingkan pada periode sebelumnya yang sebesar 196,7 juta orang, demikian hal itu pun membuat tingkat pengguna internet di Indonesia menjadi sebesar 77,02% (Bayu, 2022).

Lebih spesifik lagi, APJII menyebutkan bahwa sebanyak 99,16 persen dari kelompok pengguna usia 13-18 tahun atau anak usia sekolah sudah mengenal dan terhubung dengan internet (Riyanto, 2022). Selain itu, Badan Pusat Statistik (BPS) menyebutkan juga bahwa mayoritas anak usia 5 tahun ke atas di Indonesia sudah mengakses media sosial dengan persentase 88,99%. Selanjutnya dari jumlah tersebut, secara spesifik dijelaskan juga bahwa sebanyak 66,13% menggunakannya untuk memperoleh berita atau informasi, dan sebanyak 33,04% menggunakannya untuk mengakses tugas sekolah (Jayani, 2021). Perhitungan tersebut memperlihatkan bahwa penggunaan internet, *cyberspace*, dan media sosial dalam kegiatan pendidikan telah semakin marak dilakukan terutama oleh para siswa di Indonesia. Keadaan tersebut tentu merupakan suatu hal yang baik, namun di sisi lain tetap perlu diperhatikan bahwa penggunaan internet tidak selamanya menimbulkan hal positif namun juga negatif seperti misalnya *cyber bullying*, penyebaran konten pornografi dan kekerasan, serta lain sebagainya yang dapat merusak moral anak-anak atau siswa. Selain itu konten atau informasi yang diperoleh juga dapat mempengaruhi perilaku atau etika daripada siswa tersebut, sehingga tetap diperlukan pengawasan oleh orang tua dan para guru atas informasi yang diakses. Hal-hal tersebut menjadi dasar

dilakukannya Pengabdian Pada Masyarakat (PPM) di SMK Negeri 3 Bandung dan SMK Negeri 9 Bandung (Enni Soerjati Priowirjanto, 2022).

SMK Negeri 3 Bandung dan SMK Negeri 9 Bandung merupakan dua contoh sekolah yang sudah melaksanakan sistem pembelajaran *online* atau *E-Learning* dalam kegiatan belajar mengajarnya termasuk pada saat kondisi Pandemi COVID-19. Selain itu, SMK Negeri 3 Bandung dan SMK Negeri 9 Bandung adalah merupakan sekolah yang memiliki tujuan untuk mensosialisasikan kegiatan pembelajaran *online* yang baik, aman, dan berkualitas. Tujuan tersebut didukung dengan upaya para guru dan siswa-siswi untuk menggunakan media sosial dan *platform* pembelajaran *online* dalam berbagai kegiatan belajar mengajarnya hingga saat ini. Kedua sekolah tersebut, telah menyediakan layanan pembelajaran *online* yang optimal seperti bahan ajar yang sesuai dan memadai, serta guru-guru yang telah siap untuk memberikan pengajaran secara *online*. Tidak hanya itu, kedua sekolah tersebut juga telah menyediakan layanan Bimbingan Konseling yang diisi oleh beberapa orang guru dengan maksud dapat memantau perkembangan dan kondisi para siswanya dengan lebih optimal (Enni Soerjati Priowirjanto, 2022).

Tindak pidana terkait dengan *ITE atau cyber crime* merupakan salah satu bentuk dimensi baru dari kejahatan masa kini yang sebelumnya tidak kenal berbeda dengan tindak pidana konvensional yang memang ada aturannya dalam Hukum positif di masing-masing Negara sesuai dengan kedaulatan masing-masing Negara dan diharapkan tindak pidana *cyber crime* juga mampu diakomodasi dalam hukum positif sehingga tindak pidana ini dapat ditanggulangi dan ditangani. Seiring dengan tingginya tingkat penyalahgunaan komputer di Indonesia, pemerintah mengeluarkan undang-undang yang dapat melindungi individu dari pelaku kejahatan. Undang-undang Hak Cipta No. 19 Tahun 2002 dibuat pemerintah RI untuk melindungi hasil karya orang lain dan menegakkan etika dalam penggunaan komputer. Namun, Barat (1995) berpendapat bahwa tata tertib/aturan tidak dapat mengubah sikap seseorang terhadap penggunaan komputer, bagaimanapun, perusahaan harus fokus kepada pelatihan etika formal (Dety Nurfadilah, 2016).

Pesatnya perkembangan teknologi informasi dan komunikasi telah mengubah perilaku dan pola hidup masyarakat secara global. Perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas (*borderless*), dan perubahan sosial, budaya, ekonomi dan pola penegakan hukum secara signifikan berlangsung demikian cepat. Teknologi informasi yang canggih sekarang ini bagaikan pisau bermata dua, karena selain memberikan kontribusi dalam meningkatkan kesejahteraan, kemajuan dan peradaban manusia, sekaligus juga menjadi sarana yang efektif bagi perbuatan yang melawan hukum, etika, dan moral, yaitu kejahatan *computer* (*cyber crime*).

B. PENGERTIAN ETIKA

Etika menjelaskan mengenai beberapa peraturan, nilai, proses, norma dan langkah-langkah yang difungsikan menjadi panutan oleh seseorang individu dalam melaksanakan kegiatan sehari-hari. Asal mula pengertian dari kata etika berasal dari sebuah bahasa Yunani yang berarti *Ethos*. Yang artinya dapat dijabarkan kembali yang berarti sebuah kebiasaan. Dalam pengertian etika juga terdapat beberapa makna-makna yang berkaitan satu sama lain, antara lain meliputi: (Tanhella Zein Vitadiar dkk, 2021).

1. Makna yang pertama berarti sebuah semangat dari khas kelompok tertentu, sebagaimana contohnya seperti *ethos* kerja, kode etik, dan sekelompok profesi.
2. Makna yang kedua berarti sebuah nilai yang dimiliki dan dijadikan pedoman oleh komunitas atau kelompok masyarakat dalam mengetahui mana yang baik dan benar.
3. Makna yang ketiga berarti sebuah ilmu yang membahas dan menjelaskan beberapa prinsip dari aturan perbuatan yang efektif dan benar. Etika dapat diartikan sebagai pemikiran mengenai hal yang kritis dan dapat diterima secara rasional mengenai bentuk-bentuk norma yang dapat diwujudkan dalam perbuatan hidup seorang manusia.

Dalam mengartikan etika juga memiliki beberapa arti lain dan juga masing-masing arti tersebut memiliki perbedaan apabila dipandang dari sudut penggunanya. Bagi kalangan sosiolog, arti dari etika merupakan

sebuah adat, kebiasaan atau perilaku dari masyarakat atau orang-orang sekitar di suatu lingkungan budaya. Bagi kalangan eksekutif, arti dari etika sendiri juga berarti sebuah bentuk kewajiban dan tanggung jawab terhadap para pelanggan, organisasi dan juga para *staff*, terhadap diri sendiri dan profesi, terhadap pemerintah. Bagi kalangan asosiasi profesi, arti dari etika juga merupakan sebuah kesepakatan bersama dan pedoman yang harus diterapkan serta dipatuhi oleh semua kalangan anggota asosiasi tentang sesuatu yang harus diketahui serta dapat dinilai mana yang baik dan mana yang buruk dalam menjalankan kegiatan pelaksanaan profesi tersebut (Tanhella Zein Vitadiar dkk, 2021).

Maka dalam hal ini dapat disimpulkan bahwa etika merupakan sebuah studi yang menjelaskan dan memahami mengenai hal-hal yang berkaitan dengan sebuah hak dan kewajiban yang menunjukkan tindakan yang positif ataupun negatif. Selain itu dapat pula menunjukkan mengenai tanggung jawab yang dimiliki oleh seseorang yang mampu mempengaruhi sifat manusia terhadap moral dan solidaritas mereka terhadap lingkungan masyarakat (Tanhella Zein Vitadiar dkk, 2021).

C. MACAM-MACAM ETIKA

Etika juga memiliki berbagai macam-macam yang dapat dijelaskan dan kemudian dijelaskan berdasarkan lingkungan, jenis dan ruang lingkupnya, serta berbagai sumber yang dimiliki. Berikut merupakan macam-macam dari etika antara lain meliputi: (Tanhella Zein Vitadiar dkk, 2021).

1. Jenis Etika

Dalam hal ini, etika memiliki dua jenis, di antaranya adalah normatif dan deskriptif. Berikut merupakan penjelasan dari masing-masing etika berdasarkan jenisnya:

a. Etika Normatif, Menjelaskan bahwa etika ini membutuhkan sebuah usaha dalam penentuan dan penetapan dari perbuatan dan perilaku yang ideal. Dimaksudkan disini, yang sewajarnya dan seharusnya dilakukan oleh setiap individu dalam melakukan kegiatan di kehidupannya.
b. Etika Deskriptif, Merupakan jenis etika yang berusaha melihat sikap dari individu seseorang dan beberapa hal yang perlu diperjuangkan dan oleh setiap orang dalam meraih nilai kehidupan.

2. Ruang lingkup Etika

Etika yang dimaksudkan dalam hal ini terbagi juga menjadi 2 yaitu khusus dan umum. Penjabaran mengenai kedua hal tersebut seperti berikut ini:

a. Etika Khusus, Adalah etika yang dimiliki oleh setiap orang akan diimplementasikan dan diwujudkan berdasarkan prinsip yang ada di kehidupan masing-masing individu tersebut yang bersifat *privat*.
b. Etika Umum, Merupakan keterikatan mengenai keadaan yang menunjukkan perbuatan dasar manusia dan perilaku yang dapat diterima oleh khalayak *publik.*

3. Etika Berdasarkan Lingkungannya

Untuk menunjukkan etika yang dipengaruhi oleh lingkungan terbagi menjadi dua yaitu individual dan sosial. Berikut ini penjelasan mengenai keduanya yaitu:

a. Etika Individual, Artinya bahwa etika dapat memberikan hubungan mengenai kewajiban yang perlu dimiliki oleh individu atas hidupnya sendiri.
b. Etika Sosial, Merupakan kebalikan dari individu, tidak hanya menjelaskan tentang tanggung jawab atas dirinya sendiri, namun berkewajiban untuk berperilaku yang pantas sebagai umat manusia.

4. Etika Berdasarkan Sumbernya

Terdapat 2 jenis yang dapat dijelaskan dalam hal ini yaitu teologis dan filosofis.

a. Etika Teologis, Merupakan hubungan dari agama yang diyakini oleh individu sebagai panutan dan kepercayaan yang dimiliki oleh seseorang, yang tidak ada aturan dan batas dari agama tertentu. Perlu penegasan dalam menekankan arti dalam etika jenis ini yaitu Pertama, tidak ada hal yang membatasi etika ini pada satu agama saja, tidak ada hukum mengenai hal tersebut. Hal ini dikarenakan, total agama yang ada dalam kehidupan ini tidak hanya satu tetapi ada enam agama yang diakui. Karena pada dasarnya, setiap agama akan memberikan pembelajaran mengenai etikanya sendiri yang tidak sama dengan satu agama dan agama yang lain dan menunjukkan ciri khas dari agama

tersebut agar lebih spesifik dalam menjelaskan etika yang dimiliki seseorang atas agama yang dianutnya. Kemudian untuk yang kedua, etika memiliki ruang lingkup yang lebih umum di mana setiap individu pasti menerapkan dan mempelajari etika dalam kehidupannya. Sehingga ruang gerak mengenai penjelasan etika seseorang itu luas dan tidak memiliki bagian-bagian yang hanya terfokus pada hal kecil saja namun bagian tersebut tak terbatas. Dalam hal ini, secara tidak langsung, setiap individu perlu pemahaman dan pengetahuan mengenai cara memahami dari etika umum dan sebaliknya.

b. Etika Filosofis, Adalah kemunculannya berasal dari proses berpikir dan berfilsafat yang ditunjukkan oleh setiap orang dalam melakukan hal-hal yang memiliki nilai filosofis. Pemahaman mengenai filsafat ini perlu menguras tenaga karena studi dari filsafat sendiri adalah memahami cara pikir manusia, bagaimana manusia dalam memandang sesuatu menggunakan panca indera yang dimilikinya. Pembagian etika filosofis dapat dibedakan menjadi dua sifat, yakni empiris dan *non*-empiris. Empiris merupakan jenis ini menjelaskan mengenai bentuk suatu hal yang memiliki wujud atau berbentuk nyata. Misalnya, ketika individu mulai memahami mengenai hal yang berkaitan dengan filsafat ekonomi maka hal yang dibahas mengenai masalah ekonomi. Sedangkan sebaliknya, *non*-empiris menjelaskan hal atau bagian yang berusaha untuk berpikir sesuatu yang lebih pasti dari kejadian yang nyata. Pemahaman mengenai *non*-empiris ini mempertanyakan dan mendiskusikan mengenai suatu kejadian apa yang mampu menyebabkan keadaan tersebut dan lebih pada *factor* penyebabnya (Tanhella Zein Vitadiar dkk, 2021).

D. PENGERTIAN ETIKA HUKUM *CYBER*

Menurut Richard A. Spinello, etika *cyber* atau *Cyberethics* adalah penerapan etika yang menjelaskan tentang moral, hukum, dan isu sosial dalam pengembangan dan penggunaan teknologi *cyber* (Fardiyan, 2016). Demikian etika *cyber* tidak sekadar membahas tentang tata cara penggunaan internet yang baik, aman, dan santun, namun lebih jauh lagi etika *cyber* mengkaji permasalahan-permasalahan moral, hukum, dan isu-isu sosial yang berhubungan dengan penggunaan komputer dan jaringan

internet sebagai penunjang interaksi antar manusia (Fardiyan, 2016). Senada juga yang diungkapkan oleh Irwanto (2023) yang menyatakan bahwa etika hukum *cyber* itu bukan hanya sekedar menggunakan teknologi yang baik tetapi bagaimana cara pengguna menggunakan teknologi tersebut dengan cara beretika dalam bersosial melalui jaringan teknologi. Misalnya kita menggunakan WA, IG dan sebagainya. Jadi kita harus beretika dalam menyampaikan suatu berita atau pesan melalui jaringan tersebut.

E. PRINSIP-PRINSIP ETIKA HUKUM *CYBER*

Dalam perkembangannya, terdapat beberapa prinsip yang dapat diterapkan pada etika *cyber*, diantaranya: (Supancana, 2020).

1. Kebebasan (*Freedom*), Prinsip untuk menggunakan *cyberspace* secara bertanggung jawab (*responsibly, accountably*).
2. Keadilan (*Justice*), Prinsip *enable fair, just equitable in cyberspace.*
3. *Equity,* Prinsip mendorong tata kelola internet dengan hak-hak yang sama.
4. Damai (*Peace*), Prinsip mengembangkan "*just cyber warfare*", meningkatkan perdamaian.
5. Keamanan (*Security*), Prinsip kewajiban untuk melindungi (*obligation to protect*) dan hak untuk dilupakan (*the right to be forgotten*).
6. Inklusivitas (*Inclusiveness*), Prinsip untuk mengurangi kesenjangan antara penguasa digital (*digital winner*) dengan pihak-pihak yang kalah (*digitariat*).
7. Privasi (*Privacy*), Prinsip melindungi hak atas data pribadi (terkait *Big Data*).
8. Martabat (*Dignity*), Prinsip melindungi dan meningkatkan martabat dari setiap manusia.
9. Peran serta (*Participation*), Prinsip mendorong peran serta masyarakat dalam pembentukan etika dan hukum.
10. Kejujuran (*Honesty*), Prinsip meningkatkan transparansi melalui teknologi dan hukum.
11. Integritas (*Integrity*), Prinsip melindungi nilai yang diyakini dengan penuh keberanian dan tahan terhadap berbagai godaan.

F. PENTINGNYA MEMAHAMI ETIKA *CYBER*

Berikut adalah beberapa alasan pentingnya menerapkan etika *cyber* dalam penggunaan *cyberspace*, diantaranya adalah: (Waryanto, 2006).

1. Bahwa pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda.
2. Pengguna internet merupakan orang-orang yang hidup dalam dunia *anonymouse* sehingga terkadang tidak mengharuskan pernyataan identitas asli dalam berinteraksi.
3. Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak tidak etis seperti misalnya ada juga penghuni yang iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
4. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya "penghuni" baru di dunia maya tersebut (Enni Soerjati Priowirjanto, 2022).

G. PERSOALAN ETIKA DAN MORAL

Persoalan ITE sebagaimana dikemukakan diatas merupakan dua sisi mata uang, disatu sisi membawa manfaat yang besar bagi kehidupan umat manusia, tetapi juga memiliki sisi negatif yang biasanya dimanfaatkan oleh oknum-oknum tertentu untuk melakukan tindakan-tindakan negatif, karena sifatnya yang tidak mengenal ruang dan waktu, tanpa menguras energi serta sifatnya yang aman karena bisa dilakukan di manapun, bahkan dari gubuk kecil sekalipun, ini tentunya dilakukan tanpa pertimbangan moral dan etika.

Persoalan etika merupakan bagian dari teori nilai, dimana teori nilai merupakan salah satu dari teori filsafat, disamping teori pengetahuan dan teori hakikat, etika membicarakan tentang baik dan buruk perbuatan manusia dengan *focus* kajian tentang nilai-nilai (Juhaya S. Praja, 2011). persoalan etika biasanya dipersandingkan dengan masalah moral yang juga berkaitan dengan nilai yang baik dan buruk, sekalipun keduanya sulit untuk dipisahkan tetapi persoalan etika sifatnya tidak spontan yang mana memerlukan penalaran, mengumpulkan informasi, menguji validitas norma, kritis, serta berpedoman pada metode dalam mengambil

keputusan etis, jadi sifatnya lebih kompleks jika dibanding dengan persoalan moral (Berbard l. Tanya, 2011).

Menurut Frans Magnis Suseno dalam buku dasar-dasar etika disebutkan bahwa ajaran tentang baik dan buruk itu adalah masalah moral, ada banyak ajaran-ajaran diluar diri manusia salah satunya adalah ajaran moral olehnya itu dibutuhkan etika untuk mengkritisi ajaran moral sehingga dapat dipilih ajaran moral yang tepat (Frans Magnis Suseno, 2017). Menurut penulis terkait dengan masalah etika dan moral dan berkaitan dengan pengertian para pakar diatas bahwa jika masalah moral dan etika itu adalah persolan baik dan buruk tetapi etika itu adalah bagian terdalam dari moral, sebagaimana di bahasakan oleh Frans Magnis Suseno bahwa fungsi etika adalah mengkritisi ajaran-ajaran yang berasal dari luar etika, semisal ajaran moral, agama, dan sebagainya. Dikaitkan dengan masalah ITE maka ada berapa konsep terkait dengan moral dan etika yaitu:

Pertama adalah persoalan moral dan etika dari perspektif internal, dimana persoalan moral dan etika ini adalah merupakan sistem nilai tentang baik dan buruk, dimana pada tataran ini etika sebagai pengontrol bagi diri untuk tidak melakukan tindakan-tindakan yang tidak bermoral, apalagi jika dikaitkan dengan persoalan ITE, hal tersebut sangat penting sebagai upaya penanggulangan dari penyalahgunaan ITE, dimana langkah yang tepat adalah kembali kepada diri pribadi yang harus memiliki nilai-nilai etika (Firmansyah, 2017).

Kedua, adalah persoalan moral dan etika dari perspektif eksternal, sebagaimana disebutkan diatas bahwa persoalan moral dan etika sulit untuk dipisahkan apalagi jika dipahami secara internal, tetapi untuk membedakannya dari perspektif eksternal terlihat dari sifatnya memberikan sebuah penilaian, bahwa moral sifatnya spontan, misalnya dalam persoalan ITE ada seseorang yang melakukan perbuatan yang secara lahiriah dianggap negatif, karena sifatnya spontan maka pelaku tersebut langsung dicap tidak bermoral, berbeda dengan konsep etika yang sifatnya tidak spontan yang mana memerlukan penalaran, mengumpulkan informasi, menguji validitas norma, kritis, serta berpedoman pada metode dalam mengambil keputusan etis, jadi sifatnya lebih kompleks jika dibanding dengan persoalan moral, sebagaimana contoh diatas dalam perspektif etika hal tersebut harus butuh analisis, apa

motif atau faktor-faktor penyebab seseorang melakukan hal yang negatif, setelah proses dianalisis kemudian ditarik sebuah kesimpulan apakah itu etis atau tidak.

Ketiga, persoalan etika dan moral dari perspektif yang lain bahwa etika itu adalah bagian yang paling terdalam pada diri manusia yang mampu mengkritisi ajaran-ajaran yang bersumber dari luar diri manusia salah satunya adalah masalah ajaran moral, jika dikaitkan dengan masalah ITE atau tindak pidana *cyber crime*, maka yang paling dibutuhkan antara moral dan etika ketika berhadapan dengan teknologi adalah persoalan etika dimana persoalan etika akan menjadi jernih, akan menjadi pilihan yang tepat ketika juga dilandasi oleh nilai-nilai agama, hal ini dapat tergambarkan seperti kaca yang bening, ketika kaca itu bening maka pilihan-pilihan akan tepat, begitu pula sebaliknya ketika kaca yang menjadi suara hati itu buram, maka pilihan-pilihan itu biasanya tidak tepat. Dalam konteks agama hal-hal yang buram itu adalah dosa-dosa yang dilakukan, olehnya itu dosa-dosa itu harus dimohonkan ampunan kepada pencipta sehingga kaca itu (suara hati) bening dan berdampak pada pilihan yang tepat (Firmansyah, 2017).

H. KEJAHATAN *CYBER* (*CYBER CRIME*)

Era globalisasi tidak lagi menunjukkan cara persaingan yang dilakukan tidak secara tradisional dan konvensional dengan melakukan peperangan yang menggunakan kekuatan senjata, akan tetapi persaingan yang dilakukan pada bidang budaya, perekonomian, politik serta teknologi yang mana persaingan ini tidak menunjukkan hal yang dibatasi oleh suatu cara. Sasaran ancaman kejahatan siber (*cyber crime*) dapat terjadi pada saat penyadapan komunikasi yang melibatkan beberapa pejabat tinggi negara. Peningkatan terhadap ancaman kejahatan siber (*cybercrime*) dapat dilakukan oleh beberapa oleh negara atau *actor non* negara (*non state actor*) berdampak terhadap terjadinya *cyber warfare* atau gangguan *cyber* (*cyber violence*) (Rahmawati, 2017).

Menurut Sudarwanto mengemukakan bahwa bentuk kejahatan yang dilakukan siber adalah dengan melakukan penyerangan yang terjadi pada teknologi digital seperti *content, computer system* dan *communication techonology* yang dimiliki oleh masyarakat secara umum yang berada di

dalam *cyberspace*. Bentuk penyerangan tersebut biasanya terjadi pada jaringan komputer yang mana si pelaku akan memperoleh pengaksesan terhadap akun pribadi pengguna yang kemudian menggunakan *interface* yang dimiliki oleh korban untuk menyerang situs lain (Sudarwanto, 2009). Terdapat beberapa jenis kejahatan *cyber crime* yang terjadi antara lain:

1. *Unauthorized Access to Computer System and Service*
   Bentuk kejahatan yang dilakukan dengan masuk ke dalam sistem jaringan yang dimiliki oleh seseorang tanpa sepengetahuan atau izin dari akses suatu jaringan komputer tersebut yang mana motif yang dilakukan dapat berupa pencurian, pembobolan, sabotase atau yang lainnya sehingga pelaku akan mendapatkan keuntungan dari kejahatan tersebut.
2. *Illegal Contents*
   Bentuk kejahatan yang dilakukan adalah dengan cara memasukan beberapa data maupun informasi yang tidak benar ataupun tidak etis ke dalam teknologi internet yang mana dapat melanggar hukum sehingga masyarakat umum dapat bebas mengaksesnya dan akan mengakibatkan dampak negatif bagi lingkungan masyarakat. Sebagai contoh adalah kejahatan dengan membuat *hoax* atau berita tidak benar, pornografi.
3. *Data Forgery*
   Bentuk kejahatan yang dilakukan dengan cara menyimpan data-data dokumen yang palsu melalui penggunaan teknologi internet.
4. *Cyber Espionage*
   Bentuk kejahatan yang memanfaatkan jaringan dari teknologi internet dikarenakan penyebarannya sangat mudah dan cepat serta dapat diakses oleh siapa saja yang mana pelaku kejahatan memasukan mata-mata atau pendeteksi kedalam jaringan komputer (*computer network system*) ke korban yang dituju. Biasanya kejahatan ini digunakan untuk persaingan bisnis dalam hal penyimpanan data dan dokumen yang tersimpan dalam suatu sistem komputer yang terhubung dengan jaringan komputer.
5. *Cyber Sabotage and Extortation*
   Bentuk kejahatan yang dilakukan adalah dengan melakukan pengrusakan, mengganggu maupun penghancuran terhadap informasi,

program komputer maupun sistem jaringan komputer yang terhubung melalui internet. Penyusupan dengan memasukan virus komputer melalui sistem jaringan komputer dilakukan pada modus kejahatan ini sehingga mengakibatkan data maupun informasi dan program komputer yang digunakan oleh korban tidak dapat diakses lagi. Bentuk kejahatan ini sering disebut dengan *cyber terrorism*.

6. *Offence Againts Intellectual Property*
   Bentuk kejahatan pada modus ini adalah dengan mengarah pada HKI atau Bentuk Hak Kekayaan Intelektual yang dimiliki oleh pihak lain dengan memasukannya ke dalam sistem teknologi internet. Sebagai contoh kejahatan yang dilakukan adalah dengan cara meniru gambaran dari tampilan *website* tertentu dengan menyiarkan rahasia dagang yang merupakan rahasia dagang yang dimiliki oleh korban.
7. *Infrringemts of Pryvacy*
   Modus kejahatan ini yang dilakukan sasarannya adalah informasi yang dimiliki oleh seseorang yang bersifat rahasia dan sangat pribadi. Cara yang dilakukan adalah membobol data pribadi tersebut untuk mendapat keuntungan bagi si pelaku, sebagai contoh data yang dicari adalah nomor PIN yang ada di ATM, nomor kartu kredit (Handayani, 2016).

I. PENANGGULANGAN *CYBER CRIME* DI INDONESIA

Cyber crime adalah tindakan pelanggaran hukum yang secara khusus diatur dalam Undang-undang Nomor 11 Tahun 2008 yang mengatur tentang Informasi dan Transaksi Elektronik untuk mengembangkan pengetahuan dan kemampuan penyidik dalam dunia *cyber* (Suhendar, 2013). Kejahatan *cyber* yang memanfaatkan teknologi informasi sebagai medianya pengaturan hukumnya diatur dalam Undang-undang nomor 11 Tahun 2008 yang sekarang sudah diubah oleh Undang-undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-undang nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terdapat beberapa pasal yang menjelaskan mengenai kejahatan yang dilakukan dengan memanfaatkan teknologi internet dan jaringan komputer seperti transmisi, distribusi atau penyebaran yang dapat diakses pada konten yang *illegal* yang terdiri dari:

1. Kesusilaan (pasal 27 ayat 1 UU ITE)
2. Perjudian (pasal 27 ayat 2 UU ITE)
3. Penghinaan dan pencemaran nama baik (pasal 27 ayat 3 UU ITE)
4. Pemerasan dan pengancaman (Pasal 27 ayat 4 UU ITE)
5. Adanya berita bohong yang menyesatkan dan merugikan konsumen (Pasal 28 ayat 1 UU ITE)
6. Menimbulkan rasa benci yang didasari pada SARA (pasal 28 ayat 2 UU ITE)
7. Mengirimkan informasi yang berisikan ancaman kekerasan serta menakut-nakuti seseorang (pasal 29 UU ITE) (Sari, 2018).

Berdasarkan paparan peraturan yang disebutkan di atas terdapat beberapa hal yang perlu dilakukan agar dapat meminimalisir kejahatan *cyber* di Indonesia antara lain

a. Perlu adanya kesadaran masyarakat untuk dapat mengatasi dan menggunakan teknologi informasi dan komunikasi secara dengan tetap menerapkan UU ITE dalam melakukan transaksi elektronik (Ketaren, 2016)
b. Pemerintah harus mampu menyampaikan peraturan dan penggunaan teknologi informasi yang baik dan benar dalam bentuk penyuluhan dan sosialisasi kepada masyarakat. Pemerintah juga harus mampu dengan tegas dalam menerapkan hukum yang sudah ditentukan terhadap para pelaku kejahatan siber
c. Aparat hukum harus lebih memahami tentang hukum *cyber* (*cyber law*) sebagai tameng atau pelindung dari kejahatan *cyber* agar tidak semakin meluas dan merajalela dalam kehidupan masyarakat (Sari, 2018).

J. PENTINGNYA MENJAGA PRIVASI DUNIA MAYA

Pada era modern saat ini, Media sosial (medsos) kini menjadi hal yang sering digunakan dalam beraktivitas. Berbagai aplikasi dapat memberikan dampak negatif dan positif. Melalui medsos pula, dunia terasa dekat dan informasi cepat diperoleh. Namun, kemajuan teknologi dengan berbagai aplikasi itu menjadikan kejahatan mengintai. Pengguna aplikasi tidak menyadari jika data yang terdapat pada medsos dapat berbahaya jika

disalahgunakan. Menurut RUU Perlindungan Data Pribadi, privasi adalah data pribadi yang diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan atau *non* elektronik. Privasi juga dapat diartikan kombinasi informasi yang melekat pada diri seseorang. Privasi juga merupakan hak individu dimana setiap individu berhak untuk menentukan apakah data pribadi akan dikomunikasikan atau tidak kepada pihak lain. Perlu diketahui bahwa di Indonesia tercatat, sejumlah kasus akibat kebocoran data pribadi. Seperti dalam bentuk pesan singkat dengan menyertai sebuah tautan atau *link* yang tidak jelas, penipuan biasanya juga dilakukan melalui surel, pesan atau telepon dengan mengaku sebagai teman, saudara, perwakilan dari bank atau kartu kredit yang digunakan, perusahaan, toko *online* dan lain-lain.

Modus yang digunakan adalah dengan menyampaikan kebutuhan bantuan mendesak, informasi menang undian, menawarkan pinjaman, hutang yang harus dibayar, dan sebagainya. Tujuan dari kejahatan ini agar korban tanpa sadar memasukkan data yang dimiliki ke dalam situs web palsu, mengunduh program *malware* yang dapat menginfeksi perangkat korban melalui lampiran seperti gambar atau dokumen, atau meminta korban memberikan informasi personal yang lebih detail untuk dapat mengakses ke akun masing-masing. Data pribadi ada dua macam yaitu data umum dan data pribadi spesifik. Data pribadi seperti nama lengkap, jenis kelamin, kewarganegaraan dan agama. Data pribadi yang dikombinasikan untuk mengidentifikasikan seseorang. Sedangkan data pribadi spesifik adalah data informasi kesehatan, data *biometric*, data genetika, kehidupan atau orientasi seksual, pandangan politik, keuangan pribadi dan lain-lain.

Privasi itu adalah kesadaran. Menjaga keamanan privasi data di dunia digital dapat dimulai dari hal-hal sederhana, yaitu kesadaran tentang data pribadi. Yang melanggar privasi itu dimulai dari diri sendiri. Kadang seseorang juga tidak sadar saat memberikan data pribadi diri sendiri dalam sebuah acara, aplikasi di *handphone* atau mengunggah identitas diri di media sosial. Kebocoran data pribadi juga dapat menimbulkan berbagai dampak seperti diskriminasi atau prasangka buruk, tindak kejahatan dan kriminal. Beberapa hal yang mungkin terjadi adalah penipuan *online*,

penipuan *pishing, malware*, bom email, peretasan dan *spamming* media sosial, pencurian uang elektronik, data *diddling*, peretasan, *cyber stalking, cyber bullying*, *identity theft* dan *ransomware*. Oleh karena itu, untuk menjaga semua bentuk yang diberikan privasi oleh orang harus lebih berhati-hati dan tidak ceroboh dalam meletakkan di tempat mana saja. Maka untuk menyikapi hal ini, diperlukan beberapa tahapan yang dapat dilakukan dalam menjaga privasi agar tetap aman walaupun sedang berselancar di dunia maya, yaitu:

a. Mengubah pengaturan privasi atau keamanan. Pahami dan gunakan fitur *setting* pengamanan ini seoptimal mungkin.
b. Buat kata sandi sekuat mungkin. Ketika melakukan registrasi *online*, sebaiknya lakukan kombinasi antara huruf besar dan kecil, angka, dan simbol supaya tak mudah terlacak.
c. Rahasiakan *password* yang telah dibuat. Usahakan jangan sampai ada yang mengetahuinya.
d. Untag diri sendiri.
e. Perlu dihindari dalam memberikan segala bentuk pertanyaan, dan harus ada filter mengenai pertanyaan apalagi tentang data diri. Contohnya tempat tanggal lahir, nama bahkan alamat. Dengan adanya pertanyaan tersebut akan lebih memudahkan bagi peretas untuk mengambil identitas dan pengambilan uang yang ada di kartu kredit, karena banyak sekali pertanyaan yang diajukan tersebut sebagai keamanan untuk *database* bank.
f. Tidak perlu memberikan perhatian dan jawaban atas ponsel yang tidak memberikan kejelasan detailnya. Dikarenakan hal-hal yang perlu kita curigai ketika menemukan surat elektronik yang tidak memberikan identitas secara lengkap seperti nama pengirim ataupun darimana asalnya. Dalam kasus tersebut, maka kita biarkan saja karena tidak tahu tujuannya, bisa saja malah memberikan dampak *negative.*
g. Diharapkan untuk tidak lupa keluar atau *logout* pada setiap akun pribadi, apalagi jika menggunakan *computer* fasilitas umum. Dikarenakan orang-orang akan lebih mudah mengambil informasi.
h. Untuk setiap individu yang menggunakan wifi, perlu pemberian kata sandi yang sulit dan mudah ditebak.

K. ALASAN PENTINGNYA ETIKA HUKUM *CYBER*

Hukum (*law*) adalah peraturan perilaku formal yang ditetapkan oleh otoritas yang berwenang, seperti pemerintah, terhadap subjek atau warga negaranya. Selama sekitar 10 tahun pertama penggunaan komputer di bidang bisnis dan pemerintahan, tidak terdapat perangkat hukum yang berkaitan dengan penggunaan komputer. Hal ini dikarenakan pada saat itu komputer merupakan inovasi baru, dan sistem hukum membutuhkan waktu untuk mengejarnya (Yahfizham, 2012). Pemerintah federal Amerika Serikat merencanakan undang-undang privasi komunikasi elektronik (*Electronic Communications Privacy Act*) tahun 1968. Namun, *draft* rancangan undang-undang ini hanya mencakup data digital, komunikasi video, dan surat elektronik. Pada tahun 1970-an dikenal beberapa hukum tambahan dalam bentuk undang-undang pelaporan kredit yang wajar (*Fair Credit Reporting Act*), yang berkaitan dengan penanganan data kredit. Tahun 1978 undang-undang hak privasi federal (*Right to Federal Privacy Act*) ditetapkan, yang membatasi tindakan pemerintah federal untuk melaksanakan penyelidikan pada catatan-catatan bank.

Pada tahun 1984, kongres Amerika Serikat memperkuat undang-undang mengenai penggunaan komputer dengan mengeluarkan peraturan-peraturan yang secara khusus diterapkan pada kejahatan komputer. Undang-undang keamanan komputer usaha kecil dan pendidikan (*The Small Business Computer Security and Education Act*) ditetapkan oleh Dewan Penasihat Keamanan Komputer Usaha Kecil dan Pendidikan (*Small Business Computer Security and Education Advisory Council*). Dewan ini bertanggung jawab untuk memberi nasihat kepada kongres mengenai masalah yang berhubungan dengan kejahatan komputer terhadap usaha-usaha kecil dan untuk mengevaluasi efektivitas dari hukum pidana negara dan federal dalam mencegah dan menghukum kejahatan *computer* (Yahfizham, 2012). Kemudian pada tahun 1988, hukum lain yang ditujukan untuk membatasi pemerintah federal, undang-undang privasi dan pencocokan komputer *(Computer Matching and Privacy Act*), yang membatasi hak pemerintah federal untuk mencocokkan *file* komputer yang bertujuan untuk menentukan kelayakan program pemerintahan atau mengidentifikasi para debitor. Tidak lama setelah

undang-undang kebebasan informasi (*Freedom of Information Act*) diterapkan.

Undang-undang perangkat akses palsu dan kejahatan serta penipuan melalui komputer (*Counterfeit Access Device and Computer Fraud and Abuse Act*) menetapkan bahwa merupakan suatu kejahatan federal jika seseorang mendapatkan akses tanpa otorisasi atas informasi yang berhubungan dengan pertahanan negara atau hubungan luar negeri. Undang-undang ini juga mengenakan tindak pidana ringan pada usaha mendapatkan akses tanpa otorisasi ke suatu komputer yang dilindungi oleh undang-undang hak privasi keuangan (*Right to Financial Privacy Act*) atau undang-undang pelaporan kredit yang wajar serta menyalah gunakan informasi pada komputer yang dimiliki pemerintah federal. Setelah undang-undang komputer Amerika serikat mulai diterapkan, maka berbagai hak dan batasan yang berkaitan dengan akses data dipegang oleh pemerintah. Undang-undang kebebasan informasi (*Freedom of Information Act*) tahun 1996 memberi warga negara dan organisasi-organisasi Amerika Serikat, hak terhadap akses data yang dipegang oleh pemerintah federal dengan beberapa pengecualian. Baik pemerintah dan warga negara Republik Rakyat Cina (RRC) semakin sadar akan kebutuhan untuk menentukan privasi pribadi. Salah satu masalah adalah istilah privasi seringkali memiliki konotasi yang negatif, karena diasosiasikan dengan seseorang yang menyembunyikan sesuatu. Para aktivis privasi pribadi di Cina menuntut diadakannya peraturan yang akan melindungi data pribadi seperti tingkat pendapatan , pekerjaan, status pernikahan, sifat fisik, dan bahkan alamat dan nomor telepon.

Pada saat ini, pemerintah Cina sedang berfokus untuk menerapkan peraturan penggunaan komputer dan Internet. Peraturan-peraturan ini menyatakan bahwa penggunaan perangkat ini tidak boleh mengganggu "keamanan negara", "kepentingan sosial", "kepentingan warga negara yang berazaskan hukum", dan "privasi". Namun, hingga saat ini definisi dari istilah ini belum tersedia. Dalam menyusun argumen ini, para aktivis mengidentifikasi Uni Eropa dan Amerika Serikat sebagai model untuk undang-undang yang dibutuhkan. Penggunaan komputer di dunia bisnis diarahkan oleh nilai moral dan etis manajer, spesialis informasi, dan pengguna, serta hukum yang berlaku. Hukum adalah yang termudah untuk

diinterpretasikan karena bersifat tertulis. Tetapi etika tidak terdefinisi demikian tepat, dan mungkin bahkan tidak disetujui oleh semua anggota masyarakat. Wilayah etika komputer yang kompleks inilah yang saat ini sangat banyak diperhatikan.

Indonesia sebagai suatu negara hukum, juga memiliki perangkat hukum dan perundang-undangan yang secara khusus membahas mengenai informasi dan transaksi elektronik, yang tertuang didalam UU ITE Nomor 11 Tahun 2008. Dasar dari undang-undang adalah Pasal 5 ayat (1) dan Pasal 20 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Untuk lebih jelasnya dapat dilihat disitusnya kementrian komunikasi dan informasi (www.kominfo.go.id). Berikut ini akan diberikan pertimbangan menyangkut UU ITE Nomor 11 Tahun 2008 tersebut.

a. Bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;
b. Bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan Informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;
c. Bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;
d. Bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional;
e. Bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;

f. Bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia (Yahfizham, 2012).

L. UNSUR-UNSUR HUKUM *CYBER*

Tidak dapat terabaikan dalam mengatur norma dan nilai yang berlaku di tengah masyarakat diperlukan sebuah hukum yang tegas. Hukum ini memiliki sifat yang mengikat yang berguna dalam menjaga bagaimana setiap manusia melakukan perbuatannya dalam kesehariannya dan mengatur hal tersebut sehingga dalam wilayah tersebut memiliki keadaan yang tertib sehingga individu di dalamnya dapat merasakan keamanan dan kenyamanan. Dalam sebuah hukum juga terdapat beberapa unsur-unsur diantaranya meliputi:

a. Mengatur Tingkah Laku Masyarakat. Perlu adanya sebuah aturan di dalam hukum untuk mengolah segala bentuk komunikasi dan interaksi yang dapat menghubungkan setiap anggota masyarakat di sebuah wilayah yang memiliki hukum yang baik.
b. Dibuat Badan Resmi yang Berwajib. Bukan suatu hal yang sembarangan dalam menciptakan sebuah produk hukum. Pembuatannya bukan dari orang atau lembaga namun yang memiliki hak dan wewenang adalah badan resmi dan itu pun sudah didasarkan pada kesepakatan.
c. Peraturan Bersifat Memaksa. berbeda dengan hukum-hukum norma lainnya yang ada di tengah masyarakat dengan bersifat bebas, tingkat hukum ini memiliki sifat yang memaksa. kata memaksa dalam hal ini dapat diartikan dan ditunjukkan dengan sebuah sanksi atau hukuman untuk siapa saja yang telah melanggar atau tidak menaati hukum yang berlaku.
d. Sanksi Bersifat Tegas. Tidak ada hukum yang tidak memberikan sanksi, oleh karena itu sebuah produk hukum harus memiliki unsur adanya hukuman yang tegas. Tidak semena-mena dan asal dalam memberikan hukuman namun semua telah diatur dan termuat pada undang-undang yang telah mendapatkan kesepakatan bersama. Contoh dari

sanksi tersebut yaitu hukuman mati, diberikan denda sesuai dengan kerugian yang ditimbulkan korban dan tinggal di sel penjara (Tanhella Zein Vitadiar, 2021).

M. PERKEMBANGAN TEKNOLOGI INFORMASI DAN TRANSAKSI ELEKTRONIK

Menurut UU No 11 Tahun 2008 tentang Informasi dan transaksi Elektronik, Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. Jika dalam transaksi klasik, pembeli dan penjual harus bertemu secara langsung, maka dalam transaksi elektronik menggunakan konsep *telemarketing* yaitu perdagangan jarak jauh yang memanfaatkan internet sehingga antara pembeli dan penjual tidak perlu bertemu secara fisik. Perkembangan transaksi elektronik saat ini memberikan banyak perubahan pada banyak pelaku bisnis di dunia nyata. Mereka mulai mengembangkan usahanya di dunia maya karena memang memiliki beberapa keunggulan daripada bertransaksi di dunia nyata, misalnya saja, dengan memanfaatkan *e-commerce*, mereka tidak perlu bertemu secara langsung sehingga dapat menghemat waktu dan tenaga, dalam bertransaksi pun juga dapat secara global atau tidak terbatasi karena tempat yang jauh selain itu biaya yang dikeluarkan lebih murah.

Saat ini, transaksi elektronik atau *e-commerce* turut menjadi penggerak pertumbuhan ekonomi di Indonesia. Pada zaman dahulu, manusia hidup pada masa primitif, mereka melakukan perdagangan dengan sistem barter atau dagang tukar, yaitu jika seseorang menginginkan sesuatu yang tidak dapat dibuatnya sendiri, maka ia berusaha memperolehnya dengan cara bertukar, yakni bentuk transaksi menggunakan barang dengan barang saja yang dipertukarkan. Lalu seiring kemajuan zaman, bentuk transaksi atau perdagangan menjadi perdagangan konvensional, yaitu dengan menggunakan uang sebagai alat tukar, lalu terus terjadi kemajuan dalam bidang perdagangan dan sampai saat ini telah melahirkan model transaksi *e-commerce*. Di era globalisasi seperti saat ini, pemanfaatan teknologi informasi dan Transaksi elektronik mutlak dilakukan karena sangat berpengaruh untuk menunjang perekonomian nasional guna mewujudkan kesejahteraan masyarakat.

Dalam perspektif masa depan, dunia akan menjadi sebuah perkampungan besar, sehingga batas-batas Negara menjadi sangat kabur. Di Indonesia, jumlah pengguna internet sangat banyak, maka potensi *E-commerce* di Indonesia untuk terus berkembang di masa mendatang semakin luas karena internet ibarat bumi baru bagi *E-commerce*. Semakin mudah akses internet semakin mudah *E-commerce* untuk dilakukan. Di masa sekarang, masyarakat sudah familiar dengan *marketplace-marketplace* seperti lazada, bukalapak, shopee, akulaku, atau forum jual beli kaskus. Bahkan saat ini, aplikasi tiktok yang awalnya hanya sebagai pembuat konten video, sudah merambah ke aktivitas jual beli.

Begitu juga aplikasi facebook sudah menyediakan fitur *marketplace* untuk para penggunanya. *Website-website* tersebut merupakan contoh mudah dari implementasi *E-commerce*. Di lain sisi perkembangan *e-commerce* yang memiliki banyak kemudahan, juga memiliki sisi *negative* antara lain mengenai masalah kerahasiaan (*Confidentiality*) pesan, masalah bagaimana cara agar pesan yang dikirimkan itu keutuhannya (*integrity*) sampai ketangan penerima, masalah keabsahan (*authenticity*) pelaku transaksi dan masalah keaslian pesan agar bias dijadikan barang bukti. Di negara Indonesia, masih menjadi pertanyaan mendasar mengenai bagaimana Indonesia mengantisipasi atau menciptakan *rule of law* atas transaksi *e-commerce* ini. Walaupun internet di Indonesia masih relatif baru, tetapi relatif cepat pula meraih popularitas di kalangan masyarakat. Dalam *e-commerce* semua perbuatan hukum dilakukan secara virtual, dan bersifat tanpa batas. Berbeda dengan transaksi konvensional yang perbuatan hukumnya jelas karena dalam kesepakatan antara penjual dan pembeli dilakukan secara langsung atau tatap muka, selain itu, dalam kesepakatannya juga biasanya menggunakan tanda tangan hitam di atas putih. Dalam sistem transaksi elektronik, kesepakatan antar penjual dan pembeli terjadi saat pembeli menekan tombol setuju atau menyatakan konfirmasi kesepakatan melalui email. Saat transaksi di *marketplace*, kesepakatan terjadi ketika pembeli melakukan pembayaran atas barang yang sudah dipilihnya. Maka dari itu, adanya UU ITE di Indonesia diharapkan mampu melindungi hak dan kewajiban penjual dan pembeli dalam bertransaksi di dunia maya, sehingga walaupun tidak ada yurisdiksi wilayah hukum dalam transaksi elektronik, hak dan kewajiban

kedua pihak tidak ada yang dilanggar sehingga pada akhirnya tujuan Negara Indonesia untuk menjaga persatuan dan kesejahteraan masyarakatnya tidak terganggu dengan arus globalisasi yang terjadi di dunia saat ini. Selain itu, dalam perkembangan Teknologi Informasi dalam bidang *E-commerce* atau transaksi elektronik, penggunaan media sosial bagi masyarakat Indonesia juga memiliki tingkat popularitas yang tinggi.

Berdasarkan laporan *We Are Social*, jumlah pengguna aktif media sosial di Indonesia sebanyak 191 juta orang pada Januari 2022. Jumlah itu telah meningkat 12,35% dibandingkan pada tahun sebelumnya yang sebanyak 170 juta orang. Selain itu, Dilansir dari BBC pengguna media sosial di Indonesia, perhariannya menempati urutan tertinggi di Asia dengan rata-rata penggunaan media sosial 3-4 jam perhari. Media sosial sebuah alat atau media untuk berkomunikasi dan bersosialisasi satu sama lain dan dilakukan secara *online* yang terhubung dengan internet sehingga mempermudah manusia untuk saling berinteraksi dalam durasi yang cepat dan singkat tanpa dibatasi ruang dan waktu. Andreas Kaplan dan Michael Haeniein mendefinisikan media sosial sebagai sebuah kelompok aplikasi berbasis internet yang dibangun di atas dasar ideologi dan teknologi Web 2.0 dan memungkinkan penciptaan dan pertukaran *user-generated content* (Kaplan, Andreas M & Michael Haenlein, 2010).

Seiring dengan perkembangan zaman saat ini perkembangan media sosial meningkat sangat luar biasa cepat dan tidak bisa di cegah. Layanan dalam berkomunikasi maupun berinteraksi yang di fasilitasi oleh media sosial pun sangat beragam banyak dan mudah digunakan oleh hampir semua kalangan tanpa memiliki keahlian khusus. Adapun salah satu kebaikan inilah yang menyebabkan saat ini penggunaan media sosial dewasa ini sebagai sarana komunikasi baru telah merambah di seluruh dunia. Rata-rata masyarakat modern, seperti orang-orang yang tinggal di perkotaan bahkan sampai pelosok pedesaan telah menggunakan media *social* tanpa terkecuali. Kehadiran media sosial selain memiliki manfaat (*uses*) yaitu selain sebagai media komunikasi interaksi dan informasi, juga sebagai media hiburan. Hal ini, tentu akan menjadi motif alternatif yang dicari-cari oleh masyarakat setelah bosan pada tayangan hiburan di televisi. Selain itu media sosial dimanfaatkan kebanyakan dari mereka

sebagai motif hiburan dimana masyarakat menetapkan sebagai pelarian dari rutinitas atau masalah sehari-hari.

Dengan berkembangnya teknologi informasi yang terus berkembang, kehadiran media sosial menjadi sebuah kebutuhan yang sangat diperlukan, karena media *social* menjadi sarana komunikasi paling efektif yang dapat menjangkau langsung dan cepat kepada semua pihak, media sosial tidak hanya dimanfaatkan menjadi sarana berbagi informasi dan inspirasi akan tetapi juga menjadi sarana untuk mengekspresikan diri *(Self expression),* mengungkapkan keluh kesah atau ajang curhat dan pencitraan diri *(personal branding)*. Media sosial memiliki dampak besar pada kehidupan kita saat ini. Seseorang yang asalnya kecil bisa seketika menjadi besar dengan media sosial, begitu juga sebaliknya seseorang yang asalnya besar dalam waktu seketika menjadi kecil dengan media sosial. Dalam berbagai bidang kegiatan manusia seperti pemasaran, perdagangan, mencari kolega, memperluas pertemanan bahkan mengungkapkan pendapat atau mengkritik kebijakan pemerintah dapat dilakukan dengan memanfaatkan media sosial.

N. PENGERTIAN UU ITE

Ketika seseorang melakukan pelanggaran yang berada di lingkungan masyarakat maupun ke pemerintahan semua diatur dalam undang-undang *republic* Indonesia. Mengenai hal tersebut maka yang mengatur dengan informasi teknologi dan elektronik juga tercantum dalam UU ITE (Tanhella Zein Vitadiar, 2021). Pembuatan undang-undang tersebut dilakukan di tahun 2008 dan dibuat oleh hasil rapat anggota dewan. Keputusan yang disepakati ini setelah dilakukannya musyawarah mufakat yang membahas mengenai bidang terkait (Tanhella Zein Vitadiar, 2021). *Cyber* hadir dan diketahui oleh banyak orang dalam kehidupan sehari-hari. Bahkan saat ini hampir semua menggunakan situs jejaring sosial seperti facebook atau twitter untuk menambah relasi ataupun melakukan *update* info. Namun penggunaannya masih belum dilakukan secara optimal, sering ditemui kasus pelanggaran yang dilakukan pengguna dan berdampak pada menghilangkan nyawa seseorang. Oleh karena itu, terdapat peraturan yang membahas ancaman pelanggaran kesusilaan terdapat pada pasal 7 ayat 1, mengenai pencemaran nama baik terdapat

di pasal 27 ayat 3, serta ungkapan kebencian berdasarkan suku, agama, dan ras di pasal 28 ayat 2 dan semua itu tercantum pada UU ITE No 11 Tahun 2008. Melihat kejadian tersebut, tentu perlu dipahami bahwa dalam menggunakan aplikasi dunia maya harus bijak karena bisa terbilang kehidupan di dunia maya kejam dan mereka tidak berpikir matang dalam melakukannya dan hal ini bisa merugikan dirinya sendiri karena bisa terjerat atas pasal-pasal yang telah disebutkan diatas jika melanggarnya (Tanhella Zein Vitadiar, 2021).

Selain penjelasan terkait pelanggaran apa saja yang akan terjerat dalam undang-undang ITE, kasus yang lain adalah penyebaran video yang tidak pantas untuk dilihat seperti pornografi baik disebarkan melalui media tv atau alat komunikasi lainnya, pelaku juga akan terjerat dalam UU tersebut.

O. MAKNA DI BALIK DEFINISI INFORMASI ELEKTRONIK

Penjelasan mengenai informasi elektronik tercantum dalam Pasal 1 UU ITE dengan arti bahwa berbagai kumpulan data elektronik seperti tulisan, gambar, peta, suara, rancangan, foto, dan masih banyak lainnya yang dijelaskan dalam pasal tersebut. Berdasarkan definisi yang ada pada pasal terangkum menjadi tiga makna, bahwa: (Tanhella Zein Vitadiar, 2021).

1. Informasi Elektronik adalah sekumpulan data elektronik.
2. Informasi Elektronik yang berbentuk tulisan, suara, gambar.
3. Informasi Elektronik bisa dipahami karena ada makna di dalamnya.

Sifat yang dimiliki Informasi Elektronik dalam media penyimpanan adalah privasi atau tersembunyi. Oleh karenanya dalam pengenalan informasi ini dilihat dari wujud serta maknanya sehingga dapat dibuktikan keberadaannya. Memang menjadi sebuah persoalan rumit yang sering terjadi dalam ITE yaitu perselisihan mengenai kejahatan dan sistem keamanannya. Terdapat beberapa pasal yang telah membahas mengenai keamanan ITE, seperti di bawah ini:

1. Di dalam pasal 12 ayat 1 telah menjelaskan bahwa individu yang memiliki keterlibatan dengan memberikan tanda tangan elektronik maka perlu menyertakan keamanan dari tanda tangan yang telah digunakan.
2. Mengenai penyelenggaraan sistem elektronik yang handal dan memiliki keamanan atas tanggung jawab operasional sistem elektronik tercantum pada pasal 15 ayat 1.

Dilihat dari pasal yang disebutkan di atas, penggunaan tanda tangan elektronik memiliki sistem keamanan. Namun pada fakta yang terjadi atau situasi sebenarnya, masih banyak dijumpai dalam keberlangsungan transaksi elektronik masih kurang tingkat keamanannya. Maka dari itu, dalam pelanggaran yang menjelaskan mengenai merusak informasi atau dokumen elektronik telah diatur dalam pasal 30 sampai pasal 33 dan pasal 35, sehingga keputusan yang dapat dipertimbangkan hakim adalah: (Tanhella Zein Vitadiar, 2021).

1. Dampak dari pelaku kejahatan dapat merugikan banyak pihak.
2. Keamanan Sistem Elektronik yang diselenggarakan.

Hal yang dapat diberikan oleh hakim ketika menciptakan putusan pidana yaitu dengan memberikan denda atau hukuman jeruji bagi para pelaku pelanggar hukum yang disesuaikan dengan batasan perbuatannya pada sistem elektronik. Oleh karena itu, penciptaan undang-undang ini untuk memperingatkan para pelaku bisnis atau orang-orang yang melakukan transaksi elektronik untuk berhati-hati dan melakukan pengecekan terlebih dahulu sebelum melakukan suatu hal dan memperhatikan apa saja persyaratan minimum keamanan sistem elektronik yang termuat dalam Pasal 16 ayat 1 yang membahas mengenai kewajiban bagi penyelenggaraan sistem elektronik dalam mengoperasionalkan sistemnya agar memenuhi persyaratan berikut ini:

a. Prosedur yang dijelaskan dengan bahasa, informasi, atau simbol perlu memberikan pemahaman bagi para pihak yang melakukan penyelenggaraan sistem elektronik

b. Terdapat perlindungan ketersediaan, keotentikan, keutuhan, kerahasiaan dan terakses dalam *system* elektronik. Dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan.
c. Dapat beroperasi sesuai dengan petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut.
d. Mempunyai tata cara yang berkesinambungan dalam menjaga kebaruan, kejelasan, dan bertanggung jawab prosedur (Tanhella Zein Vitadiar, 2021).

P. RANGKUMAN MATERI

Pembahasan Etika dan Hukum membutuhkan pemahaman terlebih dahulu sehingga maknanya jelas. Secara fitrah manusia dikaruniai akal budi, perasaan dan kehendak. Akal adalah alat untuk berpikir sebagai sumber ilmu dan teknologi sehingga manusia memiliki kemampuan untuk menilai atau membedakan mana yang baik dan mana yang buruk. Etika menurut Kamus Besar Bahasa Indonesia "Ilmu tentang apa yang baik dan yang buruk, tentang hak dan kewajiban moral" Etika sebagai nilai-nilai dan norma-norma moral dalam suatu masyarakat, etika sebagai ilmu yang mempelajari tentang apa yang harus dilakukan atau yang tidak boleh dilakukan. "Etika merupakan kegiatan yang mempelajari norma moral seseorang atau norma moral suatu masyarakat, dan bagaimana menerapkan norma-norma tersebut pada kehidupan yang didasarkan pada alasan yang jelas dan benar". Etika sebagai konsep perilaku berdasarkan pada kodrat manusia yang diwujudkan melalui kehendak bebas manusia. Etik adalah prinsip-prinsip yang berhubungan dengan perbuatan salah atau benar. Etika adalah perbuatan yang berhubungan dengan etik.

Etika adalah pedoman yang digunakan untuk menjalankan suatu kepercayaan, standar atau pikiran dalam suatu individu, kelompok dan komunitas tertentu. Setiap perilaku individu akan dinilai oleh komunitasnya. Etika dalam suatu komunitas akan berbeda dengan komunitas yang lainnya. Dapat dilihat perbedaan ini dalam dunia komputer, misalnya dalam kasus pembajakan perangkat lunak

diperbanyak secara *illegal* kemudian digunakan atau dijual. Sementara itu, James H. Moor, seorang profesor di Darmouth mendefinisikan secara spesifik etika komputer/teknologi sebagai analisis mengenai sifat dan dampak *social* teknologi komputer, serta formulasi dan justifikasi kebijakan untuk menggunakan teknologi tersebut secara etis. Dalam organisasi, CIO (*Chief Information Office*) yang paling bertanggung jawab dalam sistem CBIS (*Computer Based Information System*) harus mempunyai dua aktivitas utama, yaitu:

a. Harus waspada dan sadar bagaimana teknologi *computer* mempengaruhi masyarakat.
b. Harus memformulasikan kebijakan-kebijakan yang memastikan bahwa teknologi tersebut digunakan secara tepat.

Etika dalam teknologi informasi terkait dengan moral dan hukum. Menurut Kant, "Moral adalah pengaturan perbuatan manusia sebagai manusia ditinjau dari segi baik buruknya dipandang dari hubungannya dengan tujuan akhir hidup manusia berdasarkan hukum kodrati. Kant mengatakan bahwa kehendak baik pada umumnya adalah kehendak rasional, akal budi praktis yang murni. Arti lain dari moral adalah tradisi kepercayaan mengenai perilaku benar atau salah. Sementara etika adalah suatu set kepercayaan, standar atau pemikiran yang terdapat dalam individu, kelompok dan masyarakat, dan hukum meliputi peraturan perilaku yang dipaksakan oleh otoritas berdaulat seperti pemerintah pada rakyat atau warga negaranya. Penggunaan komputer dalam bisnis diarahkan oleh nilai-nilai moral dan etika dari para manajer, spesialis informasi dan pemakai serta hukum yang berlaku. Hukum paling mudah diinterpretasikan karena berbentuk tertulis. Etika adalah acuan dari perilaku kita yang benar atau salah.

Menurut Harry Gunarto, Ph. D, dasar filosofi etika yang akan dituangkan dalam hukum teknologi informasi sering dinyatakan dalam empat macam nilai kemanusiaan universal yang meliputi hak *solitude* (hak untuk tidak diganggu), *anonymity* (hak untuk tidak dikenal), *intimicy* (hak untuk tidak dimonitor) dan *reserve* (hak untuk dapat mempertahankan informasi individu sehingga terjaga kerahasiaannya). Sedangkan menurut Hinca Panjaitan yang perlu diakomodasikan lagi adalah hak untuk

mengakses informasi atau pengetahuan dan hak untuk berkomunikasi. Etika teknologi informasi berbeda dari etika umum. Teknologi informasi menitikberatkan pada masyarakat yang memiliki pengetahuan mengenai teknologi informasi. Bidang itu menciptakan produk misalnya komputer yang dapat mempengaruhi masyarakat luas. Produk tersebut juga dapat memberikan keuntungan untuk masyarakat dan memiliki tanggung jawab pada masyarakat luas yang menggunakannya. Tanggung jawab itu meliputi keamanan dan keselamatan data, terpercaya, serta mudah untuk digunakan. Dengan berkembangnya teknologi informasi, maka berkembang pula istilah hukum teknologi informasi yang meliputi: "Peraturan perundang-undangan dan putusan-putusan pengadilan dengan berbagai penamaan seperti: *Computer Law*, *E-commerce Law*, *IT Law, On-line Law, Information and Computer Technology Law, the Law of the Internet, Law and the Information Superhighway, Information Technology Law, the Law of Information* dan sebagainya, dalam bahasa Indonesia hal inipun kemudian diadopsi dan diterjemahkan dengan istilah berbeda-beda, seperti hukum Telematika (Telekomunikasi, Media dan Informatika).

Hukum merupakan aturan formal tentang perilaku, wewenang, atau kekuasaan pemerintahan yang menentukan subjek atau kewarganegaraan. Beberapa negara telah berhasil secara konkrit membuat peraturan untuk mengatasi tindakan yang dianggap melanggar etika ke dalam bentuk undang-undang atau hokum teknologi informasi, misalnya sebagai berikut:

a. Kanada dengan jenis undang-undang *telecommunication act, broadcasting act, radiocommunication act,* dan *criminal code.*
b. Amerika serikat dengan undang-undang *freedom of information act, privacy protection act, computer security act, alectronic communication privacy act, computer fraud and abuse act, wire fraud act,* dan *tellecommucation act.*
c. Indonesia menggagas kerangka etika dan hukum teknologi informasi yang dilakukan oleh para pakar hukum Indonesia, yang dibahas melalui *mailing list,* antara lain telematika@egroup.com,mastele-commerce@egroup.com,doit@tropika.com, dan warta-ecommerce@egroup.com.

Menurut Mcleod, dalam merencanakan operasi teknologi informasi yang beretika harus memenuhi 10 tahap standar etika, yaitu:

1. Merumuskan paham etika.
2. Membentuk prosedur melalui peraturan-peraturan yang ada.
3. Menetapkan sangsi.
4. Mengakui adanya perilaku etis.
5. Memfokuskan pada program pelatihan komputer.
6. Promosikan UU kejahatan *computer* dengan memberikan informasi kepada karyawan.
7. Melaksanakan tanggung jawab yang dibebankan.
8. Mendorong program rehabilitasi etika.
9. Mendorong partisipasi masyarakat profesional untuk membuat kode etik.
10. Menetapkan budaya keteladanan.

TUGAS DAN EVALUASI

Jawablah soal berikut ini, dengan jelas:

1. Jelaskan pengertian dari Etika Hukum *Cyber*, menurut para ahli hukum minimal 6 ahli?
2. Jelaskan ciri-ciri dari Etika Hukum *Cyber*, sebutkan serta disertai penjelasan secukupnya?
3. Kebijakan hukum dalam upaya penanggulangan Kode Etik Profesi IT secara internasional berprinsip pada, berikan penjelasan secara deskriptif?
4. Salah satu dari ruang lingkup *Cyber Law* adalah Pencemaran nama baik, dapat juga dikenal dengan istilah apa, berikan penjelasan yang secukupnya disertai pasal KUHP?
5. Etika dalam berkomunikasi menggunakan internet dikenal dengan istilah apa, berikan penjelasan secara deskriptif dan berikan contohnya?

DAFTAR PUSTAKA

Ahmad M Ramli. (2004). *Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime,* Fakultas Hukum Universitas Padjajaran, 2004, hlm. 2.

Andi hamzah. (1990). *Aspek-aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta, hal. 23-24.

Barda Nawawi Arief. (2006). *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta: Rajawali Pers, hal 25.

Bayu, D. (2022) *APJII: Pengguna Internet Indonesia Tembus 210 Juta pada 2022*. Tersedia pada: https://dataindonesia.id/digital/detail/apjii-pengguna-internet-indonesia-tembus-210-juta-pada-2022 (Diakses: 5 September 2022).

Budi Raharjo, 6 Agustus 2003" Pernak-Pernik Peraturan dan Pengaturan *Cyberspace* di Indonesia", dalam *http//www.budi.insan.co.id*, hal 2, diunduh tanggal 24 Juni 2011, pukul 12.00.

Enni Soerjati Priowirjanto. 2022. SOSIALISASI MENGENAI PEMAHAMAN TENTANG ETIKA DALAM KEGIATAN PEMBELAJARAN ONLINE. Jurnal Kajian Budaya dan Humaniora – ISSN 2656-7156 Vol. 4, No. 3, Oktober 2022: 310-318

Fardiyan, A.R. (2016) "Etika Siber Dan Signifikansi Moral Dunia Maya Cyber Ethics and Moral Signification in Cyberspace," *Prosiding Seminar Nasional Komunikasi*, hal. 332–337. Tersedia pada: http://repository.lppm.unila.ac.id/2980/.

Firmansyah, Y. 2016. Modul Etika Profesi Teknologi Informasi & Komunikasi. Fakultas Teknologi Informasi Universitas Bina Sarana Informatika: Pontianak.

Firmansyah. (2017). PROBLEMATIKA TINDAK PIDANA ITE DALAM PERSFEKTIF SISTEM HUKUM. Fakultas Hukum Universitas Muhammadiyah Parepare, Jalan Jenderal Ahmad Yani KM 6 Kota Parepare Kode Pos 91113, Telpon: 0421-22757/Fax 0421-2554 Sulawesi Selatan Indonesia Email: firmansyah.abdurrahman85@gmail.com.

Gramedia (2021) *Pengertian Etika: Macam-Macam Etika & Manfaat Etika*. Tersedia pada: https://www.gramedia.com/best-seller/pengertian-etika/#Apa_itu_etika_dan_fungsinya.

Handayani, P. (2016). Penegakan Hukum Terhadap Kejahatan Teknologi Informasi (Cyber Crime). Jurnal Dimensi, 1–8.

Irwanto. (2023). Makalah Hukum Ciber. Di Presentasikan Didepan Kelas Pada Fakultas Hukum, Universitas Bina Bangsa. Kota Serang. Banten.

Jayani, D.H. (2021) *Penggunaan Internet di Kalangan Siswa Sekolah Semakin Meningkat*. Tersedia pada: https://databoks.katadata.co.id/datapublish/2021/05/03/tren-siswa-sekolah-menggunakan-internet-semakin-meningkat.

Kaplan, Andreas M.; Michael Haenlein, 2010, *"Users of the world, unite! The challenges and opportunities of Social Media"*. Business Horizons.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. Times, 5(2), 35–42. http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126.

l.Tanya, Berbard. (2011). *Penegakan Hukum Dalam terang Etika*. Yogyakarta: Genta Publishing.

Magnis Suseno, Frans. (2017). *Etika dasar, masalah-masalah Pokok Filsafat Moral*. Yogyakarta: PT Kanisius.

Miswardi, Nasfi dan Antoni (2021) "Etika, Moralitas dan Penegak Hukum," *Menara Ilmu*, 15(2), hal. 150–162.

Nasrullah, R. (2015) *Media Sosial*. Bandung: Simbiosa Rektama Media.

Natalie D Voss, Copyright 1994-1999 Jones International and Jones Digital Century, "*Crime on The Internet", Jones Telecomunications & Multimedia Encyclopedia*. *http://www.digitalcentury.com/encyclo/update/articles.html.*

Pasal 5 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), Kementrian Komunikasi dan Informasi RI.

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. Jurnal Pertahanan & Bela Negara, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193.

www.penerbitwidina.com

Roy Suryo, Kejahatan *Cyber di Indonesia*, Kompas, Nomor 3, (19 November 2001), hal V.

S. Praja, H. Juhaya. (2001). *Teori hukum dan aplikasinya*. Bandung: Pustaka setia.

Sari, N. W. (2018). Kejahatan Cyber dalam Perkembangan Teknologi Informasi Berbasis Komputer. Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan, 5(2), 577–593. http://openjournal.unpam.ac.id/index.php/SKD/article/download/2340/1887.

Sudarwanto, A. S. (2009). Cyber-Bullying Kejahatan Dunia Maya Yang "Terlupakan." In Jurnal Hukum PRO JUSTITIA (Vol. 27, Issue 1, pp. 1–16).

Sudaryono & Natangsa Surbakti. (2005). *Hukum Pidana,* Surakarta: Fakultas Hukum UMS, hal 58 dan 63.

Suhendar, A. (2013). Keterkaitan antar bidang pembinaan ketahanan nasional/ pembinaan gatra (+). Keterkaitan Antar Bidang Pembinaan Ketahanan Nasional/Pembinaan Gatra.

Tanhella Zein Vitadiar, Ginanjar Setyo Permadi, Rocky Ardiansyah Yudistira Putra, & Unzilla Savika Putri. 2021. ETIKA & HUKUM CYBER. CV. AE MEDIA GRAFIKA. Jl. Raya Solo Maospati, Magetan, Jawa Timur 63392. Telp. 082336759777. email: emediagrafika@gmail.com website: www.aemediagrafika.com.

Vanue (2021) *Manfaat Utama Menggunakan Media Sosial dalam Pendidikan*. Tersedia pada: https://venuemagz.com/literasi-digital/manfaat-utama-menggunakan-media-sosial-dalam-pendidikan/.

Waryanto, N.H. (2006) "Etika Berkomunikasi di Dunia Maya dengan Netiquette," *Seminar Nasional Matematika dan Pendidikan Matematika*, 22(1), hal. 342–362.

Yahfizham. 2012. MORAL, ETIKA DAN HUKUM (IMPLIKASI ETIS DARI TEKNOLOGI INFORMASI DAN KOMUNIKASI). Jurnal Iqra' Volume 06 No.01 Mei, 2012.

HUKUM *CYBER*

BAB 12: *CYBERBULLYING*

Stefanus Don Rade, S.H., M.H

Fakultas Hukum, Universitas Katolik Widya Mandira Kupang

BAB 12

CYBERBULLYING

A. PENDAHULUAN

Pada bab *cyberbullying* mempelajari terkait apa itu *cyberbulying*, dampak yang dialami dari *cyberbullying*, bentuk-bentuk dari *cyberbullying, body shaming* yang merupakan bagian dari *cyberbullying*, karakteristik *cyberbullies* pada *body shaming*, dan pengaturan hukum *cyberbullying* di Indonesia. Berdasarkan data terakhir Komisi Perlindungan Anak Indonesia (KPAI) tahun 2022 sebanyak 226 kasus *bullying* dengan kekerasan fisik dan mental yang terjadi di lingkungan sekolah termasuk 18 kasus *bullying* didunia maya, yang sesungguhnya jumlah kasus *bullying* lebih banyak dari pada kasus yang dirilis oleh KPAI, karena banyak kasus yang terjadi, tapi tidak dilaporkan ke KPAI atau tidak mencuat ke media. Situasi yang sesungguhnya menggambarkan lembaga pendidikan formal sejak lama tidak kondusif bagi berlangsungnya pendidikan dan pengajaran. Oleh karena itu, agar sekolah-sekolah dan lembaga-lembaga terkait lebih bertanggung jawab memperbaiki iklim proses belajar mengajar di sekolah dan perguruan tinggi.

B. PENGERTIAN *CYBERBULLYING*

Bullying adalah kejadian yang dialami dan dirasai oleh seseorang yang merasa teraniaya oleh tindakan orang lain/kelompok tertentu baik secara langsung melalui perbuatan fisik maupun verbal dan secara tidak langsung melalui sosial media yang menyakiti baik secara fisik maupun *non*fisik dari korban. *Bullying* adalah perilaku menyakiti orang lain dengan cara menyakiti mental dan juga fisik, menggertak yang dilakukan oleh individu

atau kelompok secara berulang dengan hubungan kekuasaan yang tidak setara antara *bully* dan *victim* (Roland & Vaaland, 2006). Selain itu Roland & Vaaland (2006) juga menjelaskan bahwa *bullying* merupakan pelecehan mental atau fisik *victim,* yang dilakukan oleh seseorang, diasumsikan sebagai hubungan kekuasaan yang tidak setara antara *bully* dengan *victim,* dan episode kejadiannya terus berulang dari waktu ke waktu. Rigby (2007) mengidentifikasi unsur-unsur perilaku sehingga dapat disebut *bullying.* Unsur *bullying* seperti keinginan untuk menyakiti, tindakan agresif, kekuatan yang tidak seimbang antara orang-orang yang terlibat dalam *bullying* yang melibatkan tindakan berulang dalam kurun waktu tertentu, bukan sekedar penggunaan kekuatan, tetapi rasa senang yang dirasakan oleh *bully* dan rasa tertekan di pihak *victim.*

Menurut Priyatna (Dyastuti, 2012) *bullying* adalah:

1. Perilaku menyakiti secara fisik, verbal dan psikologis yang disengaja oleh si *bully* pada *victim*nya, bukan sebuah kelalaian. Memang perbuatan yang betul-betul disengaja.
2. Perilaku menyakiti secara fisik, verbal dan psikologis itu terjadi berulang-ulang *bullying* tidak pernah dilakukan secara acak atau cuma sekali.
3. Didasari perbedaan *power* yang mencolok antara *bully* dan *victim.* Jadi perkelahian diantara anak yang kurang seimbang dari segi ukuran fisik maupun usia bukan merupakan kasus *bullying.* Dalam *bullying bully* benar-benar berbeda diatas angin *victim*nya.

Berdasarkan penelitian yang dilakukan Olweus dan Roland (James, 2010) hasil penelitian menunjukkan sebuah kesimpulan agar bisa disebut sebagai *bullying*, yaitu perilaku menyakiti dengan cara fisik, verbal dan psikologis atau bentuk kekerasan lain harus terjadi sedikitnya sekali dalam seminggu atau lebih selama periode waktu satu bulan. Berdasarkan hasil kesepakatan dari beberapa peneliti bahwa pengertian *bullying* adalah tindakan yang mengakibatkan kekerasan atau agresi secara langsung dan agresi secara tidak langsung. Tindakan kasar atau kekerasan bisa dikatakan *bullying* jika individu sebagai *victim* merasa tidak menyukai tindakan yang dilakukan oleh orang lain atau kelompok dan telah melukai perasaan *victim.* Menurut Tattum dan Tattum (Widayanti & Siswati, 2009) *bullying*

adalah "*the willful, conscious desire to hurt another and put him/her under stress".* Berdasarkan pendapat tersebut dapat dimengerti bahwa *bullying* adalah hasrat untuk menyakiti individu lain yang dilakukan secara sadar dan membuat individu tersebut merasa tertekan. *Bully* merasa bahagia jika *victim* merasa takut dan tertekan sehingga *bullying* akan dilanjutkan.

Label *' cyberbullying '* adalah masalah yang terkait dengan istilah yang digunakan untuk label fenomena *cyberbullying* di berbagai bahasa yang diturunkan dari literatur *bullying.* Englander (2012) menyatakan bahwa teknologi informasi selain dapat membawa dampak positif tetapi juga dapat membawa dampak negatif bagi para penggunanya, salah satu dampak negatif yang ditimbulkan akibat dari penggunaan teknologi informasi yang timbul di media sosial adalah muncul fenomena *cyberbullying. Cyberbullying* muncul sebagai akibat dari kehidupan sosial *online* yang dimana remaja modern dan anak-anak terlibat. Menurut Bill Belsey (Beane, 2008), presiden *Bullying*.org (Kanada), "*cyberbullying* melibatkan penggunaan informasi dan komunikasi teknologi seperti *e-mail*, ponsel dan pager pesan teks, pesan instan, situs web pribadi pemungutan suara *online* untuk mendukung disengaja, diulang dan perilaku bermusuhan oleh seorang individu atau kelompok, yang dimaksudkan untuk menyakiti orang lain. *Cyberbullying* (perundungan dunia maya) adalah kejadian yang dialami dan dirasai oleh seseorang yang merasa teraniaya oleh tindakan orang lain/kelompok tertentu melalui media elektronik baik cetak maupun *online* dengan melibatkan penggunaan informasi dan komunikasi teknologi. *Cyberbullying* menjadi makin populer karena hanya dengan beberapa ketikan di *keyboard gadget* atau komputer mengandung informasi yang merusak dapat berupa hinaan dikirim ke atau di*posting* dilaman tertentu dan dilihat oleh ribuan orang.

C. DAMPAK DARI *CYBERBULLYING*

Cyberbullying terjadi secara *online*, artinya dapat terjadi seperti diserang dari mana saja, bahkan di dalam rumah sendiri. Seperti tidak ada jalan untuk keluar. Dampak dari *cyberbullying* dapat bertahan lama dan memengaruhi seseorang dalam banyak cara yaitu secara mental seperti merasa kesal, malu, bodoh, marah, bahkan sampai level depresi; secara emosional seperti merasa malu atau kehilangan minat pada hal-hal yang

kamu sukai; dan secara fisik seperti lelah (kurang tidur) atau mengalami gejala seperti sakit perut dan sakit kepala. Kekerasan yang dialami oleh seseorang yang dilakukan oleh *cyberbullies* melalui media *cyber* atau internet, sering kali merasa depresi, merasa terisolasi, diperlakukan tidak manusiawi, dan tidak berdaya ketika diserang. Menurut Psikolog anak Vera Itabiliana Hadiwidjojo (Kompas 2015:11) (Maya, 2015) tindakan *cyberbullying* sering dialami oleh anak yang secara mental terlihat berbeda. Mereka akan cenderung terlihat pendiam, pemalu,, dan akan tertutup. Menurut Suminar (2014) *cybervictim* merasa tidak senang pergi ke sekolah, meskipun mereka senang belajar di sekolah namun mereka merasa tidak aman dan merasa terisolasi. Perasaan ditertawakan atau dilecehkan oleh orang lain dapat membuat seseorang tidak ingin membicarakan atau mengatasi masalah tersebut. Dalam kasus ekstrim, *cyberbullying* bahkan dapat menyebabkan seseorang mengakhiri nyawanya sendiri.

Dampak yang dirasakan dari *cyberbullying* (Smith *et al,* 2006) sebagai berikut:

1. Klip gambar/video dan panggilan telepon dianggap lebih berdampak dari pada *cybervictim* dari bentuk-bentuk *bullying* tradisional.
2. Situs web dan pesan teks dinilai memiliki dampak yang setara *bullying* tradisional.
3. Ruang obrolan, pesan instan dan *e-mail bullying* diyakini kurang berdampak dari bentuk-bentuk *bullying* tradisional.

Karena beberapa jenis *cyberbullying* jelas lebih berbahaya dari pada yang lain, *cyberbullying* dapat berdampak kontinum untuk *cybervictim*. Selanjutnya pertimbangan harus diberikan kepada keseriusan masalah dalam konteks dan diantaranya keadaan yang mengelilinginya. Bahwa *e-mail* atau pesan teks yang melecehkan mungkin bukan masalah yang signifikan. Cash & Bridge (Bauman *et al,* 2013) karena depresi merupakan faktor risiko yang diketahui untuk perilaku bunuh diri, penting untuk mempertimbangkan bagaimana hal itu mungkin terlibat dalam asosiasi antara pengalaman *bullying* dan perilaku bunuh diri. Penelitian sebelumnya telah ditemukan hubungan antara keterlibatan dalam *bullying* dan perilaku bunuh diri, tetapi peran depresi sebagian besar tidak ada diskusi lebih lanjut. Memahami proses dimana variabel-variabel ini terkait

akan menginformasikan upaya pencegahan dan intervensi; perilaku bunuh diri mungkin dicegah dengan menargetkan konstruksi psikologis, misalnya depresi. *Cyberbullying* dapat mempengaruhi seseorang dengan berbagai cara, tetapi tentunya masalah ini dapat diatasi dan orang-orang yang berdampak juga dapat memperoleh kembali kepercayaan diri dan kesehatan mental mereka (Karyanti *et al,* 2019).

Van Orden *et al* (Bauman *et al,* 2013) Studi saat ini dipandu oleh teori interpersonal, bunuh diri yang berpendapat bahwa keinginan untuk bunuh diri disebabkan oleh kehadiran kedua "keburukan yang digagalkan" dan "beban yang dirasakan". Kami mempertimbangkan perilaku *bullying* menjadi manifestasi keburukan yang digagalkan baik pada *cyberbullies* maupun sasaran *cyberbullies. Cyberbullies* yang perilakunya dimotivasi oleh upaya untuk mendapatkan atau mempertahankan status sosial (Sijtsema, Veenstra, Lindenberg & Salmivalli, 2019: Bauman *et al,* 2013), mencari milik dalam kelompok sebaya. *Cybervictim* adalah penerima tindakan berulang.

Ada dampak yang ditimbulkan dari *cyberbullying* diantaranya adalah dampak bagi korban,pelaku, dan yang menyaksikan (*bystander).* Dampak bagi korban diantaranya dampak psikologis berupa mudah depresi, marah, perasaan gelisah, cemas, menyakiti diri sendiri dan percobaan bunuh diri; dampak sosialnya berupa menarik diri dari dalam pergaulan, kehilangan percaya diri, lebih agresif kepada teman dan keluarga dan dampak pada kehidupan sekolah adalah penurunan prestasi akademik, rendahnya tingkat kehadiran, dan perilaku bermasalah di sekolah; dampak bagi pelaku yaitu cenderung bersifat agresif, berwatak keras, mudah marah, impulsif, lebih ingin mendominasi orang lain, kurang berempati, dan dapat dijauhi oleh orang lain dan terakhir adalah dampak bagi yang menyaksikan (*bysender)* adalah jika *cyberbullying* dibiarkan tanpa tindak lanjut, maka orang yang menyaksikan dapat berasumsi bahwa *cyberbullying* adalah perilaku yang diterima secara sosial. Dalam kondisi ini, beberapa orang mungkin akan bergabung dengan penindas karena mereka takut akan dijadikan sasaran selanjutnya dan beberapa lainnya mungkin hanya akan diam saja tanpa melakukan apapun dan yang paling parah mereka merasa tidak perlu menghentikannya.

D. BENTUK-BENTUK *CYBERBULLYING*

Bentuk-bentuk kekerasan *cyberbullying* bukan hanya kekerasan yang bisa membuat orang terluka secara fisik, kekerasan *cyberbullying* lebih kepada kekerasan yang menuju kepada psikis atau mental seseorang.

Menurut Ayuningtyas, dkk (2013) "pembajakan akun pribadi seseorang, penyebaran berita bohong atau fitnah juga termasuk perilaku *cyberbullying,* berdasarkan pengertian diatas penyebaran berita bohong tersebut juga termasuk dalam pencemaran nama baik". Menurut Utami (2013:4) bentuk-bentuk *cyberbullying* yang banyak terjadi seperti mengganti foto *account* seseorang, menghina seseorang, dan membajak *account* seseorang dengan mengganti *password.* Kekerasan *cyberbullying* bukan saja menyasar pada laki-laki atau perempuan tetapi anak-anak yang merupakan kelompok rentan juga termasuk salah satu korban didalamnya. Berdasarkan data pada Komnas Perempuan bahwa angka kekerasan terhadap perempuan di ranah siber 6,3 kali lebih banyak dibandingkan dengan tempat tinggal mereka. Pada tahun 2022, Komnas Perempuan mencatat 869 pengaduan kasus kekerasan berbasis gender (KBG) terhadap perempuan, sementara KBG yang terjadi ditempat tinggal berjumlah 136.

Melansir *Women's Media Center* dan Childnet, ada 6 tindakan yang disebut sebagai kekerasan seksual secara *online* yaitu:

1. *Revenge Porn* merupakan kejahatan digital dimana pelaku menyebarkan konten telanjang atau *sexually explicit* seseorang tanpa persetujuan orang yang ada di dalam foto atau video tersebut.
2. Komentar bernuansa seksual dan hinaan berbasis gender yaitu dengan mengeluarkan kata-kata yang bernuansa *sexually* dan hinaan yang erat kaitannya dengan persepsi masyarakat yang mengacu pada peran, perilaku, ekspresi, dan identitas seseorang, baik laki-laki maupun perempuan yang dibentuk secara sosial maupun budaya.
3. *Grooming* (merayu) yaitu tindakan yang berusaha untuk memanipulasi orang lain agar merasa tidak berdaya dengan cara membangun kepercayaan.
4. Objektifikasi Seksual yaitu tindakan yang memperlakukan seseorang sebagai alat pemuas hasrat seksual. Tindakan tersebut menganggap bahwa seseorang itu sebagai komoditas atau benda pemuas seksual tanpa memperhatikan kepribadian dan harga dirinya.

5. Menguntit yaitu tindakan mengancam atau meneror orang lain berkali-kali dalam bentuk teks, gambar, atau video yang tidak dinginkan dan membuat tidak nyaman seseorang.
6. Pornografi tanpa persetujuan

Korban *revenge porn* dilindungi oleh Undang-Undang Nomor 12 tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS). Dalam Pasal 14 UU TPKS mengatur terkait tentang kekerasan seksual berbasis elektronik. Dalam UU tersebut, setiap pelaku kekerasan seksual berbasis elektronik dapat dipidana penjara paling lama empat tahun dan/atau denda paling banyak Rp.200 juta rupiah, namun masih terdapat beberapa tindak Kekerasan Berbasis Gender Online (KBGO) belum secara spesifik dikenal dan diatur dalam ketentuan hukum di Indonesia.

Beane (2008) dalam penelitiannya, dalam penelitiannya, *cyberbullying* paling sering melibatkan panggilan telepon, teks, dan pesan instan. Sifat *bullying* elektronik atau *bullying* maya seringkali meliputi:

1. Mengirim pesan yang kasar, fulgar, atau mengancam atau gambar *online* atau melalui teks
2. Mem*posting* informasi sensitif, pribadi atau gambar tentang orang lain
3. Sengaja mengucilkan seseorang dari grup *online*
4. Berpura-pura menjadi orang lain untuk membuat *cybervictim* terlihat buruk
5. Menyebarkan kebohongan dan rumor tentang *cybervictim*
6. Menipu seseorang agar mengungkapkan informasi pribadi
7. Sifat bermain *game* sebagai tempat di mana *cyberbullying* terjadi, dapat terjadi melalui *game situs web* atau PC dan *game konsol* dengan komponen *online* (misalnya Nintendo Wii, Xbo 360, dan *Playstation* 5).
8. *Cyberbullying* dalam permainan biasanya disebut sebagai "kesedihan" dan cukup umum diantara *gamer* muda yang menggunakan IM, obrolan, dan fitur obrolan suara untuk menggoda dan mengejek pada saat *game.*

Berbagai jenis *cyberbullying* telah terjadi sampai ke *cyberstalking.* Willard (Beran & Li, 2008) ada tujuh kategori yang berbeda dari *cyberbullying* umum:

1. *Flaming:* Mengirim pesan yang kasar, vulgar tentang seseorang ke grup *online* atau ke *cybervictim* melalui *e-mail* atau pesan teks lainnya.
2. *Online Harassement:* Berulang kali mengirim pesan ofensif melalui *e-mail* atau teks lainnya mengirim pesan kepada seseorang.
3. *Cyberstalking:* Pelecehan *online* yang mencakup ancaman bahaya atau membuli dengan memberikan komentar menyakitkan.
4. *Denigration (put-downs):* mengirim pernyataan berbahaya, tidak benar, atau kejam tentang seseorang atau mem*posting* materi *online* semacam itu.
5. *Masquerade*: Berpura-pura menjadi orang lain dan mengirim atau mem*posting* materi yang membuatnya *cybervictim* terlihat buruk.
6. *Outing:* Mengirim atau mem*posting* materi tentang seseorang yang berisi halinormasi sensitif, pribadi, atau informasi yang memalukan, termasuk meneruskan pesan atau gambar pribadi.
7. *Exclusion:* Secara kejam mengucilkan, mengabaikan dan menghapus seseorang dari *group online*.

Marden (2010) membagi jenis *cyberbullying* menjadi *cyberbullying* langsung dan *cyberbullying* tidak langsung. Berikut adalah masing-masing *cyberbullying:*

1. *Cyberbullying* secara langsung
   a. *Denigration* adalah bentuk *cyberbullying* langsung, menurut Willard, adalah ketika seseorang siswa membuat situs web yang digunakan untuk mengejek atau merusak reputasi *cybervictim.*
   b. *Harassment and Stalking,* bentuk lain dari *cyberbullying* langsung termasuk berulang kali mengirim pesan yang kejam, ganas, dan/atau mengancam.
   c. *Exclusion* yaitu dengan mengucilkan seseorang dari *group online*, ini dapat dilakukan dengan "memblokir" individu atau "tidak berteman" atau menghapus teman yang pernah ditambahkan di *Facebook.*
2. *Cyberbullying* secara tidak langsung
   a. *Flaming* adalah bentuk tidak langsung dari *cyberbullying* dan didefinisikan oleh Nancy Willard (yang merupakan otoritas yang diakui pada isu-isu terkait dengan penggunaan internet aman dan

bertanggung jawab) sebagai argumen antara dua orang yang termasuk bahasa kasar, vulgar, penghinaan, dan ancaman.

b. *Impersonation* seperti membobol *e-mail* orang lain dan menggunakannya untuk mengirim pesan ganas atau memalukan bagi orang lain.
c. *Outing and Trickery,* yaitu dengan cara melibatkan seseorang dalam pesan instan dan menipu mereka agar mengungkapkan informasi pribadi atau informasi sensitif dan meneruskan atau mendistribusikannya kepada orang lain (Willard, 2007).

Willard (Konig *et al.,* 2010) *cyberbullying* melalui perilaku khusus: pembakaran, pelecehan, pencemaran nama baik, peniruan identitas, *outing*, tipu muslihat, pengucilan dan *cyberstalking*. Mencoba meringkas delapan kategori ini dalam tipologi perilaku, empat tipe utama dapat diidentifikasi: perilaku verbal tertulis (panggilan telepon, pesan teks, e-mail, instan pesan, obrolan, blog, komunitas jejaring sosial, situs web), perilaku visual (*posting*, mengirim atau berbagi foto dan video yang dikompromikan melalui ponsel atau internet), pengucilan (dengan sengaja mengucilkan seseorang dari grup *online*) dan peniruan identitas (mencuri dan mengungkapkan informasi pribadi, menggunakan nama dan akun orang lain).

E. *BODY SHAMING* BAGIAN *CYBERBULLYING*

Rezvan *et al* (2018) Dalam *body shaming*; kritik publik dan penilaian individu karena kelebihan atau kekurangan berat badan. Pelecehan yang berhubungan dengan penampilan menggunakan bahasa yang memalukan yang mengacu pada penampilan tubuh. McKinley & Hyde (Daye, *et al*, 2014). *Fat shaming* dan *body shaming* adalah subtipe kunci dari jenis pelecehan ini mendefinisikan *body shaming* sebagai kecenderungan untuk mengalami rasa malu ketika seseorang tidak hidup sesuai dengan yang diinternalisasi, yang secara kultural melanggar norma ukuran atau berat badan; melakukan pengawasan untuk terus memantau tubuh seseorang dan khawatir bagaimana tubuh seseorang muncul di mata orang lain. Keyakinan untuk kontrol penampilan menunjukkan sikap yang dicirikan oleh persepsi berhasil mengelola berat badan dan aspek penampilan.

Menurut Kenny (2017) *Body shaming* dan *body image* yang salah: peserta mengatakan bahwa masalahnya bukan hanya mempermalukan di media sosial. Lebih luas masalah: "*body shaming*", atau tekanan masyarakat yang memaksa Anda untuk mengadopsi *body image* tertentu seperti yang diinginkan. Meskipun sebagian besar remaja menyatakan bahwa perubahan masyarakat, seperti media tidak dapat diatasi, beberapa berpendapat bahwa media perlu menghentikan perusakan tubuh yang lain, perlu berhenti menggambarkan gambar "orang yang sempurna" dan perlu mengurangi berita selebriti yang memulai "diet". Mengubah ukuran manikin di toko-toko, dari ukuran 6 ke ukuran tubuh yang lebih realistis, serta perawakannya yang tinggi juga dibesarkan sebagai cara meningkatkan citra tubuh remaja. Selain itu untuk meningkatkan persepsi citra tubuh yang ideal perlu diadakan perkumpulan olahraga gratis untuk remaja.

Fredrickson & Roberts (Elíasdóttir, 2016) *body shaming* adalah konsep yang digunakan untuk individu yang sadar diri, respons negatif emosional terhadap diri sendiri. Itu muncul dalam salah langkah individu untuk mencapai standar cita-cita tubuh ideal. Crossle, *et al* (Stacey, 2017) Menurut pendapat saya, standar kecantikan fisik masyarakat kita berasal dari media *online* yang menyatakan bahwa menjadi "kurus" adalah cara ideal untuk melihat. Kebanyakan wanita yang digambarkan cantik di media *online* adalah wanita yang memiliki perut rata, payudara besar, dan pantat bulat, sedangkan pria yang digambarkan tampan berotot, tinggi, dan ramping.

Guimond (Roodt, 2015) telah melakukan penelitian, dan temuan penelitian menunjukkan bahwa ada korelasi yang signifikan antara pemberdayaan wanita dalam hal keterkaitan dengan cita-cita feminis dan misogini perempuan sebagai salah satu dari sumber utama *body shaming*, dengan feminis perempuan dengan hanya 4,94%. Lebih lanjut, penelitian ini mengungkapkan bahwa penampilan keseluruhan topik yang paling sering didiskusikan di seluruh artikel, disebutkan dalam total 93,83% artikel, dengan wajah dan rambut wanita paling sering didiskusikan dalam artikel 23,46%. Penampilan keseluruhan adalah juga topik yang paling umum dipermalukan di artikel, diikuti oleh *fashion*, bentuk tubuh dan kebugaran. Media, khususnya tabloid *jurnalisme online*, berfungsi sebagai

tempat berkembang biak untuk perbandingan sosial diri seseorang yang seharusnya berada di bawah pencapaiannya sendiri dalam hal gaya hidup, termasuk citra tubuh dan penampilan.

Body shaming melalui media sosial merupakan tindakan *cyberbullying*. Sehubungan dengan pedoman asli oleh Van Hee *et al.* (2015), kami menambahkan penghinaan jenis baru disebut *Body Shame* untuk menutupi ekspresi, mengkritik seseorang berdasarkan bentuk, ukuran, atau penampilan tubuhnya. Frisen *et al.* (Berne *et al.,* 2014) Kami melakukan penambahan *body shaming* telah menjadi hal yang penting untuk masalah kemasyarakatan yang sesuai dengan literatur yang memiliki dampak yang kuat pada *victimization* remaja dan *cyberbullies*.

Feragen & Stock (2016) Temuan ini menyangkut longitudinal sebelumnya penelitian telah mengungkapkan bahwa pengalaman menggoda lebih pada penampilan. Lunde & Frisén (Kenny, 2017) ketidakpuasan dan tekanan emosional di kalangan remaja enam tahun kemudian, dan bahwa *cybervictim* pada remaja awal adalah prediksi *self surveillance* dan *body shaming* pada akhir masa remaja. Stacey (2017) Beberapa tahun terakhir, sebagai akibat dari komunikasi "tak berwajah" Internet dan standar kecantikan fisik masyarakat yang tidak realistis, Internet memungkinkan pengguna untuk menyebabkan kerusakan emosional pada seseorang melalui *cyberbullying*.

Healthy Living Cooperative (Stacey, 2017) *Cyberbullies* menggunakan *body shaming*, sering dalam bentuk *gaslighting*, untuk menargetkan pria dan wanita yang tidak sesuai dengan standar kecantikan masyarakat. *Body shaming* didefinisikan sebagai, “pernyataan dan sikap negatif yang tidak pantas pada berat atau ukuran tubuh orang lain ”yang sering menyebabkan peningkatan ketidakamanan tubuh. Andrew (2012) bahkan berpendapat bahwa masalah *body shaming*; membuat sebagian besar wanita dirampas dari jenis dan citra tubuh mereka berdasarkan pada bagaimana media sosial menggambarkan tubuh ideal dan wanita sempurna. Penting untuk dicatat, bagaimanapun, bahwa sering media sosial juga dapat memfasilitasi *rasisme, misogyny*, *body shaming*, dan bentuk-bentuk lain menyerang, memalukan, menghina, menstigmatisasi, menyalahkan atau sebaliknya berkontribusi pada mengucilkan individu,

kelompok sosial atau organisasi, atau promosi reaksioner posisi politik (Phillips dan Milner 2017; Highfield 2016; Lupton, 2017).

F. KARAKTERISTIK *CYBERBULLIES* PADA *BODY SHAMING*

Cyberbullies sering menggunakan mekanisme pelecehan emosional yang disebut "Menyalakan gas" dan mereka menunjukkan kurangnya empati ketika menggunakan mekanisme ini. Metode intimidasi ini digunakan untuk target persepsi korban, kepercayaan diri, dan harga diri untuk mendapatkan kekuatan, apakah itu secara anonim atau tidak, pada sebuah *platform* publik, seringkali menghasilkan para korban yang ingin mendapatkan tubuh "ideal" (Stern, 2008).

Percobaan *survey* dilakukan oleh empat psikolog, sekelompok siswa harus mengisi kuesioner *cyberbullying* dan sebuah skala empati pendek. Hasilnya menggambarkan bahwa, "*cyberbullies* menunjukkan kurang responsif dari pada *non-cyberbullies*, "dan *cyberbullies* mungkin pada kenyataannya, memiliki" empati yang lebih rendah "karena mereka dapat meminimalkan kemampuan mereka untuk berempati (Steffgen *et al,* 2011). Studi ini menganalisis kemungkinan kurangnya empati yang ditemukan pada anak muda orang dewasa terlibat dalam *cyberbullying*; jarak emosional yang disediakan oleh Internet memungkinkan pengguna untuk menghindari keterlibatan empatik sepenuhnya dan bertindak tanpa konsekuensi pribadi.

Frisén (Stacey, 2017) Sebuah studi yang dilakukan di Gothenburg mensurvei siswa dari 21 sekolah yang berbeda dan menemukan bahwa para *cybervictim* melaporkan "penilaian tubuh yang lebih buruk" daripada mereka yang tidak menjadi *cybervictim*; selain itu, anak perempuan, khususnya, merasa bahwa komentar *cyberbullies* diarahkan pada penampilan tubuh. Sebagai hasilnya, banyak wanita mengembangkan kerentanan yang lebih tinggi terhadap gangguan makan.

Implikasi besar dari akses publik tanpa batas ke Internet adalah *cyberbullies* sekarang memiliki platform untuk secara publik mempermalukan orang dari belakang privasi layar mereka, sehingga menggambarkan kurangnya empati. Menggunakan komentar menyakitkan, *cyberbullies* mengalihkan perhatian dari rasa tidak aman mereka sendiri. Dengan menyoroti ketidaksempurnaan *cybervictim* terlebih dahulu,

cyberbullies dapat menghindari rasa tidak aman pribadi mereka mendapat perhatian publik (Stacey, 2017).

Sayangnya, korban dari *body shaming* sering berbagi pengalaman negatif menerima komentar menyakitkan seperti yang dilakukan. Bagi banyak *cybervictim*, komentar memaki dan memalukan ini dapat meninggalkan "bekas luka" psikologis, yang dapat mempengaruhi timbulnya kelainan makan saat para korban ini berusaha keras untuk mencapai tujuan berat badan dan bentuk tubuh yang diinginkan melalui tindakan ekstrem.

Sementara gangguan makan adalah salah satu efek yang lebih berbahaya dari *body shaming* yang dipicu oleh *cyberbullies*, bunuh diri sejauh ini hasil yang paling memilukan. Alasan saya memilih untuk menulis makalah saya tentang *cyberbullying*, khususnya tentang *body shaming*, adalah karena itu adalah masalah sosial utama yang mempengaruhi laki-laki dan perempuan dengan hasil yang berpotensi permanen, dan bahkan fatal (Stacey, 2017).

G. PENGATURAN HUKUM *CYBERBULLYING* DI INDONESIA

Menurut Syam (2015) aspek hukum *cyberbullying* menanggapi masalah *cyberbullying,* Indonesia telah memiliki peraturan perundang-undangan yang cukup untuk menindak tindak pidana *cyberbullying*, secara umum *cyberbullying* dapat saja diinterpretasikan terhadap berbagai delik yang diatur dalam hukum pidana umum di Indonesia, yaitu yang termuat dalam Kitab Undang-Undang Hukum Pidana (KUHP), UU ITE dan UU TPKS dengan menggunakan asas *lex specialis derogat lex generalis*. Pasal-pasal KUHP yang relevan dalam mengatur delik *cyberbullying* ini adalah yang tercantum dalam Bab XVI mengenai penghinaan, khususnya pasal 310 ayat (1) dan (2).

(1) Barang siapa dengan sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran, dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ratus ribu lima ratus rupiah.

(2) Jika hal itu dilakukan dengan tulisan atau gambar yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ratus ribu lima ratus rupiah.

Kedua pasal tersebut, maka pasal 310 ayat (2) dinilai lebih cocok untuk menuntut para *bully cyberbullying.* Namun memang disini tidak ditegaskan mengenai apa yang dimaksud dengan "muka umum". "Pertanyaan mengenai apakah dunia maya termasuk dalam kategori "muka umum" sudah dijawab dalam putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008, dimana mahkamah berpendapat bahwa "Penghinaan yang diatur dalam KUHP (penghinaan *offline*) tidak dapat menjangkau delik penghinaan dan pencemaran nama baik yang dilakukan di dunia *cyber* (penghinaan *online*) karena ada unsur di muka umum.

Undang-Undang Republik Indonesia No.32 Tahun 2002 tentang Penyiaran dalam Pasal 36 ayat (5) yang berbunyi: "Isi siaran dilarang: a. bersifat fitnah, menghasut, menyesatkan dan/atau bohong; b. menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau c. mempertentangkan suku, agama, ras, dan antargolongan." dan Pasal 36 ayat (6) yang berbunyi: "Isi siaran dilarang memperolokkan, merendahkan, melecehkan dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional."

Terkait dengan masalah regulasi, Indonesia belum memiliki aturan khusus tentang *cyberbullying*. Meski tidak secara spesifik mengatur *cyberbullying*, aturan terkait hal ini masih terakomodasi secara umum di dalam Undang-Undang No 11 Tahun 2008 tentang Informasi Teknologi dan Elektronik (ITE). Perbuatan yang dilarang dalam di dalam UU ITE yang terkait dengan *cyberbullying* tercantum dalam

Pasal 27 ayat:

1. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

2. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
3. Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
4. Setiap Orang 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)

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Pasal-pasal tersebut berisi tentang larangan pendistribusian dan pentransmisian informasi elektronik dan/atau dokumen elektronik yang bermuatan perbuatan kesusilaan, penghinaan, pencemaran nama baik, dan pengancaman.

Adapun peraturan tentang “muatan menghina dan/atau pencemaran nama baik” yang diatur dalam UU ITE juga mengacu pada KUHP, khususnya dalam BAB XVI tentang penghinaan. Pasal 311 KUHP memberikan dasar pemahaman atau esensi mengenai penghinaan atau pencemaran nama baik, yaitu tindakan menyerang kehormatan atau nama baik orang lain dengan maksud diketahui oleh umum. Selain pasal-pasal di atas, regulasi mengenai perlindungan terhadap *cyberbullying* telah dirumuskan secara umum pada Pasal 28D ayat (1) UUD 1945 yang menyatakan: "Setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di hadapan hukum".

Di Indonesia peraturan terkait tindakan *cyberbullying* belum diatur secara spesifik dalam hukum positif Indonesia. Tetapi melihat karakteristik dari pengertian dari tindakan *cyberbullying* tersebut, maka peraturan

perundang-undangan yang cukup relevan adalah Undang-Undang Nomor 11 Tahun 2008 Tentang ITE Pasal 45 ayat Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)

Pasal 54 UU No.35 Tahun 2014 tentang perlindungan anak sudah sangat jelas dikatakan bahwa anak di lingkungan sekolah wajib dilindungi dari tindakan kekerasan yang dilakukan oleh guru, pengelola sekolah atau teman-temannya di dalam sekolah yang bersangkutan, atau lembaga pendidikan lainnya. Pasal ini memuat sanksi pidana bagi para *bully* kekerasan terhadap anak. Ketentuan pidana ini termuat dalam Bab XII dari pasal 77 hingga pasal 90. Berikut ini adalah pasal-pasal yang bisa digunakan untuk mendakwa *bully* kekerasan di sekolah:

Pasal 80

1. Setiap orang yang melakukan kekejaman, kekerasan atau ancaman kekerasan, atau penganiayaan terhadap anak, dipidana dengan pidana penjara paling lama 3 (tiga) tahun 6 (enam) bulan dan/atau denda paling banyak Rp 72.000.000.00 (tujuh puluh dua juta rupiah).
2. Dalam hal anak sebagaimana dimaksud dalam ayat (1) luka berat, maka *bully* dipidana dengan pidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000.00 (seratus juta rupiah).
3. Dalam hal anak sebagaimana di maksud dalam ayat (2) mati, maka *bully* dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak 200.000.000.00 (dua ratus juta rupiah).
4. Pidana ditambah sepertiga dari ketentuan sebagaimana dimaksud dalam ayat (1), ayat (2), dan ayat (3) apabila yang melakukan penganiayaan tersebut orang tuanya. 2.

Pasal 81

1. Setiap orang yang dengan sengaja melakukan kekerasan atau ancaman kekerasan memaksa anak melakukan persetubuhan dengannya atau dengan orang lain, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan paling singkat 3 (tiga) tahun dan

denda paling banyak Rp 300.000.000.00 (tiga ratus juta rupiah) dan paling sedikit Rp 60.000.000.00 (enam puluh juta rupiah).

2. Ketentuan pidana sebagaimana dimaksud dalam ayat (1) berlaku pula bagi setiap orang yang dengan sengaja melakukan tipu muslihat, serangkaian kebohongan, atau membujuk anak melakukan persetubuhan dengannya atau dengan orang lain 3.

Pasal 86

Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan, memaksa, melakukan tipu muslihat, serangkaian kebohongan, atau membujuk anak untuk melakukan atau membiarkan dilakukan perbuatan cabul, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan paling singkat 3 (tiga) tahun dan denda paling banyak Rp 300.000.000.00 (tiga ratus juta rupiah) dan paling sedikit Rp 60.000.000.00 (enam puluh juta rupiah).

Pasal 86

Setiap orang yang dengan sengaja menggunakan tipu muslihat, rangkaian kebohongan, atau membujuk anak untuk memilih agama lain bukan atas kemauannya sendiri, padahal diketahui atau patut diduga bahwa anak tersebut belum berakal dan belum bertanggung jawab sesuai dengan agama yang dianutnya dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000.00 (seratus juta rupiah)

Selain kekerasan fisik, kekerasan psikis juga bisa di pidana, menurut Pasal 77 UU No. 35 Tahun 2014 tentang Perlindungan Anak, setiap orang yang dengan sengaja melakukan tindakan diskriminasi terhadap anak yang mengakibatkan anak mengalami kerugian, baik materil maupun moril sehingga menghambat fungsi sosialnya, dan penelantaran terhadap anak yang mengakibatkan anak mengalami sakit atau penderitaan, baik fisik, mental, maupun sosial dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000.00 (seratus juta rupiah).

Kekerasan di sekolah/lingkungan perguruan tinggi juga bisa di gugat secara perdata. Gugatan perdata bisa diajukan ke pengadilan negeri terhadap *bully* kekerasan di sekolah atau pihak sekolah/lingkungan perguruan tinggi sebagai lembaga berupa gugatan ganti rugi material dan imaterial dalam bentuk uang atau natura. Gugatan ini mengacu pada kitab Undang-Undang Hukum Perdata dengan pasal-pasal berikut:

1. Pasal 1365 Tiap perbuatan melanggar hukum yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut
2. Pasal 1366 Setiap orang bertanggung jawab tidak saja untuk kerugian yang disebabkan karena perbuatannya, tetapi juga untuk kerugian yang disebabkan karena kelalaian, atau kurang hati-hatinya.
3. Pasal 1367 Guru sekolah bertanggung jawab tentang kerugian yang diterbitkan oleh murid selama waktu murid itu berada dibawah pengawasan mereka, kecuali, jika mereka dapat membuktikan bahwa mereka tidak dapat mencegah perbuatan yang mesti mereka seharusnya bertanggung jawab.

Selain itu, sanksi bagi kekerasan seksual berbasis elektronik juga bisa berupa membagikan atau mentransmisikan informasi atau dokumen elektronik bermuatan seksual di luar kehendak penerima yang ditujukan terhadap keinginan seksual juga diatur dalam Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual dalam

Pasal 14

1. Setiap Orang yang tanpa hak:
    a. melakukan perekaman dan/atau mengambil gambar atau tangkapan layar yang bermuatan seksual di luar kehendak atau tanpa persetujuan orang yang menjadi objek perekaman atau gambar atau tangkapan layar;
    b. mentransmisikan informasi elektronik dan/atau dokumen elektronik yang bermuatan seksual di luar kehendak penerima yang ditujukan terhadap keinginan seksual; dan/atau
    c. melakukan penguntitan dan/atau pelacakan menggunakan sistem elektronik terhadap orang yang menjadi obyek dalam informasi/dokumen elektronik untuk tujuan seksual, dipidana

karena melakukan kekerasan seksual berbasis elektronik, dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp200.000.000,00 (dua ratus juta rupiah).

2. Dalam hal perbuatan sebagaimana dimaksud pada ayat (1) dilakukan dengan maksud:
   a. untuk melakukan pemerasan atau pengancaman, memaksa; atau
   b. menyesatkan dan/atau memperdaya, seseorang supaya melakukan, membiarkan dilakukan, atau tidak melakukan sesuatu, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp30O.0OO.00O,0O (tiga ratus juta rupiah).
3. Kekerasan seksual berbasis elektronik sebagaimana dimaksud pada ayat (1) merupakan delik aduan, kecuali Korban adalah Anak atau Penyandang Disabilitas.
4. Dalam hal perbuatan sebagaimana dimaksud pada ayat (1) huruf a dan huruf b dilakukan demi kepentingan umum atau untuk pembelaan atas dirinya sendiri dari Tindak Pidana Kekerasan Seksual, tidak dapat dipidana.
5. Dalam hal Korban kekerasan seksual berbasis elektronik sebagaimana dimaksud pada ayat (1) huruf a dan huruf b merupakan Anak atau Penyandang Disabilitas, adanya kehendak atau persetujuan Korban tidak menghapuskan tuntutan pidana.

Adapun UU TPKS mengelompokkan tindak pidana kekerasan seksual menjadi 9 jenis, termasuk kekerasan seksual berbasis elektronik. Rinciannya yakni: pelecehan seksual nonfisik; pelecehan seksual fisik; pemaksaan kontrasepsi; pemaksaan sterilisasi; pemaksaan perkawinan; penyiksaan seksual; eksploitasi seksual; perbudakan seksual; dan kekerasan seksual berbasis elektronik.

H. RANGKUMAN MATERI

Bullying adalah perilaku seorang siswa atau sekelompok siswa yang menyakiti atau menyerang secara fisik, secara verbal dan secara psikologis, dilakukan secara terus- menerus sehingga *victim* merasa tertekan. *Victim bullying* adalah siswa yang terus-menerus mengalami perilaku

menyakitkan atau serangan secara fisik, secara verbal dan secara psikologis oleh seorang siswa atau sekelompok siswa sehingga dirinya merasa tertekan.

Bentuk-bentuk *cyberbullying* diantaranya adalah membajak akun pribadi seseorang, penyebaran berita bohong atau fitnah, mengganti foto *account* seseorang dan mengganti *password.* Bentuk-bentuk *cyberbullying* dilakukan melalui media seperti pesan teks, gambar video, panggilan telepon, *e-mail, chat room, Instant Messaging (IM),* situs-situs media sosial lainnya. Faktor seseorang melakukan perilaku *cyberbullying, cyberbullying* terjadi dikarenakan faktor *intern* dan faktor *ekstern*, *cybervictim* maupun *cyberbullies* merupakan orang yang memiliki kurangnya rasa empati, pemantauan orang tua yang minim, dan keinginan menjadi *cyberbullies*, selain itu ada beberapa faktor yang mempengaruhi perilaku *cyberbullying* yaitu tradisi, pengaruh media, permusuhan dan gejala depresi.

Dampak dari tindakan *cyberbullying* menyebabkan depresi, merasa terisolasi bahkan bisa sampai terjadi tindakan yang lebih ekstrim yaitu bunuh diri, secara mental mereka terlihat berbeda. *Cybervictim* cenderung terlihat pendiam, pemalu, tertutup dan merasa tidak senang pergi ke sekolah, meskipun mereka senang belajar di sekolah. Cara mencegah dan menghentikan perilaku *cyberbullying,* orang tua harus memberikan edukasi kepada anak- anak mereka tentang perilaku *online* yang benar dan aman, serta apabila perilaku *cyberbullying.*

Tipe *cyberbullying* dan *body shaming*, dua tipe menyakiti dan *online shaming* termasuk individu yang mencari kekuasaan dan kontrol atas *cybervictim* dan *cyberbullies* yang menggertak untuk kesenangan semata menimbulkan rasa sakit dan penghinaan terhadap seseorang. Kedua "jenis" *cyberbullies* ini merusak harga diri korban dan perasaan harga diri, mengarah kepada *cybervictim* yang mengalami gangguan makan, dan bunuh diri.

Tindakan *cyberbullying* dan *body shaming* telah menjadi perhatian serius dari pemerintah. Perhatian pemerintah diwujudkan dengan pembuatan undang-undang yang mengatur tentang tindakan *cyberbullying* dan penghinaan secara *online*. Tindakan *cyberbullying* dan *body shaming* berdampak negatif bagi korban, sehingga harus segera

dihentikan. undang-undang yang dibentuk dimungkinkan untuk mengurangi tindakan *cyberbullying* dan *body shaming.*

TUGAS DAN EVALUASI

Buatlah contoh kasus tentang tindakan *cyberbullying* dan *body shaming* yang telah mendapat tindakan hukum oleh pihak kepolisian.

DAFTAR PUSTAKA

Bauman, S., Toomey, R.B. and Walker, J.L., 2013. Associations Among *Bully*ing, Cyber*bully*ing, And Suicide In High School Students. *Journal of adolescence*, *36*(2), pp.341-350.

Beane, A.L., 2008.*Protect Your Child From Bullying: Expert Advice To Help You Recognize, Prevent, And Stop Bullying Before Your Child Gets Hurt*. John Wiley & Sons.

Beran, T. and Li, Q., 2008. The Relationship Between Cyber*bully*ing And School *Bully*ing. *The Journal of Student Wellbeing*, *1*(2), pp.16-33.

Daye, C.A., Webb, J.B. and Jafari, N., 2014. Exploring Self-Compassion As A Refuge Against Recalling The Body- Related Shaming Of Caregiver Eating Messages On Dimensions Of Objectified Body Consciousness In College Women. *Body Image*, *11*(4), pp.547-556.

Dyastuti, S (2012). Mengatasi Perilaku Agresif Pelaku *Bullying* Melalui Pendekatan Konseling Gestalt Teknik Kursi Kosong.*Indonesian Journal Of Guidance and Counseling Theory and Apllication. Universitas Negeri Semarang Indonesia. ISSN 2252-637*

Englander, E.K., 2012. Spinning Our Wheels: Improving Our Ability To Respond To *Bully*ing And Cyber*bully*ing. *Child and Adolescent Psychiatric Clinics*, *21*(1), pp.43-55.

Field, E.M., 2007. *Bully blocking: Six secrets to help children deal with teasing and bullying*. Jessica Kingsley Publishers.

Karyanti, dan Aminudin., 2019. Cyberbullying & Body Shaming. K-Media.Yogyakarta

Kenny, U., 2017.*Peer Influences on adolescent body image in Ireland* (Doctoral dissertation).

Kowalski, R.M., Giumetti, G.W., Schroeder, A.N. and Lattanner, M.R., 2014. *Bully*ing In The Digital Age: A Critical Review And Meta-Analysis Of Cyberbulling Research Among Youth. Psychological bulletin, 140(4), p.1073

Lupton, D., 2017. Vitalities and visceralities: Alternative body/food politics in new digital media.

Rezvan, M., Shekarpour, S., Thirunarayan, K., Shalin, V.L. and Sheth, A., 2018. Analyzing and learning the language for different types of harassment. *arXiv preprint arXiv:1811.00644*.

Roland, E. and Vaaland, G., 2006. ZERO Teacher's guide to the zero anti-*bully*ing Programme.

Roodt, K., 2015. *(Re) Constructing Body Shaming: Popular Media Representations Of Female Identities As Discursive Identity Construction* (Doctoral Dissertation, Stellenbosch: Stellenbosch University).

Smith, P.K., Mahdavi, J., Carvalho, M. and Tippett, N., 2006. An Investigation Into Cyber*bully*ing, Its Forms, Awareness And Impact, And The Relationship Between Age And Gender In Cyber*bully*ing. *Research Brief No. RBX03-06. London: DfES*.

Stacey, C., 2017. The Walk of (Body) Shame: The Detrimental Repercussions of Cyber*bully*ing. *The Boller Review*, *2*.

Stavanger: Centre for Behavioural Research, University of Stavanger.

Steffgen, G., Pfetsch, J., König, A., & Melzer, A. (2011). Are cyber bullies less empathic? Adolescents' cyber*bully*ing be havior and empathic responsiveness. Cyberpsychology, Behavior, and Social Networking.

Stern, R. (2008). *The Gaslight Effect: How To Spot And Survive The Hidden Manipulation Others Use To Control Your Life*. London: Fusion.

Widayanti, C.G. and Siswati, S., 2009. Fenomena *Bully*ing Di Sekolah Dasar Negeri Di Semarang: Sebuah Studi Deskriptif. *Junal Psikologi Undip*.

HUKUM *CYBER*

BAB 13: INVESTIGASI HUKUM *CYBER*

Dr. Deasy Soeikromo, S.H., M.H

Fakultas Hukum, Universitas Sam Ratulangi Manado

BAB 13

INVESTIGASI HUKUM *CYBER*

A. PENDAHULUAN

Perkembangan internet yang sangat cepat saat ini, telah menjadi alat bantu yang sangat diandalkan oleh manusia untuk meringankan pekerjaan yang dilakukan. Internet banyak membantu manusia, melalui aplikasi internet hasil perkembangan Teknologi Informasi dan komunikasi yang memudahkan manusia dalam berkomunikasi dan meminimalisasi jarak dan waktu. Selain manfaat yang dapat diperoleh melalui internet yang didukung kecanggihan Teknologi Informasi dan komunikasi yang digunakan, juga terdapat potensi bahaya yang telah banyak merugikan bagi para pengguna internet melalui dunia maya. Internet telah membuka kesempatan orang lain untuk berbuat curang, memberi kesempatan kepada orang-orang yang memiliki kemampuan dan berniat jahat untuk melakukan tindak *criminal* melalui internet. Istilah *cyber crime* atau Kriminal *online*, dapat diartikan sebuah perbuatan yang melanggar hukum yang dilakukan secara *online*. Kriminal *online* terjadi sebagai konsekuensi dari penggunaan internet yang bebas dan tanpa batas (*borderless*), dimana batas-batas negara dihilangkan, dan manusia bebas berselancar atau berlanglangbuana, untuk mencari mengambil dan menyebarkan informasi tanpa ada lagi yang membatasi. Kebebasan berinteraksi di internet atau aktivitas *online* yang dilakukan telah menyebabkan banyak terjadi kejadian kriminal *online*, berupa penyebaran virus, *hacking*, *skimming*, pencurian data, transaksi belanja, dll. Dampak dari kriminal *online* telah sangat merugikan dan meresahkan sehingga peran hukum

cyber (*Cyber law*) melalui proses investigasi kasus untuk menghindari atau mengungkap fakta terhadap kejahatan secara *online* sangat diperlukan.

B. PENGERTIAN DAN IMPLEMENTASI HUKUM *CYBER*

Pada masyarakat modern yang sangat akrab dengan teknologi Informasi saat ini, kemajuan teknologi informasi dan komunikasi telah berperan dan menjadi salah satu penentu keberhasilan karena teknologi Informasi dan komunikasi telah digunakan dihampir semua bidang kehidupan. Kemajuan yang diraih dari pemanfaatan teknologi informasi dan komunikasi (TIK) umumnya dilihat dari sudut pandang Perkembangan teknologi informasi yang pesat, sehingga seharusnya juga diantisipasi dengan aturan hukum yang mengatur dan dapat digunakan sebagai sebuah pedoman. Aktivitas melalui pemanfaatan TIK dapat memberi dampak baik positif, maupun dampak negatif yang tentu harus diantisipasi dan diatur melalui hukum yang berkaitan dengan pemanfaatan teknologi informasi dan komunikasi tersebut secara langsung.

Secara hukum kegiatan melalui media siber meski bersifat virtual, kegiatan ini dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Dengan demikian dalam pemanfaatan ruang siber sudah tidak pada tempatnya lagi untuk mengkategorikan sesuatu melalui ukuran dan *standart* hukum konvensional dalam konteks untuk diajukan objek dan perbuatan, karena *standart* hukum konvensional apabila digunakan memiliki banyak celah dan kelemahannya sehingga akan ditemui banyak kesulitan dan aspek-aspek berupa tindakan yang akan lolos dari jeratan hukum.

Berarti bahwa kegiatan siber, meski merupakan sebuah kegiatan virtual akan tetapi berdampak sangat nyata, dengan alat bukti yang bersifat elektronik. Tentunya bila dilihat dari subjek pelaku akan dikualifikasikan sebagai orang yang telah melakukan perbuatan hukum secara nyata, melalui dunia maya. Demikian juga pada transaksi dagang elektronik atau dikenal dengan kegiatan *e-commerce,* dalam transaksinya akan berisi dokumen-dokumen elektronik sebagai bukti dan memiliki kedudukan yang setara dengan dokumen-dokumen atau alat bukti yang dibuat di atas kertas.

Saat ini keamanan di *cyberspace* menjadi *focus* utama dari penggunaan internet. Untuk mempertahankan keamanan di *cyberspac*e terdapat tiga pendekatan *yaitu*: pertama yaitu pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Cara untuk mengatasi gangguan keamanan melalui pendekatan teknologi sifatnya mutlak dilakukan, karena pemanfaatan internet tanpa adanya pengamanan jaringan akan mudah untuk disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak oleh orang lain.

Indonesia saat ini masih menjadi negara dengan tingkat kejahatan tertinggi, terutama pada kasus-kasus transaksi melalui internet berdasarkan prosentase jumlah transaksi dan pelanggaran hukum yang telah terjadi. Dalam konteks ini setidaknya ada dua hal yang dapat dilihat: Pertama, teknologi informasi dianggap sebagai pedang bermata dua, di samping memberikan manfaat juga dapat berubah menjadi instrumen perbuatan melawan hukum yang potensial dilakukan, dan kedua menunjukkan betapa perlunya untuk segera membenahi sektor hukum di bidang ini, termasuk membuat hukum positif yang terkait dengan aktivitas *Cyber law.*

Beberapa istilah yang digunakan di tingkat internasional seperti hukum yang mengatur kejahatan teknologi Informasi, biasanya digunakan istilah *cyber law* atau hukum siber. Istilah lain yang digunakan seperti hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*), dan hukum mayantara. Hukum mayantara seperti yang disampaikan oleh Barda Nawawi Arief, bahwa: "tindak pidana mayantara", identik dengan "tindak pidana di ruang siber (*cyber space*) atau yang biasa dikenal dengan istilah "*cybercrime*" dengan maksud menyatakan tindak pidana di ruang siber Ketika menggunakan internet.

Perkembangan terakhir saat ini telah masuk pada suatu pendekatan hukum baru yang lebih dikenal dengan istilah hukum *cyber* atau hukum telematika. Hukum *cyber* atau *cyber law*, secara internasional selalu digunakan untuk kegiatan hukum yang berhubungan dengan pemanfaatan teknologi informasi dan komunikasi. Disamping itu terdapat juga, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah *Cyber Law* berkaitan dengan hukum *cyber*, istilah ini berasal dari *Cyberspace Law*

yang memiliki ruang lingkup terutama berhubungan dengan aspek-aspek yang berkaitan dengan orang perorangan atau subyek hukum, khususnya dalam penggunaan dan pemanfaatan teknologi internet, sejak saat seseorang memulai *online*, masuk dan memanfaatkan *cyber* atau dunia maya. Penggunaan istilah *cyber law* saat ini lebih populer karena, dari aktivitas pemanfaatan *cyber* mulai timbul kejahatan-kejahatan yang ada di dunia maya yang lebih dikenal sebagai *Cybercrime*. Hamidin, (2010, h.81) menyatakan *Cybercrime* merupakan bentuk-bentuk kejahatan yang timbul karena memanfaatkan teknologi internet, juga terdapat beberapa pendapat yang mengidentikkan *cybercrime* dengan *computer crime*. Sementara Wahid dan Labib, (2005, h.65) menyatakan kejahatan *cyber* (*cyber crime*) sering dipersepsikan sebagai kejahatan yang dilakukan dalam ruang atau wilayah siber

Cyberlaw, dapat diartikan sebagai seperangkat aturan yang dibuat oleh suatu negara tertentu, dan peraturan yang dibuat itu hanya berlaku pada masyarakat Negara tersebut. *Cyber Law* dapat juga diartikan sebagai hukum yang digunakan di dunia maya (*cyberspace*), dimana umumnya lebih banyak dikenal dengan penggunaan internet. *Cybercrime* berkaitan dengan tindak kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya dalam penggunaan internet yang menjadi aktivitas/transaksi di dunia maya.

Internet saat ini telah menghadirkan *Cyberspace* dengan realitas virtual yang menawarkan pada semua pengguna fasilitas, kecepatan interaksi, harapan dan berbagai kemudahan. Namun demikian dalam perkembangannya kemudian muncul persoalan-persoalan baru, yaitu kejahatan yang dinamakan *cyber crime* yang melibatkan orang yang mahir menggunakan *computer* dan internet, yang menyasar baik sistem jaringan *computer*, komputer itu sendiri, maupun fasilitas lainnya yang menjadi target untuk melakukan berbagai kejahatan.

Pencurian atau pemalsuan data dan Informasi telah menjadi sasaran baru, yang dapat merugikan materi maupun reputasi pihak lain karena saat ini data dan informasi telah menjadi bagian dari Bisnis/komoditi sehingga upaya-upaya dalam memberi perlindungan terhadap aset-aset baik pribadi maupun perusahaan saat ini sangat diperlukan. Bentuk

perlindungan yang dapat dilakukan yaitu melalui hukum Pidana, baik melalui sarana *penal* maupun *non penal*.

Terhadap tantangan penggunaan internet termasuk penyalahgunaan yang dilakukan oleh pihak-pihak yang memiliki kepentingan tertentu, termasuk pada tantangan komunikasi global lewat Internet, maka Undang-Undang yang diharapkan (*ius konstituendum*) berupa perangkat hukum yang akomodatif dan mampu menjawab tantangan perubahan yang cepat, serta mampu mengantisipasi terhadap masalah-masalah yang kemudian akan muncul, termasuk pengaruh *negative* dari penyalahgunaan Internet dengan berbagai kepentingan yang kemudian dapat menimbulkan korban-korban karena menderita kerugian materi dan *non* materi.

Secara khusus Indonesia belum memiliki Undang-undang *Cyber law* yang secara detail kemudian mengatur mengenai *Cyber crime*. Namun demikian kita telah memiliki beberapa hukum positif, yang mengatur meski berlaku umum, yang dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana komunikasi dan interaksinya.

Kegiatan Siber meskipun sifatnya virtual namun dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang siber sudah tidak pada tempatnya lagi untuk kategorikan sesuatu dengan ukuran dalam kualifikasi hukum konvensional untuk dijadikan obyek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan siber adalah kegiatan virtual yang berdampak sangat nyata, meskipun alat buktinya bersifat elektronik. Dengan demikian, subyek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Edrisy (2019, h. 1) menggunakan istilah hukum Siber dengan pertimbangan bahwa *Cyber* jika diidentikkan dengan “dunia maya” akan cukup menghadapi persoalan Ketika terkait pembuktian dan penegakan hukumnya. Pertimbangan lain adalah para penegak hukum akan menghadapi kesulitan bila harus membuktikan suatu kasus/ persoalan yang diasumsikan sebagai “maya” atau sesuatu yang tidak terlihat alias semu.

C. PERKEMBANGAN HUKUM *CYBER* DAN KRIMINAL *ONLINE*

1. Perkembangan Hukum *Cyber*

Perkembangan teknologi Informasi dan komunikasi saat ini sangat cepat yang telah memunculkan berbagai media komunikasi yang sangat cepat menyampaikan berbagai informasi dalam ruang dan waktu yang sangat singkat (*persecond*). Pengembangan IT termasuk pada alat komunikasi berupa *computer*, telah memunculkan sistem komunikasi baru berbasis jaringan yang umumnya sering disebut jaringan kerja (*network*) yang bisa diakses melalui internet dengan menggunakan *computer* sebagai medianya. Saat ini dapat dilihat bahwa adanya pemanfaatan teknologi Informasi dan komunikasi telah banyak memberikan kemudahan serta manfaat yang besar bagi manusia sebagai penggunanya. Kecepatan penyelesaian transaksi yang cepat, telah banyak membantu menyelesaikan permasalahan terhadap kegiatan-kegiatan yang dilakukan manusia dari pekerjaan yang sederhana sampai pada jenis pekerjaan yang sulit yang membutuhkan bantuan teknologi untuk penyelesaiannya.

Namun demikian diperlukan kebijakan serta upaya-upaya untuk melindungi Informasi, termasuk didalamnya membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya agar pendekatannya dapat komprehensif.

Uraian sebelumnya memberi gambaran bahwa pemanfaatan/ penggunaan teknologi informasi saat ini sangat strategis dan berdampak luas pada aktivitas kehidupan manusia sehingga dibutuhkan pengaturan secara khusus dengan cara dibentuknya suatu undang-undang yang secara khusus kemudian akan dapat menanggulangi kejahatan pada penggunaan/ berkaitan dengan teknologi informasi.

Aturan yang akan dibentuk berkaitan dengan penggunaan teknologi informasi agar diterima masyarakat, didalamnya harus mempertimbangkan semua aspek baik (suprastruktur, infrastruktur, kepakaran, termasuk aspirasi internasional dalam hal keamanan internet) juga berbagai kepentingan harus diselaraskan dan diserasikan, sehingga dapat memberikan kepastian hukum terhadap para pengguna.

Pembentukan peraturan perundang-undangan di dunia *cyber* yang diharapkan tersebut, berpangkal pada keinginan masyarakat untuk mendapatkan jaminan keamanan keadilan dan kepastian hukum secara

tegas. Demikian juga sebagai norma hukum *cyber* atau *cyber law*, nantinya akan dapat mengikat pada setiap individu untuk tunduk dan mengikuti segala kaidah-kaidah yang telah diatur dalam peraturan tersebut.

Teknologi internet termasuk penggunaannya di Indonesia, berkembang secara cepat dan banyak orang yang tidak menduga terhadap kecepatan perubahan yang terjadi, sebagai konsekuensi pemanfaatan teknologi internet.

Pada awalnya internet di Indonesia hanya dikenal oleh sebagian kecil orang yang memiliki minat di bidang *computer*, kemudian internet sudah mulai dikenal masyarakat luas, dan dalam tahun-tahun terakhir saat ini pengguna jasa internet meningkat secara sangat pesat dengan fitur-fitur baru yang memudahkan bagi para pengguna, serta kecepatan akses yang semakin cepat. Pada awalnya masyarakat pengguna internet, memanfaatkan fasilitas internet, hanya sebagai sarana hiburan dan penyaluran *hobby*. Saat ini pemanfaatan teknologi internet, sudah sangat beragam dan seiring makin pesatnya perkembangan teknologi komunikasi dan informasi melalui internet, telah diikuti juga dengan munculnya berbagai kejahatan yang dilakukan menggunakan media internet.

Internet dalam penggunaannya, semakin lama semakin canggih dan kompleks, hal ini memberikan peluang baru bagi pihak-pihak yang ingin memperoleh keuntungan.

Telah memunculkan kejahatan yang sangat canggih dan sulit, dideteksi termasuk diketahui pelakunya. *Cyber crime* yang populer digunakan masyarakat dapat diartikan kejahatan dunia maya atau tidak riil. Sehingga seolah-olah tidak ada tindak pidana atau kejahatan karena suatu tindak pidana harus pasti obyek dan subyek hukumnya, *locus delicti* serta *tempus delictinya* (Riswandi, 2006:32).

Pelaku kejahatan di internet memanfaatkan peluang, melakukan aksinya secara aman, karena internet merupakan sarana/media komunikasi yang tidak terlihat (maya). Dalam melaksanakan aksinya, kemudian pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui atau diketahui dengan jelas siapa pelaku, dan dimana aksi tersebut dilakukan. Termasuk didalamnya adalah kejahatan yang muncul, yang menimbulkan persoalan karena jaringan-jaringan komputer yang dipergunakan oleh berbagai pihak, kemudian

disalahgunakan oleh para pelaku kejahatan untuk kepentingan kejahatannya, Tindakan ini kemudian dikenal sebagai kejahatan komputer (*computer crime*).

Terhadap kejahatan yang dilakukan ini kemudian dikenal masyarakat sebagai *cyber crime* atau tindak pidana mayantara (*cyber space*) (Arief, 2002 h. 239). Perkembangan *cyber crime* saat ini, dapat secara jelas diikuti terjadinya, karena dunia sekarang tanpa batas, yang telah menyebabkan perubahan sosial secara signifikan (termasuk tata nilai) yang berlangsung juga dengan cepat. Perubahan secara cepat pada sikap dan pola perilaku masyarakat akibat berkembangnya teknologi informasi dan komunikasi, yang menyebabkan munculnya pandangan bahwa dunia seperti flat (*flattener*). Kecepatan penyampaian Informasi saat ini, juga menyebabkan berbagai Informasi dari berbagai peristiwa dibelahan dunia, termasuk kejahatan maya, dari berbagai belahan bumi, gambar dan beritanya dapat dihadirkan seketika, bahkan saat ini banyak yang disampaikan secara *live*/*real time* atau biasa dikenal siaran langsung menggunakan berbagai media/kanal berita.

2. Deskripsi tentang Kejahatan Online (*Criminal online*)

Kejahatan *on line* tercipta, karena rapuhnya *security*/pengamanan jaringan maupun data perorangan atau perusahaan. Ada tiga pendekatan yang dapat dilakukan untuk mempertahankan keamanan di *cyberspace*, pertama yaitu pendekatan teknologi, kedua pendekatan sosial budaya-etika, dan ketiga pendekatan hukum. Langkah pengamanan untuk mengatasi gangguan keamanan, maka pendekatan teknologis bersifat mutlak untuk dilakukan, sebab tanpa pengamanan jaringan akan sangat rapuh dan mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak oleh pihak lain.

Seperti kita ketahui bahwa Indonesia telah menjadi salah satu negara dengan tingkat kejahatan tertinggi dalam kasus-kasus transaksi melalui internet berdasarkan prosentase jumlah transaksi dan pelanggaran hukum yang dilakukan. Hal ini menunjukkan bahwa ada dua hal yang harus diperhatikan, yaitu: Pertama teknologi informasi merupakan pedang bermata dua, disamping memberikan manfaat juga dapat menjadi alat untuk melakukan perbuatan melawan hukum yang potensial, dan kedua

menunjukkan betapa perlunya untuk segera membenahi sektor hukum di bidang ITE, termasuk merancang hadirnya hukum positif yang berhubungan dengan aktivitas *Cyber*.

Dalam praktik Jika kita melihat disiplin ilmu sosial ada yang berkembang dengan pesat sejalan dengan perkembangan teknologi, maka itulah ilmu hukum. Perkembangan teknologi informasi yang sangat cepat telah menyebabkan eksistensi hukum dibidang ekonomi yang kemudian dikenal dengan istilah *Cyber Law* mendapat perhatian khusus dari banyak pihak, khususnya terhadap *Cyber Law*. Demikian juga secara internasional respon dari negara-negara di dunia tampak sangat cepat, sebagai contoh Amerika Serikat, Kanada dan Masyarakat Eropa secara responsif menanggapi perkembangan teknologi informasi ini dengan pembuatan regulasi di bidang teknologi Informasi dan *cyber*, bahkan juga telah ditindaklanjuti melalui kerjasama multilateral dengan membentuk instrumen internasional seperti *International chamber of commerce* (ICC). Ditingkat Asia dan Asean juga yang dilakukan negara tetangga seperti Malaysia, India dan Singapura, secara cepat menyikapi perkembangan ITE dan *Cyber Law* melalui pembuatan berbagai regulasi di bidangnya dan dimasukkan dalam hukum positif di negaranya.

3. Investigasi Hukum *Cyber*

Investigasi hukum *Cyber* sangatlah penting dilakukan, karena investigasi atau penyidikan yang dilakukan pihak yang berwenang seperti Kepolisian RI, akan banyak membantu untuk mengungkapkan kejahatan maya yang telah terjadi, baik dari segi pelaku, motif, dan dasar atau pendekatan hukum yang dapat dilakukan akibat kerugian yang diakibatkan melalui tindak pidana *cyber crime*.

Pendekatan hukum yang dapat dilakukan berhubungan dengan permasalahan yang dibahas mengenai tindak pidana mayantara (*cyber crime*) yang menggunakan sarana internet untuk ketentuan hukumnya, yang dipakai tetap mengacu pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) dan Undang-undang tentang Informasi dan Transaksi Elektronik.

Sebagai contoh pada UU ITE Pasal 45B, UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, mengatur bahwa: Setiap orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp.750.000.000,00 (tujuh ratus lima puluh juta rupiah). Pasal ini mengatur secara jelas ancaman hukuman Pidana terhadap pelaku kejahatan *cyber*, baik Pidana penjara maupun denda yang ditentukan.

Aturan Undang-undang ini perlu diadakan, karena kejahatan *cyber* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga perlu penanganan dan pengaturan khusus di luar KUHP untuk dapat memberikan efek jera dan memberikan kepastian hukum bagi para korban.

Perkembangan teknologi informasi saat ini yang sangat pesat harus dapat di antisipasi dengan aturan hukum untuk memberikan perlindungan. Terkait didalamnya adalah aparat kepolisian maupun kejaksaan yang menjadi Lembaga atau aparat penegak hukum yang memegang peran penting dalam proses investigasi dalam upaya penegakan hukum terhadap kejahatan *cyber*. Untuk suatu perkara pidana, agar dapat sampai pada tingkat penuntutan dan pemeriksaan pada sebuah sidang pengadilan, maka sebelumnya harus melewati beberapa tindakan-tindakan pada tingkat penyidik seperti investigasi awal yang dilakukan, maupun Tindakan lainnya yang akan dilakukan sebagai sebuah tahapan dalam pengumpulan barang bukti ataupun kepentingan lainnya.

Dalam proses perkara pidana, tahapan-tahapan yang harus dilalui, meliputi:

a. Tahapan penyidikan dari aparat kepolisian
b. Tahap penuntutan yang dilakukan Jaksa (Penuntut Umum)
c. Tahap pemeriksaan pada sidang pengadilan.

Pada saat dilakukannya penyidikan oleh aparat kepolisian, maka para penyidik akan melakukan serangkaian langkah yang diperlukan termasuk investigasi pada kejahatan *Cyber*, guna mendapat alat bukti yang

diperlukan yang akan digunakan pada persidangan pengadilan. Bila oleh penyidik, kasus yang disidik tidak memiliki cukup bukti, atau peristiwa tersebut ternyata bukan merupakan tindak pidana maka penyidikan akan dihentikan demi hukum.

Saxunova, (2012), menyatakan pelaksanaan investigasi *Cyber fraud*, dapat dilakukan bila ada sesuatu kegiatan yang dinilai mencurigakan atau tidak wajar yang dapat berpotensi sebagai tindak kejahatan. Pada perusahaan atau instansi Tim investigasi yang dibentuk dapat terdiri dari ketua, anggota, perwakilan pihak manajemen, supervisor dan seorang konsultan hukum.

Tahapan kegiatan investigasi dapat dirancang dengan urutan seperti:

a. Membuat rencana investigasi
b. Deteksi dan analisis tindak kejahatan, mempersiapkan jadwal investigasi
c. Pengumpulan data atau bukti
d. wawancara
e. Dokumentasi hasil temuan sesuai *standart* yang ditentukan.

Dalam kegiatan investigasi Asosiasi Pemeriksa *Fraud* yang bersertifikasi atau ACFE, menyatakan bahwa pengumpulan barang bukti dari investigasi termasuk dokumen internal meliputi *file* pribadi, catatan telepon, *file computer* dan perangkat elektronik lain yang digunakan termasuk yang terhubung (Sharma, *et, al.,* 2020). Dalam pelaksanaannya terdapat 4 jenis barang bukti yang dapat digunakan sebagai landasan untuk melakukan investigasi, seperti: *Testimonial Evidence, Documentary Evidence, Physical Evidence,* dan *Personal Observation* (Ashcroft *et al.,* 2004:96).

Bukti investigasi dapat dimulai dari kecurigaan atas *anomaly* kegiatan yang ada, sehingga dianggap perlu untuk dilakukan investigasi, untuk melihat apakah terjadi *crime/fraud* dalam perusahaan atau suatu divisi yang menjadi target. Sedangkan untuk *Testimonial evidence* berkaitan dengan *testimony* dari individu yang dilakukan melalui proses *interview*, interogasi maupun tes kejujuran untuk memperoleh informasi.

Bukti berupa *Documentary evidence* diperoleh dari sebuah dokumen baik cetak maupun dokumen *file*/folder *computer* dengan teknik menggunakan pemeriksaan dokumen, *data mining*, pencarian *data public*, audit, trasir di *computer*, analisis dokumen keuangan, hingga memeriksa *database* dan email instansi maupun pihak terkait. *Phsyical Evidence* dapat diperoleh dari *finger print*, barang/*property* yang hilang/dicuri, pada tahapan ini dalam pengumpulan bukti akan diperlukan bantuan dari ahli forensik. Tahapan lain yaitu Personal *observation*, merupakan hasil dari investigasi yang dirasakan baik dilihat, didengar oleh indra dari investigator sendiri saat melakukan investigasi. Pada kasus *cyber crime/fraud* barang bukti yang ditemukan dapat menjadi barang bukti utama baik *Documentary Evidence* yang terdiri dari barang bukti digital dan dokumen fisik yang akan menunjang proses investigasi yang dilakukan.

Bukti Digital dapat didefinisikan sebagai informasi atau data yang berharga untuk proses investigasi yang dapat digunakan sebagai bukti untuk mendukung ataupun menolak dugaan tindak *criminal* dan disimpan, diterima ataupun ditransmisikan menggunakan perangkat elektronik (*National Forensic Science Technology Center*, 2014). Bukti Digital dapat diambil dari semua perangkat digital mulai dari *computer*, telepon, laptop, kamera, cctv, PDA, IoT, *harddisk*, USB dan lain sebagainya. Bukti digital memiliki beberapa karakteristik yang perlu diperhatikan oleh para investigator agar barang bukti tersebut tetap dapat diterima dimeja pengadilan, karakteristik tersebut yakni:

a. Tersembunyi seperti bukti sidik jari atau DNA
b. Tanpa batas atau *borderless* dan melampaui batas yurisdiksi
c. Dapat diubah, rusak, atau hancur
d. Sensitif terhadap waktu.

Untuk melakukan assesmen, harus menggunakan *tools* tertentu dan tenaga yang telah terlatih sehingga barang bukti tetap *authentic*. Setelah barang bukti diamankan akan dilakukan *imaging* atau akuisisi menggunakan *forensics tools* seperti *Encase*, FTK, *Belkasoft* dan *tools* lainnya. Untuk pemeriksaan dan analisis menggunakan kopian dari *original copy* bukti yang sudah diakuisisi. Pemeriksaan bukti digital dilakukan

sesuai prosedur yang telah ditetapkan dan dilakukan oleh pemeriksa yang telah dilatih mengenai digital *forensic*.

Pemeriksaan yang tidak sesuai prosedur dapat merusak bukti digital dimana hal tersebut akan sangat merugikan bagi penyelidikan yang telah dilaksanakan.

Perlu diperhatikan bahwa pada kasus *cyber crime/fraud* dapat dilakukan investigasi, akan tetapi apabila investigasi yang akan dilakukan pada kasus *cyber fraud* terlalu lama perencanaannya, maka barang bukti digital dapat hilang sehingga dalam tahapan *readiness* harus ditentukan SOP dari perusahaan/instansi yang bersangkutan untuk mencegah dampak lebih buruk dari tindakan *fraud* apalagi yang dilakukan oleh pegawai internal atau kejahatan yang dilakukan orang dalam (*cyber crime*).

D. RANGKUMAN MATERI

Investigasi hukum *Cyber* penting untuk dilakukan, karena investigasi diperlukan perusahaan atau instansi bila ada sesuatu kegiatan yang dinilai mencurigakan atau tidak wajar (*fraud*) yang dapat berpotensi sebagai tindak kejahatan. Perusahaan dapat membentuk Tim investigasi yang terdiri dari ketua, anggota, perwakilan pihak manajemen, supervisor dan seorang konsultan hukum, dengan tahapan yang ditentukan sesuai *standart* dan waktu yang disepakati.

Pada investigasi pengumpulan barang bukti penting dilakukan termasuk didalamnya dokumen internal meliputi *file* pribadi, catatan telepon, *file computer* dan perangkat elektronik lain yang digunakan. Terdapat 4 jenis barang bukti yang dapat digunakan sebagai landasan investigasi, yaitu: *Testimonial Evidence, Documentary Evidence, Physical Evidence,* dan *Personal Observation.*

Bukti Digital meliputi informasi atau data yang berharga untuk proses investigasi yang dapat digunakan sebagai bukti untuk mendukung ataupun menolak dugaan tindak *criminal* dan disimpan, diterima ataupun ditransmisikan menggunakan perangkat elektronik. Bukti Digital dapat diambil dari semua perangkat digital mulai dari *computer*, telepon, laptop, kamera, cctv, PDA, IoT, *harddisk*, USB dan lain sebagainya. Pemeriksaan yang tidak sesuai prosedur dapat merusak bukti digital dimana hal tersebut akan sangat merugikan bagi kepentingan penyelidikan.

TUGAS DAN EVALUASI

Jawablah pertanyaan berikut ini dengan memberi penjelasan yang diperlukan untuk memperkuat argumentasi saudara, sebagai hasil analisa terhadap masalah-masalah, sebagai berikut:

1. Jelaskan apa yang dimaksud kriminal *online* dan berikan contohnya.
2. Jelaskan penyebab terjadinya kriminal *online* dan cara mengatasinya.
3. Jelaskan tentang investigasi kriminal *online*
4. Jelaskan bagaimana cara melakukan investigasi kriminal *online*
5. Jelaskan pendekatan hukum untuk dilakukannya investigasi kriminal *online*.

DAFTAR PUSTAKA

Arief, B Nawawi (2006). *Tindak Pidana Mayantara*, Jakarta: PT. Raja Grafindo.

Ashcroft, J, Daniels, D. J., & Hart, S V. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. National Institute of Justice, 7(2), 95–111.

Dikdik M. Arief Mansur, dan Elisatris Gultom, (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: PT. Grafika Aditama.

Edrisy, Ibrahim F, (2019). *Pengantar Hukum Siber*. Lampung: Sri Wawai Publishing.

Hamidin, Aep S. (2010). *Tips & Trik Kartu Kredit Memaksimalkan dan Mengelola Resiko Kartu Kredit*, Yogyakarta: MedPress.

Riswandi, B. Agus (2006). *Hukum Cyberpace*, Yogyakarta: Gita Nagari.

Saxunova, D. (2012). *Investigation of Suspected Fraud*. International Journal of Business and Management Studies, (elektronický zdroj). New York. Vol.1, No.2 (2012), pp. 347-364

Sharma, P., Arora, D., & Sakthivel, T. (2020). *Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications*. Procedia Computer Science, 167 (2019), 907–917.

Undang-undang No. 19 Tahun 2016, *tentang Informasi dan Transaksi Elektronik*. Jakarta: Pemerintah Republik Indonesia.

Wahid, Abdul dan M. Labib (2005). *Kejahatan Mayantra* (Cyber Crime), Bandung: PT Refika Aditama.

HUKUM *CYBER*

BAB 14: PENEGAKAN HUKUM *CYBER*

Dr. Henny Saida Flora, S.H., M.Hum., M.Kn., M.H.Kes

FH Unika Santo Thomas Medan

BAB 14

PENEGAKAN HUKUM *CYBER*

A. PENDAHULUAN

Pengertian dari kejahatan dunia maya atau *cyber crime* merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi dengan menggunakan internet sebagai media untuk melakukan tindak kejahatan. Kemajuan teknologi berimplikasi pada perkembangan kejahatan. Kejahatan yang dulunya dianggap sebagai suatu kejahatan apabila adanya kontak fisik antara pelaku dan korban dalam melakukan tindak kejahatan bertransformasi menjadi kejahatan di dunia maya atau *cyber crime* yang dapat dilakukan tanpa adanya kontak fisik antara pelaku dan korban secara langsung dengan menggunakan media internet dan alat elektronik lainnya. Dampak dari adanya internet memberikan peluang kepada para pelaku kejahatan untuk melakukan kejahatan yang lebih tersembunyi dapat menembus ruang dan waktu dengan jangkauan yang luas, bahkan global. Kejahatan di dunia maya dapat dilakukan dimana dan kapan saja dengan syarat adanya jaringan internet dan peralatan yang memadai. Penanganan *cyber crime* bukanlah suatu hal yang mudah untuk diatasi, selain karakteristik *cyber crime* itu sendiri, regulasi hukum di Indonesia yang sudah ada belum dapat menjangkau perkembangan kejahatan yang dilakukan di dunia maya. Peraturan Perlindungan data pribadi yang ada di Indonesia hanya didasarkan pada Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Substansi yang tercantum dalam Undang-undang Informasi dan Transaksi Elektronik atau UU ITE berisi perlindungan hak

pribadi, asas perdagangan secara *e-commerce*, masalah yurisdiksi, asas persaingan usaha-usaha tidak sehat dan perlindungan konsumen, asas hak atas kekayaan intelektual, asas *cyber crime*, dan hukum internasional.

Seiring dengan semakin pesatnya perkembangan komunikasi melalui internet, memunculkan pula berbagai kejahatan yang dilakukan dengan media internet. Tidak dapat dipungkiri bahwa penggunaan internet yang canggih dan cepat tersebut memunculkan pula kejahatan yang sangat canggih dan sulit untuk diketahui pelakunya. Hal ini disebabkan karena internet merupakan suatu media komunikasi yang tidak terlihat (maya), sehingga pelaku kejahatan dapat dengan mudah menghilangkan jejak tanpa dapat diketahui dengan jelas. Terlepas dari manfaat yang diperoleh dengan kemajuan teknologi di bidang komputer, belakangan muncul persoalan ketika jaringan-jaringan komputer yang dipergunakan oleh berbagai pihak tersebut disalahgunakan oleh pihak-pihak tertentu untuk kepentingan yang berseberangan, atau dikenal dengan kejahatan komputer (*computer crime*). Dalam istilah lain, kejahatan ini lebih dikenal dengan *cyber crime* atau tindak pidana mayantara *(cyber space)* (Barda Nawawi Arief, 2002). Dunia sekarang tanpa batas, sehingga telah menyebabkan perubahan sosial secara signifikan yang berlangsung dengan begitu pesatnya perubahan masyarakat akibat berkembangnya teknologi informasi dan komunikasi, sehingga dunia telah diibaratkan seperti mengkerut. Bermacam-macam peristiwa, termasuk kejahatan, dari berbagai belahan bumi, gambar dan beritanya dapat dihadirkan seketika, bahkan ada yang dapat disajikan secara real tim.

Fenomena perkembangan *cyber crime* ini, sebenarnya bukan hanya sekedar masalah nasional, regional, atau kawasan suatu negara tertentu, tetapi sudah menjadi perhatian dunia internasional karena memang jangkauan *cyber crime* ini bersifat global (*boarderless*). Itulah sebabnya dalam berbagai forum internasional seperti *Internasional Information Industry* (IIIC) 2000 *Mellenium Congress* yang diselenggarakan di Quebec pada 19 September 2000, Asosiasi Teknologi Informasi Canada (*Information Technology Association of Canada*) sangat mengkhawatirkan permasalahan ini. Bahkan Panitia Kerja Perlindungan Data *(Data Protection Working Party*) Dewan Eropa menyatakan bahwa *cyber crime* merupakan bagian sisi paling buruk dari masyarakat Informasi (*cyber crime*

is part of the seamy side of the information society) (Barda Nawawi Arief, 2002). Sehubungan dengan hal tersebut upaya penanggulangannya dilakukan dengan melakukan kriminalisasi terhadap *cyber crime*

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum. Politik hukum pidana merupakan bagian dari kebijakan penegakan hukum (*law enforcement policy*). Penggunaan upaya hukum termasuk hukum pidana, sebagai salah satu upaya mengatasi masalah sosial, termasuk dalam bidang kebijaksanaan penegakan hukum. Di samping bertujuan untuk mencapai kesejahteraan masyarakat pada umumnya, maka kebijaksanaan penegakan hukum ini pun termasuk dalam kebijaksanaan sosial, yaitu segala usaha yang nasional untuk mencapai kesejahteraan masyarakat (Arief, 2014).Kejahatan baru ini sangat berdampak pada berbagai aspek bidang kehidupan. Banyak yang menganggap bahwa keberadaan KUHP tidak mampu menjangkau kejahatan baru tersebut sehingga pemerintah menginisiasi lahirnya aturan tentang *cyber crime*. Berdasarkan dokumen yang ada, Undang-undang tentang Informasi dan Transaksi Elektronik (UU ITE), yaitu Undang-undang Nomor 19 Tahun 2016 atas perubahan atas Undang-undang Nomor 11 Tahun 2008 (Hermawan, 2019).

Kesesuaian antara karakteristik pelaku *cyber crime* dengan paradigma pemidanaan dalam pidana kerja sosial atau pidana pengawasan sehingga tujuan pemidanaan akan dapat tercapai. Sejalan dengan pandangan Widodo, dalam mengantisipasi *cyber crime*, Kitab Hukum Pidana mencoba memperluas cakupan untuk dapat menjaring kejahatan *cyber crime*. Menurut Widodo, penjatuhan pidana kepada para pelaku *cyber crime* adalah langkah yang kurang tepat dan kurang bijak. Hal ini disebabkan oleh ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistem pembinaan narapidana di Lembaga Permasyarakatan sehingga tujuan pemidanaan sebagaimana diatur dalam Undang-undang Permasyarakatan tidak akan tercapai. Menurutnya, sebagai pengganti pemidanaan tersebut adalah pidana kerja sosial atau pidana pengawasan (Widodo, 2013), sedangkan menurut Barda Nawawi Arief, jika dilihat dari sudut pandang hukum pidana, upaya penanggulangan *cyber crime* khususnya di Indonesia dapat dilihat dari berbagai aspek, yaitu aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat

bukti/pembuktian), aspek kriminalisasi (formulasi tindak pidana), dan aspek yurisdiksi. Barda Nawawi Arief mengatakan kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakikatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*). Oleh karena itu, hal tersebut termasuk bagian dari 'kejahatan hukum pidana' (*penal policy*), khususnya kebijakan formulasinya. Selanjutnya menurut Arief, kebijakan kriminalisasi bukan sekedar kebijakan menetapkan/merumuskan/memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah Bagaimana kebijakan formulasi/ legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu. Kebijakan penanggulangan *cyber crime* secara teknologi, diungkapkan juga dalam IIIC *(International Information Industry Congress)* yang menyatakan*: "The IIIC recognizes that government action and international traties to harmonizes laws and coordinate legal procedurs are key in the fight against cybercrime, but warns that these should not be relied upon as the onlu instuments. Cybercrime is enabled by technology and requires a healthy reliance on technology for ots solutions".* Sementara dalam hal menangani dan menyelidiki *cyber crime* adalah peran dari *cyber police* dan *virtual police*. Peran dari *virtual police* sendiri adalah memberikan edukasi kepada masyarakat terkait dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE), sedangkan peran dari *cyber police* adalah menindaklanjuti kasus jika tindakan yang dilakukan oleh masyarakat tersebut tidak bisa ditegur oleh *virtual police*. Singkatnya, *virtual police* muncul sebelum diselidiki lebih lanjut oleh *cyber police*. Cara kerja dari polisi virtual adalah dengan memberikan peringatan kepada akun di media sosial yang diduga melanggar, hal ini tentu saja dilakukan setelah adanya pertimbangan dari pendapat ahli bukan semata-mata pendapat subjektif penyidik. Selanjutnya saat akun mengunggah tulisan gambar yang berpotensi melanggar maka, petugas akan menyimpan tampilan unggahan tersebut untuk dikonsultasikan dengan tim ahli yang terdiri dari ahli

pidana, ahli bahasa, dan ahli informasi dan transaksi elektronik. Jika ahli mengatakan konten tersebut memuat pelanggaran pidana, langkah selanjutnya adalah diajukan ke direktur siber atau pejabat yang ditunjuk siber memberikan pengesahan. Kemudian, *virtual police alert* dikirim secara pribadi ke akun yang bersangkutan secara resmi. Peringatan akan dikirimkan lewat *direct message*, sebab kepolisian tidak ingin peringatan dari *virtual police* kepada pengguna media sosial tersebut diketahui oleh pihak lain, karena bersifat rahasia. Kehadiran *virtual police* ini cenderung masih baru di kalangan masyarakat, padahal diketahui pihak kepolisian sudah memiliki tim siber yang fungsinya tidak jauh berbeda dengan polisi virtual. Masih banyak masyarakat yang belum mengetahui perbedaan antara polisi virtual dan polisi siber, salah satu alasannya yaitu kurangkan pengedukasian kepada masyarakat dengan cakupan yang lebih luas. Badrul Zaman menjelaskan perbedaan dari keduanya yaitu jika polisi virtual lebih mengedepankan upaya preventif, sedangkan polisi siber sudah pasti melakukan penegakan hukum sesuai regulasi yang ada karena polisi siber sudah dapat mendeteksi melanggar rambu-rambu UU ITE.

B. BENTUK *CYBER CRIME*

1. *Unauthorized Access to Computer System and Servic*e Kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet. Misalnya pada saat masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker* juga telah berhasil menembus masuk ke dalam *database* berisi data para pengguna jasa *America Online* (AOL), sebuah perusahaan Amerika Serikat yang bergerak di bidang *e-commerce*, yang memiliki tingkat

kerahasiaan tinggi (*Indonesian Observer*, 26/06/2000). *Situs Federal Bureau of Investigation* (FBI) pun tidak luput dari serangan para *hacker*, yang berakibat tidak berfungsinya situs ini dalam beberapa waktu lamanya.

2. *Illegal Contents* Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Misalnya pemuatan suatu berita bohong atau fitnah yang mendiskreditkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan lain sebagainya.
3. *Data Forgery* Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
4. *Cyber Espionage* Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.
5. *Cyber Sabotage and Extortion* Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer

yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

6. *Offense against Intellectual Property* Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain.
7. *Infringementsof Privacy* Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, informasi penyakit yang dirahasiakan dan sebagainya.

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain: (Deris Setiawan, 2005).

a. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyberspace),* sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya
b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet
c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara

Menurut Setiadi, perbuatan yang dapat dikategorikan sebagai kejahatan di bidang *cyber crime* dapat dibagi menjadi 2 (dua) kategori antara lain:

1. Kejahatan umum yang menjadikan komputer sebagai alat atau sarana (bantu) untuk melakukan kejahatan tersebut. Dalam hal ini langsung atau tidak langsung komputer berperan dalam proses terjadinya tindak pidana lain misalnya;
   a. *Carding* atau penipuan/penyalahgunaan kartu kredit, yaitu penggunaan kartu kredit secara ilegal/tidak sah untuk memesan atau membeli barang via internet dengan cara mencantumkan nomor kartu kredit milik orang lain untuk pembayaran barang yang dipesan.
   b. Penipuan internet *banking*, yaitu melalui media internet melakukan transfer atau pengambilan atau transaksi perbankan dengan menggunakan *website* salah satu bank dan dunia perbankan melalui internet
   c. Pengancaman/Terorisme, yaitu melalui internet dan pemerasan terhadap pihak lain untuk mencapai tujuannya.
   d. Pornografi, yaitu penyebaran gambar porno serta wanita panggilan melalui internet
2. Kejahatan dengan sasaran targetnya adalah fasilitas komputer serta sistem teknologi informasi sehingga komputer selain sebagai sasaran/ korban atau secara umum dikenal sebagai istilah *kacking/cracing* yang menyerang program-program operasi jaringan komputer misalnya:
   a. *Dos Attack* yaitu menyerang sistem operasi pada setiap komputer
   b. *Defacing*, yaitu merubah (menambah dan mengurangi) tampilan suatu *website*/*homepage* tertentu secara ilegal
   c. *Phreking* yaitu penyerangan dengan virus atau *worm* dan program-program jahat lainnya Bonet atau robot *Network* yaitu jaringan dari para pemilik mesin-mesin akan masuk kedalam pusat komputer yang dikontrol oleh pelaku (Budi Raharjo, 2002:32).

Menurut Budi Raharjo selama ini perusahaan pengaman jaringan komputernya banyak menagani masalah kejahatan dunia maya (*cyber crime*) beberapa perbuatan dalam bentuk:

1. Pencurian dan penggunaan *account* internet milik orang lain. Salah satu kesulitan dari sebuah ISP *(internet service provider*/penyedia layanan internet) adalah adanya *account* pelanggan mereka yang

dicuri yang digunakan secara tidak sah. Yang dicuri hanya informasi sehingga orang yang kecurian tidak merasakannya. Pencurian akan terasa efeknya apabila informasi tersebut digunakan oleh yang tidak berhak, akibat pencurian ini pengguna dikenakan biaya atas penggunaan *account* tersebut.

2. Membajak situs web. Kegiatan ini adalah kegiatan yang paling sering dilakukan *cracker* yaitu mengubah halaman web, yang lebih dikenal dengan *deface*. Pembajakan dilakukan dengan mengeksploitasi lubang keamanan suatu situs.
3. *Probing* dan *Port scaning* Salah satu langkah yang dilakukan *cracker* sebelum masuk ke *server* yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan *port scaning* atau *probing* untuk melihat servis-servis apa saja yang tersedia di server target. Yang bersangkutan memang belum melakukan kegiatan pencarian atau penyerangan akan tetapi kegiatan yang dilakukan sudah mencurigakan.
4. Virus Penyebaran virus pada umumnya melalui email, dan sering kali juga orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Kemudian virus ini dikirimkan ke tempat lain melalui emailnya.
5. *Denail of Service (DoS) dan Distributed DoS (DoS*) *attack* DoS *attack* merupakan serangan yang bertujuan untuk melumpuhkan target sehingga tidak dapat memberikan pelayanan. Serangan ini tidak melakukan pencurian, penyadapan atau pemalsuan data akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial.

   DoS attack merupakan peningkatan dari serangan DoS *attack* dengan melakukannya dari puluhan komputer secara serentak. Efek yang dihasilkan lebih dasyat dari DoS *attack* saja.
6. Kejahatan yang berhubungan dengan nama domain (*Domain name*). Nama domain digunakan untuk mengidentifikasikan perusahaan atau merk dagang. Namun banyak orang mencari keuntungan dengan mendaftarkan nama domain perusahaan orang lain dan menjualnya dengan harga yang lebih mahal. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain (Budi Raharjo, 2002:32).

C. PENGATURAN *CYBER CRIME* DI INDONESIA

Indonesia belum memiliki Undang-Undang khusus/*cyber law* yang mengatur mengenai *cybercrime* Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, diantaranya:

a. Kitab Undang-Undang Hukum Pidana Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* yaitu:

1. Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang diambil dengan menggunakan *software card* generator di Internet untuk melakukan transaksi di *ecommerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.
2. Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.
3. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku mengetahui rahasia korban.
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan email kepada teman-teman korban tentang

suatu cerita yang tidak benar atau mengirimkan email ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang terlarang atau *illegal*.
7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet, misalnya kasus-kasus video porno para mahasiswa, pekerja atau pejabat publik.
8. Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
9. Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta

Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi-instruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/*software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp 20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 per keping. Maraknya pembajakan *software* di Indonesia yang terkesan dimaklumi tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah)."

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik.

Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang-Undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

1. Akses ke jaringan telekomunikasi
2. Akses ke jasa telekomunikasi
3. Akses ke jaringan telekomunikasi khusus

d. Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang Nomor 15 Tahun 2002 merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. (Buletin, 2006)

Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Ahmad P Ramli (2005: 55-56) menjelaskan penentuan hukum yang berlaku, dikenal adanya beberapa asas yang dapat digunakan, yaitu:

a. *Subjective territoriality*, yang menekankan bahwa keberlakuan hukum pidana ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
b. *Objective territoriality,* yang menyatakan bahwa hukum yang berlaku adalah akibat utamanya perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
c. *Nationality,* yang menentukan bahwa negara mempunyai yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku tindak pidana.
d. *Passive nationality*, yang menekankan yurisdiksi berdasarkan kewarganegaraan dari korban kejahatan.
e. *Protective principle*, yang menyatakan bahwa berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan diluar wilayahnya. Azas ini pada umumnya diterapkan apabila korbannya adalah negara atau pemerintah.
f. *Universality*, bahwa setiap negara berhak untuk menangkap dan menghukum pelaku kejahatan.

Munculnya kejahatan *cyber crime* merupakan suatu fenomena yang membutuhkan penanggulangan secara cepat dan akurat.

D. UPAYA PENANGANAN KEJAHATAN MAYANTARA (*CYBERCRIME*)

Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang IT. Disamping terdapat perlindungan hukum, terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan. Pemerintah dalam melakukan upaya menanggulangi kejahatan mayantara dengan skala nasional telah menerapkan peraturan Perundang-Undangan yang mengatur secara khusus mengenai IT. Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kejahatan yang tanpa mengenal batas ini bisa saja sangat

membahayakan jika tidak ditanggulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodirnya.

Cybercrime membutuhkan global *action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Adapun langkah penting yang harus dilakukan setiap negara dalam penanggulangan *cybercrime* adalah:

a. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
b. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*
c. Meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya upaya pencegahan kejahatan agar tidak mudah terjadi.
d. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian *ekstradisi* dan *mutual assistance treaties*

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace*, pertama adalah pendekatan teknologi, kedua pendekatan sosial budaya-etika dan ketiga pendekatan hukum. Untuk mengatasi keamanan gangguan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak.

E. SIFAT KEJAHATAN *CYBER CRIME*

Sifat Kejahatan *Cybe crime* dapat digolongkan sebagai berikut (Ramli, 2004)

a. *Cyber crime* sebagai Tindakan Kriminal

Cyber crime sebagai tindakan kriminal merupakan kejahatan yang dilakukan dengan motif kriminalitas yang menggunakan internet sebagai sarana kejahatan seperti pencurian nomor PIN ATM dan *Carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet, dan pemanfaatan media internet (*webserver, mailing list*) untuk menyebarkan material bajakan. Pengirim *e-*

mail anonym yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

b. *Cyber Crime* sebagai Kejahatan abu-abu

Jenis kejahatan di internet masuk ke dalam wilayah "abu-abu"oleh sebab itu sulit menentukan apakah Tindakan ini merupakan Tindakan kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah *probing atau portscanning*. Ini adalah sebutan untuk Tindakan pengintaian terhadap sistem milik orang lain dengan cara mengumpulkan informasi sebanyak-banyaknya dari *system* tersebut untuk disalahgunakan.

Bentuk-bentuk tindak pidana *cyber* dapat dikelompok dalam dua kategori, yaitu:

1. Tindak pidana biasa (konvensional) memakai komputer dan internet sebagai sarana (alat);
2. Tindak pidana baru yang menjadikan komputer dan internet serta perangkatnya sebagai sasaran (objek).

Jadi dalam tindak pidana pertama, tetap merupakan tindak pidana yang sudah dikenal atau diatur dalam KUHP Indonesia, tetapi memakai jaringan komputer dan internet. Sedangkan jenis kedua, memang tindak pidana yang lahir seiring dengan pemakaian komputer dan internet serta perangkatnya.

F. SASARAN KEJAHATAN *CYBER*

Sasaran kejahatan *cyber crime* dapat dikelompokkan sebagai berikut (Hinca, 2005)

a. *Cyber crime* yang menyerang individu (*Againts Person*), Sasaran jenis kejahatan ini ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Salah satu contoh kejahatan ini adalah pornografi yang merupakan kegiatan yang dilakukan dengan membuat, memasang,

mendistribusikan, dan menyebarkan material yang berbau pornografi,cabul serta mengekspos hal-hal yang tidak pantas

b. *Cyberstalkin*g yaitu kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan *computer*, misalnya dengan menggunakan email yang dilakukan secara berulang-ulang seperti halnya *terror* di dunia *cyber*. Gangguan tersebut bisa saja berbau seksual, *religious*, dan lain-lain.
c. *Cyber-Tresspass*, yaitu kegiatan yang dilakukan melanggar norma area privasi orang lain seperti misalnya *web hacking*, *breaking* ke *PC, Probing, Port Scanning.*
d. *Cyber crime* menyerang hak milik *(Againts Property)* yaitu *cyber crime* yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan *computer* secara tidak sah melalui dunia *cyber*, pemilikan informasi elektronik secara tidak sah/pencurian informasi, *carding, cybersquatting, hijacking,* data *forgery* dan segala kegiatan yang bersifat merugikan hak milik orang lain.
e. *Cyber crime* menyerang pemerintah (*Againts Covernment*), dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terrorism* sebagai Tindakan yang mengancam pemerintah termasuk juga *cracking* ke situs resmi pemerintah atau situs militer.

G. RANGKUMAN MATERI

Penegakan hukum yang dilakukan terhadap tindak pidana *cybercrime* dilakukan dengan menerapkan Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Upaya dalam melakukan penanggulangan kejahatan mayantara atau *cybercrime* telah mengacu pada Undang-Undang Informasi dan Transaksi Elektronik, dan berbagai upaya lain seperti upaya preventif seperti pemblokiran, edukasi terhadap masyarakat, dan hal-hal positif lainnya yang dapat mencegah terjadinya suatu kejahatan, serta melakukan upaya represif yang mana upaya ini dilakukan setelah terjadinya suatu tindak pidana, seperti penjatuhan sanksi terhadap pelaku.

TUGAS DAN EVALUASI

1. Jelaskan Pengertian *Cyber Crime* dan pengaturannya
2. Jelaskan bentuk-bentuk *Cyber Crime*
3. Jelaskan bagaimana penanganan kejahatan *Cyber Crime*
4. Jelaskan sasaran kejahatan *Cyber Crime*
5. Jelaskan Faktor Penyebab timbulnya *Cyber Crime* dan Bagaimana Karakteristiknya.
6. Jelaskan Sejarah *Cyber Crime*

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, 2005*, Kejahatan Mayantara (Cyber Crime), P*T. Refika Aditama, Bandung

Agus Rahardjo, 2002, *Cybercrime pemahaman dan upaya pencegahan kejahatan berteknologi*, PT Citra Aditya Bakti , Bandung

Ahmad Ramli, 2004*, Prinsip-prinsip Cyber Law Dan Kendala Hukum Positif Dalam Menanggulangi Cyber Crime*, Fakultas Hukum Universitas Padjajaran, Bandung

Andi Hamzah, 1990, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta

Arief, Barda Nawawi, 2014, *Tindak PIdana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*, Rajawali Press, Jakarta.

Asril Sitompul*, Hukum Internet*, 2001, PT. Citra Aditya Bakti, Bandung

Budi Agus Riswandi, *Hukum Cyberpace*, 2006, Gita Nagari, Yogyakarta.

_____, 2003, *Hukum dan Internet di Indonesia*, UII Yogyakarta

Barda Nawawi Arief, 2006, *Tindak Pidana Mayantara*, PT. Raja Grafindo, Jakarta

Budhijanto, Danrivanto, 2013, *Hukum Telekomunikasi,Penyiaran dan Teknologi Informasi; Regulasi dan Konvergansi,* REfika Aditama, Bandung

Budi Raharjo, 2002. *Memahami Teknologi Informasi,* Elexmedia Komputindo, Jakarta

Deris Setiawan, 2005, *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta

Dikdik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi,* Refika Aditama, Bandung

Edmon Makarim, 2004, *Kompilasi Hukum Telematika*, PT. Raja Grafindo. Jakarta

Hinca, 2005, *Membangun Cyber Law di Indonesia yang Demokratis*, Sinar Grafika, Jakarta

Ramli, Ahmad, M, 2004, *Cyberlaw dan HAKI Dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung.

Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang *Informasi dan Transaksi Elektronik.*

----------, Undang-Undang No 36 Tahun 1999 tentang *Telekomunikasi*

----------, Undang Nomor 15 Tahun 2002 tentang *Tindak Pidana Pencucian Uang*

----------, Undang-Undang No 19 Tahun 2002 tentang *Hak Cipta*

----------., Undang-Undang Nomor 1 Tahun 1946 tentang *Peraturan Hukum Pidana*

GLOSARIUM

A

Agresif: Perilaku menyakiti orang lain baik secara langsung atau tidak langsung

Aspek: Kategori gramatikal verba yang menunjukkan lama dan jenis perbuatan

---

B

Blog: Sarana bagi pengguna untuk menyampaikan buah pikirannya secara bebas dalam sebuah situs *online* yang biasanya milik pribadi atau milik bersama (institusi atau komunitas)

Body Shaming: Perilaku menghina bentuk tubuh orang lain.

Budaya: Kebiasaan untuk menyakiti orang lain sehingga peristiwa *bullying*, *cyberbullying* dan *body shaming* dianggap suatu yang biasa

Bully: Pelaku yang terlibat pada peristiwa *bullying*

Bullying: Perilaku menyakiti seseorang secara fisik, verbal dan psikologis yang dilakukan oleh seorang individu atau kelompok.

C

Cyber Crime: Kejahatan yang terjadi di dunia maya (menggunakan media internet)

Cyber Crime: Kriminal *online*, diartikan sebagai perbuatan yang melanggar hukum yang dilakukan secara *online*.

Cyber Law: Hukum yang mengatur tentang kejahatan-kejahatan yang terjadi di dunia maya

Cyber Law: Istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Istilah lain yang juga digunakan adalah hukum Teknologi Informasi (*Law of Information Techonology*) Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara.

Cyberbullies: Anak-anak yang menjadi pelaku dalam peristiwa *cyberbullying*

Cyberbullying: Perilaku menyakiti orang lain yang dilakukan dengan menggunakan media sosial dan alat elektronik, dengan mengirim pesan fulgar, mengancam, mempermalukan, memberikan komentar negatif, mengirim foto orang lain tanpa izin untuk mempermalukan *Cybervictim*.

Cybervictim: Anak-anak yang menjadi korban dalam peristiwa *cyberbullying*

D

Depresi: Dampak yang diakibatkan dari peristiwa *bullying*, *cyberbullying* dan *body shaming* yang mengakibatkan

Direct Message: Pesan langsung yang dikirim secara *online*

DUHAM: Deklarasi Universal Hak Asasi Manusia atau *The Universal Declaration on Human Rights* adalah deklarasi tentang hak asasi manusia yang dikeluarkan oleh Majelis Umum PBB

Dunia Maya: Ruang informasi dan komunikasi dalam internet

E

Editor: Orang atau program yang melakukan penyuntingan (pengeditan), perubahan pada suatu naskah, berita, audio, gambar, video, film baik di media cetak, media elektronik maupun di media baru

Efek: Dampak yang ditimbulkan oleh tindakan *bullying*, *cyberbullying* dan *body shaming* bagi orang yang terlibat dalam peristiwa tersebut. Seperti *cybervictim* dan *cyberbullies*.

Ekosistem: Suatu sistem ekologi yang terbentuk oleh hubungan timbal balik tak terpisahkan antara makhluk hidup dengan lingkungannya.

Ekstrim: Perilaku yang paling berbahaya dari peristiwa *bullying*, *cyberbullying* dan *body shaming*

Elektronik: Alat yang dibuat berdasarkan prinsip elektronika serta hal atau benda yang menggunakan alat tersebut

Elektronik: Alat yang dibuat berdasarkan prinsip elektronika; hal atau benda yang menggunakan alat-alat yang dibentuk atau bekerja atas dasar elektronika, seperti komputer, laptop dan ponsel.

e-mail: Singkatan dari *electronic mail* atau dalam bahasa Indonesia disebut surat elektronik merupakan sarana dalam mengirim surat yang dilakukan melalui media internet.

Emosional: Perasaan yang menyangkut aspek psikologis yang mengakibatkan gangguan priaku pada *Cybervictim* atau *Cyberbullies*.

Empati: Keadaan mental yang membuat seseorang merasa atau mengidentifikasi dirinya dalam keadaan perasaan atau pikiran yang sama dengan orang atau kelompok lain

Etika Deskriptif: Jenis etika yang berusaha melihat sikap dari individu seseorang dan beberapa hal yang perlu diperjuangkan dan oleh setiap orang dalam meraih nilai kehidupan.

Etika Individual: Bahwa etika dapat memberikan hubungan mengenai kewajiban yang perlu dimiliki oleh individu atas hidupnya sendiri.

Etika: Juga memiliki beberapa arti lain dan juga masing-masing arti tersebut memiliki perbedaan apabila dipandang dari sudut penggunanya.

Etika: Mengenai beberapa peraturan, nilai, proses, norma dan langkah-langkah yang difungsikan menjadi panutan oleh seseorang individu dalam melaksanakan kegiatan sehari-hari.

Etika: Sebuah studi yang menjelaskan dan memahami mengenai hal-hal yang berkaitan dengan sebuah hak dan kewajiban yang menunjukkan tindakan yang positif ataupun negatif.

Etika Normatif: Bahwa etika ini membutuhkan sebuah usaha dalam penentuan dan penetapan dari perbuatan dan perilaku yang ideal.

Etika Sosial: Kebalikan dari individu, tidak hanya menjelaskan tentang tanggung jawab atas dirinya sendiri, namun berkewajiban untuk berperilaku yang pantas sebagai umat manusia.

F

Faktor Ekstern: Faktor yang berasal dari dalam diri *Cybervictim* dan *cyberbullies* sehingga terlibat dalam peristiwa *bullying*, *cyberbullying* dan *body shaming*

Fenomena: Peristiwa luar biasa terjadi pada perilaku *bullying*, *cyberbullying* dan *body shaming*

Fisik: Jasmani atau badan yang menjadi sasaran dalam peristiwa *bullying*.

Fungsi Moral: Juga dapat menjadi kendali dalam mengatur hal-hal yang akan dilakukan di masyarakat. Hukum ini dapat didefinisikan sebagai sebuah aturan yang di dalamnya memuat nilai, norma dan sanksi yang berfungsi untuk mengawasi serta memberikan arahan kepada manusia untuk memiliki tingkah laku yang baik sehingga dapat menciptakan

kehidupan yang adil, tertib dan damai dan tidak kekacauan yang timbul.

G

Gender: Jenis kelamin laki-laki atau perempuan dan bagaimana keterlibatan gender dalam peristiwa *bullying*, *cyberbullying* dan *body shaming*

Globalisasi: Proses masuknya informasi, pemikiran, gaya hidup, dan teknologi ke ruang lingkup dunia.

H

***Hacking*:** Aktivitas penyusupan ke dalam sebuah sistem komputer dan jaringan dengan tujuan untuk menyalahgunakan dan merusak sistem.

HaKI: Hak Atas Kekayaan Intelektual

HAM: Hak Asasi Manusia atau HAM adalah sebuah konsep hukum dan *normative* yang menyatakan bahwa manusia memiliki hak yang melekat pada dirinya karena ia adalah seorang manusia

Hubungan Privasi Ini dengan Orang Lain: Ketika seseorang mampu menentukan seberapa jauh orang tersebut memberikan izin untuk orang lain memasuki kehidupannya dan bagaimana seseorang membuka diri kepada orang lain dikarenakan sebagian besar ketika seseorang terlalu ikut campur dalam kehidupannya akan memberikan rasa nyaman, sehingga adanya privasi ini sebagai hak manusia untuk tidak merasakan tekanan dan gangguan dari orang lain.

Hukum Privat: Suatu hubungan mengolah sebuah hubungan diantara suatu individu dengan individu lainnya atau antar sesama manusia dengan lebih mengarah dan memberikan keutamaan pada kepentingan perorangan.

Hukum Publik: Sebuah aturan dalam mengolah mengenai sebuah hukum yang berkaitan dengan warga negara dengan negara yang di dalamnya terdapat suatu kepentingan yang berguna untuk masyarakat umum.

I

ICCPR: Konvenan Internasional tentang Hak-Hak Sipil dan Politik atau *International Covenant on Civil and Political Rights* adalah sebuah perjanjian multilateral yang ditetapkan oleh Majelis Umum Perserikatan Bangsa-Bangsa berdasarkan Resolusi 2200A pada tanggal 16 Desember 1966

Informasi Elektronik: Satu atau sekumpulan data elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic* data *interchange*, surat elektronik, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, *symbol* atau perporasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya

Instan: Cara yang dilakukan tanpa proses yang lama.

Internet: Jaringan besar yang saling berhubungan dari jaringan-jaringan *computer* yang menghubungkan orang-orang dan komputer-komputer di seluruh dunia, melalui telepon, satelit dan sistem-sistem komunikasi yang lain

Internet: Kependekan dari *interconnection-networking* adalah seluruh jaringan komunikasi yang menggunakan media elektronik, yang saling terhubung menggunakan standar sistem global *Transmission Control Protocol/Internet Protocol Suite* (TCP/IP) sebagai protokol pertukaran paket (*packet switching communication protocol*) untuk melayani miliaran pengguna di seluruh dunia.

Investigasi: Penyelidikan dengan mencatat atau merekam fakta melakukan peninjauan, percobaan, dan sebagainya dengan tujuan memperoleh jawaban atas pertanyaan tentang peristiwa, sifat, atau khasiat suatu zat dan sebagainya.

Investigasi Hukum Cyber: Investigasi hukum pada perusahaan atau instansi bila ada suatu kegiatan yang mencurigakan atau tidak wajar (*fraud*) yang dapat berpotensi sebagai tindak kejahatan.

IPR: *Intellectual Property Right*

ITE: Informasi dan Transaksi Elektronik

J

Jejaring Sosial: Aplikasi yang memungkinkan pengguna untuk terhubung menggunakan profil pribadi atau akun pribadinya, seperti Facebook

Jurnalisme: Kegiatan menghimpun berita, mencari fakta dan melaporkan peristiwa

---

K

Karakteristik: Ciri-ciri yang berbeda. Individu yang saling bergabung akan membentuk kelompok peran individu yang terlibat dalam peristiwa *bullying*, *cyberbullying* dan *body shaming*

KI: Kekayaan Intelektual

Kognitif: Berhubungan dengan atau melibatkan kognisi. Berdasar kepada pengetahuan faktual yang empiris.

Konsekuensi: Akibat dari peristiwa *bullying*, *cyberbullying* dan *body shaming* untuk peran yang terlibat.

Konten: Informasi yang tersedia melalui media atau produk elektronik. Istilah ini umumnya merujuk pada isi dari status facebook, instagram, twitter, youtube dll

Kreator: Pembuat konten

Kriminal: Berkaitan dengan kejahatan (pelanggaran hukum) yang dapat dihukum menurut undang-undang pidana

KUHP: Kitab Undang-Undang Hukum Pidana Sekumpulan peraturan yang mengatur mengenai perbuatan pidana secara material di Indonesia

---

L

M

Media Elektronik: Sarana media massa yang mempergunakan alat elektronik modern, misalnya radio, televisi dan film

Media Sosial: Media sosial merupakan suatu media *online*, dengan para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, wiki, forum, dan dunia virtual

Media: Alat yang digunakan untuk melakukan *cyberbyllying* dan *body shaming*

Menggoda: Kekerasan verbal bentuk yang paling berbahaya dan *bullying* tahan lama

***Misogyny**:* Kebencian atau tidak suka terhadap wanita atau anak perempuan. Misogini dapat diwujudkan dalam berbagai cara, termasuk diskriminasi seksual, fitnah perempuan, kekerasan terhadap perempuan, dan objektifikasi seksual perempuan secara langsung atau *online*.

Moral: Salah satu hukum perilaku yang diterapkan kepada setiap individu dalam bersosialisasi dengan sesamanya sehingga terjalin rasa hormat dan menghormati antar sesama.

Moral: Sebuah hokum dari penerapan perbuatan yang dilakukan oleh masing-masing orang dalam melaksanakan komunikasi dan sosialisasi antar sesama oleh karena itu dapat menumbuhkan perasaan yang saling menghormati atas setiap individu.

N

Negatif: Pengaruh kuat yang mendatangkan akibat merugikan diri sendiri dan orang lain dalam peristiwa *bullying, cyberbullying* dan *body shamming.*

Netizen: Seseorang yang aktif terlibat dalam komunitas maya atau internet pada umumnya

---

O

Online: Segala bentuk komunikasi yang menggunakan, Tetapi secara spesifik mengacu pada obrolan atau percakapan yang terjadi pada peristiwa *cyberbullying* atau *body shamming.*

Opini: Sebuah gagasan atau pikiran untuk menerangkan preferensi atau kecenderungan tertentu terhadap ideologi dan perspektif yang memiliki sifat tidak objektif

---

P

Penyimpangan: Proses, cara, perbuatan menyimpang atau menyimpangkan.

Platform: Rencana kerja; program untuk mencegah dan menangani *bullying*, *cyberbullying* dan *body shaming*

Ponsel: Telepon genggam atau telepon seluler (disingkat ponsel) atau *handphone* (disingkat HP) adalah perangkat telekomunikasi elektronik yang digunakan dalam peristiwa *cyberbullying* atau *body shamming.*

Power: Kekuatan individu yang ditunjukkan dalam peristiwa *bullying*, *cyberbullying* dan *body shaming*

Privasi: Sering disebut dengan *privacy* yang artinya sebagai sebuah kemampuan dari tiap individu atau beberapa kelompok dalam menahan keingintahuannya atas kehidupan pribadi seseorang dan urusan yang dipendam untuk dirinya sendiri dari *public* sehingga memerlukan kontrol penuh atas segala informasi yang masuk mengenai dirinya.

Psikologis: Berkenaan dengan psikologi; bersifat kejiwaan yang diakibatkan oleh peristiwa *bullying*, *cyberbullying* dan *body shaming llying*

Q

R

Rasis: Suatu sistem kepercayaan atau doktrin yang menyatakan bahwa perbedaan biologis yang melekat pada ras manusia menentukan pencapaian budaya atau individu bahwa suatu ras tertentu lebih superior dan memiliki hak untuk mengatur ras yang lainnya sehingga menjadi salah satu *factor* penyebab *bullying* atau *cyberbullying*

Rumor: Gunjingan dapat berkembang dari mulut ke mulut atau dibicarakan di media sosial

---

S

SARA: Akronim dari suku, agama, ras dan antar golongan yang berkembang di masyarakat.

Sebaya: Hampir sama (kekayaannya, kepandaiannya, dan sebagainya); seimbang; sejajar dalam segi usia untuk peran yang terlibat dalam peristiwa *bullying* atau *cyberbullying*.

Substansi: Inti atau isi pokok yang berasal dari bahasa Inggris yaitu *substance*

T

Terisolasi: Usaha untuk mengucilkan individu yang menjadi *victim* dalam peristiwa *bullying* atau *cyberbullying*

Tipologi: Ilmu yang mempelajari tentang pengelompokan berdasarkan tipe atau jenis.

Tradisional: Aksi dan tingkah laku *bullying* yang tidak melibatkan media elektronik, pelaku saling berhadapan.

Transaksi Elektronik: Perbuatan yang dilakukan dengan menggunakan *computer*, jaringan *computer*, dan/atau media elektronik lainnya

Transaksi Elektronik: Perbuatan hukum yang dilakukan dengan menggunakan *computer*, jaringan *computer* dan/atau media elektronik lainnya.

Transmisi: Pengiriman (penerusan) pesan dan sebagainya dari seseorang kepada orang (benda) lain

---

U

UU: Undang-Undang

V

Verbal: Perilaku *bullying*, *cyberbullying* dan *body shaming* melalui perkataan atau ucapan yang ditulis dalam sebuah kolom komentar di media sosial.

Victim: Individu yang terlibat dalam peristiwa *bullying* sebagai korban

Vulgar: Ungkapan atau penggunaan kata yang dianggap tidak sesuai dengan bahasa standar atau merupakan ciri ucapan atau tulisan orang yang tidak terdidik

---

W

WTO: *World Trade Organization*

X

Y

Z

PROFIL PENULIS

Dr. Juanrico Alfaromona Sumarezs Titahelu, S.H., M.H

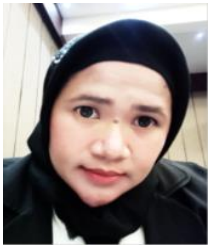
Penulis lahir di Jakarta, 23 November 1980. Penulis merupakan alumnus Fakultas Hukum Universitas Sam Ratulangi Manado dan meraih gelar Sarjana Hukum (S.H) pada tahun 2004. Kemudian melanjutkan studi Magister Ilmu Hukum pada Program Pascasarjana Universitas Sam Ratulangi Manado dan meraih gelar Magister Hukum (M.H) tahun 2006. Tahun 2008 penulis diangkat sebagai CPNS pada Fakultas Hukum Universitas Pattimura Ambon dan tahun 2010 diangkat sebagai PNS dengan status dosen tetap. Penulis kemudian melanjutkan studi S3 dan meraih gelar Doktor Ilmu Hukum pada Program Doktor Fakultas Hukum Universitas Hasanuddin Makassar tahun 2016. Saat penulis dipercayakan sebagai Ketua Bagian Hukum Pidana Fakultas Hukum Universitas Pattimura periode 2020-2024. Beberapa artikel telah banyak diterbitkan di jurnal nasional dan internasional diantaranya *Strengthening Pela-Gandong Alliance Based on John Rawls' Theory of Justice* (2015), *The Essence of Human Rights Violations in Social Conflict in Maluku (After the Riots in 1999)* (2019), *Legal Efforts Of Special Detachment 88 Anti-Terror Investigator, Poice Of Republik Of Indonesia After The Decision Of The Constitutional Court Number 130/PUU/2015* (2021), Kejahatan Terhadap Kekayaan Negara (2021). Selain itu penulis juga aktif dalam kegiatan penelitian dan pengabdian masyarakat. Beberapa *Book Chapter* yang dikerjakan dan diterbitkan oleh Penerbit Widina yaitu Metode Penelitian Hukum (Februari 2023).

Dr. Kasmanto Rinaldi, S.H., M.Si

Penulis lahir pada 11 Mei 1984 di Kota Tengah, Kecamatan Kepenuhan, Kabupaten Rokan Hulu. Beliau Menempuh Pendidikan Sarjana Hukum di Universitas Pancasila Jakarta sampai Tahun 2007 Jakarta. Selanjutnya pada Tahun 2009 dia menamatkan pendidikan Magister Kriminologi di Universitas Indonesia dengan Penelitian di Bareskrim Mabes Polri Terkait Kebijakan Diskresi Dalam Penyidikan Tindak Pidana. Pada tahun

2018 beliau Menyelesaikan Pendidikan Doktoralnya Dalam Bidang Kriminologi di Fisip Universitas Indonesia dengan Disertasi Tentang Korupsi dilihat dari *Cultural* dan *Constitutive Criminology*. Saat ini beliau merupakan Telah meraih Jabatan Fungsional *Associate Profesor* dalam Bidang Kriminologi di Universitas Islam Riau. Selain Menjadi Sekretaris Komisi V Bidang Pembangunan dan Kerjasama Senat Universitas Islam Riau Periode 2021-2025, beliau juga menjabat sebagai Wakil Dekan III Bidang Mahasiswa, Alumni dan Kerjasama di FISIPOL UIR. Dalam keorganisasian, beliau juga beberapa kali terlibat dalam Organisasi Publik antara lain sebagai Tim Pakar dan Narasumber di Humas Polda Riau, Asesor Nasional BKD Dosen, Wakil Ketua Presidium Asosiasi Prodi Kriminologi Indonesia, Ketua Bidang Pengembangan di Organisasi Masyarakat Hukum Pidana dan Kriminologi Riau, Anggota Asosiasi Dosen Pengajar Anti Korupsi Indonesia serta Asosiasi Pengajar Viktimologi Indonesia. Selain mengajar di Program Sarjana Fisipol, Beliau juga tercatat sebagai Dosen pascasarjana Ilmu Hukum Mata Kuliah Kriminologi, Kebijakan Kriminal serta Hukum dan Hak Asasi Manusia. Selain mengajar beliau juga aktif sebagai narasumber berbagai media cetak dan elektronik baik lokal maupun nasional serta telah melakukan berbagai penelitian dan kajian serta juga seringkali mengadakan Konferensi/Seminar/Lokakarya/ Simposium yang berskala Internasional.

Ika Atikah, S.H.I., M.H



Penulis telah menamatkan S1 Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta tahun 2008 dengan IPK 3.58. Kemudian melanjutkan S2 tahun 2009 Program Studi Ilmu Hukum Konsentrasi Hukum Ekonomi dan lulus tahun 2011 dengan IPK 3.52. Bidang keilmuan penulis hukum perdata, hukum ekonomi syariah, hukum jaminan, hukum perjanjian, hukum perbankan, hukum perlindungan konsumen, hukum acara perdata. Penulis bekerja sebagai dosen sejak tahun 2012-sekarang. Tercatat sebagai dosen tetap PNS Fakultas Syariah UIN Sultan Maulana Hasanuddin Banten dan Tutor Program Studi Ilmu Hukum FHISIP UT. Penulis telah menghasilkan karya ilmiah berupa buku Hukum Acara Peradilan Agama, Pengantar Ilmu

Ekonomi, Aspek Hukum dalam Ekonomi, Hukum Pasar Modal, Aspek Hukum Bisnis, Etika Profesi dan Aspek Hukum Kesehatan, Metode Penelitian Hukum, dan *Fintech* Syariah. Selain buku, penulis memiliki karya ilmiah artikel terbit di jurnal bereputasi *Consumer Rights Protection Against Price Gouging During The Covid-19 Pandemic in Indonesia*, Vol. 13 No.2 (2022): UUM *Journal of Legal Studies* (**Scopus Q3**), Implementasi *E-Court* dan Dampaknya Terhadap Advokat Dalam Proses Penyelesaian Perkara di Indonesia *Proceeding-Open Society Conference* 2018, *Consumer Protection And Fintech Companies in Indonesia*: *Innovations and Challenges of The Financial Services Authority*, Jurnal Hukum dan Peradilan 2020 (**Sinta 2**), Penguatan Merger Bank Syariah BUMN dan Dampaknya Dalam Stabilitas Perekonomian Negara, Jurnal Salam: Sosial dan Budaya Syar-I 2021 (**Sinta 4**), Eksistensi Kompilasi Hukum Ekonomi Syariah (KHES)) Sebagai Pedoman Hakim Dalam Menyelesaikan Perkara Ekonomi Syariah Di Pengadilan Agama, Jurnal Muamalatuna 2019 (**Sinta 4**), Perusahaan *leasing* dan *Debt Collector* dalam Penagihan Kredit Macet Kendaraan Debitur, Buletin Adalah UIN JKT, 2018, Peran Pemerintah Terhadap Proteksi Hak-Hak Konsumen dalam Transaksi Ekonomi Syariah, *Prosiding* Seminar Nasional Prodi Hukum Ekonomi Syariah Universitas Muhammadiyah Purwokerto, 2018, *The Urgency of Mortgage Agreement As An Effort to Realize The Trust By Bank As Creditor*, Jurnal Hukum dan Peradilan 2021 (**Sinta 2**), Hak Cipta Sebagai *Collateral* Dalam Jaminan Fidusia, Jurnal Muamalatuna 2019 (**Sinta 5**), Pengaturan Hukum Transaksi Jual Beli Online (*E-Commerce*) di Era Teknologi, Jurnal Muamalatuna 2019 (**Sinta 5**), Hak Cipta Sebagai *Collateral* Dalam Jaminan Fidusia, Jurnal Muamalatuna 2019 (**Sinta 5**), Pengaturan Hukum Transaksi Jual Beli *Online* (*E-Commerce*) di Era Teknologi, Jurnal Muamalatuna 2019 (**Sinta 5**), *Existence of Local Government toward the Implementation of Coaching and Legal Supervision for Franchisee Business*, Jurnal Cita Hukum Fakultas Syariah dan Hukum UIN Jakarta 2018 (**Sinta 2**), Urgensi Perjanjian Hukum Jaminan Hak Tanggungan Sebagai Upaya Perwujudan Kepercayaan Kreditur Lembaga Perbankan di Indonesia, Jurnal Hukum Prioris Universitas Trisakti 2020 (**Sinta 3**), Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia, 2023 (**Sinta 4**), *Intellectual Property Rights as The Resource for Creative Economic in*

Indonesia, Jurnal Penelitian Hukum *De Jure* 2022 (**Sinta 2**), Ilmu Hukum Berparadigma Pancasila di Era Globalisasi: Sebuah Tantangan Liberalisasi Ekonomi dan Teknologi, Jurnal Wajah hukum 2022 (**Sinta 4**), *Urgency of Akad as The Protection of Rahn Consumer*, Jurnal Hukum Islam 2021 (**Sinta 2**), Perlindungan Nasabah Ekonomi Syariah Melalui Transaksi Gadai dalam Perspektif Fiqih Muamalah, Jurnal Hukum Islam 2021 (**Sinta 4**), Parate Eksekusi Obyek Jaminan Hak Tanggungan dalam Rangka Perlindungan Hukum bagi Kreditor Perbankan, Jurnal al-Ahkam 2015 (**Sinta 5**).

La Ode Ali Mustafa, S.H., M.H

Penulis lahir di Buton Sulawesi Tenggara pada tanggal 17 Mei 1966, pendidikan SD Negeri Bola Kabupaten Buton tamat Tahun 1980, SMP Negeri Batauga Buton tamat 1983, SMA PEGRI Kabupaten Buton tamat tahun 1986, lanjut kuliah Strata Satu (S1) Fakultas Hukum Univ Muslim Indonesia Makassar lulus tahun 1993, Strata Dua (S2) Fakultas Hukum Universitas Hasanuddin Makassar lulus tahun 2011. Pada tahun 1994 mengajar di fakultas Hukum Universitas Dayanu Ikhsanuddin, pada tahun 2013 lulus sebagai Dosen Profesional pada Fakultas Hukum Universitas Dayanu Ikhsanuddin Baubau Pada tahun 2004 mengikuti Pelatihan Metodologi Penelitian Dosen Muda di Kopertis Wilayah IX Makassar, Kemudian pada tahun 2008 mengikuti Pelatihan Metodologi Penelitian Kualitatif di Universitas Erlangga. Surabaya. Pengajar Mata Kuliah Hukum Pidana, Delik-delik dalam KUHP, Perbandingan Hukum Pidana, Sistem Peradilan Menduduki jabatan wakil Dekan 2 tahun 2000-2004, Wakil Dekan 1 tahun 2004-2009, Ketua Prodi tahun 2013-2019, Wakil Dekan 2 tahun 2022-2023. Dekan Fakultas Hukum tahun 2023-sekarang.

Dr. Margie Gladies Sopacua, S.H., M.H

Penulis merupakan Dosen tetap pada Fakultas Hukum Universitas Pattimura Ambon sejak tahun 2009, dan lahir di Ambon, tanggal 31 Oktober 1981. Penulis merupakan alumnus Fakultas Hukum Universitas Sam Ratulangi Manado dan meraih gelar Sarjana Hukum (S.H) Pada Tahun 2004, dan melanjutkan studi Magister Ilmu Hukum pada Program Pascasarjana Universitas Sam Ratulangi Manado dengan konsentrasi pada bidang Pidana dan Hak Asasi Manusia dan meraih gelar Magister Hukum (M.H) tahun 2006. Kemudian pada tahun 2016 Penulis melanjutkan studi S3 Doktor ilmu Hukum pada Program Studi Doktor Fakultas Hukum Universitas Hasanuddin Makassar dan meraih gelar Doktor (Dr) pada Tahun 2019, selain itu juga penulis aktif pada Lembaga Bantuan Hukum dan Klinik Hukum (LBHKH) Fakultas Hukum Universitas Pattimura hingga saat ini. Penulis juga giat dalam pelaksanaan Tri Dharma salah satunya menulis pada *book chapter* berjudul "Sosiologi Kesehatan", "Hukum Pidana", "Tindak Pidana Dalam KUHP", "Pengantar Ilmu Hukum", "Pendidikan Anti Korupsi" yang diterbitkan oleh Penerbit Widina Bhakti Persada tahun 2022 dan "Metode Penelitian Hukum" dan Hukum dan HAM"yang diterbitkan oleh Penerbit Widina Bhakti Persada tahun 2023.

Dr. Nanda Dwi Rizkia, S.H., M.H., M.Kn., M.A

Ketertarikan penulis tentang politik dimulai pada tahun 2009 silam. Hal tersebut membuat penulis untuk masuk ke sekolah ilmu hukum di Universitas Islam Bandung, lulus tahun 2009, penulis kemudian melanjutkan pendidikan Program Magister Ilmu Hukum, jurusan hukum bisnis, di Universitas Pancasila, Jakarta, lulus tahun 2016, dan melanjutkan kembali Program Doktor Ilmu Hukum di Universitas Padjajaran, Bandung, lulus tahun 2019. Penulis melanjutkan kembali di 2020 dengan mengambil Magister Kenotariatan Universitas Jayabaya, dan Managemen Administrasi Publik di Institut Ilmu Sosial dan Managemen STIAMI, Depok, Penulis memiliki kepakaran dibidang hukum bisnis, hukum pasar modal, hukum surat

berharga, hukum perusahaan, hukum pajak, hukum hak kekayaan intelektual, hukum perdata, filsafat hukum, teori hukum, dan hukum perdata internasional, Hukum Persaingan Usaha, Hukum Perbankan, Filsafat Hukum, Hukum Adat, Hukum Perikatan, Metodologi Penelitian Hukum, Hukum Jaminan, untuk mewujudkan karier sebagai dosen profesional, dan juga sebagai advokat, penulis pun aktif menulis buku dan beberapa karya ilmiah nasional maupun internasional dengan harapan dapat memberikan kontribusi positif bagi bangsa dan negara yang sangat tercinta ini atas dedikasi dan kerja keras dalam menulis buku. Email Penulis: nandadwirizkia.law@gmail.com

Judy Marria Saimima, S.H., M.H

Penulis lahir di Ambon, 14 Desember 1989..Penulis menamatkan pendidikan sarjana di Fakultas Hukum Universitas Pattimura pada tahun 2011, dan pada tahun 2012 melanjutkan studi di Pascasarjana Program Studi Ilmu Hukum Universitas Pattimura dan memperoleh gelas Magister Hukum pada tahun 2014. Penulis mulai bekerja sebagai dosen tetap Fakultas Hukum Universitas Pattimura, sejak tahun 2018. Ini merupakan karya kedua penulis sebagai akademisi.

Dr. Yanti Amelia Lewerissa, S.H., M.H

Penulis adalah dosen tetap Fakultas Hukum Universitas Pattimura, Ambon. Penulis lahir di Ambon pada tanggal 26 April 1981. Penulis menempuh pendidikan S1 pada Fakultas Hukum Universitas Pattimura, Ambon (lulus Tahun 2004), S2 pada Fakultas Hukum Universitas Diponegoro, Semarang (lulus Tahun 2009) dan S3 pada Fakultas Hukum Universitas Hasanuddin, Makassar (lulus Tahun 2021). Sejumlah penelitian yang pernah penulis *publish* ke jurnal nasional maupun internasional antara lain: *Criminal Policy of Hate Speech in Social Media Against The Religious Dignity of Society in The Digital Century*, *ASSEHR Vol 187, Atlantis Press, 2018*, *Destructive Fishing Criminal Policy in Fisheries Management Area 715 Seram Sea* (*Dialogos*

Journal Vol 25 No 2 Tahun 2021), Kebijakan Kriminal Perburuan Burung Wallacea di Kepulauan Aru (*Jurnal Sasi Vol 27 No 3 Tahun 2021*), *Criminal Policy of The Exploitation of Flying Fish Eggs in Southeast Maluku Waters* (*Jurnal Belo Vol 8 No 1 Tahun 2022*), *Criminal Policy Corruptiom Natural Resources in The Fisheries Sector*, Jurnal Sasi Vol 29 No 1 Tahun 2023, *Social Media and Violence Against Women in Terms of Human Rights Perspective, OSF Preprints*, 2023, Manfaat pemidanaan dalam Penanggulangan Tindak Pidana Narkotika, Jurnal Tatohi, Vol 2 No 12 tahun 2023.

Fahririn, S.H., M.H

Penulis dosen Fakultas Hukum Universitas Sahid, Penulis lahir di Padang tanggal 8 Desember 1992. Penulis adalah dosen tetap pada prodi ilmu hukum Universitas Sahid. Menyelesaikan Pendidikan S1 pada jurusan Ilmu Hukum Universitas Andalas dan melanjutkan S2 pada Jurusan Ilmu hukum Universitas Andalas. Penulis menekuni bidang hukum pidana seperti hukum pidana, Kejahatan Korporasi, tindak pidana korupsi, kriminologi dan viktimologi. Selain mengajar penulis adalah Ketua Lembaga Konsultasi dan Bantuan Hukum universitas sahid yang aktif memberikan pengetahuan seputar hukum disosial media seperti youtube dan tiktok.

Dr. Betsy A Kapugu, S.H., M.H

Penulis lahir di Amurang Minahasa Selatan Sulawesi Utara. Menyelesaikan Pendidikan Strata tiga (S3) di Universitas Hasanuddin pada Tahun 2022. Berprofesi sebagai Dosen tetap pada Fakultas Hukum Universitas Sam Ratulangi Manado.

Dr. Irwanto, S.Pd.T., M.T

Penulis lahir di Jambu, 10 Oktober 1983 merupakan Dosen bidang Pendidikan Vokasional Teknik Elektro, Fakultas Keguruan dan Ilmu Pendidikan (FKIP) Universitas Sultan Ageng Tirtayasa (UNTIRTA), Serang-Banten. Semua Pendidikan mulai dari program Sarjana, Magister dan Doktor di selesaikan di Universitas Negeri Yogyakarta Dengan Jurusan Pendidikan Teknologi dan Kejuruan (PTK). Juga, telah menulis puluhan artikel ilmiah dan ilmiah populer. Ia pernah melakukan studi banding bidang vokasional antara lain, Malaysia, Singapura untuk menambah wawasan studi dalam bidang Pendidikan Vokasional Teknik Elektro (PVTE) tersebut, sehingga keahlian yang dimiliki adalah Manajemen Pendidikan Kejuruan, Psikologi Kejuruan, Pendidikan Teknologi Kejuruan, Media Pembelajaran Kejuruan yang ditekuni sampai sekarang ini.

Stefanus Don Rade, S.H., M.H

Penulis lahir di Kupang, Nusa Tenggara Timur pada tanggal 24 September 1997. Menyelesaikan Taman Kanan-Kanak dan Sekolah Dasar di STA. Maria Assumpta pada tahun 2009, kemudian melanjutkan ke SMP Negeri 8 Kupang tamat tahun 2012, kemudian melanjutkan ke SMA Negeri 2 Kupang tamat tahun 2015 dan melanjutkan studi program sarjana tamat tahun 2019 dan program pascasarjana tamat tahun 2021 dari Fakultas Hukum Universitas Nusa Cendana dengan predikat *cumlaude*. Mengawali karier sebagai advokat setelah lulus sarjana dan karier menjadi seorang dosen pada tahun 2022 di Fakultas Hukum Universitas Katolik Widya Mandira Kupang. Aktif menulis di jurnal nasional maupun jurnal internasional. Penulis bisa dihubungi ke e-mail: stefanusdonrade@unwira.ac.id.

Dr. Deasy Soeikromo, S.H., M.H

Penulis dosen tetap di Fakultas Hukum, Program Magister Ilmu Hukum Universitas Sam Ratulangi Manado. Mendapatkan gelar Sarjana Hukum, pada Fakultas Hukum UNSRAT Manado (1999). Gelar Magister Hukum Pascasarjana UNSRAT (2001), dan Doktor Ilmu Hukum pada Program Pascasarjana UNPAD Bandung (2011). Saat ini menjadi dosen pada program studi S1 Ilmu Hukum dan S2 Hukum Bisnis Fakultas Hukum UNSRAT serta Dosen Hukum Bisnis pada Fakultas Ekonomi dan Bisnis UNSRAT Manado. Pengalaman menulis buku: 1. Pendidikan Kewarganegaraan (*Book Chapter*, Bab. 7) Penerbit Widina Bhakti Persada Bandung, tahun 2022.

Dr. Henny Saida Flora, S.H., M.Hum., M.Kn., M.H.Kes

Penulis merupakan Dosen Fakultas Hukum pada Program Studi Ilmu Hukum Universitas Katolik Santo Thomas Medan, Penulis aktif menulis di Media Cetak, dan juga aktif melakukan penelitian yang diterbitkan di berbagai jurnal nasional maupun Internasional. Penulis juga berprofesi sebagai seorang mediator *non* hakim. Email: hennysaida@yahoo.com

HUKUM CYBER

Setiap negara yang memfasilitasi kehidupan bernegara dengan penggunaan sistem elektronik dan internet yang maju, secara tidak langsung perkembangan *cyber law* di dalamnya turut maju. Hukum Siber atau *Cyber law* erat kaitannya dengan upaya pencegahan tindak pidana dan penanganan tindak pidana. *Cyber law* adalah aspek hukum yang ruang lingkupnya meliputi aspek orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat memasuki dunia maya. *Cyber Law* ini merupakan istilah yang berasal dari *cyberspace law*.

Istilah hukum diartikan sebagai padanan dari kata *cyber law*, yang saat ini secara *international* digunakan untuk istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain yang juga digunakan adalah Hukum TI (*Law of Information Teknologi*), Hukum dunia maya (*Virtual Word Law*), dan Hukum Mayantara.

Kegiatan siber/*cyber* meskipun bersifat virtual dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Kegiatan siber/*cyber* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Dengan demikian subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Sehingga Hukum Siber/*Cyber law* bukan saja keharusan, melainkan sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada sekarang ini, yaitu dengan banyaknya berlangsung kegiatan *cyber crime*.

ISBN 978-623-459-725-7

Penerbit widina
www.penerbitwidina.com