Realita kehidupan masyarakat hari ini harus diakui bukan hanya terjadi dalam dunia nyata atau fisik tetapi juga terjadi pada realitas lain dalam ruang mayantara. Tingginya keingintahuan masyarakat untuk menggali informasi mendorong intensitas yang tinggi pada penggunaan ruang mayantara dalam kehidupan bermasyarakat. Untuk mengakomodasi segala aktivitas masyarakat dalam ruang mayantara tentu demi terciptanya perlindungan hukum, perlu diadakan peraturan yang memuat aturan-aturan dalam ruang mayantara.

Pembahasan mengenai hukum mayantara atau dapat disebut sebagai hukum siber telah dibahas tidak hanya satu atau dua tahun belakangan. Banyak ilmuwan hukum di berbagai negara yang telah menganalisa dan melihat kebutuhan pengaturan hukum pada ruang mayantara. Pengaturan terhadap ruang mayantara adalah sebuah keniscayaan bagi diakomodasinya perlindungan hukum bagi seluruh rakyat.

Buku Hukum Mayantara (Konstitusi Mayantara hingga Pembentukan Kelembagaan) ditulis untuk melengkapi literatur dan kajian ilmiah yang telah ada. Buku ini ditulis dengan mempertimbangkan kebutuhan hukum mayantara di masa yang akan datang sehingga didalamnya terdapat berbagai gagasan mengenai hukum mayantara.

Buku ini diawali dengan pembahasan tentang Dunia Siber yang secara spesifik akan menjelaskan mengenai sejarah dan perkembangan dunia siber di dunia, lalu lapisan yang terdapat dalam dunia siber, serta kaitan dunia siber dengan berbagai aspek kehidupan sosial. Pembahasan kemudian dilanjutkan dengan pembahasan tentang Konstitusi Mayantara yang mengulas tentang konsep Konstitusi Mayantara dan perkembangan konstitusi mayantara di berbagai negara. Konsep ini masih sangat segar untuk dijadikan bahas kajian karena masih sangat minim bahkan belum ada literatur yang membahas mengenai Konstitusi Mayantara sebelumnya. Selanjutnya, dalam pembahasan pada BAB III dibahas mengenai Cyber Crime yang mengulas mengenai kajian teoritis dan tindak pidana pencucian uang digital serta deepfake yang menjadi fenomena kejahatan dalam dunia mayantara saat ini.

Buku ini juga membahas mengenai konsep Data Pribadi yang tidak dapat dilepaskan dari kehidupan masyarakat saat ini. Selain itu pula turut dibahas mengenai Hukum Mayantara di Indonesia yang berlaku saat ini dan juga mengenai gagasan Masa Depan Hukum Mayantara di Indonesia. Pada BAB akhir buku Hukum Mayantara (Konstitusi Mayantara hingga Pembentukan Kelembagaan) dibahas mengenai gagasan segar mengenai Pembentukan Badan Keamanan dan Ketahanan Siber.

PUSTAKA AKSARA

ISBN 978-623-6168-86-8
9 786236 168868

Muhammad Irfan Hilmy, dkk

HUKUM MAYANTARA : KONSTITUSI MAYANTARA HINGGA PEMBENTUKAN KELEMBAGAAN

PUSTAKA AKSARA

PUSTAKA AKSARA

HUKUM MAYANTARA :
Konstitusi Mayantara hingga Pembentukan Kelembagaan

Muhammad Irfan Hilmy, dkk

HUKUM MAYANTARA
Konstitusi Mayantara hingga Pembentukan Kelembagaan

Muhammad Irfan Hilmy
Averos Ananta
Wahyu Mahdi
Atanasya M.
Trian M.

PUSTAKA AKSARA

HUKUM MAYANTARA
Konstitusi Mayantara hingga Pembentukan Kelembagaan

Penulis : Muhammad Irfan Hilmy, Averos Ananta, Wahyu Mahdi, Atanasya M., Trian M.
Desain Sampul : Ikrimah NS
Tata Letak : Adam Akbar

ISBN : 978-623-6168-86-8

Diterbitkan oleh : **PUSTAKA AKSARA, 2021**
Redaksi:
Jl. Karangrejo Sawah IX nomor 17, Surabaya
Telp. 0858-0746-8047
Laman : www.pustakaaksara.co.id
Surel : info@pustakaaksara.co.id

Anggota IKAPI

Cetakan Pertama : 2021

PENGANTAR PENULIS

Perkembangan dunia selama berabad-abad merupakan keniscayaan yang tidak dapat diingkari. Berkembangnya pengetahuan, disisi lain mendorong efisiensi dan efektivitas pekerjaan manusia menjadi lebih mudah. Banyak hal nyata yang dirasakan oleh manusia selama berpuluh tahun kebelakang, misalnya dengan adanya transportasi telah mempermudah manusia untuk berpergian. Bahkan dengan adanya transportasi modern telah mempersingkat waktu berpergian antar benua yang dahulunya dilakukan selama berbulan-bulan. Kemudahan ini menjadi berkah bagi umat manusia karena mendorong fleksibilitas yang tinggi dalam beraktivitas.

Perkembangan pengetahuan juga telah mendorong manusia untuk menciptakan dunia baru yang berada diluar dunia nyata. Dunia tersebut berbeda dari dunia fisik (*physically world*) yang dipahami saat ini, ruang tersebut tidak terlihat secara fisik melainkan beroperasi secara virtual. Dunia itu kemudian dikenal dengan berbagai istilah seperti dunia mayantara ataupun siber.

Keberadaan dunia mayantara menjadi salah satu media penting untuk memudahkan aktivitas manusia. Dunia mayantara juga mendorong hubungan intens antara manusia yang satu dengan yang lainnya. Bahkan dunia mayantara saat ini telah menjadi media untuk mendekatkan pemerintah dengan rakyatnya. Konsep *e-government* yang telah diimplementasikan di berbagai negara telah menunjukkan trend efisiensi dan efektifitas urusan pemerintahan terutama dalam segi administrasi pemerintahan. Tingginya intensitas penggunaan ruang mayantara tentu tidak hanya menghasilkan berkah kemudahan bagi umat manusia, sisi lainnya ruang mayantara telah menggeser banyak tindak pidana yang semula dilakukan didalam dunia fisik menjadi didalam dunia mayantara. Oleh karenanya perlu regulasi lebih komprehensif mengenai kebutuhan menanggapi perkembangan dunia mayantara.

Selain itu perlu juga dilakukan pembatasan melalui Konstitusi terkait hubungan pemerintah dan rakyat dalam dunia

mayantara secara tegas melalui gagasan Konstitusi Mayantara. Hal ini selaras dan sejalan dengan prinsip negara hukum maupun konstitusionalisme untuk melakukan pembatasan terhadap tindakan pemerintah dalam rangka melindungi rakyatnya. Buku ini akan banyak menjelaskan dan memaparkan mengenai hukum mayantara saat ini dan gagasan hukum mayantara di masa yang akan datang. Proses kontemplasi dalam pembuatan buku ini telah menghantarkan beberapa gagasan dalam bidang hukum termasuk salah satunya adalah mengenai Konstitusi Mayantara.

Buku ini juga berisi mengenai rekomendasi amandemen kelima untuk memasukkan gagasan Konstitusi Mayantara ke dalam UUD 1945. Hal ini tidak dapat dipungkiri mengingat perkembangan aktivitas manusia yang pesat, sehingga untuk menjamin perlindungan hukum perlu diatur melalui Konstitusi pembatasan yang jelas dan tegas. Selain itu terdapat gagasan lain seperti pembentukan badan yang khusus mengenai siber sebagai salah satu bentuk terobosan yang aplikatif untuk menangani segala sesuatu persoalan dalam dunia siber.

Perkembangan dunia mayantara mendorong terbitnya buku ini sebagai salah bentuk partisipasi akademis untuk memberikan sumbangsih pemikiran dan pandangan penulis mengenai dunia mayantara. Buku ini ditulis melalui pendekatan hukum yang tekstual dan kontekstual. Selain itu melalui buku ini, penulis menganalisa dengan berbagai perbandingan ketentuan hukum mayantara dengan negara lain. Tidak dapat dipungkiri bahwa ada banyak gagasan cemerlang terkhusus mengenai ruang mayantara yang sudah diterapkan di negara lain namun belum diterapkan di Indonesia. Oleh karenanya perlu ada gagasan terkait hukum mayantara untuk diterapkan di Indonesia.

Medan, 20 April 2021

PENULIS

DAFTAR ISI

BAB I
DUNIA SIBER

A. DUNIA SIBER

Perkembangan teknologi mutakhir memberi harapan baru pada lahirnya berbagai perubahan mendasar dalam berbagai bidang kehidupan dan relasi sosial (Piliang, 2001). Dengan ditemukannya internet di tahun 1969 pola komunikasi masyarakat yang awalnya hanya bisa dilakukan dengan bertatap muka secara langsung ataupun dengan surat-menyurat, perlahan bergeser seiring dengan terciptanya pilihan untuk berkomunikasi secara virtual menggunakan Internet. Ruang yang dapat menghubungkan setiap orang tanpa mengindahkan jarak yang membatasi ini disebut sebagai *Cyberspace* atau Dunia Siber.

Terdapat berbagai definisi mengenai dunia siber, menurut pendapat Benedikt Kitchin (1998) "*Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial, or 'virtual' reality.*" Pandangan berbeda disampaikan oleh Batty, menurut Batty (1997), "*Interactivity between remote computers defines cyberspace... cyberspace is not necessarily imagined space – it is real enough in that it is the space set up by those who use remote computers to communicate.*" Lalu menurut Dodge dan Kitchin (2001) "*The conceptual space within ICTs (information and communication technologies), rather than the technology itself.*" Ada sebuah benang merah dari ketiga definisi di atas, yaitu mengenai konsep ruang nyata yang telah bermetaforis kedalam ruang virtual.

Dunia siber secara sederhana memiliki cakupan dan skala yang luas serta berpengaruh bagi kehidupan manusai. Kondisi ini telah menciptakan sebuah realitas baru bagi hampir semua manusia. Dunia siber juga mendorong pergeseran nilai dan kebiasaan manusia dari bentuk yang konvensional menjadi digital.

Jones (1997) menyebut dunia siber sebagai dunia virtual yang telah menyediakan bentuk baru dari ruang umum (*new*

public space). Dunia siber memberikan penggunanya cara baru untuk berinteraksi baik dalam aspek ekonomi, politik, sosial, dan sebagainya (Camp and Chien, 2000). Realitas di dunia siber inilah yang menjadikan internet sebagai ruang terbuka bagi siapa saja untuk berinteraksi.

Public Space dalam dunia siber sering kali disamakan dengan *public sphere*, walaupun begitu pada kenyataannya dua istilah ini mempunyai sebuah perbedaan mendasar. Papacharissi (2002) menegaskan bahwa "*A virtual space enhances discussion; a virtual sphere enhances democracy*". Konteks dunia siber sebagai *virtual public space* bisa dilihat dari pengguna internet yang menggunakan situs jejaring sosial seperti Facebook dan Twitter sebagai ruang untuk berinteraksi dan menambah relasi sosial baru. Sedangkan perwujudan ruang publik dapat dilihat dari adanya grup-grup diskusi maupun forum perbincangan politik yang diadakan dalam dunia siber.

Dunia siber telah menjelma sebagai ruang virtual yang memfasilitasi publik untuk melakukan berbagai interaksi melalui beragam jenis komunikasi di dalam internet (Trevor Barr, 2000).

Dunia siber merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan komputer (sensor, tranduser, koneksi, transmisi, prosesor, signal, pengontrol) yang dapat menghubungkan peralatan komunikasi (komputer, telepon genggam, instrumentasi elektronik, dan lain-lain) yang tersebar di seluruh penjuru dunia secara interaktif. Istilah dunia siber secara sederhana sering digunakan untuk merujuk pada sebuah jaringan, yang saat ini dikenal dengan nama internet. Definisi dunia siber lebih luas daripada sekedar diksi "internet" yang hanya menjadi salah satu bagian dari dunia siber.

Dunia siber juga meliputi perangkat komputasi, baik yang terhubung dengan internet atau tidak, dan jaringan-jaringan, baik jaringan itu merupakan bagian dari internet ataupun tidak (David Clark, 2014). Misalnya berkomunikasi melalui jaringan telepon GSM, mengganti saluran sebuah

televisi digital atau bahkan saat menggunakan mesin ATM (Jason Whittaker 2004).

Dunia siber adalah suatu ruang konseptual yang tercipta di dalam teknologi informasi dan telekomunikasi yang saling terhubung. Jika dipetakan secara konseptual, dunia siber terdiri dari berbagai elemen yang saling terkait satu sama lain, keterhubungan yang tercipta diantara mereka adalah bentuk dunia siber itu sendiri. Jason Whittaker (2004) memetakan elemen-elemen terkait dalam dunia siber ini menjadi empat (4) bagian, yaitu (1) Teknologi Informatika; (2) Jaringan Telekomunikasi dan Internet; (3) Media, Hiburan dan Kultur; (4) Keuangan.

B. SEJARAH DAN PERKEMBANGAN DUNIA SIBER

Awal revolusi teknologi yang memungkinkan terjadinya bentuk pertukaran informasi dan kegiatan telekomunikasi secara instan ini dapat ditarik hingga saat ditemukannya telegraf ditahun 1836 oleh Samuel Finley Breese Morse, dibandingkan proses komunikasi dan pertukaran informasi menggunakan surat yang dapat memakan waktu berminggu-minggu, teknologi komunikasi menggunakan jaringan kawat ini hanya membutuhkan waktu kurang dari satu hari untuk proses komunikasi dan pertukaran informasi yang terjadi lintas benua.

Selain telegraf, konsep teknologi komunikasi yang proses transmisinya membutuhkan suatu alat sebagai perantara ini juga dapat ditemukan dalam Telepon yang proses transmisinya menggunakan jaringan kabel. Namun berbeda dengan telegraf ataupun telepon (model kuno), cara dunia siber untuk menghubungkan penggunanya dan mentransmisikan komunikasi serta informasi yang dimiliki, tidak lagi bergantung pada sebuah alat transmisi.

Kegiatan telekomunikasi dan informasi ini tentu tidak dapat dilepaskan dari keberadaan internet yang lahir pada masa perang dingin. Selain persaingan dalam kemajuan ekonomi, perang dingin juga menitikberatkan pada persaingan

dalam bidang teknologi di antara negara-negara yang terlibat. Diterbangkannya Sputnik I, satelit pertama yang ditemukan oleh Uni Soviet ditahun 1957, membuat Amerika Serikat merasa tersaingi karena pada masa itu sinyal yang dikeluarkan oleh satelit pertama yang ada di luar angkasa itu mampu ditangkap oleh semua operator radio yang ada di dunia. Di tahun 1958 Presiden Amerika Serikat Dwight D. Eisenhower membentuk Advanced Research Projects Agency (ARPA) agar bisa segera mengungguli perkembangan teknologi yang berhasil diciptakan Uni Soviet karena ditakutkan hal itu akan mengancam keamanan nasional Amerika Serikat.

Di tahun 1961 seorang ilmuwan Massachusetts Institute of Technology (MIT), Leonard Kleinrock, menerbitkan sebuah penelitian tentang memungkinkannya bentuk komunikasi terjadi diantara komputer dengan menggunakan metode yang disebut sambungan paket (Packet Switching), metode ini adalah pengembangan dari sistem yang ditemukan oleh Paul Baran di tahun 1960. Jika *circuit switching*, yang bentuk penggunaannya dapat dijumpai dalam telepon hanya memungkinkan komunikasi antara orang-orang yang sudah ditentukan di awal, berbeda dengan *packet switching* yang memungkinkan terjadinya interaksi sosial melalui jaringan sehingga jalur dari data interaksi yang dapat disimpan dan dipindahkan sebagai paket ini dapat diakses oleh banyak pengguna. Pada tahun selanjutnya seorang peneliti MIT lain bernama J. C. R. Licklider, menerbitkan sebuah penelitian lain tentang memungkinkannya interaksi sosial melalui sebuah jaringan yang disebut Jaringan Komputer Intragalaksi (*Galatic Network*).

Saat itu Amerika Serikat sedang bersiap untuk menghadapi perang yang melibatkan negara blok barat dan blok timur. Lalu muncul persepsi mengenai bagaimana supaya setelah perang terjadi kegiatan komunikasi tetap dapat dilakukan dan bagaimana teknologi ini memungkinkan orang-orang untuk saling berbagi informasi lewat komputer.

Visi J.C.R Licklider tentang *Galatic Network* sebagai jaringan komputer yang memungkinkan komunikasi umum di antara pengguna komputer ini adalah konsep awal dari ARPANET (*Advanced Research Projects Agency Network*) yang merupakan cikal bakal dari Internet. ARPANET yang ditemukan pada tahun 1969, telah menyediakan protokol yang akan menghubungkan komputer di situs yang berbeda dan memiliki ketahanan jaringan file sehingga mampu merutekan ulang informasi jika terjadi kegagalan di bagian mana pun (Hafner dan Lyon 1996; Naughton 1999). Awalnya hanya ada empat Jaringan komputer yang terhubung dalam sebuah *LAN (Local Area Network*) tersendiri, namun dalam perkembangannya jaringan-jaringan LAN ini mulai dihubungkan satu dengan yang lainnya hingga akhirnya membentuk sebuah *WAN (Wide Area Network)* inilah kemudian yang disebut sebagai cikal bakal dari *cyberspace* atau dunia siber.

Walaupun begitu pada awal penemuannya, jumlah komputer yang terhubung dalam jaringan ARPANET masih terbatas karena jaringan komputer ini awalnya hanya di peruntukan bagi kalangan universitas yang ingin berbagi dan berkomunikasi tentang penelitian yang mereka lakukan.

Sepanjang tahun 1970-an tidak ada hal signifikan yang terjadi dalam proses pengembangan jaringan ini, hingga akhirnya pada tahun 1980-an ditemukan *Domain Name System* (DNS). Ditemukannya DNS membawa beberapa perubahan yang semakin memudahkan pengguna untuk menggunakan jaringan. Misalnya sebelum DNS ditemukan untuk mengakses sebuah server, seorang user selain harus menghafal IP dan nama komputer juga harus memasukkan secara manual versi terbaru dari file HOSTS disetiap lokasi jaringan internet. Dengan DNS, alamat IP komputer server secara otomatis akan diterjemahkan menjadi sebuah nama domain. Dengan sistem ini jaringan-jaringan yang ada dalam ARPANET dapat terhubung dengan lebih mudah.

Diperkenalkannya prototipe komputer sederhana yang dapat digunakan sebagai komputer pribadi oleh masyarakat awam diakhir tahun 1970-an memberikan angin segar tentang pemakaian komputer yang bisa digunakan oleh semua orang. Ditemukannya server situs pertama bernama *World Wide Web* di tahun 1989 dan halaman situs pertama di tahun 1991 oleh Tim Berners-Lee, yang bekerja di *European Organization for Nuclear Research* (CERN) adalah awal dari terwujudnya potensi ini. *World Wide Web* (WWW) adalah sebuah bentuk layanan yang dapat diakses melalui Internet. Layanan ini menghubungkan berbagai dokumen dan sumber-sumber lain yang dapat diakses melalui *hyperlink* dan *Uniform Resource Locator* (URL).

Selain penemuan server web pertama ini, Berners-Lee juga telah mengembangkan HTTP dan HTML, sebagai bentuk bahasa pemrograman yang memungkinkan komunikasi antar server web, dan memungkinkan suatu halaman web untuk diedit isinya. WWW awalnya ditujukan agar para ilmuwan dapat saling berbagi informasi secara otomatis, dengan menggunakan WWW memungkinkan para ilmuwan di seluruh dunia untuk mengakses pengetahuan ilmiah secara instan dan bebas, dan saling berkontribusi pada pengetahuan ilmiah dengan saling menambahkan informasi. Perusahaan seperti *National Center for Supercomputer Applications* (NCSA) dan *Netscape*, dalam perkembangannya ikut mengadopsi penemuan Berners-Lee ini dan mempopulerkan penggunaan web bagi lebih banyak orang.

Di tahun 1993, CERN mengeluarkan sebuah pernyataan resmi bahwa hak intelektual dari WWW, dapat digunakan pula oleh masyarakat awam. Pernyataan tegas CERN itu berbunyi, "*CERN relinquishes all intellectual property rights to this code, both source and binary and permission is given to anyone to use, duplicate, modify and distribute it.*" Pernyataan ini telah membuka internet sebagai ruang bebas dimana setiap orang dapat memposting apa pun yang mereka inginkan, sekaligus mengembangkan aplikasi, dan program apapun yang mereka mau di Internet.

Dengan meningkatnya penggunaan komputer hingga menjangkau awam, jumlah jaringan yang terbentuk juga semakin banyak. Pada tahun 1992, komputer yang saling tersambung membentuk jaringan sudah melampaui satu juta komputer dan pada tahun 1994 situs yang ada di dalam internet telah bertumbuh hingga angka 3000 alamat halaman. Sekarang ditahun 2021 ada lebih dari 1,83 miliar situs web di seluruh dunia. Perkembangan pesat ini dipicu oleh segmentasi penggunaan internet yang dewasa ini tidak hanya dapat digunakan sebagai media pertukaran informasi, melainkan telah mencakup perdagangan global, media bersosialisasi, aktivitas politik dan lain sebagainya.

Aharon Kellerman (2007) dalam penelitiannya yang berjudul "*Cyberspace Classification and Cognition: Information and Communications Cyberspaces*" telah membagi dunia siber dalam dua ruang, yaitu *Information cyberspace (IC)* dan *communications cyberspace (CC).*

Information Space atau ruang informasi adalah sebuah set atau sistem informasi berbentuk digital, yang terdiri dari informasi-informasi yang telah terorganisasi dalam ruang khusus seperti halaman website, termasuk halaman utama dan laman pencarian. Dalam *Information space* juga terdapat set informasi digital yang besar, misal dalam bentuk arsip data atau katalog perpustakaan digital. Informasi digital yang ada dalam *information space* (IC) dapat tersimpan dalam bentuk tulisan (tekstual) dan gambar (grafis), informasi ini dapat di jangkau dalam ruang virtual yang ada di dalam dunia siber dan akan terus tersimpan tanpa batas waktu tertentu. Dokumen informasi digital yang tersebar di ruang siber, kebanyakan adalah informasi yang memang dimaksudkan supaya diketahui umum.

Selanjutnya, *Communications cyberspace* (CC) sebagai ruang yang mengakomodasi pengguna dalam ruang siber untuk saling berkomunikasi, lewat berbagai mode komunikasi yang telah tersedia. Komunikasi ini bisa terjadi secara interpersonal ataupun secara terbuka di dalam *Social*

Networking System. Bentuk-bentuk komunikasi interpersonal (privat) dalam dunia siber bisa terjadi lewat komunikasi video, email, fax, SMS, telepon ataupun aplikasi pengiriman pesan, sedangkan komunikasi dalam ruang terbuka (publik) dapat terjadi di Blog ataupun media sosial.

C. LAPISAN DALAM DUNIA SIBER

Internet adalah sebuah bagian dari dunia siber, *US Department of Defense* mendefinisikan dunia siber sebagai domain global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi informasi yang saling bergantung termasuk Internet, jaringan telekomunikasi, sistem komputer, serta prosesor dan pengontrol tertanam. Untuk memahami dunia siber dengan lebih baik, David Clark (2010) telah melakukan pembagian kategori terhadap dunia siber yang mencakup beberapa lapisan. Semua lapisan di bawah ini mempunyai kedudukan yang sama pentingnya. Terdapat keterhubungan yang saling mengikat diantara mereka. Diurutkan dari lapisan terbawah, berikut 4 (empat) lapisan utama di dalam dunia siber:

1. ***The Physical Layer***

   Lapisan fisik adalah fondasi dari dunia siber, lapisan ini mencakup komponen geografis sebagai lokasi fisik elemen jaringan yang dalam hal ini terkait dengan domain komputer dan komponen fisik jaringan yang terkait semua perangkat keras dan komponen fisik lain yang mendukung jaringan, juga konektor fisik.

   Lapisan ini sebagai tempat bagi perangkat keras dibangun atau disusun, seperti PC dan servernya, *supercomputer* dengan jaringan listriknya, sensor dengan transdusernya, serta internet dengan berbagai macam jaringan dan saluran-saluran telekomunikasinya. Komunikasi dalam dunia siber dapat terjadi melalui kabel atau fiber, melalui transmisi radio, atau dengan pengangkutan fisik dari perangkat komputasi dan penyimpanan dari satu tempat ke tempat lain.

2. ***The Logical Layer***

Lapisan logis adalah lapisan atau layer yang mengandung komponen-komponen *logical network* bersifat teknis seperti *Domain Name System (DNS), Directory Services*, dan Protokol-protokol jaringan seperti Protocol TCP/IP. Lapisan logis juga terdiri dari *logical connection* yang ada antara node jaringan. Node adalah perangkat apa pun yang terhubung ke jaringan komputer. Node dapat berupa komputer, telepon seluler, atau berbagai peralatan jaringan lainnya. Pada jaringan protokol Internet (IP), node dimaksudkan pada perangkat apa pun yang memiliki alamat IP

3. ***The Information Layer***

Information layer atau lapisan informasi adalah tempat dapat diaksesnya **informasi** yang tersedia. Informasi di dalam dunia maya terdiri dari bermacam-macam bentuk mulai dari musik dan video, halaman di dalam *world wide web*, hingga transkrip buku dan arsip foto. Karakteristik dari informasi yang ada di dunia siber, dewasa ini telah mengalami beberapa perubahan drastis jika dibandingkan dengan karakteristik informasi saat data pertama kali digunakan dalam komputer. Pemrosesan data sudah dilakukan bahkan ketika komputer belum saling terhubung dalam dunia siber, data-data yang telah diproses ini nantinya akan disimpan dalam sebuah *disk* atau kaset. Awalnya sebuah data atau informasi dianggap bersifat statis, dan harus tersimpan dalam satu bentuk fisik yang khusus.

Dengan adanya dunia siber, meskipun sampai sekarang beberapa pihak masih menggunakan arsip informasi bersifat statis, namun banyak orang yang telah beralih pada arsip informasi yang bersifat dinamis dalam dunia siber. Seorang pengguna dalam dunia siber dapat membuat suatu halaman web miliknya sendiri yang dengan

bebas orang tersebut dapat memasukkan informasi apapun yang ia inginkan.

4. *Lapisan Pengguna*

Lapisan teratas dari dunia siber adalah lapisan tempat orang-orang sebagai pengguna dunia siber berada. Merekalah yang menentukan dan membentuk karakter *cyberspace* dengan berbagai cara. Tidak akan ada halaman *website* tanpa adanya seorang pengguna yang membuatnya. Komponen pengguna di dalam dunia siber, sama pentingnya dengan komponen fisik hingga logis yang telah dijelaskan diatas.

D. DUNIA SIBER DAN BERBAGAI ASPEK KEHIDUPAN SOSIAL

Tidak dapat dipungkiri bahwa dunia siber memiliki peranan yang begitu luas dalam kehidupan modern saat ini. Peran tersebut dapat terlihat dari hadirnya berbagai macam fitur yang berkaitan dengan siber dalam kehidupan masyarakat. Ada beberapa hal yang akan dibahas mengenai dunia siber dalam berbagai aspek kehidupan sosial yakni diantaranya adalah sebagai tekonologi informatika, jaringan telekomunikasi internet, media, hiburan, kultur, dan dalam aspek keuangan.

1. Teknologi Informatika

Teknologi informatika adalah elemen yang bertindak sebagai dasar infrastruktur dari dunia siber. Berbagai perangkat komputasi adalah salah satu bentuk dari perangkat keras yang terkait dengan elemen teknologi informatika dalam dunia siber. Perangkat komputasi sebagai perangkat keras utama ini dapat dirincikan mulai dari komputer, hingga perangkat komputasi *wireless* seperti tablet, pc, laptop, smartphone, dan sejenisnya. Sedangkan perangkat keras pendukung misal, kabel, router, prosesor, satelit dan pengalih jaringan (*network switcher)*

Perangkat-perangkat keras dalam lingkup dunia siber tentu berkaitan erat juga dengan perangkat lunak. Perangkat keras dibantu oleh perangkat-perangkat lunak yang menjalankan suatu sistem operasi yang menciptakan sebuah ruang dalam dunia siber, misal aplikasi browser, pengiriman pesan, media sosial, dan perangkat lunak lain yang menjadi wadah interaksi pengguna dunia siber. Bagian virtual dari dunia siber dibentuk oleh koneksi elektronik dan oleh data yang dikirim antara dan disimpan dalam potongan infrastruktur fisik yang ia miliki.

2. Jaringan Telekomunikasi dan Internet

Dunia siber adalah ruang yang bertransformasi karena adanya jaringan informasi dan komunikasi (Dodge dan Kitchin, 2001). Teknologi informatika sebagai infrastruktur fisik dunia siber adalah hal yang membentuk suatu koneksi jaringan sistem teknologi dan komunikasi. Koneksi ini dibentuk dengan tujuan untuk mentransmisikan, menukar, atau membagikan data dan sumber daya. Misal dua atau lebih komputer yang terkoneksi melalui kabel atau router, akan membentuk suatu jaringan komputer. Koneksi ini juga bisa terbentuk melalui bentuk-bentuk konektivitas nirkabel seperti jaringan telepon seluler, LAN Nirkabel, *Bluetooth, Wi-Fi* dan satelit.

3. Media, Hiburan dan Kultur

Perkembangan teknologi komunikasi dan informatika telah memungkinkan industri media untuk memproduksi jenis media yang lebih beragam, kondisi ini bisa dilihat dari konvergensi media yang tidak terbatas dalam bentuk konvensional saja, dan dapat pula ditemukan dalam bentuk digitalnya. Situs *streaming* musik, film, televisi, game *online*, dan media sosial adalah beberapa contoh dari bentuk digital media berkembang pesat belakangan waktu ini.

Kehadiran dunia siber telah menjadi katalis bagi transformasi yang terjadi di dalam media konvensional. Jika

selama ini proses penyampaian informasi dalam media konvensional tanpa ada timbal balik langsung dari pembaca, saat ini dengan adanya dunia siber para pembaca dapat memberikan umpan balik langsung misalnya melalui kolom komentar. Para pengguna media digital, tidak lagi berposisi sebagai objek yang hanya menerima informasi, tetapi dapat lebih terlibat aktif karena interaksi yang dimungkinkan terjadi dalam dunia siber. Di era media digital khalayak dimungkinkan untuk melakukan umpan balik langsung.

Hubungan virtual dan lingkungan virtual membentuk budaya siber, perkembangan teknologi informasi saat ini telah mencapai titik terbentuknya dunia paralel di dunia nyata (Spielmann, Y. 2000). Manifestasi dari budaya siber meliputi berbagai interaksi manusia yang dimediasi oleh dunia siber. Telah terjadi transformasi atas bentuk interaksi sosial masyarakat yang awalnya terjadi secara nyata (*face-to-face*) sekarang dapat dilakukan melalui sebuah realitas virtual bernama dunia siber sebagai medium interaksi sosialnya. Budaya siber merupakan wujud dari perpaduan yang ada diantara budaya personal komputer, telepon dan internet.

Pierre Levy (2001) mendeskripsikan budaya siber sebagai budaya yang lahir karena interaksi masyarakat dengan internet. Budaya siber dapat disimpulkan sebagai segala bentuk budaya yang tercipta karena penggunaan jaringan komputer sebagai sarana komunikasi, hiburan hingga bisnis.

Salah satu budaya baru dari adanya dunia siber yakni seperti adanya komunitas *online*, *game multiplayer online*, dan jejaring sosial (Bell, 2001).

4. Keuangan

Konsepsi batas wilayah yang tidak lagi berlaku dalam dunia siber telah mendukung globalisasi dan perkembangan ekonomi global. Implementasi teknologi informasi dan

penggunaan internet, dalam kegiatan ekonomi telah menciptakan bentuk-bentuk baru dari kegiatan ekonomi yang terjadi di masyarakat. Hal yang turut dipengaruhi oleh perkembangan teknologi informasi dan komunikasi ini adalah kerja sama lintas Negara (Jeff Madura, 2006).

Informasi yang begitu mudah mengalir, komunikasi yang begitu mudah terjalin menimbulkan minat banyak perusahaan di dunia untuk menjalin kerja sama atau memperluas pasarnya di belahan dunia lain dalam rangka peningkatan laba perusahaannya. Kondisi ini terlihat dari perjanjian-perjanjian perdagangan antar negara yang telah disepakati seperti GATT dan NAFTA. Salah satu bentuk dari interaksi dan kerja sama yang timbul dari negara-negara di dunia ini dapat dilihat dari pasar keuangan internasional. Pasar keuangan internasional merupakan pertemuan antara pembeli dan penjual yang subjeknya adalah antar negara yang bersangkutan, untuk memperdagangkan produk keuangan dalam berbagai cara.

Kemudahan dalam proses perdagangan internasional ini juga didorong oleh sistem perbankan yang ikut menyelenggarakan layanannya di dalam sistem elektronik berbasis teknologi digital yang terkait dengan dunia siber. Salah satu contohnya dapat dilihat dari ATM (*automated teiler machine*) yang beroperasi lewat jaringan intranet intuisi keuangan yang menaunginya.

BAB II
KONSTITUSI MAYANTARA

A. KONSTITUSI DAN KONSTITUSIONALISME

Menurut Carl Schmidt istilah konstitusi mengacu pada berbagai macam penggunaan istilah. Segala sesuatunya baik itu manusia, benda, kegiatan bisnis, dan asosiasi bagaimanapun juga termasuk konstitusi dan juga segala sesuatu yang dikonsepkan dapat memiliki Konstitusi. Arti konstitusi yang teramat luas tersebut akan bias apabila digunakan dalam tulisan ini, oleh karenanya konstitusi yang dimaksud disini bersifat terbatas pada Konstitusi Negara saja. Menurut Schmidt, konstitusi negara itu secara terbatas dapat diartikan sebagai penggambaran suatu negara dan termasuk masyarakatnya, konstitusi juga merupakan konkretisasi persatuan politik, lalu konkretisasi terhadap tipe dan bentuk negara. Secara sederhananya konstitusi merupakan "*complete condition of political unity and order*" (Schmidt, 2008).

Lain hal dengan Hans Kelsen yang mengartikan konstitusi secara formal. Menurutnya, konstitusi merupakan sebuah dokumen yang kemudian dinamakan "Konstitusi" – tertulis – yang tidak hanya memuat norma yang mengatur penciptaan norma hukum, melainkan juga norma-norma tentang subyek lain yang penting secara politis dan norma yang terkandung didalamnya dapat dihapus dengan prosedur khusus dan persyaratan yang lebih ketat daripada norma biasa (Hans Kelsen, 1978). Pandangan normatif Kelsen memang cenderung merujuk pada ketentuan konstitusi tertulis saja.

Pada dasarnya konstitusi-lah yang menjadi hukum tertinggi suatu negara untuk menjadi "rel" acuan bernegara. Pengaturan didalam konstitusi merupakan hal abstrak yang perlu diterjemahkan kedalam peraturan teknis agar dapat dilaksanakan di masyarakat. Oleh karenanya, pelaksanaan terhadap hukum dibawahnya (undang-undang dan peraturan teknis lainnya) harus sesuai, selaras, dan seirama dengan Konstitusi. Hal inilah yang diartikan oleh C.F Strong bahwa :

> "*Constitution is a collection of principles according to which the power of the government, the rights of the foverned, and the relations between the two ar adjusted*" (C.F Strong, 1996).

Sebagai hukum tertinggi pada suatu negara maka keberadaan konstitusi sangatlah penting dalam penyelenggaraan negara. Oleh karenanya Sri Soemantri mengatakan bahwa tidak ada satu negara pun di dunia ini yang tidak mempunyai konstitusi karena keberadaannya yang sangat fundamental. Pentingnya lagi menurut A. Hamid S. Attamimi bahwa konstitusi menjadi pegangan dan pemberi batas terhadap apa yang dijalankan oleh kekuasaan negara (Miriam Budiardjo, 1986).

Konstitusi ini kemudian mewujud untuk melindungi kepentingan rakyat. Apalagi pada negara-negara modern yang sudah mengakui adanya hak asasi manusia yang harus ditegakkan tanpa tebang pilih kepada setiap orang didalam wilayah negara. Dengan konstitusi maka rakyat tidak perlu khawatir dengan tindakan semena-mena penguasa. Hal ini dikarenakan konstitusi menjadi konsensus negara modern dengan masyarakatnya untuk mendirikan sendi-sendi negara. Konsensus itu pula yang mengikatkan negara untuk tidak dapat bertindak bebas tanpa batas, disitulah konstitusi membatasi kehendak perilaku negara agar tidak semena-mena.

Sejarah kelam yang panjang dibawah pendudukan kolonialisme dan imprealisme membuat konstitusi menjadi sesuatu hal yang wajib dimiliki oleh setiap negara saat ini. Bahkan negara-negara monarki saat ini telah bertransformasi menjadi negara monarki yang konstitusional demi kepentingan serta kenyamanan hubungan rakyat dan negara. Konstitusi menjadi sebuah keniscayaan politik untuk membatasi kekuasaan yang tidak terbatas menjadi terbatas agar penyelenggaraan negara dapat berjalan teratur dan tertib.

Dalam sejarahnya, konstitusi memang menjadi alat yang sangat ampuh untuk menjaga ketertiban pemerintah dalam bernegara. Misalnya dalam konstitusi milik Romawi yang membatasi elemen monarki dengan menerapkan prinsip *checks*

and balances dalam pemerintahan. Awalnya, sebelum ada Konstitusi Republik, Romawi dipimpin oleh sebuah monarki yang kemudian raja-rajanya diturunkan secara paksa dari takhta kepemimpinan. Lalu dengan lahirnya Republik sekitar 500 sebelum masehi membatasi kekuasaan monarki yang tidak terbatas tersebut. Memang konstitusi Romawi bukanlah konstitusi tertulis sebagaimana konstitusi yang banyak digunakan saat ini. Konstitusi Romawi merupakan sekumpulan preseden yang diingat maupun tercatat, lalu kumpulan keputusan negarawan, kumpulan adat istiadat, kebiasaan, konsep pemerintahan yang disatukan dengan sejumlah UU. Meskipun dalam perkembangannya, Konstitusi Romawi hanya menjadi sekedar aturan senat belaka karena ada pergeseran dan inkonsistensi terhadap metode pemerintahan bergaya Republik.

Alam Konstitusi modern juga perlu diilhami sebagai sesuatu yang terlihat maupun sesuatu yang tidak terlihat namun nyata adanya. Konstitusi selalu berobjek pada pembatasan praktik pemerintahan yang ada didalam dunia fisik, seperti pembatasan kekuasaan depotisme melalui Konstitusi pada abad pertengahan, lalu pengaturan mengenai hak-hak yang berhubungan dengan dunia fisik. Namun sukar ditemukan ketentuan hak-hak masyarakat dalam dunia mayantara termasuk didalam UUD 1945. Ketentuan mengenai ruang mayantara belum diatur secara tegas didalam UUD 1945 dan cenderung hanya mengakomodir hak yang bersifat fisik saja.

Perlu ada paradigma yang visioner untuk melihat kebutuhan pembatasan dan perlindungan secara rigid yang diatur melalui Konstitusi dalam persoalan dunia mayantara. Jangan sampai pengaturan konstitusi luput pada dunia yang tidak terlihat namun nyata adanya. Perumusan hak secara tegas dalam dunia mayantara melalui konstitusi perlu dirumuskan dan ditegaskan. Mengingat perkembangan dunia saat ini yang semakin mengaburkan batas-batas kedaulatan negara secara digital. Dengan digitalisasi global maka akan ada banyak

kemungkinan terhadap tindakan hukum yang melewati lintas batas negara, bahkan tanpa perlu melalui izin dari otoritas negara.

Selain itu alam konstitusi modern juga perlu untuk mengilhami dan menyadari mengenai kemungkinan adanya gaya pemerintahan digital yang menghubungkan rakyat dengan pemerintahan secara langsung melalui mekanisme digital (seperti mengontrol masyarakat) akan berlangsung secara otoriter. Rujukan otoriter disini bukanlah otoriter yang bersifat fisik belaka seperti tindakan represif fisik, melainkan tindakan otoriter yang terjadi dalam dunia mayantara. Pengaturan konstitusi terhadap dunia mayantara agar tidak terjadi *over controlling* terhadap masyarakat oleh pemerintah secara diam-diam maupun terang-terangan.

Gagasan pengaturan pada alam konstitusi yang bersifat mayantara menjadi hal fundamental untuk mendorong gagasan konstitusionalisme bernegara. Sebagaimana arti konstitusionalisme yang diartikan oleh Walton H. Hamilton yakni "*Constitutionalism is the name given to the trust which men repose in the power of words engrossed on parchment to keep a government ini order*" (Jimly Asshiddiqie, 2018). Pembatasan terhadap pemerintahan adalah niscaya harus dilakukan untuk mendorong penyelenggaraan negara yang menghormati hak-hak rakyatnya. Ketentuan demikianlah yang akan mendorong pembatasan dalam dunia mayantara sehingga terdapat secara tegas pembatasan tindakan pemerintah dalam dunia mayantara.

Dinamika penyelenggaraan negara yang berjalan secara estafet tentu berpotensi akan melahirkan pemerintahan yang otoriter dan semena-mena. Konsep konstitusionalisme akan menengahi dan membatasi jalan tersebut sehingga tindakan pemerintahan yang tidak sejalan dengan hak asasi manusia dapat dihindarkan. Jangan sampai penglihatan yang tidak peka terhadap perubahan zaman hanya akan menjadikan masyarakat sipil sebagai korban dari tindakan otoritarianisme negara yang tidak dilindungi oleh negara. Maka perkembangan

zaman juga perlu dibarengi dengan perkembangan hukum yang dapat mengakomodasi perlindungan hak masyarakat. Pelajaran berharga dapat dipetik dari sejarah konstitusionalisme Yunani yang dianggap tidak memiliki kemampuan untuk bergerak seiring dengan adanya perubahan zaman sekaligus dalam memenuhi kebutuhan baru yang muncul (C.F Strong, 1996).

Konstitusionalisme dalam dunia mayantara perlu dibentuk sebagai kesatuan pandangan yang visioner dalam melihat tantangan dan ancaman terhadap kebebasan masyarakat sipil dimasa yang akan datang. Keniscayaan terhadap zaman ini harus dibarengi juga dengan keniscayaan pada konstitusionalisme mayantara untuk membatasi kekuasaan pemerintah dalam dunia mayantara. Konstitusi yang akan memberikan legitimasi terhadap perlindungan setiap orang dalam dunia mayantara. Tentu selaras dengan cita-cita konstitusionalisme dalam membatasi kekuasaan pemerintah.

Konstitusionalisme modern sejak akhir abad ke-18 yang ditandai melalui lahirnya konstitusi Amerika dan Perancis harus senantiasa diuji dalam menjawab tantangan zaman. Pemberlakuan konstitusi serta muatan yang terdapat didalamnya pada abad ke-18 tentu berbeda dengan urgensi pengaturan muatan konstitusi saat ini. Pemahaman mengenai konstitusi pun tidak sepenuhnya sama dengan masa lampau, misalnya terkait dengan kesetaraan perempuan maupun kebebasan pers. Dunia mayantara sebagai sesuatu yang mutakhir pun perlu ditanggapi secara konstitutif untuk meletakkan gagasan dasar sebagai suatu prinsip konstitusionalisme modern dalam menghadapi tantangan zaman.

B. KONSTITUSI MAYANTARA

Penggunaan kata "konstitusi mayantara" memang masih sangat asing dalam literatur hukum di dunia. Penggunaan kata konstitusi yang diikuti dengan label khusus memang banyak

sekali digunakan dalam beberapa abad kebelakang. Misalnya *green constitution* yang merujuk pada konstitusi yang mengatur persoalan lingkungan (*enviromentalism*), lalu ada gagasan mengenai Konstitusi Ekonomi yang menggambarkan substansi konstitusi yang memuat mengenai gagasan fundamental ekonomi negara, adapula gagasan Konstitusi Keadilan Sosial, dan berbagai penggunaan labelisasi pada konstitusi. Hal tersebut menunjukkan identifikasi mendasar pada arah dan gagasan suatu konstitusi negara.

Berbagai macam gagasan tersebut pada akhirnya ditujukan untuk mendorong prinsip konstitusionalisme. Konstitusi mayantara merujuk pada konstitusi yang berisi pengaturan mengenai ruang mayantara. Ruang mayantara dalam hal ini yakni diantaranya adalah tentang hak privasi, pertahanan negara dalam dunia siber, Keamanan mayantara, yurisdiksi kekuasaan mayantara, *cencorship* dan segala sesuatu yang mengatur tentang ruang mayantara.

Konstitusi mayantara secara *letterlijk* banyak diatur oleh negara-negara di dunia pada abad ke 20 dengan memasukkan ketentuan mengenai ruang mayantara di dalam Konstitusinya. Penggunaan kata *telephone, mail,* dan *faximile* ditemukan dalam beberapa konstitusi negara di dunia. Kata-kata tersebut merujuk pada media dalam dunia mayantara karena sifatnya yang lintas batas dan berada pada dunia yang "ada" namun tidak "nyata". Perkataan *telephone* dalam hal ini mengacu tidak hanya *telephone* kabel saja melainkan *telephone* yang tidak menggunakan kabel, misalnya *handphone*.

Ketentuan dunia mayantara dalam konstitusi menjadi hal penting mengingat transisi dan ekspansi aktivitas manusia kedalam dunia "lain" yang kemudian dikenal sebagai dunia mayantara. Transisi dan ekspansi ini tentu membutuhkan perlindungan hukum yang tegas untuk melindungi serta membatasi kekuasaan negara dalam dunia mayantara. Urgensi memasukkan pengaturan dunia mayantara dalam konstitusi menjadi hal penting karena akan menghindari hal-hal yang mengancam rakyat dan demokrasi yang pelakunya adalah

negara. Pengaturan tersebut dapat mencegah terjadinya tindakan otoriter negara dalam dunia mayantara (digital authoritarianism).

Sebagaimana prinsip konstitusionalisme maka pembatasan dalam dunia mayantara melalui konstitusi adalah hal penting agar hasrat kuasa negara menjadi terbatas. Kecenderungan melakukan pembatasan yang berlebihan dan tidak sesuai hukum dapat terjadi apabila tidak ada konsensus bersama rakyat yang diwujudkan melalui Konstitusi. Isu hangat yang lahir belakangan tahun ini adalah mengenai *cencorship* atau melakukan sensor pada tindakan tertentu. Tindakan *cencorship* ini masuk kedalam ranah pembatasan yang dilakukan oleh negara namun yang perlu dipahami adalah apakah *cencorship* tersebut sesuai dengan hukum atau malah berlawanan dengan hukum.

Censorship dalam dunia konvensional sebenarnya sudah banyak terjadi sebelum adanya dunia mayantara. *Censorship* dalam dunia konvensional apabila dilakukan secara semena-mena tanpa ada dasar hukum atau bahkan berlawanan dengan hukum dapat dilabeli sebagai tindakan yang otoriter dari penguasa. Istilah ini kemudian berkembang dengan perluasan makna tindakan otoriter menjadi *digital authoritarianism*. Perkembangan istilah ini sejalan dengan modernisasi teknologi komunikasi yang menjadi kebutuhan di era modern seperti saat ini.

Tindakan otoriter melalui media digital akan menjadi lebih berbahaya ketimbang dengan otoritarianisme di dunia konvensional. Hal ini dikarenakan pengetahuan serta kesadaran terhadap tindakan *digital authoritarianism* cenderung lebih rendah karena memang pada kenyataannya tidak ada tindakan fisik yang membuat determinasi efek lebih besar untuk mengompori massa. Namun menurut Fredrik Erixon dan Hosuk Lee-Makiyama (2011) tindakan *digital authoritarianism* mengakibatkan efek berjenjang yakni dari keamanan/kestabilan nasional, hubungan luar negeri, hak asasi manusia, dan perdagangan.

Negara-negara yang masih menganut sistem pemerintahan yang otoriter di dunia banyak yang beradaptasi dan mengadopsi sistem otoriter sebagai langkah mendaulat pemerintahan otoriter untuk terus berkuasa dengan cara-cara otoritariannya. Salah satu negara otoriter yang dapat dijadikan contoh dalam kuasa ini adalah Republik Rakyat China (RRC). Pemerintahan China telah menjadikan internet menjadi salah satu cara untuk meningkatkan perekonomian dan perindustrian negaranya, selain itu China telah merubah internet menjadi alat untuk mengontrol dan menstabilkan politik nasional. Hal ini dapat dilihat dengan meningkatnya penangkapan yang berkaitan dengan penggunaan internet, lalu adanya spionase dalam dunia maya, membuat internet menjadi alat kuasa pemerintahan untuk menguasai masyarakatnya bahkan menaruh pengaruh lebih dalam geopolitik di luar negeri (Erixon & Lee-Makiyama, 2011).

Berdasarkan data dari *freedom house,* China menjadi negara yang melanggar kebebasan internet terburuk di dunia pada tahun 2018 karena benar-benar telah mengendalikan secara penuh rakyatnya dengan menggunakan sistem sensor dan pengawasan yang berlebihan sehingga menghilangkan ruang privasi kebebasan manusia di Internet. Cara ini merupakan cara yang kejam untuk menghilangkan kebebasan seseorang di dunia mayantara demi kepentingan untuk mengontrol rakyatnya melalui teknologi. Bahkan China, Rusia, dan beberapa negara otoriter lainnya juga meminta kepada perusahaan yang menyimpan data privasi milik warganya untuk dapat diakses oleh badan keamanan setempat. Lalu beberapa negara lain seperti Mesir dan Iran juga melakukan hal yang mengarah pada *digital authoritarianism* dengan melakukan pembatasan pada media sosial serta pemblokiran atas media sosial dan layanan komunikasi milik asing (Adrian Shahbaz, 2018).

Keadaan di China dan beberapa negara otoriter lainnya menggambarkan praktik *over surveillances* negara terhadap rakyatnya yang menghilangkan ruang privasi bagi setiap

orang. Berbahayanya lagi dalam konteks demokrasi dengan adanya *digital authoritarianism* menjadi salah satu alat bagi *competitive authoritarianism* dalam kepentingan elektoral politik. *Digital authoritarism* dalam praktik *competitive authoritarianism* dapat dilihat dengan masifnya kecurangan dan pengendalian media oleh petahana terhadap lawan politiknya. Indikasi adanya *digital authoritarianism* dalam *competitive authoritanism* adalah spionase terhadap lawan politik, jurnalis, dan kritikus pemerintah melalui ruang mayantara (Levitsky & Lucan A. Way, 2002). Keadaan ini menjadi hambatan bagi demokrasi untuk bertumbuh dan berkembang menjadi sistem yang lebih terbuka kedepannya. Proses elektoral tentu akan menjadi tidak adil dan seimbang, sehingga proses demokrasi hanya akan mengarah pada arah yang oligarkis dan terbatas.

Penggunaan *digital authoritarianism* dalam kuasa otoritarian juga dapat dilihat dalam kudeta yang dilakukan oleh junta militer Myanmar kepada pemerintahan demokrasi. Pasca dilakukannya kudeta, junta militer yang dipimpin oleh Jenderal Min Aung Hlaing telah melakukan pembatasan terhadap ruang mayantara. Beberapa media sosial bahkan diblokir oleh junta militer, seperti Facebook yang diblokir sejak tanggal 4 Februari 2021, lalu sehari setelahnya, Twitter juga diblokir oleh junta militer, bahkan Wikipedia tidak luput dalam blokir junta militer Myanmar pada 18 Februari. Akses internet melalui *mobile data* juga diblokir pada tanggal 15 maret termasuk tiga hari setelahnya junta militer memblokir *public wi-fi* secara bertahap sebelum diblokir penuh dan tidak dapat diakses oleh masyarakat. Junta militer pun tidak segan-segan untuk memblokir semua jaringan pada tanggal 2 April imbas dari meningkatnya serangan kepada junta militer (Andrea Januta & Minami Funakoshi, 2021). Keadaan di Myanmar tidak hanya menunjukkan penguasaan secara otoritarian dalam dunia konvensional melainkan dalam dunia mayantara.

Banyak sekali bentuk dari tindakan *digital authoritarianism* yang banyak tidak disadari dan diketahui karena sifatnya yang tidak kasat mata. Misalnya saja tentang

penggunaan data pribadi masyarakat yang diolah oleh negara dalam usaha-usaha yang berkaitan dengan intelijen dan pertahanan negara. Persoalan mendasar sebenarnya apakah boleh negara dalam rangka intelijen dan pertahanan negara melakukan spionase dan tindakan yang berkenaan dengan data pribadi (pengumpulan, pengolahan, pengendalian) dilakukan secara diam-diam tanpa diketahui oleh masyarakat. Menjawab persoalan ini maka yang perlu diketahui adalah terkait dengan hak privasi dan pembatasan hukum dalam hak-hak yang dapat dilanggar menurut hukum.

Pada dasarnya hak privasi masuk dalam *derogable right* yakni hak yang dapat dibatasi pemenuhannya dalam keadaan darurat. Untuk mengidentifikasi suatu keadaan masuk dalam rezim darurat atau tidak maka menurut Alexander N. Domrin (2006) ada beberapa hal yang perlu diperhatikan yakni bilamana terjadi Invasi asing, bencana, pemogokan dan kerusuhan dibidang vital perekonomian, gangguan penting dalam pelayanan publik, kesulitan dalam bidang ekonomi dan keuangan, tindakan publik yang bertujuan subversi rezim konstitusional, dan pelanggaran serius yang mengancam ketertiban umum dan keamanan.

Pembatasan hak privasi hanya dapat dilakukan apabila terjadi situasi yang dianggap darurat dan mematuhi prinsip-prinsip yang terdapat dalam *siracausa principles* yakni pembatasan terhadap HAM dapat dilakukan dengan adanya keadaan *prescribed by law, in a democratic society, public order, public health, public morals, national security, public safety, rights and freedoms of other or the rights or reputations of others*. Pengaturan mengenai pembatasan ini untuk menjamin tindakan pemerintah dalam rezim darurat dilaksanakan secara demokratis.

Dengan begitu pelanggaran terhadap hak privasi dalam rezim darurat apabila memenuhi *siracausa principles* sebagai prinsip umum tidaklah bertentangan dengan hukum. Namun apabila negara sebagai instrumen kekuasaan yang menggunakan data pribadi untuk kepentingan yang tidak

diketahui masyarakat maka dapat dikategorikan sebagai tindakan *digital authoritarianism.* Masyarakat memiliki hak untuk mendapatkan informasi terkait dengan tujuan penggunaan data oleh pemerintah meskipun untuk alasan-alasan militeristik. Pelanggaran terhadap hak privasi dalam dunia mayantara terkait data pribadi apabila dianalogikan dengan privasi dalam dunia konvensional sebenarnya sama. Misalnya seperti dalam dunia konvensional tidak boleh memasuki rumah orang tanpa seizin pemilik rumah, begitu pula dalam dunia mayantara tidak boleh mengakses data pribadi atau menggunakan data pribadi tanpa seizin pemilik data. Dua hal tersebut mencontohkan keadaan serupa tentang hak untuk mengakses privasi seseorang namun yang membedakan keduanya hanyalah antara dunia konvensional dan dunia mayantara. Kedua hal tersebut dapat pula dilanggar karena ada pembatasan hak menurut hukum misalnya pemerintah dapat masuk kedalam rumah seseorang tanpa izin saat rezim darurat berlaku seperti di Amerika Serikat dan Perancis.

Dalam Konstitusi Mayantara terdapat perluasan perspektif pada aspek kedaulatan negara. Kedaulatan negara yang secara konvensional hanya diartikan daratan dan lautan diperluas maknanya kepada kedaulatan pada ruang mayantara. Kedaulatan negara ini berkaitan pada yurisdiksi negara untuk menetapkan, menegakkan, dan mengadili secara hukum pada wilayah berdaulat (Darrel C. Menthe, 1998). Tindak pidana pun tidak dapat lagi diartikan secara konvensional karena tindakan kejahatan dalam dunia siber ini tidak terbatas pada ruang tertentu. Bisa saja kejahatan dilakukan dari Amerika lalu yang menjadi target adalah Indonesia. Dengan kejahatan yang dilakukan di Amerika, tentu Indonesia tidak memiliki kedaulatan teritorial untuk menegakkan hukum walaupun ada asas nasionalitas pasif dalam hukum pidana namun Indonesia masih perlu melakukan koordinasi salah satunya dengan instrumen *mutual legal assistance* (MLA) atau perjanjian ekstradisi.

Kajian Konstitusi Mayantara dalam hal kedaulatan di ruang mayantara hanya sebatas mengenai status kedaulatan negara terhadap ruang mayantara. Kalau negara memiliki kedaulatan di ruang mayantara, lantas apa yang menjadi batas terhadap yurisdiksi negara dalam ruang mayantara sedangkan mayantara merujuk pada dunia yang tidak berbatas atas ruang sehingga kendali terhadap ruang mayantara dapat dilakukan dimana saja. Ruang mayantara tidak memiliki dimensi fisik sehingga untuk menentukan batasan kedaulatan juga akan rancu karena semua negara dapat mengakses ruang mayantara "milik" negara lain. Misalnya negara Amerika Serikat mengakses situs milik pemerintah Indonesia atau sebaliknya. Hal ini menunjukkan bahwa ruang mayantara tidak memiliki batas dimensi fisik yang jelas.

Ruang mayantara hanya perpaduan jaringan antar komputer, sistem informasi, serta infrastruktur telekomunikasi saja. Banyak kejadian peretasan terhadap situs resmi negara di dunia yang oleh sebagian orang mengklasifikasikan bahwa tindakan tersebut mengganggu kedaulatan negara yang menjadi korban peretasan. Menurut *the U.S International Strategy for Cyberspace* ada beberapa aktivitas yang dianggap memenuhi kualifikasi pelanggaran kedaulatan dalam teritori mayantara, yakni diantaranya adalah serangan pada jaringan, mengeksploitasi jaringan, dan tindakan melalui dunia mayantara yang menyebabkan adanya ancaman terhadap perdamaian, stabilitas, kebebasan publik, dan privasi.

Berbagai macam pelanggaran tersebut dapat disalahkan atas pelanggaran kedaulatan mayantara apabila ruang mayantara tersebut menunjukkan wilayah negara tertentu. Untuk menentukan itu maka menurut Wolff Heintschel Von Heinegg (2012) bahwa yang dimaksud sebagai ruang mayantara yang menjadi kedaulatan negara adalah dunia mayantara yang infrastukturnya terletak pada wilayah suatu negara yang dilindungi prinsip kedaulatan teritorial. Namun yang perlu dikecualikan dalam hal kedaulatan mayantara adalah terhadap objek yang berada diluar angkasa seperti

satelit. Menurutnya infrastruktur siber semacam satelit dalam pelaksanaan kedaulatannya tidak mengacu pada platform atau negara yang membawanya, melainkan mengacu pada registrasi satelit tersebut.

Untuk batasan terhadap garis batas ruang mayantara antar negara terdapat beberapa pendapat salah satunya adalah pendapat Satriyo Wibowo dalam tesisnya yang mengatakan *Network Access Point* (NAP) dan *Internet Exchange Point* (IXP) lebih tepat dikatakan sebagai garis batas ruang mayantara. Menurutnya kedua hal ini lebih tepat dinyatakan sebagai garis batas mayantara karena menjadi titik temu antara *IP Address* nasional dan internasional (Satriyo Wibowo, 2015).

Berkaca dari Amerika Serikat, menurut Darel Menthe ada tiga hal berkaitan dengan yurisdiksi dalam ruang siber yang berlaku di Amerika Serikat, yakni:

1. *Theory of The Uploader and the Downloader* yang menekankan bahwa dalam dunia siber terdapat dua komponen utama yaitu *uploader* (pihak yang memberikan informasi) dan *downloader* (pihak yang mengakses informasi)
2. *Theory of Law of the Server* menjelaskan bahwa penyidik memperlakukan lokasi server halaman web secara fisik dicatat atau disimpan selaku data elektronik.
3. *Theory of International Space* menjelaskan bahwa *cyberspace* dianggap sebagai suatu lingkungan hukum yang terpisah dengan hukum konvensional yang mana setiap negara memiliki kedaulatan yang sama.

Konsep Konstitusi mayantara mendorong pembatasan terhadap aktivitas pemerintah dalam ruang mayantara. Negara-negara di dunia perlu mendorong terselenggaranya konsep pembatasan kekuasaan negara pada ruang mayantara melalui pengaturan dalam konstitusi sebagai usaha menegakkan prinsip konstitusionalisme dalam zaman modern. Konstitusi mayantara juga mendorong prinsip transparansi negara dalam proses pemerintahan yang dijalankan melalui ruang mayantara.

Tidak dapat dipungkiri bahwa gaya pemerintahan dunia saat ini beralih pada gagasan *electronic government* yang mengakibatkan intensitas penggunaan ruang mayantara dalam merumuskan kebijakan publik dan berinteraksi dengan masyarakat semakin tinggi. Maka tentu hak-hak masyarakat dan kewajiban pemerintah dalam ruang mayantara perlu diatur secara rigid. Pasal-pasal hak asasi dalam konstitusi tidak hanya lagi berbicara masalah hak menerima informasi melainkan juga kewajiban pemerintah dalam mengeluarkan informasi yang kredibel dan transparan. Pengaturan mengenai batasan pengolahan data pribadi pun seharusnya dimasukkan dalam konstitusi untuk menjamin proses pengolahan data pribadi yang diolah oleh negara sesuai dengan kesepakatan pengolahan dan terbuka dalam prosesnya.

Urgensi pengaturan Konstitusi mayantara merupakan hal yang mendesak mengingat perkembangan zaman yang pesat. Penggunaan teknologi yang tinggi, pergeseran komunikasi, dan gaya pemerintahan yang bertransformasi ke dalam pemerintahan modern menyebabkan pengaturan dunia mayantara harus diatur dalam Konstitusi demi kepastian hukum.

C. KONSTITUSI MAYANTARA DI BERBAGAI NEGARA

Tidak semua konstitusi di Dunia yang secara tegas mengakui adanya ruang mayantara dalam konstitusinya. UUD 1945 pun tidak mengenal secara *letterlijk* perkataan mayantara atau kalimat yang menyinggung dunia mayantara. Dalam kawasan ASEAN ada dua negara yang dalam konstitusinya menyinggung tentang dunia mayantara. Dalam konstitusi Kamboja dan Vietnam disinggung persoalan hak privasi dalam melakukan komunikasi melalui telepon.

Telepon merupakan salah satu media yang berkaitan dengan dunia siber, telepon disini bukan diartikan sebagai telepon jadul yang masih menggunakan sambungan kabel melainkan telepon yang dipahami saat ini, seperti telepon genggam. Menurut Merriam-Webster:

"*Telephone is an instrument for reproducing sounds at a distancespecifically : one in which sound is converted into electrical impulses for transmission (as by wire or radio waves)*".

Konstitusi Kamboja dan Vietnam mengatur "telepon" dalam konstitusinya sebagai salah satu hak yang melekat kepada setiap individu rakyatnya. Dalam Konstitusi Kamboja hal tersebut tercantum dalam *article 40 The Constitution of the Kingdom of Cambodia* disebutkan "*The protection of the rights to the inviolability of residence and to the confidentiality of correspondences by mail, telegram, telex, facsimile and telephone shall be guaranteed*" . Melihat dari rumusan tersebut yang tercantum dalam Konstitusi Kamboja tidak hanya telepon, melainkan termasuk juga pada surel, telegram, bahkan faximile. Konstitusi Kamboja tersebut menegaskan perlindungan privasi didalam dunia mayantara yang memberikan batas kepada negara untuk masuk ke dalam ruang-ruang privat yang ada didalam dunia mayantara.

Vietnam juga memasukkan ketentuan "telepon" sebagai hak privasi dalam *article 21 The Constitution of the Socialist Republic of Vietnam 2013* yakni "*Everyone enjoys the secrecy of correspondence, telephone conversations, telegrams, and other forms of exchange of personal information*" tidak hanya itu, di dalam Pasal 21 juga dijelaskan bahwa "*No one is illegally allowed to open, control, and confiscate others' correspondence, telephone conversations, telegrams, and other forms of exchange of personal information*".

Dua negara Asia Tenggara tersebut-lah yang telah mengatur secara *letterlijk* hak privasi dalam dunia mayantara. Pengaturan secara *letterlijk* didalam konstitusi negara-negara di dunia mengenai dunia mayantara sebenarnya telah banyak diadopsi. Diantaranya dalam Konstitusi Brazil, Nigeria, Jerman, Afghanistan, Albania, Azerbaijan, Bahamas, Meksiko, Peru, Belanda, Swedia, Serbia, Slovakia, Armenia, Algeria, Romania, Turki, Iran, Kazakhstan, Portugal dan Swiss. Negara-negara tersebut mengatur beberapa media dalam dunia siber seperti

permasalahan jaringan, kebebasan dalam televisi dan radio, jaringan internet, telekomunikasi, bahkan ada yang mengatur persoalan *cencorship* yakni Serbia.

Dalam Konstitusi Brazil pengaturan mengenai dunia mayantara telah diatur sejak tahun 1988 melalui konstitusi 1988. Pengaturan mengenai dunia mayantara di Brazil tidak hanya berkaitan pada hak privasi yang masuk dalam BAB Hak Asasi Manusia melainkan juga pada ruang mayantara sebagai entitas pertahanan. Hal tersebut dapat dilihat dari ketentuan ruang mayantara dalam BAB Pertahanan Negara. Konstitusi Brazil menyatakan secara tegas bahwa tindakan untuk melanggar batas dunia mayantara dapat terjadi apabila ada keadaan darurat. Konstitusi Brazil membolehkan adanya pelanggaran batas terhadap hak didalam dunia mayantara ketika terjadi keadaan darurat yang termuat dalam *Sec. 1 Art. 136 Paragraph 1 Constitution of the Federative Republic of Brazil* yakni "*The decree instituting the state of defense shall determine the period of its duration, shall specify the areas to be encompassed and shall indicate, within the terms and limitations of the law, the coercive measures to be in force from among the following:*

1. *restrictions to the rights of:*
2. *assembly, even if held within associations;*
3. *secrecy of correspondence;*
4. *secrecy of telegraph and telephone communication."*

Muatan dalam Konstitusi Brazil tersebut secara langsung telah memberikan gambaran mengenai Konstitusi Mayantara yang rigid mengatur mengenai pembatasan dan pembolehan terhadap aktivitas masyarakat (hak) dalam dunia mayantara serta pembatasan terhadap hak tersebut ketika dalam keadaan darurat. Dalam perspektif pertahanan negara tentu hal ini sangat penting, memang pelanggaran terhadap hak yang masuk dalam kategori *derogable right* tidak disalahkan dalam keadaan darurat. Namun Konstitusi Brazil memberikan penegasan yang tegas dalam Konstitusinya mengenai hak dalam bertelekomunikasi melalui media siber.

Pengaturan ruang siber dalam konstitusi semata-mata untuk menjaga kebebasan dan nilai hak asasi manusia didalamnya. Keadaan yang paling buruk dalam demokrasi digital perlu diantisipasi dengan pengaturan yang mendasar mengenai dunia siber. Sebagai bahan diskusi yang menarik, dalam konstitusi Serbia dinyatakan secara tegas mengenai *censorship* yang tidak diterapkan di Serbia terhadap media-media. Hal tersebut tertuang dalam *Art. 50 Freedom of Media* yang menyatakan:

> "*Censorship shall not be applied in the Republic of Serbia. Competent court may prevent the dissemination of information through means of public informing only when this is necessary in a democratic society to prevent inciting to violent overthrow of the system established by the Constitution or to prevent violation of territorial integrity of the Republic of Serbia, to prevent propagation of war or instigation to direct violence, or to prevent advocacy of racial, ethnic or religious hatred enticing discrimination, hostility or violence.*"

Censorship menjadi salah satu bentuk praktik dalam *digital authoriatarianism* selain bentuk pengawasan yang berlebihan (*over surveillances)* terhadap media siber dan manipulasi informasi dalam dunia mayantara. Hal ini memang berkaitan dengan tujuan dan kepentingan negara untuk menguasai serta mengontrol informasi di ruang mayantara. China memang menjadi negara modern yang menerapkan *censorship* secara ketat. China melakukan *censorship* dengan melakukan pemblokiran pada VPN, pembatasan terhadap alamat IP, dan berbagai langkah lainnya yang membatasi masyarakat untuk mengakses media asing. China juga secara ketat mengawasi informasi yang beredar di ruang mayantara dengan melakukan *censorship* yang ketat termasuk juga melakukan penghapusan konten serta kritik yang disampaikan kepada pemerintah melalui ruang mayantara. Aktivisme serta kritik terhadap pemerintah yang aktif di internet juga berpotensi berujung pada pidana penjara. Hal ini diakibatkan

kebijakan yang ketat dari pemerintah China untuk mengawasi hal yang demikian.

Dalam mengawasi serta mengontrol aktivitas masyarakatnya di ruang mayantara, China pun menerapkan UU Keamanan Nasional yang dapat memidanakan masyarakat dan perusahaan media sosial yang dianggap kontennya mencerminkan aktivitas pro-demokrasi.

Pengaturan mengenai *censorship* di berbagai Konstitusi negara-negara di dunia memang masih sangat langka. Bahkan dari beberapa negara yang diteliti hanya Serbia yang konstitusinya mengatur mengenai *censorhip*. Pembatasan terhadap *censorship* dalam Konstitusi sebenarnya akan membuka ruang demokrasi dan kebebasan untuk memberi serta mendapatkan informasi menjadi lebih luas. Tindakan negara dalam melakukan penyensoran tentu dapat dibenarkan apabila ada hal-hal yang bertentangan dengan hukum, seperti penyebaran hoax, pelecehan atas orang lain, atau akibat suatu informasi mengakibatkan terlanggarnya hak orang lain. Tindakan *censorship* tidak dapat semata-mata hanya beralasan pada kepentingan pemerintah semata dengan dalih menganggu ketertiban. Dalih seperti itu jangan sampai menjadi alasan untuk membungkam kritik dan informasi yang menerangkan kinerja pemerintah.

Lain hal misalnya dengan Iran, menurut Marcus Michaelsen dalam penelitiannya tentang praktik otoriter digiital di Iran disebabkan karena adanya ancaman siber lintas negara dan terhadap gagasan demokrasi barat yang mendorong Iran untuk menerapkan penyensoran serta pengawasan dalam dunia mayantara. Hal ini dilakukan sebagai alasan keamanan serta pertahanan negara dalam ranah siber. Dalam posisi geopolitik, Iran memang menjadi oposisi negara-negara barat, khususnya Amerika Serikat sehingga mengubah pandangan mereka terhadap dunia mayantara menjadi medan pertempuran strategis yang sewaktu-waktu bisa mengancam instabilitas negaranya (Michaelsen & Glasius, 2018). Tindakan penyensoran ataupun pembatasan Iran terhadap akses media

asing yang dianggap mengancam dapat dibenarkan selama hal tersebut dianggap mengancam kedaulatan negara.

Pembatasan dalam dunia mayantara khususnya penyensoran tidak dapat secara langsung dilabeli sebagai tindakan otoriter. Terlalu prematur apabila mengatakan segala tindakan penyensoran merupakan wujud dari otoriterisasi pemerintah. Keadaan seperti di Iran dapat menjadi alasan pembenar dari tindakan negara untuk melakukan penyensoran yakni dengan alasan kedaulatan negara.

Selain Serbia, negara yang mengatur Konstitusi mayantara lainnya adalah Meksiko. Ketentuan dalam konstitusi Meksiko juga dapat dikatakan sebagai konstitusi yang hampir mendekati ketentuan Konstitusi mayantara. Dalam *Article 6 Mexico Constitution* dijelaskan bahwa

> "*The State shall guarantee access to information and communication technology, access to the services of radio broadcast, telecommunications and broadband Internet. To that end, the State shall establish effective competition conditions for the provision of such services*".

Klausula "*information and communication technology*" menegaskan bahwa negara mengakomodasi perlindungan terhadap masyarakatnya dalam ruang komunikasi dalam mayantara. Memang negara-negara seperti yang disebutkan diatas yang mengatur mengenai Konstitusi Mayantara juga memasukkan klausula seperti *telephone* yang menunjukkan pengaturan terhadap ruang mayantara. Namun klausul *information communication technology* (ICT) dalam Konstitusi Meksiko memiliki arti yang lebih luas dari sebatas komunikasi melalui media *telephone*. Melainkan melindungi pada segala sesuatu yang berkaitan dalam ruang mayantara.

Pengaturan ICT dalam Konstitusi Meksiko lebih luas artinya daripada hanya sebatas telekomunikasi. Menurut K. Ratheeswari, ICT merujuk pada teknologi yang menyediakan akses untuk mendapatkan informasi melalui telekomunikasi. Berbeda dengan *information technology* (IT), ICT cakupannya

lebih luas yakni juga termasuk ke dalam teknologi komunikasi yang didalamnya terdapat jaringan internet, telepon selular, dan perantara komunikasi modern lainnya.

Pengaturan yang lebih luas dalam Konstitusi Meksiko terhadap perlindungan pada ruang siber tentu lebih melegitimasi pembatasan terhadap negara dalam ruang mayantara. Namun dalam praktiknya menurut laporan *Association for Progressive Communications* (APC), ditemukan adanya otoritas yang tidak berwenang menggunakan *malicious software* untuk tujuan *surveillance*. Bahkan pengawasan oleh otoritas tidak berwenang tersebut dilakukan salah satunya adalah untuk melawan lawan politik. Di sisi lain, terdapat banyak pemblokiran dan *censorship* yang belum dilaporkan di Meksiko. Menurut APC, kebebasan berekspresi melalui internet di Meksiko pun turut terancam karena banyak terjadi kekerasan pada jurnalis.

Konstitusi mayantara dalam konstitusi negara-negara di dunia, kebanyakan hanya berkaitan dengan televisi, dan telepon, diantaranya Afghanistan, Nigeria, Albania, Algeria, Azerbaijan, Bahamas, Rep. Democratic Congo, Romania, Kazakhstan, dan Swiss. Ketentuan lain yang ada didalam konstitusi beberapa negara di dunia berkaitan dengan Konstitusi mayantara adalah ketentuan mengenai telekomunikasi. Klausula telekomunikasi dapat ditemukan pada beberapa konstitusi negara di dunia, misal Peru, dan Mexico.

Apabila berkaca definisi telekomunikasi dari Cambridge Dictionary, telekomunikasi diartikan "*the sending and receiving of messages over distance, especially by phone, radio, and television*". Artinya telekomunikasi sifatnya lebih luas daripada penyebutan media siber seperti *phone, radio,* maupun *television*.

Di Peru ketentuan telekomunikasi terdapat dalam *Article 2 Peru Constitution* yang menegaskan bahwa *Communications, telecommunications, or any private correspondence may only be opened, seized, intercepted, or tapped by the authority of a warrant issued by a judge and with all the guarantees provided in the law.*

Any matter unrelated to the circumstances under examination shall be kept secret. Peru mempertegas bahwa ketentuan untuk membuka telekomunikasi hanyalah berdasarkan pengadilan.

Dalam UUD 1945 sendiri secara *letterlijk* memang belum ada klausul yang secara tegas menyatakan Konstitusi Mayantara. Namun bukan berarti hal tersebut tidak melindungi masyarakat dalam beraktivitas di dunia mayantara. Sebenarnya banyak juga diantara konstitusi negara-negara di Dunia yang tidak mencakup klausula dunia mayantara. Namun tidak dimasukkannya klausul yang mengatur dunia mayantara bukan berarti juga meniadakan perlindungan dalam dunia mayantara. Diantara banyak negara termasuk Indonesia, ketentuan seperti itu secara *implisit verbis* terdapat dalam pasal-pasal yang berkaitan dengan hak-hak dasar seseorang.

Di negara-negara lain yang tidak mengatur Konstitusi Mayantara secara *explisit verbis* juga memuatnya dalam hak-hak dasar. Paling sederhana misalnya perihal "*freedom of speech*" yang sifatnya masih sangat luas. Bayangkan saja Konstitusi Amerika Serikat dan Perancis yang dibentuk sebelum dikenalnya sistem jaringan internet yang baru dikenal pada abad 20, tentu arah pembahasannya tidak mengarah kesana namun dalam konteks ke dunia "nyata". Lalu pertanyaannya apakah ketentuan tersebut dapat dianggap juga mengakomodasi ke dalam dunia mayantara? Di beberapa negara memang ketentuan "*freedom of speech*" juga melingkupi dunia mayantara.

Dalam metode penafsiran konstitusi pun tidak hanya bertumpu pada penafsiran *original intent* dari pembentukan konstitusi apabila memang saat pembentukannya tidak ada bahasan menganai dunia mayantara. Penafsiran teleologis dapat menjadi rujukan yang tepat untuk melakukan tafsir konstitusi bila disesuaikan dengan kebutuhan masyarakat. Metode penafsiran ini dapat menjadi pilihan apabila teks konstitusi sebelumnya tidak mengenal maupun membahas dunia mayantara, dengan metode inilah penafsiran konstitusi

disesuaikan dengan hubungan dan perkembangan terhadap situasi sosial yang baru (Sudikno M & A. Pittlo, 1993).

D. KONSTITUSI MAYANTARA DALAM UUD 1945

Memang secara *letterlijk* dalam UUD 1945 tidak ditegaskan klausula mengenai ruang mayantara. Namun apabila ditelusuri melalui *original intent* amandemen UUD 1945, maka dapat ditemukan pembahasan mengenai ruang mayantara. Pembahasan mengenai ruang mayantara dalam proses amandemen juga tidak membahas secara holistik ketentuan yang mengatur ruang mayantara. Selain melalui *original intent,* pengakuan terhadap eksistensi dunia mayantara juga dapat dilihat melalui beberapa Putusan Mahkamah Konstitusi yang mengakui adanya eksistensi dunia mayantara.

Lebih jauh lagi apabila melihat proses dalam risalah sidang BPUPKI dan PPKI juga tidak ditemukan risalah rapat yang membahas tentang dunia mayantara. Proses perdebatan dalam rapat saat itu memang berfokus pada landasan dasar negara seperti bentuk negara maupun ideologi negara. Selain itu juga, pembahasan mengenai ruang mayantara memang belum dikenal sebagaimana ruang mayantara saat ini. Dahulu yang dikenal hanyalah perangkat radio maupun telepon yang belum canggih seperti saat ini. Sehingga kesadaran untuk mengatur ruang mayantara masih jauh dari perbincangan karena paradigma yang terbangun pada masa sidang itu hanyalah paradigma dunia nyata yang memiliki bentuk fisik.

Pada pembahasan proses amandemen UUD 1945, dalam naskah komprehensif buku ke-8 perubahan UUD 1945 ada beberapa poin yang membahas atau menyerempet sedikit mengenai persoalan yang berhubungan dengan dunia siber. Diantaranya ada yang menyinggung mengenai *censorship* dan internet. Dalam salah satu pembahasan mengenai hak untuk mendapatkan dan mengolah informasi disinggung bahwa dalam konteks mendapatkan serta mengolah informasi tersebut tidak boleh bertentangan dengan Ketuhanan Yang Maha Esa. Pembatasan terhadap hak dalam informasi yang demikian

hanya semata-mata bila bertentangan dengan nilai-nilai Ketuhanan. Pendapat tersebut disampaikan sebagai berikut:

> *"Yang kedua, yang berkaitan dengan censorship perkembangan teknologi internet atau segala macam. Menurut saya justru harus ada censorship dalam konteks paham yang bertentangan dengan Ketuhanan Yang Maha Esa. Seperti kalau kita tidak misalkan, kalau Negara ini melindungi dari dekadensi moral generasi muda, pornografi di internet juga harus sebenarnya. Hanya persoalannya mampu atau tidak melakukan sensor di internet itu persoalan lain. Tapi kalau Negara ini punya kesadaran untuk melindungi penduduknya dari hal-hal yang bertentangan dari Ketuhanan Yang Maha Esa, justru itu harus diatur dengan segala upaya yang harus dilakukan. Jadi menurut saya di sini kaitannya dengan HAM menurut saya betul hak mendapatkan informasi mengolah dan lain sebagainya itu memang diatur tapi selalu itu harus dalam konteks tidak bertentangan dengan Ketuhanan Yang Maha Esa karena kita jelas-jelas berdasar atas Ketuhanan Yang Maha Esa."*

Pembahasan tersebut memang bukanlah dalam kerangka utuh untuk membicarakan ruang mayantara melainkan hanya bagian dari satu pembahasan mengenai kebebasan untuk mendapatkan dan mengolah informasi. Meskipun demikian hal tersebut telah menunjukkan bahwa ada kesadaran mengenai penggunaan ruang siber walaupun pembahasannya tidak dilakukan secara khusus dan mendalam.

Masih dalam kerangka hak mendapatkan dan mengolah informasi bahkan diusulkan adanya Badan Sensor yang nantinya akan melakukan penyensoran terhadap penyebaran paham. Hal tersebut diungkapkan oleh Gregorius Seto Harianto dari Fraksi Kebangkitan Kebangsaan Indonesia sebagai berikut:

> *"Berpikir implikasinya nanti kalau ayat ini kita cantumkan dalam Undang Undang Dasar Negara melindungi penduduk dari penyebaran paham-paham dan seterusnya. Salah satu cara penyebaran adalah internet, Koran, dan sebagainya, berarti Negara punya badan sensor. Nanti akan lahir badan sensor*

yang implikasinya bisa macam-macam dengan alasan menjaga supaya anda tidak paham itu ada sensor ini implikasinya bisa berat kemerdekaan pers, ilmu pengetahuan, dan seterusnya ditanyakan oleh Gus Yus tadi. Jadi memang kita harus hati-hati, saya setuju maknanya, saya mengerti, itu saja, tetapi implikasinya bisa sulit itu."

Gregorius Seto Harianto dalam pandangannya tersebut tidak hanya menyinggung pembatasan melalui penyensoran dalam ruang mayantara melainkan juga pada ruang nyata seperti koran. Meskipun begitu memang tidak banyak hal yang dapat digali sebenarnya mengenai perdebatan dalam ruang mayantara melalui naskah komprehensif perubahan karena memang pembahasannya terbatas dan tidak membahas secara khusus mengenai ruang mayantara.

Tidak adanya pembahasan mengenai ruang mayantara secara khusus dalam perubahan UUD 1945, tidak dapat menjadi alasan untuk tidak mengatur mengenai hukum mayantara dalam UU. Hal ini menjadi menarik karena UUD memang tidak secara *explisit verbis* memasukkan diksi-diksi mengenai ruang mayantara, namun sebenarnya turut melindungi hal-hal yang berada dalam ruang mayantara. Hal tersebut dapat dilihat misalnya dari pembentukan UU Informasi dan Transaksi Elektronik yang disahkan pada tanggal 25 Maret 2008 yang kemudian dikenal dengan UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur mengenai persebaran informasi serta transaksi dalam ruang mayantara.

Lalu Mahkamah Konstitusi dalam beberapa putusannya pun secara tegas mengakui adanya ruang mayantara sebagai entitas yang tidak bisa dilepaskan dengan hukum. MK menganggap bahwa ruang mayantara dapat dipersamakan dengan dunia nyata namun dengan media yang berbeda. Hal ini dapat dilihat dalam Putusan MK No 50/PUU-VI/2008 yang berkaitan dengan gugatan atas nama Nariiswandi Piliang alias Iwan Piliang yang menggugat Pasal 27 ayat (3) dan Pasal 45 ayat (1) UU ITE. Pasal *a quo* dianggap sebagai pasal yang

mencengkram kebebasan pemohon selaku wartawan dalam menjalankan tugas jurnalistik di ruang mayantara.

Pemohon mendalilkan bahwa terdapat pertentangan antara Pasal *a quo* dengan beberapa pasal yang ada didalam UUD 1945, seperti Pasal 28D ayat (1), Pasal 28E ayat (2) dan ayat (3), serta Pasal 28F. Dalam pandangannya, MK berpendapat bahwa lahirnya ruang mayantara merupakan konsekuensi dari adanya proses globalisasi. Dari putusan tersebut MK terlihat berorientasi terhadap perlindungan hak orang-orang atas aktivitas yang ada di ruang mayantara sehingga meminimalisir tindakan dalam ruang mayantara yang mengusik nilai-nilai kemanusiaan.

Dalam memandang entitas mayantara, MK menganggap meskipun aktivitas yang terjadi dalam ruang mayantara bukanlah aktivitas layaknya dalam dunia nyata namun aktivitas tersebut masih tetap melibatkan masyarakat yang ada di dunia nyata dan terikat hukum. Oleh karenanya sekalipun ruang mayantara beroperasi penuh secara virtual namun tetap harus ada pembatasan dan pengaturan oleh hukum sehingga aktivitas yang dilakukan dalam ruang mayantara tidak membawa dampak buruk bagi masyarakat.

Mengenai perbedaan mendasar dari ruang mayantara dan dunia nyata, MK berpandangan bahwa pembeda utama antara interaksi di dunia nyata dan dunia mayantara hanyalah perbedaan sudut media yang digunakan. Aktivitas yang dilakukan dalam dunia mayantara juga dapat berdampak pada kehidupan manusia yang berada dalam alam nyata.

Pengaturan dalam ruang mayantara mengenai pembatasan kebebasan berekspresi memang dilematis, di sisi lain pembatasan diperlukan untuk melindungi kehormatan serta hak-hak masyarakat agar tidak dicederai melalui media mayantara. Namun pembatasan dalam ruang mayantara cenderung bersifat sangat luas dan multitafsir, sehingga dapat menjadi "senjata makan tuan" bagi kebebasan di Indonesia.

Selain MK, pemerintah pun memandang aktivitas di ruang mayantara dapat dikategorikan sebagai tindakan atau

perbuatan hukum yang nyata meskipun bersifat virtual. Hal ini disampaikan dalam pemberian keterangan pemerintah pada perkara sidang No 20/PUU-XIV/2016 dengan pemohon atas nama Setya Novanto.

Kalau diukur dengan ukuran *letterlijk* memang ketentuan mengenai Konstitusi Mayantara tidak ada dalam UUD 1945. Namun dalam praktik nyatanya terdapat pengakuan, pembatasan, serta perlindungan terhadap segala aktivitas dalam ruang mayantara. UUD 1945 tidak dapat diartikan secara sempit hanya berdasar pada teks tertulisnya saja, namun harus lebih luas daripada itu. Bukan berarti secara otomatis tidak ada perlindungan di ruang mayantara hanya akibat karena tidak adanya rumusan pasal dalam UUD 1945 yang mengatur secara *letterlijk* klausula ruang mayantara.

Memang kedepannya perlu dirumuskan secara tegas dengan memasukkan klausula ruang mayantara dalam UUD 1945. Pengaturan ini dibutuhkan semata-mata untuk melindungi martabat manusia dalam ruang mayantara. Perkembangan internet dan aktivitas yang dapat menjadi tidak terkendali dalam ruang mayantara perlu disiasati dengan pembentukan hukum dan Konstitusi yang memuat ruang mayantara. Sebagaimana yang disampaikan oleh Geeta Anand (1997) bahwa "*The growing public awareness of the internet is unwieldy and chaotic side has led to calls for regulation and governance*". Oleh karenanya memasukkan rumusan klausula ruang mayantara dalam UUD 1945 akan menegaskan kedudukan atas perlindungan hukum sesuai dengan prinsip-prinsip negara hukum dan konstitusionalisme.

BAB III
CYBER CRIME

A. *CYBER CRIME*

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet dapat dikatakan sebagai *cyber crime* (Ari Juliano Gema, 2000). Dari pengertian tersebut tampak *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif hadirnya aplikasi internet. Definisi ini mencakup seluruh kejahatan yang dalam modus operandinya menggunakan fasilitas intenet.

Penyerangan di dunia siber bermula pada tahun 1988 yang dikenal dengan istilah *cyber attack*. Pada saat itu terdapat seorang mahasiswa yang sukses menciptakan sebuah *worm* atau virus yang menyerang program komputer. Selain itu penyerangan tersebut berhasil mematikan sekitar 10% keseluruhan jumlah komputer yang ada di dunia dan tersambung ke jaringan internet. Hal ini yang menjadikan awal mula *cyber crime* dan sekarang hampir menyerang di semua negara (M. Asrul Azis, 2019).

Kemudian, pada tahun 1994 ditemukan anak berusia 16 tahun bernama Richard Pryce yang dijuluki sebagai "*the hacker*" atau "*Datastream Cowboy*". Dia mendapatkan panggilan tersebut karena masuk secara illegal kedalam ratusan sistem komputer rahasia diantaranya adalah pusat data *Griffits Air Force*, *National Aeronatics and Space Administration* (NASA), dan *Korean Atomic Research Institute*. Setelah dilakukan penyelidikan, diketahui bahwa bocah tersebut belajar *hacking* dan *cracking* dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor. Namun, hingga saat ini keberadaan sang mentor tidak diketahui oleh siapapun (M. Asrul Azis, 2019). Dalam perkembangannya *cyber crime* akan terus ada dan memunculkan "spesies" baru serta harus mendapatkan perhatian khusus dari seluruh penduduk dunia.

Dari literatur dan referensi yang ada menunjukkan bahwasanya munculnya *cyber crime* pertama kali di Indonesia tidak bisa ditentukan secara pasti. Akan tetapi, dapat dikemukakan pada tahun 1990-an merupakan masuknya fenomena *cyber crime* di Indonesia. Menelaah putusan pengadilan, ada yang menyatakan bahwa kasus *cyber crime* pertama kali yang disidangkan di Indonesia adalah kasus pemakaian nama domain mustikaratu.com di Pengadilan Negeri Jakarta Selatan. Kasus ini memperkarakan seorang terdakwa bernama Tjandra Sugijono dengan dakwaan Pasal 382 *bis* KUHP dan Pasal 48 ayat 1 *juncto* Pasal 19 huruf b UU No.5 Tahun 1999 tentang Larangan Praktik Monopoli dan Persaingan Usaha Tidak Sehat. Dalam pemeriksaan tersebut, majelis hakim Pengadilan Negeri Jakarta Selatan memutuskan perbuatan yang didakwakan tidak terbukti sehingga Tjandra Sugijono dibebaskan dari seluruh dakwaan (Muhammad Haidar Ali, 2012).

Terlepas dari hal itu, kasus *cyber crime* di tanah air yang muncul kepermukaan terungkap karena laporan tertangkapnya pelaku kejahatan siber ataupun laporan dari korban yang mengalami kerugian baik materiil ataupun non materiil. Faktanya, awal mula hadirnya *cyber crime* banyak terjadi di kota besar Indonesia. Misalnya, di kota Bandung tak sedikit Warung Internet (warnet) yang dijadikan sebagai sarang *cyber crime*. Tak bisa dipungkiri, Bandung merupakan kota tertinggi kedua setelah Yogyakarta. Warnet di kota tersebut yang terdaftar di Asosiasi Warung Internet (Awari) berkisar 400 warnet dari total 600 warnet yang ada di kota Bandung. Mereka yang tidak tergabung dalam asosiasi tersebut karena memang tidak ada ketentuan yang mewajibkan mereka bergabung dalam suatu wadah organisasi. Adapun kasus *cyber crime* langsung menimpa ketua Asosiasi Warnet Bandung yang menjadi korban *cyber crime* karena warnet miliknya digunakan oleh pelanggan (pelaku) untuk melakukan *carding* yaitu kejahatan internet dengan cara membobol kartu kredit orang lain untuk bertransaksi (Wahid dan Labib,2005).

Praktik *cyber crime* juga terjadi di Yogyakarta dan diberitakan melalui majalah Tempo. Kasus tersebut bermula dari seorang pemuda yang berusia 22 tahun bernama Petrus Pangkur bersama tiga temannya yang sesama *cracker*. Kasusnya terjadi pada sekitar bulan Maret dan April 2001 dimana para pelaku membobol kartu kredit orang lain sebesar Rp. 5 Milyar. Kasus ini terungkap berkat adanya pemberitahuan melalui surat dari Departemen Luar Negeri dan Kepolisian Internasional. Kepolisian wilayah tersebut langsung melakukan pelacakan dan pada akhirnya pelaku dapat ditangkap (Mansur dan Gultom, 2005).

Apabila ditelisik lebih mendalam, Indonesia merupakan negara yang rentan terhadap perang siber. Pada tahun 1998, Indonesia terlibat perang siber dengan Tiongkok dan Taiwan berkaitan dengan konflik sosial dan politik. Kemudian di tahun selanjutnya Indonesia juga terlibat perang siber dengan Portugal mengenai kasus referendum Timor Timur (Manthovani, 2006).

Selain itu, salah satu situs resmi unit kerja Kementerian Pertahanan Republik Indonesia diretas oleh *hacker* yakni *website* milik Direktorat Jenderal Potensi Pertahanan yang mengalami perubahan di bagian laman dan biasa disebut dengan *defacing* (Erwin Kurnia N.M., 2015). Situs tersebut diretas oleh *Cyber Vampire Team* (CVT) dengan menuliskan laman tersebut "*Oops Myanmar Hacker was here*". Kemudian para *hacker* menuliskan kalimat lagi dalam bahasa Inggris, yakni "*Hello Indonesia Government, you should be proud with uneducated Indo script kiddies. Coz they believe (defacing/Ddosing) to other country website is the best solution for them. If you would sympathize the white programmers/developers of your country and how they are feeling. You can catch such script kiddies. Coz CVT are ready to provide those kiddies information*" (Ineu Rahmawati, 2017).

Melihat kenyataan ini, hampir dipastikan *cyber crime* akan terus berkembang pesat di Indonesia seiring dengan penggunaan teknologi dalam seluruh lini kehidupan masyarakat Indonesia. Ketiadaan peraturan perundang-

undangan yang mumpuni dan tumpang tindih kewenangan antar lembaga yang menangani *cyber crime* menjadi salah satu hambatan dalam penanganan kejahatan siber. Diperlukan adanya reformulasi dari seluruh aspek untuk meminimalisir kejahatan siber, walaupun pada hakekatnya *cyber crime* akan terus berkembang seiring pesatnya penggunaan teknologi informasi (TI).

B. KAJIAN TEORI CYBER CRIME

Secara etimologi *cyber crime* berasal dari dua rangkaian kata, yaitu *cyber* dan *crime*. Menurut Kamus Bahasa Inggris-Indonesia *cyber* berarti maya, sedangkan *crime* diartikan dengan kejahatan. Berdasarkan hal tersebut, dapat ditarik kesimpulan bahwasanya *cyber crime* merupakan kejahatan dunia maya (Echols dan Shadily, 2003).

Sedangkan menurut terminologi, terdapat beberapa perbedaan pendapat dari para pakar atau praktisi mengenai definisi *cyber crime*. Indra Safitri mempunyai pandangan bahwa yang dimaksud dengan *cyber crime* adalah jenis kejahatan yang berkaitan dengan pemanfaatan teknologi informasi serta mempunyai karakteristik yang kuat menggunakan rekayasa teknologi dan mengandalkan tingkat keamanan yang tinggi serta kredibilitas dari sebuah informasi yang disampaikan dan dapat diakses oleh pengguna internet (Muhammad Haidar Ali, 2012).

Sementara itu, Kepolisian inggris mengartikan *cyber crime* sebagai segala sesuatu pemakaian jaringan komputer untuk tindakan kriminal dengan menggunakan kemudahan teknologi digital. Dalam beberapa kepustakaan, *cyber crime* juga sering diidentikkan dengan *computer crime*. *The US Departement of justice* memberikan pengertian *computer crime* adalah "*any illegal act requiring knowledge of computer for its perpetration, investigation, or prosecution*". Dimana hal tersebut mempunyai arti setiap perbuatan melanggar hukum yang membutuhkan pengetahuan tentang komputer untuk menangani, menyelidiki, dan untuk menuntutnya (Wahid dan Labib,2005).

Pernyataan senada diungkapkan dalam laporan Kongres Perserikatan Bangsa-Bangsa (PBB) No.10 Tahun 2000 yang menyatakan *cyber crime* ataupun *computer-related crime* mengakomodir secara keseluruhan bentuk baru dari kejahatan yang menyasar pada komputer, jaringan komputer dan pengguna komputer serta bentuk-bentuk kejahatan tradisional yang saat ini ditempuh menggunakan bantuan peralatan komputer. Barda Nawawi Arief juga menyumbangkan pemikirannya yang menggunakan istilah "tindak pidana mayantara" untuk menyebut *cyber crime*. Dengan frasa tindak pidana mayantara dimaksudkan identik dengan tindak pidana di dunia siber (*cyber space*) atau yang biasa juga dikenal dengan istilah "*cyber crime*" (Wahid dan Labib,2005).

Dilihat dari beberapa yang definisi yang telah dipaparkan diatas terlihat bahwasanya setiap pakar mempunyai perspektifnya masing-masing tentang *cyber crime* atau kejahatan dunia siber. Sebagaimana yang dikatakan Muladi bahwa hingga detik ini belum ada parameter baku mengenai definisi *cyber crime* (Wahid dan Labib,2005). Selain itu dapat pula dikatakan bahwa *cyber crime* memiliki karakteristik yang khas dibandingkan kejahatan konvensional, yaitu:

1. Perbuatan dilakukan menggunakan peralatan apapun yang berhubungan dengan internet.
2. Perbuatan dilakukan secara illegal, tidak etis dan tanpa hak tersebut terjadi dalam ruang siber sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
3. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
4. *Cyber crime* mengakibatkan kerugian materiil maupun immaterial (waktu, nilai, jasa, uang, barang, martabat, harga diri, kerahasiaan informasi yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
5. Perbuatan tersebut sering dilakukan secara transnasional (melintasi batas negara). (Ari Juliano Gema, 2000)

Dalam kajian strategis keamanan siber nasional *cyber crime* didefinisikan sebagai setiap situasi dan kondisi serta kemampuan yang dinilai dapat melakukan serangan ataupun segala sesuatu yang merugikan sehingga mengancam kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sistem informasi (Iwan dkk, 2012).

Cyber crime adalah sebuah istilah untuk menggambarkan aktivitas kejahatan yang menggunakan jaringan komputer selaku alat, tujuan ataupun tempat terjadinya kejahatan tersebut. Sejak aktivitas manusia yang dialihkan ke dunia siber efek dari Pandemi COVID-19, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 88.414.296 serangan digital di Indonesia antara 1 Januari-12 April 2020, dengan jenis serangan terbanyak yakni *Trojan Activity* sebanyak 56% (Fauzan Hanafi, 2021). Pihak INTERPOL melaporkan hal yang serupa bahwa pandemi ini telah meluweskan pelaku untuk melakukan kegiatan penyerangan siber seperti pencurian data, penipuan komersil, hingga penyebaran informasi hoax (INTERPOL, diakses pada 13 April 2021). Hal ini menimbulkan kekhawatiran mengingat masifnya peningkatan pengguna *Internet* yang berbanding lurus dengan penggunaan aplikasi media sosial dan *e-commerce* di Indonesia. Mengacu data dari *Digital 2020 October Global Statshor Report*, terdapat 160 juta pengguna media sosial di Indonesia pada Januari 2020 yang berarti jumlah pengguna media sosial di Indonesia meningkat 12 juta (+ 8,1%) antara April 2019 dan Quartal pertama 2020 dan menimbulan kenaikan signifikan terhadap pengguna *Internet* global sebesar 60% dari total populasi dunia sebanyak 7,81 miliar orang. Sedangkan untuk pengguna *e-commerce* di Indonesia, per-Oktober 2020 sebesar 87% dari total pengguna Internet yang berusia 16 – 18 tahun, dan 79% diantaranya menggunakan smartphone (We Are Social, 2020)

Terdapat beberapa faktor yang menyebabkan penanganan kejahatan di dunia maya membutuhkan penanganan yang komprehensif salah satunya berasal dari

karakteristik *cyber crime* itu sendiri. Adapun ciri-ciri khusus dari *cyber crime* adalah:

1. *Non-Violence* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik (*Minimize of physical contact*);
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. (Tubagus Ronny Rahman Nitibaskara, 2001)

Apabila melihat ciri ke-3 dan ke-4 yaitu menggunakan peralatan dan teknologi serta memanfaatkan jaringan telematika global, tampak jelas bahwasanya *cyber crime* dapat dilakukan dimana saja, kapan saja serta berdampak kemana saja, seakan-akan tanpa batas (*borderless*). Hal tersebutlah yang menjadikan *cyber crime* sebagai salah satu dari kejahatan transnasional. Adapun jenis-jenis kejahatan yang termasuk dalam kategori cyber crime diantaranya:

1. *Cyber-terorism: National Police Agency of Japan* (NPA) mendefinisikan *cyber-terorism* sebagai *electronic attacks through computer network against critical infrastructures that have potential critical effects on social and economic activities of the nation.*
2. *Cyber-pornography*. Penyebarluasan *obscene materials* termasuk *pornography*, *indecent exposure*, dan *child pornography*.
3. *Cyber-harrasment*: Pelecehan seksual melalui *e-mail, websites*, atau *chat programs*.
4. *Cyber-stalking*: *Crimes of talking* melalui penggunaan komputer dan internet.
5. *Hacking*: penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum.
6. *Carding* ("*credit-card fraud*"): melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. *Carding* terjadi pada seseorang dimana dia bukan pemilik kartu kredit lalu menggunakan kartu kredit tersebut secara melawan hukum. (Mansur dan Gultom, 2005)

Sementara itu, *cyber crime* menurut Sutanto terdiri dari dua jenis, yaitu:

1. Kejahatan yang menggunakan Teknologi Informasi sebagai fasilitas. Contoh konkret *cyber crime* jenis ini adalah pembajakan, pornografi, pemalsuan dan pencurian kartu kredit, penipuan melalui e-mail, perjudian online, penipuan dan pembobolan rekening bank, dan terorisme. Selain itu, *cyber crime* jenis ini mencakup materi internet yang bersinggungan dengan isu suku, agama, ras, dan antar golongan (SARA) yang menyebarkan ujaran kebencian melaui jejaring dunia maya.
2. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran. *Cyber crime* jenis ini tidak memanfaatkan internet dan komputer sebagai sarana melakukan tindak kejahatan, akan tetapi dijadikan sebagai obyek sasaran kejahatan. Contoh jenis kejahatannya adalah pengaksesan ke suatu sistem secara ilegal (*hacking*), perusakan situs internet dan server data (*cracking*) atau *defacting*. (Sutanto, Sulistiyo dan Sugiarto, 2005)

Berkaitan dengan hal tersebut, menurut Ari Juliano Gema (2000) sebagaimana yang dikutip oleh Abdul Wahid dan Muhammad Labib dalam bukunya yang berjudul "Kejahatan Mayantara (*Cyber Crime*)" menyatakan bahwa *cyber crime* dapat dikelompokkan dalam beberapa bentuk, yaitu:

1. *Unauthorized Access to Computer System and Service*. Kejahatan ini dilakukan dengan cara memasuki/menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari sang pemilik. Adapun motifnya beraneka ragam diantaranya adalah sabotase dan pencurian data.
2. *Illegal Contents*. Kejahatan ini dilakukan dengan cara memasukkan data atapun informasi ke media internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum. Contohnya adalah pornografi, persebaran berita

bohong, agitasi termasuk juga delik politik bisa dikategorikan ke jenis ini apabila menggunakan media ruang siber.

3. *Data Forgery*. Bentuk kejahatan ini dilakukan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptles document* melalui internet.
4. *Cyber Espionage*. Bentuknya kejahatannya yaitu memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer kepada sasaran yang telah ditargetkan. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau datanya tersimpan dalam suatu sistem yang *computeraized.*
5. *Cyber Sabotage and Extortion*. Kejahatan ini dilakukan dengan membuat gangguan, perusakan terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Pada umumnya, kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu tertentu sehingga data, program komputer atau sistem jaringan komputer tidak bisa digunakan, ataupun tidak berjalan sebagaimana mestinya. Kejahatan ini kadang disebut dengan *cyber terrorism*.
6. *Offence Againts Intellectual Property*. Kejahatan ini ditujukan terhadap Hak Atas Kekayaan Intelektual (HAKI) yang dimiliki oleh pihak lain di internet. Contoh sederhananya adalah meniru tampilan web suatu situs tertentu, penyiaran rahasia dagang yang merupakan rahasia dagang pihak lain.
7. *Infringements Of Privacy*. Kejahatan ini ditujukan terhadap informasi seseorang yang bersifat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara *computerized*. Apabila diketahui oleh orang lain akan mengakibatkan kerugian secara materiil atau immaterial, seperti nomor kartu kredit, nomor pin Anjungan Tunai Mandiri (ATM) dan sebagainya. (Ari Juliano Gema, 2000)

Prof Eddy O.S. Hiariej dalam bukunya yang berjudul Prinsip-Prinsip Hukum Pidana mengemukakan bahwasanya ada lima kata kunci terkait *cyber crime*. Pertama, *illegal access* yakni sengaja memasuki atau mengakses sistem komputer tanpa hak. Kedua, *illegal interception* adalah suatu perbuatan dengan sengaja menangkap pengiriman data komputer dengan perantara teknologi. Ketiga, *data interference* adalah perbuatan tanpa izin dan sengaja melakukan penghapusan dan perusakan pada bagian data komputer. Keempat, *system interference* yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer. Kelima, *missue of devices* mencakup penyalahgunaan perlengkapan komputer, password komputer, program komputer ataupun kode masuk komputer. Kejahatan tersebut dalam perkembangannya banyak ditemukan antara alat yang digunakan oleh pelaku dan akibat perbuatan tidak berada dalam satu tempat yang sama (Prof Eddy O.S. Hiariej, 2015).

Ancaman *cyber crime* terjadi karena adanya kepentingan dari berbagai individu atau kelompok tertentu dalam tatanan kehidupan masyarakat yang menimbulkan berbagai ancaman fisik, baik nyata ataupun semu dengan menggunakan kode-kode komputer *(software*) untuk melakukan pencurian informasi, kerusakan sistem, manipulasi informasi dan menggunakan perangkat keras (*hardware*) untuk melakukan kerusakan terhadap sistem, penyebaran data dan informasi tertentu untuk melakukan tindakan propaganda (Iwan dkk, 2012).

Dalam menanggulangi kejahatan siber tentunya dibutuhkan suatu teori sebagai landasan berpikir dan berbuat. Dalam konteks ini, teori kriminologi bisa digunakan sebagai sarana memahami modus pelaku kejahatan siber. Setidak-tidaknya terdapat empat teori kriminologi yang dapat digunakan untuk menganalisa *cyber crime*, yaitu:

1. Teori anomi digunakan sebagai alat analisis untuk mengetahui penyebab orang melakukan kejahatan siber. Teori anomi beranggapan bahwa hadirnya kejahatan karena

dalam tatanan masyarakat belum ada norma yang mengatur aktifitas tersebut (*normlessness*). Menurut Agus Rahardjo, dalam tataran praktinya ada sekelompok orang yang menolak kehadiran hukum untuk mengatur aktifitas di dunia maya. Sedangkan menurut kelompok ini, dunia maya adalah ruang yang bebas sehingga pemerintah tidak mempunyai hak dan kewenangan untuk campur tangan. Landasan pemikiran ini bermula adanya *Declaration offitidepence of Cyberspace* dari John Perry Ballow dan *Hacker Manifesto* yaitu Loyd Blankeship (Rahardjo, 1976). Selanjutnya dipaparkan bahwa pendapat pro maupun kontra mengenai ada atau tidaknya hukum yang mengatur kejahatan siber bertitik tolak pada kesenjangan karakteristik kejahatan dengan hukum pidana konvensional. Karakteristik penggunaan internet sebagai basis kegiatan bersifat lintas batas sehingga akan kesulitan untuk diketahui yurisdiksinya, padahal hukum pidana konvensional yang berlaku di Indonesia bertumpu pada batasan tetorial. Ketentuan-ketentuan hukum pidana konvensional tersebut ternyata tidak bisa menyelesaikan kasus yang melibatkan internet secara optimal (Rahardjo, 1976). Walaupun demikian, karena saat ini sudah ada peraturan perundang-undangan yang mencakup *cyber crime*, maka anomi (yang diartikan sebagai ketiadaan norma secara objektif) tidak menjadi argumen yang kuat bagi pelaku kejahatan siber. Akan tetapi, jika anomi diartikan sebagai "anggapan" individu bahwa tidak ada norma (secara subjektif) tentang kejahatan siber di Indonesia maka teori dan anggapan tersebut dapat dipahami.

2. Teori asosiasi diferensial dapat digunakan sebagai alat analisis untuk mencari penyebab seseorang melakukan kejahatan siber. Berdasarkan teori ini, pada hakekatnya kejahatan merupakan hasil dari suatu proses pembelajaran dan komunikasi yang berlangsung dari seseorang pada kelompok intim. Teori tersebut sejalan dengan karakteristik pelaku kejahatan siber sebagaimana diungkapkan oleh Sue

Titus Reid, bahwa "*They may have learned their acts from others in the same employ; thus, differential association cannot be ruled out* (Reid, 1976). Pelaku kejahatan telah mempelajari perbuatan pihak lainnya dalam pekerjaan yang sama; begitu pun prinsip asosiasi diferensial tidak dapat dikesampingkan dalam mempelajari kejahatan.

3. Teori kontrol sosial dapat digunakan sebagai alat analisis untuk mencari faktor-faktor yang menyebabkan seseorang melakukan kejahatan siber. Menurut teori ini, pelaku melakukan suatu kejahatan karena ikatan sosial dalam diri seseorang tersebut melemah atau tidak mempunyai ikatan sosial dengan masyarakat sekitarnya. Hal tersebut biasanya terjadi pada kalangan remaja.
4. Teori netralisasi dapat digunakan sebagai alat analisis, karena beberapa teknik netralisasi sebagaima dikatakan oleh Sykes dan Matza menjadi alasan dari para pelaku kejahatan siber di Indonesia, misalnya dalam kasus *defacing*. Teori netralisasi memandang bahwa tingkah laku menyimpang atau kejahatan dilakukan seseorang karena didasarkan pada pemikirannya sendiri dan didorong oleh beberapa kondisi di luar individu, sehingga para pelaku berusaha mencari alasan pembenar atas perbuatannya melalui proses rasionalisasi. (Djanggih dan Qamar, 2018)

Berdasarkan uraian teori kriminologi diatas dan dihubungkan dengan fenomena kejahatan siber saat ini diperlukan suatu evaluasi terhadap penerapan hukum dan dibutuhkan harmonisasi hukum di bidang teknologi informasi. Melihat pesatnya perkembangan teknologi informasi dan diiringi munculnya hal baru yang diikuti dengan celah hukum, maka pemangku kebijakan harus cepat mengantisipasi dan menangani hal ini (Rumampuk, 2015).

C. TINDAK PIDANA PENCUCIAN UANG DIGITAL

Kemajuan revolusi industri telah membawa perubahan terhadap bidang ekonomi dan sosial di dalam perkembangan

sistem dunia yang dinamis. Perkembangan ini telah menginovasi dunia ilmu pengetahuan dan teknologi untuk membantu kegiatan manusia dalam berbagai sektor, terutama meningkatkan pelayanan jasa keuangan kepada masyarakat seperti adanya *Internet Banking*, *Mobile Banking,* dan *electronic fund transfer*. Disamping pelayanan, era digital juga telah mempengaruhi bagaimana perkembangan mata uang virtual (*Crypto currency*) sebagai alternatif alat pembayaran yang sah. Awalnya, mata uang ini digunakan baik dalam *game online* maupun komunitas digital (Virtual Currencies Working Group, 2014). Namun karena dianggap lebih efisien daripada uang konvensional, *crypto currency* pun dibeberapa negara menjadi alat pembayaran yang praktiks.

Mata uang virtual dibuat oleh sekelompok orang atau badan hukum dan digunakan untuk pertukaran barang atau jasa. Pernggunaan *crypto currency* membawa dampak yang sangat positif bagi efisiensi dalam kehidupan. Namun, hal demikian juga menimbulkan dampak negatif disertai risiko dalam melakukan kegiatan bisnis. Pernyataan serupa telah disampaikan oleh Yunus Husein yang mengatakan bahwa perkembangan teknologi canggih dapat dikategorikan layaknya sebagai "pisau bermata dua" (Husein, 2004). Selain berkontribusi dalam peningkatan kesejahteraan dan kemajuan peradaban, hal ini dapat menjadi sarana efektif melakukan perbuatan kejahatan. Salah satu kejahatan modern yang termasuk dalam kategori transaksi keuangan adalah tindak pidana pencucian uang (TPPU) atau *money laundering*.

Mengacu Black's Law Dictionary, *money laundering* diartikan sebagai berikut:

> "*Term used to describe investment or other transfer of money flowing from racekteering, drug transactions, and either illegal sources into legitimate channels so that its original source can not be traced*."

Pencucian uang pada dasarnya merupakan penyamaran aset kekayaan sehingga tidak dapat terdeteksi oleh sistem

(Sutedi, 2008). Selain itu, dalam pembuktian pencucian uang harus dibuktikan dua jenis sumbernya yakni apakah tindak pidana merupakan tindak pidana sendiri atau disertai dengan tindak pidana asal (*predicate crime*) (Irman, 2017).

Pencucian uang konvensional memiliki tiga metode umum yakni *placement, layering* dan *integration (*Kristyanto, 2021). *Placement* adalah pelaku tindak pidana melakukan penempatan dana hasil perbuatan kriminal kedalam sistem keuangan seperti mengonversikan uangnya menjadi mata uang asing. *Layering* adalah pelapisan untuk menghilangkan jejak dari uang hasil tindak pidana tersebut, baik asal-usul uang tersebut, maupun ciri-ciri dari uang seperti mengaburkan asal-usul uang dengan menyimpannya dalam berbagai rekening bank. *Integration* adalah tahap akhir dari seluruh proses sebelumnya dengan menyatukan dana yang dihimpun seolah-olah melalui cara yang legal seperti menarik tunai satu persatu uang dari berbagai rekening yang berbeda. Dalam praktiknya ketiga kegiatan tersebut pada umumnya dilakukan secara runtun menjadi satu kesatuan.

Sedangkan metode yang digunakan dalam praktik pencucian uang digital diantaranya adalah *Buy and Sell Conversions, Offshore Conversions,* dan *Legitimate Business Conversions* merupakan pengembangan dari metode yang disebutkan dengan menghapus jarak dan waktu melalui transaksi virtual (Utami, 2021).

Pelaku TPPU menggunakan sarana digital untuk meminimalisir kemungkinan dideteksinya tindak pidana. Maka karena sifatnya yang digital, pencucian uang modern juga telah mengarah kepada konteks kejahatan yang berbasis teknologi dan informasi (*cyber crime*) (Arief, 2006).

Kiagus Ahmad Badaruddin selaku Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) mengatakan bahwa penggunaan mata uang virtual dapat meningkatkan terjadinya kejahatan keuangan seperti pencucian uang dan pendanaan terorisme. Ia menjelaskan bahwa keuntungan yang dihasilkan dari 11 kejahatan internasional,

seperti perdagangan narkoba, perdagangan gelap senjata hingga perdagangan manusia berkisar antara US$1,6 triliun hingga US$2,2 triliun per tahun. Kejahatan di bidang ekonomi juga telah mempengaruhi aliran dana illegal lintas negara (Illicit Financial Flows/IFF). Apalagi dengan munculnya *virtual asset* seperti *cryptocurrency* yang sulit dilacak (Wicaksono, 2020).

Pencucian uang virtual ini adalah kejahatan multidimensi dengan penggunaan sarana modern. Perkembangan hukum sendiri harus dapat mengikuti perkembangan bentuk kejahatan serupa namun tidak gegabah dalam merumuskan aturan yang mengaturnya agar tidak terjadi tumpang tindih aturan atau perumusan aturan yang belum komprehensif.

Mengacu data dari buletin statistik Pusat Pelaporan dan Analisis Transaksi keuangan (PPATK) bulan Oktober 2020, dugaan delik asal TPPU melalui Laporan Transaksi Keuangan Mencurigakan (LTKM) yaitu penipuan, narkotika, dan korupsi. PPATK telah menerima LTKM sejak Januari 2003 s.d. Oktober 2020 telah mencapai angka sebanyak 558.933 LTKM atau bertambah 10,9 persen dibandingkan jumlah kumulatif LTKM pada akhir Desember 2019. Sejak diberlakukannya UU TPPU, pelaporan LKTM meningkat sejak Januari 2011 s.d. Oktober 2020 dan tercatat sebanyak 495.009 LTKM atau tahunan meningkat 530,0 persen dibandingkan periode sebelum diberlakukannya UU TPPU (PPATK, 2020).

Pencucian uang digital ini tentu berbeda dengan proses pencucian yang menggunakan sistem *transfer* uang elektronik maupun pengubahan aset yang berputar yang jalurnya masih bisa dilacak oleh jaringan sistem lembaga keuangan. Terlebih apabila proses pencucian dilakukan di situs yang memudahkan pengguna untuk menukarkan uang riil menjadi barang virtual sehingga tidak dapat dijangkau oleh lembaga resmi dunia nyata. Disebutkan oleh *Financial Action Task Force* (FATF) bahwa pelaku pencucian uang sekarang semakin sulit terjerat. Kesulitan tersebut karena pembuktian yang cepat yakni dengan pemisahan antara harta hasil kejahatan lewat dunia siber

dengan tindakan kejahatan pelaku sehingga tidak terlacak oleh aparat hokum

Dalam *game online*, pelaku pencucian uang melakukannya dengan membuka akun pada situs dunia virtual. Dengan membuat akun baru, pencuci uang dapat membeli uang virtual tersebut dengan mentransfer kepada rekening milik perusahaan virtual tersebut.

Salah satu contoh kasus TPPU Digital adalah yang terjadi pada layanan mata uang digital Costa Rica yang dikenal dengan *Liberty Reserve*. Dengan adanya layanan mata uang digital tersebut dapat mengkonversi mata uang konvensional menjadi mata uang *Liberty Reserve*, dana ini bisa dikirimkan dan diterima secara anonim. Penerima dapat mengonversi *Cryptocurrency* tersebut kembali menjadi uang tunai (Kainama, 2017). Pada Mei 2013, pihak berwenang Amerika Serikat telah menutup layanan tersebut. Pendiri *Liberty Reserve* dan beberapa orang kepercayaannya didakwa dengan tindakan mencuci uang. Menurut Richet, penutupan *Liberty Reserve* tidak akan menghentikan praktik pencucian uang mengingat ada banyak alternatif lain, seperti *WebMoney*, *Bitcoins*, *Paymer*, dan *PerfectMoney*.

D. *DEEPFAKE*

Secara gramatikal *deepfake* sendiri merupakan padanan dari kata *deep-learning*[1], dan *fake* atau palsu (Nguyen, Thanh Thi, 2019). Teknik ini bekerja dengan menempatkan wajah orang yang menjadi target ke video orang yang menjadi sumber sehingga menciptakan video dimana target terlihat seperti melakukan atau mengatakan hal-hal yang dilakukan oleh sumber.

Dengan penerapan teknik tersebut maka suara, gambar, dan video akan dapat dimanipulasi untuk menirukan seseorang dan membuat target, terlihat seperti melakukan

[1] Deep-learning is a type of **machine learning** based on artificial **neural networks** in which multiple layers of processing are used to extract progressively higher level features from data. (Dalam English Oxford Living Dictionary)

sesuatu yang sumber sedang lakukan secara realistis sehingga jika hanya dilihat sekilas keberadaan manipulasi suara, foto atau video tidak dapat disadari, apalagi lewat kacamata awam. Kemunculan *deepfake* mungkin akan menjadi salah satu pengabur garis yang bisa membedakan mana informasi palsu dan mana informasi asli.

Deepfake hanyalah salah satu dari teknik manipulasi foto, video dan audio yang telah ditemukan oleh manusia saat ini. Dalam satu abad terakhir teknik manipulasi foto, video dan audio telah berkembang begitu pesat. Berikut ini adalah analisis perkembangan segala macam teknik terkait manipulasi foto dan video dari masa ke masa.

1. **Perkembang Awal Teknik Manipulasi Foto dan Video Era *Pre-Digital***

   Penggunaan teknik manipulasi dalam produk media visual telah berlangsung bahkan sejak diciptakannya fotografi di awal pertengahan abad ke-19. Kebiasaan mengoreksi foto, lahir bersamaan dengan teknik fotografi di pertengahan abad kesembilan belas dan akarnya terletak jauh di dalam teknologi film analog, *darkrooms* dan pengembang fotografi (Fineman, 2012).

   Awal penggunaannya dapat dilihat dalam potret berjudul *Sherman and His Generals* (1865) (Library of Conggress) karya Mathew Brady, salah seorang fotografer pada masa Perang Sipil Amerika Serikat. Isi dari potret tersebut adalah Jenderal Serikat Tentara, William Tecumseh Sherman, bersama para staff terdekatnya yang berjumlah tujuh orang. Dalam potret orisinalnya sebenarnya hanya ada Sherman dan enam orang staff-nya yaitu Oliver Otis Howard, William Babcock Hazen, Jefferson Columbus Davis, Joseph Anthony Mowe, John Alexander Logan, Sherman, dan Henry Warner Slocum, padahal seharusnya ada delapan orang yang masuk di potret tersebut. Hal itu karena Francis P. Blair yang seharusnya ikut masuk di dalam potret orisinal tersebut tidak dapat menghadiri pemotretan saat itu, sehingga Mathew Brady kemudian

memotretnya sendirian secara terpisah, lalu menggabungkan kedua potret tersebut dengan teknik montase foto.[2] Sehingga akhirnya terciptalah potret final *Sherman and His Generals* (1865) versi delapan orang yang sekarang tersebar luas dan diabadikan pula di dalam *Library of Congress,* begitulah cerita singkat tentang potret tersebut yang dituturkan oleh Mathew Brady melalui deskripsi fotonya di situs National Portrait Gallery (National Potret Gallery).

Selanjutnya penggunaan teknik serupa juga dapat dilihat dalam potret karya John Paul Filo yang berjudul Kent State Shootings (1970) (Paul Filo, 1970)-Penembakan Kent State (1970). Momen yang tertangkap dalam potret tersebut adalah Mary Ann Vecchio (14) yang terlihat berteriak saat melihat tubuh Jeffrey Miller yang telah ditembak oleh Pengawal Nasional Ohio dalam pembantaian di Universitas Kent State tahun 1970, foto memilukan yang kemudian memenangkan penghargaan Pulitzer di tahun berikutnya. Namun jika dalam jepretan karya Brady ada sesuatu yang ditambahkan, maka dalam potret karya John P. Filo ini ada sesuatu yang dihilangkan. Hingga sekarang ada dua versi dari potret tersebut yang tersebar luas, yaitu potret orisinalnya yang ikut memperlihatkan sebuah tiang hitam tepat di tengah foto, dan potret hasil manipulasinya yang menghilangkan tiang itu hingga tak berbekas. Versi dari potret yang telah dimanipulasi itu bahkan sempat dipublikasikan pula dalam beberapa majalah seperti *TIME*, *People* and *LIFE* (Bronx Documentary Center Altered Image).

2. Perkembangan Awal Teknik Manipulasi Foto dan Video Era *Post-Digital*

Permulaan dari bentuk digital teknik manipulasi foto, video dan audio pada masa *post digital* dapat ditarik sejak

[2] Pencahayaan dengan enlarger (alat pembesar) terhadap beberapa negatif film untuk menghasilkan efek penambahan gambar, R. Amien Nugroho (2006: 221)

tahun 1970, saat dimana *Super Paint* ditemukan oleh Richard Shoup, seorang Ilmuwan Komputer dari Amerika. *Super Paint* adalah salah satu bentuk awal penggunaan teknologi digital dalam pembuatan animasi komputer, manipulasi video dan karya seni kreatif, yang sekarang telah menjadi bagian utama dalam dunia hiburan dan desain industri. *SuperPaint* yang di desain pada awal 1970 merupakan sistem digital pertama yang diciptakan untuk penciptaan grafis dalam film dan konten TV, dan digunakan secara khusus untuk pembuatan bagian kredit di program TV dan film (Shoup, 2001). Jika sebelumnya teknik manipulasi hanya dapat digunakan dalam produk media visual tidak bergerak seperti karya fotografi, saat ini pengembangan teknologi tersebut dapat juga memanipulasi produk media visual bergerak seperti video.

Pada masa itu *Morphing* adalah salah satu teknik yang cukup sering digunakan dalam manipulasi foto atau video digital ini. *Morphing*, yang berasal dari kata Metamorfosis, merupakan efek visual atau animasi yang diciptakan komputer yang memperlihatkan perubahan sebuah citra sehingga yang tampak adalah bagaimana objek A secara ajaib dapat berubah menjadi objek B. Seperti dalam film *Terminator 2 : Judgment Day* (1991), dimana teknik ini digunakan untuk mengubah *Polyalloy*, robot dari masa depan, menjadi bermacam-macam citra, seperti seorang petugas polisi, lalu menjadi seorang perempuan hingga senjata tajam. Pada awal penemuannya teknik manipulasi digital ini hanya digunakan dalam program-program TV ataupun film, karena meskipun sudah menggunakan bantuan teknologi digital, penciptaan ilusi *morphing* yang kompleks dan tampak nyata seperti yang terlihat dalam film-film barat pada masa itu memerlukan dukungan perangkat keras dan lunak yang mumpuni juga puluhan insinyur grafis yang handal. Sehingga sampai saat itu teknik manipulasi ini tidak dapat dilakukan oleh awam dan hanya beberapa ahli grafis untuk digunakan secara eksklusif dalam

dunia hiburan karena besarnya anggaran yang dibutuhkan untuk menerapkan teknologi ini.

Digitalisasi teknik manipulasi produk media visual tidak bergerak seperti karya fotografi mulai berkembang pesat di tahun 1990, saat *Adobe system* mengeluarkan *Photoshop 1.0*, yang dapat dikatakan merupakan versi awam perangkat lunak untuk manipulasi foto digital. Untuk menggunakannya tidak lagi diperlukan keterampilan khusus ataupun komputer (perangkat keras) yang kompleks, perangkat lunak ini dapat diakses oleh awam dan dapat digunakan bahkan di komputer pribadi mereka. *Photoshop* awalnya hanya menargetkan desainer grafis sebagai pangsa pasar mereka, namun dalam perkembangannya juga akhirnya digunakan oleh fotografer, seniman, juga jurnalis dan dengan diperkenalkannya kamera digital di akhir tahun 1990 membuat teknik manipulasi foto atau gambar yang telah didukung oleh *Photoshop* menjadi dapat di akses atau dilakukan oleh masyarakat luas.

Sedangkan digitalisasi teknik manipulasi video mulai berkembang dan bisa digunakan secara luas oleh masyarakat umum sejak dikeluarkannya *Premiere Elements* perangkat lunak untuk mengedit video yang memang dikhususkan untuk awam oleh *Adobe* ditahun 2006. Hanya dengan komputer pribadi mereka, perangkat lunak ini memudahkan penggunanya untuk menciptakan transisi antar video yang ingin digabungkan, memotong bagian video yang tidak diinginkan, memasukkan audio yang diinginkan atau grafis dan animasi ke dalam video yang sedang diedit.

Sampai saat itu teknik manipulasi video atau foto digital hanya dikenal sebagai salah satu cara instan untuk menjaga estetika, memperkuat pesan yang ingin disampaikan lewat mereka, dan hal-hal lain yang telah menjadi pembenaran atas pengaplikasian teknik manipulasi video atau foto ini dalam sebuah karya. Tentu saja yang

kemudian membedakan antara manipulasi video dan foto masa dulu dan sekarang adalah betapa mudahnya sekarang teknik ini bisa dipraktikkan, bahkan oleh orang awam, tidak lagi dibutuhkan kemampuan khusus yang memerlukan pelatihan berbulan-bulan untuk mempraktikkannya. Tidak diperlukan proses manual selama berhari-hari seperti yang dilakukan pada potret karya Mathew Brady ataupun John Paul Filo di tahun 1900an, menempelkan kedua *frame*, untuk kemudian menggabungkan semuanya dalam satu film negatif menggunakan teknik montase foto atau menutupi bagian yang ingin dihilangkan dari foto dengan *masking* di teknik *darkroom*.

3. Perkembangan Saat Ini Teknik Manipulasi Foto dan Video Era *Post-Digital*

Teknik mesin yang dikenal sebagai *GANs* adalah teknologi yang digunakan untuk menggabungkan serta menempatkan wajah seseorang (target) yang ada di dalam foto dan video baru ke wajah seorang lain (sumber) di suatu foto dan video lainnya. Untuk menghasilkan video *deepfake* yang mampu menipu mata, diperlukan data imaji yang besar dari berbagai macam sudut pandang, ekspresi dan pergerakan melalui foto dan video asli yang telah beredar, dan menjadi target yang dipelajari untuk ditirukan oleh sistem pembelajaran mesin, dalam menciptakan video yang diinginkan (Rana, 2020).

Reface adalah salah satu aplikasi berbasis *mobile* yang ikut menjalankan algorithma *deepfake*, aplikasi ini dapat ditemukan serta diunduh secara bebas di *Apple App store* yang tersedia di *iOS* juga *Google Play Store* di *android*. Platform ini telah diunduh sebanyak lebih dari 52 juta kali di dunia. Layanan ini mengizinkan penggunanya untuk menempel wajah mereka di atas *GIFs*[3], video juga foto populer yang tersedia di aplikasi tersebut dan menciptakan ulang *GIFs*, video atau foto versi wajah penggunanya dan

[3] GIF'S: *Graphics Interchange Format*

bukan lagi versi asli seperti yang tersebar di internet. Dengan mengunduh secara gratis aplikasi tersebut, hanya dengan usapan jemari di layar, dalam beberapa menit foto yang telah dimasukkan, secara otomatis akan dimanipulasi oleh algoritma yang dijalankan oleh aplikasi tersebut sesuai keinginan dari pengguna.

Dalam statistik yang dibuat oleh *Sensity*, jumlah video hasil manipulasi dengan algoritma sejenis *deepfake* yang tersebar di internet sejak tahun 2018 telah meningkat secara signifikan. Dalam data yang disajikan *Sensity*, berdasarkan 500 sumber yang terindikasi rentan dan marak terjadi penyebaran video hasil manipulasi tersebut, dalam waktu kurang dari 6 bulan, terhitung dari bulan Juni 2020 hingga bulan Desember 2020, tercatat peningkatan hampir dua kali lipat dalam jumlah penyebaran video *deepfake* di Internet dari 49.081 video di bulan Juni hingga mencapai 85.047 video di bulan Desember.

4. Pornografi dan Penyalahgunaan *DeepFake*

Adebayo & Ojedokun (2018) menegaskan pengguna internet semakin mudah terpapar pornografi melalui penyebarluasan pornografi di internet, baik secara sukarela, maupun tidak sukarela sebagai bagian dari situasi dunia internet.

Di tahun 2019 dunia maya sempat gempar karena keberadaan sebuah website bernama *DeepNude*, situs tersebut menawarkan sebuah layanan dimana penggunanya dapat melucuti pakaian yang digunakan oleh seseorang di dalam foto yang telah ia masukkan sehingga orang itu terlihat telanjang. Programmer website itu mengklaim bahwa proses manipulasi yang terjadi dalam website tersebut hanya membutuhkan waktu 30 detik untuk selesai. Setelah mendapatkan kecaman, situs ini pun akhirnya tidak beroperasi lagi.

Namun program-program serupa ternyata terus bermunculan bahkan dapat ditemukan beberapa saluran di

aplikasi Telegram yang menjalankan Bot sejenis dengan program *DeepNude* ini. Menurut laporan berjudul '*Automating Image Abuse Deepfake bots on Telegram*' yang dikeluarkan oleh Sensity, di dalam saluran utamanya terdapat lebih dari 45 ribu anggota yang telah bergabung, dan hingga Juli 2020 sebanyak 24.168 foto-foto hasil manipulasi itu telah dibagikan secara publik di saluran ini. Dapat dilihat bahwa teknologi ini, dengan segala kemudahan dalam pengoperasiannya telah menimbulkan kasus-kasus penyebaran foto dan video pornografi hasil manipulasi di Internet. Teknologi ini kemudian dapat memicu peningkatan kasus *Revenge porn* yang tersebar di Internet.

Revenge porn adalah "*sexually explicit material which is created and widely disseminated to humiliate, threaten or harm a person who has broken off a relationship*..." Penyebarluasan informasi bermuatan pornografi ini dilakukan tanpa adanya *consent* dari salah satu pihak, dan didasari oleh balas dendam. Menurut Anastasia Powel dan Nicola Henry (2017) *Revenge porn* dalam hal ini terkait dengan tiga (3) kategori yaitu :

a. pembuatan foto dan video asusila dan seksual tanpa persetujuan;
b. penyebaran foto dan video asusila dan seksual tanpa persetujuan;
c. pengancaman dan pemerasan untuk menyebarkan foto dan video asusila dan seksual yang seseorang miliki.

Dengan teknologi manipulasi foto dan video ini, untuk melakukan *revenge porn* pelaku tidak lagi membutuhkan foto dan video asusila yang secara langsung melibatkan korban di dalamnya, karena mereka bisa memanipulasi foto dan video pornografi yang dimiliki oleh seorang bintang film pornografi, dimana wajah bintang film itu akan menjadi sumber dan wajah korban menjadi target. Wajah korban akan ditempel di wajah dan badan bintang

film pornografi sehingga yang terlihat adalah bahwa korban secara langsung terlibat dalam video asusila itu, sebab dengan *deepfake* bahkan mimik dan pergerakan wajah seseorang pun dapat ikut ditiru. Kasus penyalahgunaan *deepfake* dalam penciptaan video asusila palsu ini sempat di alami oleh salah seorang jurnalis di India, Ranna Ayub yang terjadi pada tahun 2018.

Dilihat dari sudut pandang normatif dan secara etis, jenis penyalahgunaan teknologi ini tentu dapat dikatakan sebagai bentuk baru dari pelanggaran privasi seksual dan kekerasan seksual melalui foto dan video (Maddocks, 2020).

5. *Deepfake*: Kepentingan Politik dan Penyalahgunaan

Dalam dunia politik, setiap tokohnya mempunyai kubu dan pendukung masing-masing. Apalagi seorang tokoh politik ternama yang mempunyai daya tarik yang besar kepada masyarakat, setidaknya apa pun yang keluar dari mulut mereka kemungkinan akan dipercaya dan ikut diamini oleh pendukung mereka. Lalu kemungkinan apa yang akan terjadi jika muncul *deepfake* atas tokoh-tokoh politik yang mengatakan pernyataan palsu yang dapat mencoreng nama mereka atau menimbulkan dampak buruk bagi dunia politik?

Dalam kontestasi politik teknologi *deepfake* mempunyai potensi untuk disalahgunakan dalam praktik *black campaign*. Praktik yang biasanya dilakukan oleh partai atau pihak oposisi, dilakukan dengan menyebarkan keburukan, kejelekan, fitnah dan berita bohong dengan tujuan menjatuhkan nama politisi tersebut, sehingga dia menjadi tidak disenangi oleh khalayak pendukungnya dan bahkan masyarakat umum (Piliang 2005).

Donald Trump adalah salah satu politikus sempat yang menjadi korban penyalahgunaan *deepfake*. Pada tahun 2018 di laman Twitter dan Facebook resmi partai politik Belgia, Sosialistiche Partij Anders, sempat tersebar sebuah video *deepfake* Donald Trump yang secara eksplisit terdengar

mengajak negara-negara lain untuk mengeluarkan diri mereka dari *Paris Climate Agreement*, seperti yang telah dilakukan Amerika Serikat.

Menurut laporan yang dikeluarkan oleh kanal berita harian Gallup, tepat setelah video tersebut keluar pada tanggal 20 Mei 2018, peringkat mingguan elektabilitas Donald Trump di Amerika Serikat sempat turun sebanyak 2%, dari 42% sepanjang tanggal 14-20 Mei 2018 menjadi 40% sepanjang tanggal 21-27 Mei 2018. Hal ini kemudian menunjukkan bagaimana penyebaran foto dan video hasil manipulasi dapat menjadi ancaman politis terhadap elektabilitas tokoh-tokoh politik yang wajahnya digunakan sebagai target dalam penciptaan video *deepfake* ini, dan dapat dijadikan senjata untuk melakukan *black campaign* oleh partai atau kubu oposisi.

Hal ini dikarenakan berita palsu (termasuk *deepfake*) yang dibagikan di sosial media, punya kecenderungan untuk lebih cepat tersebar dibandingkan kampanye politik biasa. Belum lagi melihat kecenderungan masyarakat untuk lebih mempercayai berita-berita yang sejalan dengan pendapat/pandangan politik mereka dan mendiskreditkan berita yang tidak sesuai dengan apa yang mereka yakini (Thaler, 2018). Pendapat masyarakat yang dewasa ini cenderung dibentuk oleh sentimen dan kepercayaan, bukan fakta dan rasio, adalah salah satu faktor yang menyebabkan munculnya tren baru dalam komunikasi politik dimana yang menjadi masalah krusial bukan lagi soal moral, etis atau tidaknya dan berdasar fakta, melainkan apa yang bekerja untuk menarik masa.

Dapat dilihat bahwa penyalahgunaan teknologi ini dapat berujung pada ujaran kebencian, disintegrasi masyarakat, dan konflik. Kepercayaan masyarakat kepada institusi politik bisa terkikis dan hal ini dapat memperdalam polarisasi di antara kelompok-kelompok sosial. Teknologi *deepfake* memungkinkan terciptanya realitas alternatif dimana selebritas dan pemimpin publik mengatakan dan

melakukan hal-hal yang tidak pernah mereka lakukan, sehingga menipu publik yang tidak sadar.

Digitalisasi telah membuat teknologi manipulasi foto, video dan audio menjadi lebih umum dan dapat dilakukan bahkan oleh orang awam, belum lagi penetrasi internet yang semakin meningkat setiap tahunnya membuat foto, video dan audio hasil manipulasi ini dapat tersebar semakin cepat di kalangan masyarakat umum.

Hal yang menyebabkan video hasil manipulasi cenderung mudah dipercayai disebabkan oleh cepatnya manusia untuk mempercayai materi audiovisual. Teori ini biasa disebut *processing fluency* yang mengacu pada bias kognitif bawah sadar kita yang mendukung informasi berbentuk visual hingga diproses lebih cepat jika dibandingkan dalam bentuk teks. Mungkin kita sudah terbiasa dengan fakta bahwa foto dapat dimanipulasi, namun dalam kasus audio dan video, kita akan cenderung percaya bahwa rekaman video dan audio yang kita tonton telah menangkap apa yang kita lihat dengan mata kita sendiri atau dengar dengan telinga kita sendiri, sehingga mereka telah berfungsi sebagai perpanjangan dari persepsi kita, sehingga lebih mudah untuk dipercaya.

Tersebarnya foto, video dan audio hasil manipulasi *deepfake* di media sosial adalah salah satu bentuk pencemaran data pribadi seseorang. *Handbook on European Data Protection Law* (2014) menyebutkan bahwa sebuah informasi disebut berisi data milik seseorang jika ia bisa diidentifikasi lewat informasi ini dan jika seseorang meskipun tidak diidentifikasi, lewat penjabaran yang ada di informasi itu bisa diketahui identitas subjek data melalui penelusuran lebih lanjut. Hal ini sejalan dengan definisi data pribadi dalam konteks data yang termuat secara elektronik dan non-elektronik yang diatur dalam Peraturan Pemerintah Nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, maka ditafsirkan bahwa jika di dalam foto dan video identitas seseorang secara jelas

terlihat atau identitasnya dapat dikenali atau diidentifikasi melalui foto dan video tersebut, maka mereka dapat dikategorikan sebagai data pribadi miliknya.

6. Jerat Hukum atas penyalahgunaan *DeepFake*

Internet adalah tempat dimana penyebaran foto dan video hasil manipulasi ini sering terjadi, sehingga secara umum pelaku penyebaran dapat dijerat oleh Undang Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengatur tentang berbagai perlindungan atas kegiatan yang memanfaatkan internet sebagai medianya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya.

Revisi UU ITE No. 19 tahun 2016 melarang penghinaan dan pencemaran nama baik melalui internet, secara umum tindakan penyebaran *deepfake* berbentuk foto dan video memenuhi unsur-unsur di dalam pasal 27 ayat (3) Revisi UU ITE No. 19 tahun 2016 yang berbunyi:

> "*Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan mentransmisikan dan membuat dapat diaksesnya Informasi Elektronik dan Dokumen Elektronik yang memiliki muatan penghinaan dan pencemaran nama baik.*"

Pelaku dengan sengaja dan tanpa hak atau persetujuan dari korban telah menyebarkan foto dan video hasil manipulasi *deepfake* di internet, sehingga mencemari data pribadi dan nama baik korban, karena telah menyebarkan kebohongan mengenai korban lewat video tersebut.

Unsur pencemaran nama baik dalam pasal 27 ayat (3) Revisi UU ITE No. 19 tahun 2016 disebut ikut terpenuhi karena jika merujuk pada Pasal 310 ayat (1) Kitab Undang-undang Hukum Pidana, pencemaran nama baik diartikan sebagai perbuatan menyerang kehormatan atau nama

baik seseorang dengan menuduhkan sesuatu hal yang maksudnya terang supaya hal itu diketahui umum. Secara umum video *deepfake* merupakan salah satu bentuk misinformasi digital, dan dapat dikatakan sebagai bentuk pencemaran nama baik karena terdapat unsur menuduh melakukan sesuatu, unsur menyerang kehormatan dan unsur menyiarkan tuduhan supaya diketahui umum.

Mengingat bahwa kejahatan penghinaan sebagaimana terkandung pada pasal 310 KUHP berlaku sebagai delik aduan, begitu pula pasal 27 ayat (3) Revisi UU ITE No. 19 tahun 2016 yang ikut mengatur mengenai kejahatan penghinaan dan pencemaran nama baik melalui internet, berlaku sebagai delik aduan dan hanya dapat diproses apabila diadukan oleh orang yang merasa dirugikan. Digunakan penilaian subjektif oleh korban untuk menentukan apakah konten atau bagian dari Informasi atau Dokumen Elektronik ia rasa telah menyerang kehormatan atau nama baiknya atau tidak dalam penerapan pasal ini pada suatu kasus.

Pelaku yang telah menyerang nama baik dan kehormatan korban saat menyebarkan video tersebut secara digital, lewat tuduhan melalui video *deepfake* yang memperlihatkan korban tampak mengatakan dan melakukan sesuatu yang tidak pernah ia katakan/lakukan, hingga menimbulkan misinformasi digital terhadap korban, atas perbuatannya berdasarkan pasal 45 ayat (4) Revisi UU ITE No. 19 tahun 2016 diancam pidana penjara paling lama 4 (empat) tahun dan denda paling banyak Rp750.000.000,00.

BAB IV
DATA PRIBADI

A. MENELAAH KONSEP PERLINDUNGAN DATA PRIBADI

Pada abad ke 21, teknologi berkembang sedemikian pesat. Seiring dengan masifnya pemakaian teknologi yang canggih dalam sistem telekomunikasi, masyarakat sebagai penggunanya seolah-olah mendapat dunia baru, konsep ini sering dinamakan sebagai *cyberspace* (Arsyad Sanusi, 2005). *Cyberspace* atau dunia maya merupakan tempat di mana komunikasi secara *online* terjadi. Istilah *cyberspace* diperkenalkan pertama kali oleh novelis sains-fiksi, William Gibson, dalam bukunya yang berjudul Neuromancer. Pada saat itu, tahun 1984, Gibson melihat semacam integrasi antar komputer dengan manusia (Vivia, 2008).

Saat ini sudah banyak aplikasi atau layanan yang memudahkan manusia dalam melakukan kegiatan sehari-hari, seperti dalam aspek mobilisasi ada Gojek, dalam aspek pendidikan ada Ruang Guru, dalam aspek komunikasi ada Telegram, dan masih banyak jenis aplikasi lainnya—dilansir dari Statista, pada Desember 2020 ada sebanyak 2,950,000 aplikasi yang bisa diunduh di Google Play Store. Persoalannya, jika kita hendak menggunakan aplikasi tersebut akan ada mekanisme untuk melakukan registrasi atau *sign up* terlebih dahulu. Biasanya, pada saat itulah aplikasi akan meminta izin untuk mengakses data pribadi pengguna.

Data pribadi diartikan sebagai semua informasi yang memiliki keterkaitan dengan identitas atau sebagai sesuatu yang wajar yang dapat mengidentifikasi seseorang baik secara langsung maupun tidak langsung (Dewi Puspasari, 2020). Alan Westin mendifinisikan privasi sebagai klaim dari individu, kelompok, atau lembaga untuk menentukan sendiri mengenai kapan, bagaimana, dan sampai sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain (Alan Westin, 1967).

Terkait dengan jenis dari data pribadi sangat bervariasi, yang paling sering digunakan adalah nama, alamat tinggal, nomor telepon, dan alamat surel. Selanjutnya, kumpulan data pribadi tersebut diproses menggunakan teknik atau model pemrograman untuk dapat diakses dalam skala besar yang kemudian menghasilkan sebuah informasi yang berguna dalam menentukan suatu keputusan atau menjalankan suatu program (Hurson & Sarbazi Azad, 2016). Data pribadi ini biasanya disimpan dalam suatu entitas tertentu yang bisa saja mengalami "kebocoran", apabila hal tersebut terjadi maka semua data pribadi yang ada di dalamnya akan diketahui secara bersamaan (Kamleitner & Mitchell, 2019).

Revolusi digital atau revolusi data telah menciptakan sebuah inovasi baru dalam kapasitas untuk memperoleh, menyimpan, memanipulasi, dan mentransmisikan volume data secara nyata (*real time*), luas, dan kompleks (Djafar, 2019). Dampak dari revolusi digital adalah data menjadi entitas yang dapat dikapitalisasi dan sangat tinggi nilainya. Pemerintah maupun swasta berlomba-lomba mencari terobosan teknologi pengolahan data yang efisien tetapi tidak mengurangi kuantitas dari data yang dapat diolah.

Menurut Gartner, dalam pengolahan data skala besar (*big data*), aspek yang ditekankan adalah peningkatan ukuran data (*volume*), laju peningkatan data yang dihasilkan (*velocity*), peningkatan rentang format dan representasi yang digunakan (*variety*), serta aspek kepercayaan dan ketidakpastian yang berkaitan dengan data dan hasil analisis data tersebut (*veracity*) (Stuart & Basker, 2013). Seiring dengan semakin banyaknya diskursus tentang konsep *big data*, terdapat dua karakteristik tambahan yang juga erat kaitannya dengan konsep *big data*: validitas dan nilai. Validitas itu berhubungan dengan salah benarnya suatu data. Sedangkan nilai mengarah kepada makna eksplisit dari suatu data dalam konteks tertentu.

Tindakan pengumpulan data dalam skala besar dapat menimbulkan kerentanan apabila tidak dikelola dengan baik. Sebab, salah satu hal yang bisa didapatkan dari pengolah data

adalah dapat mengetahui kebiasaan, kesukaan, bahkan kegiatan sehari-hari dari pemilik data. Pemroses data dapat mengetahuinya dengan hanya melihat kombinasi atau algoritma. Apabila terdapat batasan yang dilanggar, tindakan tersebut tentu melanggar privasi individu dan bisa berimplikasi kepada tindakan yang merugikan atau bahkan melanggar hukum, seperti kasus Milyader Republikan, Robert Mercer yang membayar Cambridge Analytica senilai $15 juta untuk menggarap kampanye senator Ted Cruz. Alhasil, tindakan tersebut berhasil dibongkar oleh karyawan anonim Cambridge Analytica sendiri yang menyatakan bahwa perusahaan memanen data pribadi dari 50 juta lebih profil akun Facebook tanpa seizin pemilik akun—menurut mantan karyawan Cambridge, kejadian itu merupakan salah satu kebocoran data terbesar dalam sejarah jejaring sosial (Rossenberg, 2018).

Diduga pula data pribadi tersebut diolah untuk kepentingan kampanye Presiden Trump pada tahun 2016. Akan tetapi, jika data tersebut dipergunakan secara bijak, akan membuahkan hal yang positif pula, salah satunya adalah dapat membantu tempat kerja dalam mencocokan karyawan dengan pekerjaan yang tepat (The White House, 2016). Hal tersebut sangat bermanfaat karena saat ini sering terjadi "bias afinitas" dalam perekrutan karyawan—bahkan HRD (*Human Resource Departement*) yang bermaksud baik sering memilih kandidat hanya atas dasar karakeristiknya yang sama dengannya (Goldberg, 2005).

Ditengah menjamurnya perusahaan *startup* di Indonesia, pemerintah harus mempersiapkan perlindungan hukum sehingga dapat memberikan rasa aman bagi konsumen *startup* tersebut. Di Indonesia, perusahaan *startup* sering kali menjadi korban pencurian data oleh peretas. Seperti yang dialami oleh salah satu startup unicorn di Indonesia, Tokopedia, 91 juta akun pengguna dan 7 juta akun *merchant* meliputi nama, *password hash*, alamat surel, nomor telepon, jenis kelamin, dan tanggal lahir diperjualbelikan di *darkweb* seharga $5.000 atau setara 72 juta rupiah. Setali tiga uang dengan yang dialami oleh

Tokopedia, pada 11 Mei 2020 kelompok peretas ShinyHunters mengklaim memiliki 1,2 juta data pengguna Bhinneka. Namun, sejauh ini, satu-satunya peraturan yang dapat mengatur secara luas lalu lintas perdagangan digital di dunia adalah *General Data Protection Regulation* (GDPR).

Selain itu adapula bentuk penyalahgunaan data pribadi lainnya yang saat ini marak terjadi yakni berupa *spam*, *doxing*, dan jual beli data pribadi. Spam adalah segala bentuk pesan atau surat elektronik, terlepas dari apa pun isinya, yang dikirimkan ke banyak penerima yang sebenarnya tidak menghendaki datangnya pesan tersebut (Astagiri, 2010). Spam sangat lumrah ditemukan pada surel. Isi dari surel spam tersebut biasanya berupa penawaran jasa atau suatu produk, menawarkan tips dan trik terkait suatu hal, jasa judi, dan masih banyak lagi. Surel yang sering berisikan 'sampah' tersebut sering kali mengganggu produktifitas pengguna karena surel yang penting akan tertimbun oleh spam. Cindy M. Rise menjabarkan jenis kerugian yang ditimbulkan akibat dari spam sebagai berikut, *cost shifting*, *waste of resources*, dan *content* (Rise, 2002).

Doxing atau *dropping documents* umumnya memiliki konotasi negatif—bukan hanya karena dianggap melanggar privasi seseorang tetapi juga karena sering digunakan sebagai semacam mekanisme balas dendam (Rise, 2002). Tindakan *doxing* ini bisa mengancaman demokrasi Indonesia karena ketika seseorang tidak setuju atas argumentasi orang lain, yang diserang justru bukan argumentasinya melainkan pribadi dari orang tersebut (*ad hominem*) ataupun hal-hal lain yang tidak memiliki relevansi dengan argumentasi tersebut. Seperti yang dialami oleh mantan jurnalis TopSkor, Zulfikar Akbar—kasus bermula dari pengusiran terhadap Abdul Somad ke Hongkong. Zulfikar Akbar mengomentari kejadian itu dalam cuitan di akun twitternya @zoelfick, "Ada pemuka agama rusuh ditolak di Hongkong, alih-alih berkaca justru menyalahkan negara orang. Jika Anda bertamu dan pemilik rumah menolak, itu hak yang punya rumah. Tidak perlu teriak di mana-mana bahwa

Anda ditolak. Sepanjang Anda diyakini memang baik, penolakan itu tak akan terjadi." Postingan tersebut memicu tekanan dan serangan terhadap Zulfikar di media sosial dalam bentuk *doxing*, upaya persekusi, hingga pada akhirnya Zulfikar dipanggil Manajemen TopSkor dan memberhentikannya pada 26 Desember 2017 (Banimal, Juniarto, & Ikaningtyas, 2020). Dilansir dari riset yang dilakukan SAFEnet (*Southeast Asia Freedom of Expression Network*), sepanjang tahun 2020, jurnalis merupakan profesi yang memiliki kerentanan korban *doxing* tertinggi, yakni sebanyakan 13 kasus. Padahal, kebebasan pers merupakan salah satu pilar demokrasi yang bisa dibilang keberadaanya paling independen karena berada di luar sistem negara.

Sedangkan jual beli data pribadi merupakan tindakan penyalahgunaan yang paling sering terjadi di Indonesia. Pengguna telepon genggam pasti pernah menerima pesan ataupun telepon dari nomor yang tidak dikenal. Modus operandinya biasanya berupa pengumuman mendapat hadiah, meminta bantuan berkedok saudara kecelakaan, menawarkan suatu produk, dan masih banyak lagi. Bahkan, lebih parahnya, penjual data pribadi atau telemarketer berani menjual data-datanya secara terbuka melalui *e-commerce*. Data pribadi yang dijual biasanya berupa nama, nomor telepon, tanggal lahir, NIK, dan nomor kartu kredit. Hasil penelurusan dari tim riset Tirto.id mengungkap bahwa data dijual dari harga 350 ribu rupiah mendapat 1.000 data hingga 5 juta rupiah mendapat 1 juta data dan terbukti beberapa nama dalam *file* yang diperoleh dari penjual adalah valid atau data yang masih aktif (Mawa Kresna, 2019).

Menurut riset yang dilakukan oleh Hootsuite (We are Social) (2020), pada tahun 2020 pengguna aktif sosial media di Indonesia sebesar 160 juta atau 59% dari total populasi di Indonesia dan mengalami peningkatan sebesar 6,3% atau 10 juta dalam rentan satu tahun (Januari 2020—Januari 2021). Artinya, setiap tahun semakin banyak data pribadi yang tersebar melalui media sosial.

Sayangnya perkembangan tersebut tidak diimbangi dengan pertumbuhan tingkat kesadaran masyarakat dalam menjaga data pribadinya. Padahal, perkembangan teknologi digital tersebut menimbulkan konvergensi. Yang mana akibat dari konvergensi secara sosial telah dirasakan oleh seluruh lapisan masyarakat baik itu positif maupun negatif (BPPT, 2007). Akan tetapi, masyarakat masih terjebak pola pikir ekonomi (pengorbanan sekecil-kecilnya untuk memperoleh keuntungan sebesar-besarnya) tanpa mempedulikan efek buruk yang akan ditimbulkan. Masyarakat juga terlalu terlena dan bersifat naif saat menggunakan internet. Tanpa mereka sadari, saat menjelajah *web*, *chatting*, bahkan FTP (*files transfer protocol*) sekalipun, sebagian kecil identias diri pribadi dapat diketahui oleh pengelola layanan yang bersangkutan atau bahkan orang lain (Yuwinanto, 2011).

B. AWAL MULA KONSEP DATA PRIBADI

Pada tahun 2021, hampir 60% penduduk di Bumi merupakan pengguna aktif internet. Implikasinya adalah semakin buramnya garis pembeda antara hal yang sifatnya privasi dan publik. Atas nama kebebasan perpendapat, manusia bebas mengemukakan argumentasinya di ruang-ruang publik. Yang mereka tidak sadari adalah ada kemungkinan informasi pribadi mereka tersebar. Dalam ruang publik, selalu ada entitas yang kedudukannya lebih tinggi dan kuat daripada 'warga negara kelas dua'. Lebih jauh lagi, karena ruang publik erat kaitannya dengan negara—setidaknya saat ini ia memegang posisi terkuat, karenanya akan cenderung mengintervensi ruang privat dan bertujuan untuk memengaruhi kepentingan dan nilai-nilai yang membentuk ruang tersebut (Blume, 2010). Sehingga, kelompok tersebut tidak memiliki proteksi dan kedaulatan atas privasinya.

Sebenarnya, jauh sebelum revolusi digital, diskursus terkait privasi sudah eksis pada saat penggunaan kode-kode kuno, seperti di wilayah Yunani, Romawi, dan Anglo-Saxon (Toriqul Islam & Karim, 2019). Konsep privasi memiliki akar

sejarah yang luas dalam diskusi sosiologis dan antropologis terkait tentang betapa luasnya nilai dan pelestarian dalam berbagai budaya (De Cew, 2012). Selain itu, konsep tersebut memiliki asal sejarah dalam diskusi filosofis yang populer, salah satu pemikiran yang paling disorot adalah dari Sang Filsuf, Aristoteles, tentang demarkasi antara ruang publik dari aktivitas politik dan ruang pribadi yang terkait dengan keluarga dan kehidupan rumah tangga. Dalam pemikiran Yunani Kuno, komunitas politk (*polis*) tidak hanya berbeda dengan asosiasi natural atau biologis yang berpusat di rumah (*oikos*)—tetapi juga bertentangan langsung (Arendt, 1958).

Di Yunani Kuno, data pribadi seseorang kebanyakan tertulis di batu. Perang merupakan pemicu utama data pribadi banyak orang harus dicatat. Perekrutan individu untuk bertugas di masa perang atau wajib militer membutuhkan koleksi data pribadi yang sangat banyak (Beckles, 2017). Alhasil, penguasa saat itu berinisiatif untuk mengumpulkan data pribadi penduduknya guna melindungi mereka atau untuk memberikan hak-haknya (penyediaan layanan dan perdagangan).

> Menurut Arendt, "*The distinction between a private and a public sphere of life corresponds to the household and the political realms, which have existed as distinct, separate entities at least since the rise of the ancient city-state; but the emergence of the social realm, which is neither private nor public, strictly speaking, is a relatively new phenomenon whose origin coincided with the emergence of the modern age and which found its political form in the nation-state*." Arendt menegaskan konsep privat dan publik merupakan dua hal yang terpisah.

Bukti-bukti lain yang menunjukkan perlindungan privasi atau data pribadi sudah menjadi fokus pada masa itu adalah dalam *Code of Hammurabi* yang dalamnya membahas prinsip pertanggungjawaban untuk perlindungan atau pengaturan data pribadi (R William London, 2013). Salah satunya yang

tertulis pada Pasal 21: "*If a man breaks into a house, they shall kill and hang him in front of that very breach.*"

Kemudian *Hippocratic Oath*" klasik yang berisi pernyataan privasi terkait pasien mereka:

> "*What may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, whichon no account one must spread abroad, I will keep to myself,holding such things shameful to be spoken about*."

C. PERLINDUNGAN HAM TERHADAP DATA PRIBADI

Deklarasi Universal Hak Asasi Manusia (DUHAM) merupakan dokumen pertama yang mengakui eksistensi hak asasi manusia (HAM). DUHAM memberi landasan bagi negara-negara anggota Perserikatan Bangsa-Bangsa (PBB) maupun bukan anggota PBB dalam hak penegakan hak asasi mansuia. Terdapat dua pasal yang membahas perlindungan data pribadi dan privasi secara pasti yakni pada Pasal 3 dan 17.

Pasal 3 memberi penegasan bahwa setiap orang memiliki hak untuk hidup, kebebasan, dan keamanan seseorang. Kemudian, Pasal 17 menekankan bahwa setiap orang berhak untuk tidak menginformasikan kepada orang lain terkait apa-apa yang menyangkut dirinya dan tidak seorang pun boleh merampas privasi orang lain. Pasal 3 dan 17 memberi perlindungan terhadap hak privasi dalam arti luas atau tidak secara spesifik (Natamiharja & Mindoria, 2019). Hal tersebut dapat dipahami karena sifat dari deklarasi adalah *general* dan termasuk ke dalam *soft law*. Prinsip yang tertulis di dalam DUHAM akan diadopsi ke dalam hukum nasional negara-negara anggota PBB maupun bukan anggota PBB.

General Data Protection Regulation

Perlindungan data pribadi dan privasi di Uni Eropa telah diakui sebagai hak dasar dalam *The European Union Charter of Fundamental Rights*. Sebelum berlakunya *General Data Protection Regulation* (GDPR), Uni Eropa telah memiliki Directive 95/46/EC. Namun, aturan tersebut dianggap kurang relevan karena tidak memberikan sanksi yang tegas bagi entitas di luar

Uni Eropa. Setelah melalui diskursus sejak tahun 2015, pada tahun 2016, Uni Eropa akhirnya merumuskan GDPR. Berikut adalah beberapa perubahan utama yang terdapat pada GDPR (Russel & Fuller, 2017):

(1) *Increased territorial scope*
(2) *Enhanced data inventory requirements*
(3) *Increased penalties*
(4) *Appointment of a Data Protection Officer (DPO)*
(5) *Broader obligations for Data Controllers (organisations that collect and manage EU citizen data)*
(6) *Direct obligations for Data Processors (any company that processes personal data on behalf of a Data Controller)*
(7) *More timely data breach reporting*
(8) *Right to data portability*
(9) *Right to erasure ('right to be forgotten')*
(10) *Stronger Data Subject consent*

GDPR merupakan aturan hukum yang mengikat bagi negara-negara Uni Eropa maupun bukan negara Uni Eropa. Keberlakuan GDPR dapat mengabaikan yurisdiksi suatu negara. Tidak peduli apakah suatu aktifitas pemrosesan data pribadi atau perusahannya berada di wilayah Uni Eropa atau tidak, seluruh aktifitas bisnis di seluruh dunia akan tunduk kepada GDPR dengan syarat mereka mengarahkan aktifitas pemrosesan data tersebut ke wilayah Uni Eropa. Hal ini tertulis dalam *Article* 3 GDPR yang berbunyi:

> *(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*
> *(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Contoh sederhananya adalah dalam urusan pariwisata. Indonesia sebagai negara yang cukup aktif dalam mempromosikan wisatanya kepada negara-negara Eropa harus kooperatif dengan aturan GDPR. Indonesia harus memberikan jaminan perlindungan terhadap data pribadi setiap warga negara Uni Eropa sebagaimana telah diatur oleh *European Union Agency for Fundamental Rights and Council of Europe* (Hermanto Sirait, 2019).

Akan tetapi, tidak ada aturan hukum yang dapat menjangkau seluruh aspek yang ada. Dalam kasus ini, ketentuan di dalam GDPR tidak berlaku bagi seluruh aspek yang berkaitan dengan pemrosesan data pribadi, aspek-aspek tersebut diantaranya (Lambert, 2018):

(1) Dalam kegiatan yang berada di luar ruang lingkup undang-undang UE.
(2) Oleh negara-negara anggota ketika melakukan kegiatan yang termasuk dalam ruang lingkup Bab 2 *Title* V dalam Perjanjian Uni Eropa.
(3) Oleh individu dengan tujuan murni kegiatan pribadi atau rumah tangga.
(4) Oleh otoritas yang berkompeten untuk tujuan pencegahan, penyelidikan, deteksi, atau penuntutan pelanggaran pidana atau pelaksanaan hukuman pidana, termasuk perlindungan dan mencegah ancaman keamanan publik.

Pengacara dan pebisnis beranggapan bahwa GDPR memberlakukan hukuman yang tegas untuk setiap ketidakpatuhan terhadap perlindungan data pribadi dan privasi karena sanksi yang dikenakan bisa sampai Rp.340 miliar (US $ 24,58 juta) dalam euro atau 4 % dari omset global yang mana itu merupakan angka yang sangat besar (Supriyadi, 2018). Meskipun sanksinya cukup besar, sudah ada perusahaan yang terkena sanksi oleh keberlakuan GDPR, yakni Google.

Dilansir dari The New York Times, di bawah otoritas perlindungan Perancis, Google didenda sebesar € 50 juta atau sekitar $ 57 juta karena tidak mengungkapkan dengan benar kepada pengguna bagaimana data dikumpulkan di seluruh layanannya—termasuk mesin pencari, Google, Maps, dan Youtube untuk menampilkan iklan yang dipersonalisasi (Satariano, 2019).

Terkait dengan prinsip-prinsip yang digunakan GDPR sebagai pedoman pelaksanaan tercantum pada Pasal 5 ayat (1) Bab II GDPR yang berbunyi:

(1) *processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);*
(2) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (purpose limitation);*
(3) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);*
(4) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);*
(5) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (storage limitation);*

(6) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).*

Dari segi penegakan hukum, *Data Protection Officer* (DPO) merupakan lembaga yang mengawasi strategi perlindungan data perusahaan dan implementasinya untuk memastikan kepatuhan dengan peryaratan GDPR (Nate Lord, 2020). Tugas dari DPO telah ditentukan pada Pasal 39 ayat (1) GDPR yang berbunyi:

(1) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(2) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(3) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(4) to cooperate with the supervisory authority;
(5) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

D. PERBANDINGAN PERLINDUNGAN DATA PRIBADI

1. Amerika

Pada tahun 1789, James Madison yang merupakan Presiden keempat Amerika Serikat memasukan amandemen keempat sebagai salah satu bagian dari Deklarasi Hak-Hak

Amerika Serikat. Isi amandemen keempat tersebut adalah sebagai berikut:

> "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*."

Kasus *Boyd v. United States* merupakan pemantik awal dari amandemen ke empat ini. Sehingga Mahkamah Agung menyatakan bahwa amandemen ini harus menjadi perlindungan dari semua interfensi pemerintah terhadap privasi,

> "*... It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense, it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment*."

Jika dibedah, amandemen ini terdiri dari dua klausula (Clancy, 2011). Yang pertama, *reasonableness clause* dan *merely specifies*. Artinya, dalam rangka melakukan penegakan hukum, petugas harus memiliki alasan masuk akal. Yang kedua, *warrant clause*. Artinya, petugas harus menjamin (di bawah sumpah) bahwa ketika melakukan penggeladahan harus dapat dipertanggungjawabkan dan memiliki alasan yang logis mengapa menggeledah tempat tersebut.

Atas dasar amandemen ke empat ini, individu memiliki hak untuk *to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*. Hak ini memberi batasan kepada kekuasaan kepolisian untuk menangkap dan mencari orang, properti mereka, dan rumah

mereka. Amandemen ini juga menegaskan bahwa tidak ada surat perintah yang dikeluarkan tanpa alasan yang jelas. Secara praktis, amandemen ini berdampak kepada penerapan hukum pidana. Apabila polisi menyita barang bukti dengan cara yang ilegal maka bukti itu tidak dapat diajukan ke pengadilan. Bahkan, Banjamin Cardozo berpendapat terdakwa harus dibebaskan karena polisi melakukan pelanggaran.

Di Amerika Serikat, hak privasi sering dikaitkan dengan keinginan seseorang untuk dibiarkan dalam kesendirian (*the right to be alone*) dan kebutuhan akan hal tersebut harus dapat diimplikasikan dalam perlindungan hukum (Dimitri, 2011). Pada 15 Desember 1980, Samuel Warren dan Louis Brandeis mengkonsepsikan gagasan tentang hak atas privasi dalam Harvard Law Review yang berjudul *The Right to be Alone*.

Latar belakang dari tulisan mereka adalah dari kondisi perkembangan bisnis modern yang mulai mengintervensi ranah privasi, publikasi hal personal yang membuat turunnya standar sosial dan moralitas, penderitaan mental, tereduksinya hak-hak individu, dan hal negatif lainnya (Warren & Brandeis, 1890). Mereka juga berasumsi bahwa gosip tidak lagi menjadi sumber daya bagi orang-orang yang menganggur dan keji tetapi telah menjadi perdagangan yang dilakukan oleh industri seperti halnya barang bekas. Sehingga, perlindungan privasi individu seharusnya tidak hanya diarahkan kepada intervensi pers, fotografi, atau perangkat modern lainnya yang merekam.

Dalam sistem hukum *common law*, hukum menjamin hak setiap individu untuk menentukan sejauh mana pikiran, sentimen, dan emosinya dikomunikasikan kepada orang lain. Seorang individu memiliki otoritas penuh atas segala kekayaan yang dimilikinya, baik berupa materi yang berwujud maupun tidak berwujud. Konsekuensinya adalah jika tidak ada izin dari pemegang otoritas, seseorang atau pun pers tidak memiliki hak untuk menginformasikan atau

pun sekedar mengetahui kekayaan tersebut. Konsep tersebut setali tiga uang dengan konsep hak untuk tidak diserang atau dipukuli, hak untuk tidak dipenjara, hak untuk tidak dituntut secara jahat, dan hak untuk tidak dicemarkan nama baiknya. Lebih lanjut, konsep tersebut tidak hanya melindungi dari publikasi yang melanggar hukum atau menyesatkan. Namun, bisa atas dasar dugaan pelanggaran suatu kontrak tersirat atau kepercayaan atau keyakinan. Bahkan, secara eksplisit mereka mengatakan bahwa perlindungan yang sama diberikan pada emosi dan sensasi yang diekspresikan dalam komposisi musik atau karya seni lain seperti pada komposisi sastra dan kata-kata yang diucapkan, pantomim yang diperankan, sonata yang dipertunjukan.

Samuel Warren dan Louis Brandeis juga memberi penjelasan terkait limitasi dari perlindungan privasi atau istilah lainnya adalah privasi tidaklah bersifat absolut. Pembatasan tersebut dijabarkan sebagai berikut (Yuniarti, 2019):

(1) tidak menutup kemungkinan untuk mempublikasikan informasi pribadi seseorang untuk kepentingan publik;
(2) tidak ada perlindungan privasi apabila tidak ada kerugian yang diderita;
(3) tidak ada privasi apabila orang yang bersangkutan telah menyatakan persetujuan bahwa informasi pribadinya akan disebarkan kepada umum;
(4) persetujuan dan privasi patut mendapat perlindungan hukum karena kerugian yang diderita sulit untuk dinilai.

Fair Kredit Reporting Act 1970 (AS-FCRA) merupakan UU pertama yang secara eksplisit melindungi data pribadi dari kemungkinan terburuk data yang telah dikomputerisasi. UU tersebut digunakan sebagai upaya perlindungan konsumen dalam dunia perkreditan yang

jikalau terdapat kesalahan data akibatnya bisa parah. Presiden Richard Nixon menjustifikasi kondisi tersebut. Dia menyatakan bahwa terdapat sisi gelap dari upaya perkembangan teknologi informasi yang dapat berdampak kepada aspek finansial.

Saat ini, meskipun Amerika sering dikritik karena minimnya UU federal yang mengatur perlindungan data pribadi dan privasi, mosaik UU yang mengatur berbagai industri dan penggunaan data memberikan perlindungan yang rinci dan kuat (Reed, 2018). Walaupun *California Consumer Privacy Act* 2018 akan memicu kondisi rezim hukum Amerika serupa dengan GDPR, Amerika masih membutuhkan waktu yang lama untuk menyeragamkan negara bagiannya memiliki UU perlindungan data pribadi dan privasi.

2. Singapura

Pada tahun 2012, Singapura resmi memiliki UU yang mengatur tentang privasi dan perlindungan data pribadi. Fokus utama dari *Personal Data Protection Act* (PDPA) Singapura adalah untuk "*curb excessive and unnecessary collection of individuals' personal data by businesses, and include requirements such as obtaining consent of individuals to disclose their personal information*" (Inside Privacy, 2011). Sebelum berlakunya UU ini, kondisi hukum data pribadi Singapura belum cukup komprehensif dan masih tersebar dibeberapa UU sektoral. Bahkan, tidak ada perlindungan hukum bagi individu untuk meminta bantuan hukum terhadap siapa pun dalam kaitannya dengan penanganan informasi tanpa persetujuannya (Chick, 2013).

Implikasi dari berlakunya PDPA adalah seluruh organisasi dan pihak swasta diharuskan memenuhi standar minimum dari apa yang telah ditetapkan PDPA. Ketentuan terdapat pada Pasal 4 ayat (3) PDPA yang berbunyi, "*An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by*

the organisation itself." Dalam UU ini, organisasi didefinisikan sebagai *includes any individual, company, association or body of persons, corporate or unincorporated, whether or not – formed or recognised under the law of Singapore or resident, or having an office or a place of business, in Singapore*. Organisasi memiliki batasan dalam mengumpulkan, menggunakan, dan pengungkapan data klien-kliennya, yakni *nature of the protection*. Walaupun mengedepankan persetujuan dari pemilik data, organisasi tidak bisa selamanya meminta persetujuan individu yang terkait dengan penggunaan data pribadinya. Ada batasan lain yang dinamakan "*a reasonable person would consider appropriate in the circumstances*" dan organisasi harus memberitahu alasan penggunaan data sebelum melakukan pemrosesan data.

Individu juga memiliki otoritas dalam mengendalikan persebaran data pribadi miliknya. Seperti yang telah tertulis di Pasal 22 ayat (1) PDPA, "*An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation*". Kecuali organisasi memiliki alasan yang logis untuk tidak melakukan koreksi, organisasi harus melakukan koreksi sesegera mungkin dan menyebarluaskan data pribadi yang telah dikoreksi kepada organisasi lain yang juga memiliki kepentingan dalam penggunaan data pribadi tersebut. Ini merupakan manifestasi dari konsep perlindungan, keterbukaan, dan kendali individu atas informasinya sendiri.

Singapura juga memiliki komisi yang spesifik menangani perlindungan data pribadi, yakni *Personal Data Protection Commission* (PDPC) yang melekat pada *The Info-communications and Media Development Authority* (IMDA). Fungsi dari PDPC adalah sebagai berikut:

a) *to promote awareness of data protection in Singapore;*
b) *to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection;*
c) *to advise the Government on all matters relating to data protection;*

d) *to represent the Government internationally on matters relating to data protection;*
e) *to conduct research and studies and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;*
f) *to manage technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or inter-governmental organisations, on its own behalf or on behalf of the Government;*
g) *to administer and enforce this Act;*
h) *to carry out functions conferred on the Commission under any other written law; and*
i) *to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order published in the* Gazette.

PDPA mengadopsi pendekatan berbasis pengaduan dan audit. Dengan demikian, PDPC akan memiliki kekuatan untuk menindak organisasi yang tidak taat dengan ketentuan yang telah ditetapkan oleh pemerintah. Komisi tersebut juga dapat memberi sanksi denda kepada organisasi yang tidak taat tersebut. Apabila ada organisasi atau individu yang menghalang-halangi PDPC dalam menjalankan tugas dan kewenangannya maka subjek hukum tersebut dapat dikenakan hukuman pidana. Hal ini sangat baik dalam mewujudkan prinsip akuntabilitas dan transparansi.

3. Malaysia

Jika kita meninjau aturan hukum di negara yang berbatasan langsung dengan Indonesia, yakni Malaysia, hak atas privasi tidak dijamin di dalam konstitusi mereka. Lebih dari 10 tahun lalu, proyek *Multimedia Super Corridor Malaysia* atau MSC mendorong pemerintah Malaysia untuk beralih ke negara ekonomi berbasis ilmu pengetahuan (Yusoff,

2011). Hingga pada akhirnya, pada 10 Juni 2010, Malaysia secara resmi memiliki *Personal Data Protection Act* (PDPA). Mayoritas substansi dari PDP dipengaruhi oleh *Hong Kong Personal Data (Privacy) Ordinance* 1995 dan *Britania Raya Data Protection Act* 1998. Namun, PDPA ini tetap dimodifikasi supaya cocok dengan kultur masyarakat dan perkembangan zaman.

PDPA mendefinisikan data pribadi sebagai segala informasi atau opini yang berhubungan dengan identifikasi diri atau dapat mengidenfitikasi kehidupan seseorang yang diproses secara manual ataupun elektronik. Akan tetapi, informasi yang diproses menyangkut tujuan pelaporan kredit yang dijalankan oleh agen pelaporan kredit tidak termasuk karena berada di bawah aturan *Credit Reporting Agencies Act* 2009. Limitasi lain dari berlakunya undang-undang ini adalah hanya berlaku pada sektor swasta, sehingga badan-badan pemerintah Malaysia tidak tunduk pada undang-undang ini (Djafar & Santoso, 2020).

Implementasi dari PDPA dapat melindungi subjek dari pemilik data ketika melakukan transaksi komersial. Hal ini bertujuan untuk memberi kepastian kepada subjek pemilik data sebelum datanya diproses oleh pengolah data bahwa data pribadinya diproses sesuai dengan protokol yang aman.

Dengan berlakunya PDPA sebagai hukum positif di Malaysia maka subjek hukum (pemilik data) memiliki hak sebagai berikut:

a) *The right of acces to personal data;*
b) *The right to correct personal data;*
c) *The right to withdraw consent to processing of personal data;*
d) *The right to prevent processung likely to cause damage or distress;*
e) *The right to prevent processing for direct marketing purposes.*

Dari segi keamanan transfer data lintas negara, PDPA memberi batasan. PDPA tidak memperbolehkan transfer data pibadi kecuali kepada subjek-subjek yang ditelah

berkerja sama dengan Menteri Informasi, Kebudayaan, dan Komunikasi atau terdapat pengecualian lain seperti persetujuan individu untuk pelaksanaan kontrak serta negara atau tempat yang menjadi tempat mentransfer data pribadi dapat memberikan jaminan perlindungan data pribadi yang sama setara dengan yang PDPA berikan (Greeneaf, 2014).

The Organizationfor Econimic and Coorperation Development (OECD) turut andil dengan merumuskan suatu *guidelines* atau prinsip dasar dalam rangka perlindungan data pribadi dan privasi yang dapat dijadikan suatu acuan dalam membuat sebuah aturan hukum (Saiful Rizal, 2019), prinsip-prinsip tersebut diatur sebagai berikut:

a) Collection limitation principle
b) Data quality principle
c) Purpose specification principle
d) Use limitation principle
e) Security safeguards principle
f) Openness principle
g) Individual participation principle
h) Accountability principle

Prinsip tersebut digunakan Malaysia sebagai bahan kajian dalam PDPA. Sehingga, undang-undang ini dapat secara tegas memberi perlindungan dan kepastian hukum kepada warga negaranya.

Atas dasar berlakunya undang-undang inilah Malaysia membentuk Pesuruhjaya Perlindungan Data Pribadi. Lembaga tersebut memiliki fungsi sebagai berikut:

a. memberi nasihat kepada Menteri tentang kebijakan nasional untuk melindungi datapribadi dan semua hal lain yang relevan.
b. menerapkan dan menegakkan hukum perlindungan data pribadi, termasuk perumusankebijakan dan prosedur operasi.

c. mempromosikan dan mendorong asosiasi atau badan yang mewakili pengguna datauntuk memberikan kode praktik dan menyebarluaskan kode.
d. memantau perkembangan pemrosesan data pribadi, untuk memperhitungkankemungkinan dampak dari pengembangan tersebut terhadap privasi individu sehubungan dengan data pribadinya.
e. memantau dan mengawasi kepatuhan terhadap ketentuan Undang-Undang ini, termasukpenerbitan surat edaran, pemberitahuan penegakan hukum atau instrumen lain kepada siapa pun.
f. berkomunikasi dan bekerja sama dengan orang-orang yang melakukan fungsiperlindungan data pribadi di tempat mana pun di luar Malaysia sehubungan dengan hal-hal yang menjadi kepentingan bersama, termasuk hal-hal yang memengaruhi privasi individu terkait dengan data pribadi mereka.
g. untuk melakukan kegiatan apa pun dan untuk melakukan hal-hal yang mungkin diperlukan,untuk memberikan yang baik dan pantas untuk administrasi Undang-undang ini, atau tujuan lain yang konsisten dengan Undang-Undang ini sebagaimana dapat diarahkan oleh Menteri.

4. Indonesia

Pada amandemen kedua Undang-Undang Dasar 1945, Indonesia telah memperluas cakupan bahasan pada BAB mengenai HAM. Salah satunya bahasannya terkait dengan jaminan atas hak privasi, sebagaimana tertuang pada dua pasal berikut:

Pasal 28 H ayat (4): *Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-sewenang oleh siapa pun.*

Pasal 28 G ayat (1): *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 ketakukan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Tidaknya menjelaskan soal hak atas perlindungan data pribadi dan privasi tersebut, konstitusi telah menjamin ketentuan pengaman atau *safeguards clause* terkait dengan HAM tersebut dan hal ini dapat ditermukan pada Pasal 28 J UUD Tahun 1945 yang menyatakan, "*Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis*." Mahkamah Konstitusi menetapkan perlindungan data pribadi dan privasi bukan merupakan suatu hak yang tidak dapat dikurangi. Dasar dari pernyataan tersebut terdapat pada Pasal 28 J ayat (2) UUD Tahun 1945.

Walaupun perlindungan data pribadi dan privasi sudah diamanatkan oleh konstitusi. Akan tetapi, hingga sampai saat ini Indonesia masih belum memiliki undang-undang yang mengatur perlindungan data pribadi dan privasi secara spesifik. Pengaturan terkait perlindungan data pribadi dan privasi masih terpisah dibeberapa peraturan perundang-undangan, menurut riset yang dilakukan oleh Elsam, terdapat 30 peraturan yang menyinggung persoalan tersebut, seperti pada UU 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 43 Tahun 2009 tentang Kearsipan, UU No. 8 Tahun 1997 tentang Dokumen Perusahaan, UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan, UU No. 36 Tahun 2009 tentang Kesehatan, UU No. 36 Tahun 1999 tentang Telekomunikasi, dan UU 24 Tahun 2013 tentang Perubahan atas UU No. 23 Tahun 2006 tentang Administrasi Kependudukan, dan masih banyak lagi.

UU Hak Asasi Manusia juga memberi justifikasi terhadap perlindungan data pribadi dan privasi dalam beberapa pasalnya. Pasal-pasal tersebut adalah:

Pasal 14: (1) *Setiap orang berhak untuk berkomunikasi dan memperoleh informasi yang diperlukan untuk mengembangkan pribadi dan lingkungan sosialnya*. (2) *Setiap orang berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan sejenis sarana yang tersedia.*

Pasal 29 ayat (1): *Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya*.

Pasal 31: (1) *Tempat kediaman siapapun tidak boleh diganggu*. (2) *Menginjak atau memasuki suatu pekarangan tempat kediaman atau memasuki suatu rumah bertentangan dengan kehendak orang yang mendiaminya, hanya diperbolehkan dalam hal-hal yang telah ditetapkan oleh undang-undang*.

UU Informasi dan Transaksi Elektronik (UU ITE) menerapkan hak pribadi (*privacy rights*). Yang kemudian dalam penjelasan UU tersebut dijelaskan sebagai berikut:

a. hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;
b. hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai;
c. hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik merupakan peraturan pelaksana dari UU ITE. PP tersebut menyatakan penyelenggara sistem elektronik wajib memperoleh persetujuan dari pemilik data pribadi sebelum melakukan penggunaan atau pemanfaatan data pribadi. Namun demikian, PP No. 82 Tahun 2012 tidak merefleksikan prinsip-prinsip dasar perlindungan data pribadi secara lebih detail. Ruang lingkup yang lebih luas terdapat pada Permen Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Pasal 2 ayat (1) mengatur

cakupan dari keberlakuan Permen ini, yakni perlindungan dalam hal perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Selain itu, terdapat pula PP No. 71 Tahun 2019 yang diharapkan dapat memenuhi dan menjalankan seluruh itikad baik dari UU ITE.

BAB V
HUKUM MAYANTARA DI INDONESIA

HUKUM MAYANTARA DI INDONESIA

1. Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Pidana (KUHP) berlaku atas dasar Aturan Peralihan Pasal II UUD 1945 dan mulai diperbaharui mulai tahun 1946 melalui UU Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana (Bambang Hartanto, 2013). Sifat KUHP dalam sistem hukum di Indonesia adalah sebagai aturan hukum yang bersifat umum. Sehingga, karena sistem hukum di Indonesia menganut asas *lex specialis derogat legi generalis*, KUHP dapat dikesampingkan ketika terdapat aturan pidana yang bersifat khusus. Ketentuan ini secara eksplisit telah diatur dalam KUHP, yakni pada Pasal 63 ayat (2).

Pasal 1 KUHP berbunyi "*tidak ada perbuatan pidana jika sebelumnya tidak dinyatakan dalam suatu ketentuan undang-undang*." Pasal ini merupakan manifestasi dari asas *nullum delictum noela poena siena praveia legi peonali* yang berarti ketentuan pidana dalam undang-undang hanya dapat diberlakukan terhadap suatu tindak pidana yang terjadi sesudah ketentuan pidana dalam undang-undang itu diberlakukan, dengan kata lain, ketentuan pidana dalam undang-undang itu hanya berlaku untuk waktu kedepan (Tongat, 2008). Jika menggunakan logika dari ketentuan ini, apabila tidak ada undang-undang yang mengatur tentang *cyber crime* maka kejahatan tersebut tidak dapat dipidanakan.

Berkaitan dengan jenis *cyber crime,* Heru Soepraptomo (2001) membaginya sebagai berikut:

a. Penipuan komputer (*computer fraud*) yang mencakup:
   1) Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan menggunakan sarana komputer/siber dengan melawan hukum, ialah

dalam bentuk penipuan data dan penipuan program, dengan cara:

Memasukkan instruksi yang tidak sah, yang dilakukan oleh seorang yang berwenang (atau tidak), yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya melakukan transfer sejumlah uang). Lalu mengubah data input; yang dilakukan dengan cara memasukkan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum (misalnya memasukkan data gaji pegawai melebihi yang seharusnya). Lalu merusak data; dilakukan seseorang dengan merusak *print out* atau *output* dengan maksud untuk mengaburkan, menyembunyikan data atau informasi untuk maksud yang tidak baik. Serta Penggunaan komputer untuk sarana melakukan perbuatan pidana, misalnya dalam pemecahan informasi/kode lewat komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.

2) Perbuatan pidana penipuan, yang didalamnya termasuk unsur perbuatan lain, seperti menghindarkan diri dari kewajiban (misalnya pajak) atau untuk memperoleh sesuatu yang bukan hak/miliknya melalui sarana komputer.
3) Perbuatan curang untuk memperoleh secara tidak sah harta benda milik orang lain, misalnya seseorang dapat mengakses komputer mentransfer rekening orang ke rekeningnya sendiri.
4) Konspirasi penipuan, ialah perbuatan pidana yang dilakukan beberapa orang bersama-sama untuk melakukan penipuan dengan sarana komputer.

b. Perbuatan pidana penggelapan, pemalsuan pemberian informasi melalui komputer yang merugikan pihak lain dan menguntungkan diri sendiri.

c. Perbuatan pidana komunikasi, ialah hacking yang dapat membobol sistem *online* komputer yang menggunakan sistem komunikasi. *Hacking*, ialah melakukan akses terhadap sistem komputer tanpa seizin atau dengan melawan hukum sehingga dapat menembus sistem pengamanan komputer yang dapat mengancam berbagai kepentingan.
d. Perbuatan pidana perusakan sistem komputer, baik merusak data atau menghapus kode-kode yang menimbulkan kerusakan dan kerugian. Contohnya adalah berupa penambahan atau perubahan program, informasi, media, sehingga merusak sistem; atau dengan sengaja menyebarkan virus yang dapat merusak program dan sistem komputer; atau pemerasan dengan menggunakan sarana komputer/ telekomunikasi.
e. Perbuatan pidana yang berkaitan dengan hak milik intelektual, hak cipta, dan hak paten, ialah berupa pembajakan dengan memproduksi barang-barang tiruan untuk mendapatkan keuntungan melalui perdagangan.

Jika menggunakan pendapat tersebut sebagai dasar pengklasifikasian tindak pidana *cyber crime* maka terdapat beberapa delik dalam KUHP yang memiliki keterkaitan dengan hal tersebut. Berikut merupakan beberapa tindak pidana dalam KUHP yang *modus operandinya* dimungkinkan menggunakan teknologi informasi:

a. Pasal 378 KUHP terkait dengan tindak pidana pemalsuan. Pengadilan Negeri sudah sering menjatuhi putusan tindak pidana pemalsuan yang menggunakan media *online*. Salah satunya adalah Putusan Hakim Pengadilan Negeri Sleman No. 94/Pid.B./2002/PN.SLMN dengan terdakwa Petrus Pangkur, terdakwa melakukan tindak pidana penipuan (pemalsuan surat kartu kredit/*carding*) secara *online*.
b. Pasal 369 KUHP terkait dengan tindak pidana pemerasan dan pengancaman. Namun karena sudah terdapat aturan

yang bersifat khusus, dalam penuntutan tindak pidana pemerasan dan pengancaman melalui internet dapat menggunakan Pasal 27 ayat (4) UU ITE.

c. Pasal 263 KUHP terkait dengan tindak pidana pemalsuan surat. Teknologi informasi dapat menjadi katalis dalam melakukan tindak pidana ini karena komunikasi antar pelaku akan semakin mudah.
d. Pasal 362 KUHP terkait dengan tindak pidana pencurian. Tipikal tindak pidana pencurian yang menggunakan teknologi adalah kasus *unauthorized acces to computer system and service* dan *craking* (Mansur dan Gultom, 2005).
e. Pasal 363 KUHP terkait dengan tindak pidana *skimming*. *Skimming* merupakan tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu secara ilegal (Wardani dan Maskun, 2019). Pelaku akan mendapatkan nomor kartu kredit atau debit korban dengan menggunakan *skimmer*. Dengan menggunakan *skimmer*, pelaku dapat menggandakan data dari suatu kartu ATM kepada ATM kosong lainnya.

Perkembangan zaman mengakibatkan lahirnya berbagai jenis tindak pidana baru. Sehingga perlu pengaturan yang bersifat khusus untuk dapat menyelesaikan berbagai persoalan ini. Mengenai hal ini Soedjono Dirdjosisworo (2002) menyatakan "Perubahan dan penyesuaian sosial serta perkembangan teknologi selama setengah abad sejak 1958 (UU NO.73/58) demikian pesatnya, dan kepesatan perkembangan sosial dan teknologi serta semakin berpengaruhnya globalisasi yang terus didorong oleh teknologi informasi dan komunikasi sangatlah terasa bahwa Kitab Undang-Undang Hukum Pidana sudah sejak lama tidak mampu secara sempurna mengakomodasi dan mengantisipasi kriminalitas yang meningkat, baik kualitatif maupun kuantitatif dengan jenis,

pola, dan *modus operandi* yang tidak terdapat dalam KUHP dan contoh yang paling menonjol adalah *cyber crime*."

2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

UU Informasi dan Transaksi Elektronik atau yang biasa disingkat dengan UU ITE merupakan produk hukum yang secara khusus mengatur tentang *cybercrime*. Ferdinandus Setu, Plt. Kepala Biro Humas Kementerian Komunikasi dan Informatika (Kominfo) mengatakan UU ITE adalah unifikasi dari dua jenis Rancangan Undang-Undang (RUU), yakni RUU Tindak Pidana Teknologi Informasi yang diusulkan oleh Universitas Padjajaran dan RUU E-*Commerce* yang diusulkan oleh Universitas Indonesia (Kominfo, 2019). Setelah Pemerintah menyelaraskan kedua RUU tersebut, melalui Surat Presiden RI No.R/70/Pres/9/2005 pada tanggal 5 September 2005, naskah undang-undang ini secara resmi dilimpahkan kepada DPR RI. Panja berlangsung mulai 29 Juni 2007 sampai 31 Januari 2008 dengan 23 kali rapat dengar pendapat dan terakhir rapat paripurna DPR RI tanggal 25 Maret 2008 (Soemarno Partodihardjo, 2008).

Dalam perumusannya, UU ITE mengacu kepada beberapa peraturan yang sudah berlaku secara internasional maupun peraturan di berbagai negara di Eropa, Amerika, dan Asia. Salah satunya adalah *Convention on Cybercrime* (COC), konvensi ini bertujuan untuk mengharmonisasikan hukum dari negara-negara anggota, baik hukum materiil maupun prosedural, termasuk pengaturan mengenai kerja sama internasional dalam menangani *cybercrime* (Setiawan dan Arista, 2013). Substansi yang ada dalam konvensi ini dijadikan acuan utama dalam pembentukan peraturan perundang-undangan mengenai tindak pidana siber oleh negara-negara di dunia, termasuk diterapkan dalam UU ITE (Josua Sitompul, 2012).

Kehadiran UU ITE merupakan usaha untuk melindungi baik masyarakat selaku konsumen jasa maupun pelaku industri dalam mengembangkan inovasi produk layanannya, selain itu diharapkan dapat lebih mendorong pengembangan penggunaan teknologi secara lebih meluas serta sekaligus dapat memberikan keamanan serta kepastian hukum dalam seluruh kegiatan transaksi (Nazarudin Tianotak, 2011). Undang-undang ini juga dapat melindungi dan menunjang keamanan nasabah perbankan dalam melakukan transfer dana secara elektronik. Selain itu, dalam kaitannya dengan tindak pidana, UU ITE akan menjadi *lex specialis* dari pemidanaan kejahatan-kejahatan yang menggunakan media elektronik atau jaringan komputer.

Dalam konsiderannya, undang-undang ini menyoal beberapa isu, yakni pembangunan nasional, globalisasi informasi, perkembangan dan kemajuan teknologi informasi, sikap dalam penggunaan dan pemanfaatan teknologi informasi, perdagangan dan pertumbuhan perekonomian nasional, dan aspek keamanan dalam menggunakan teknologi informasi. Undang-undang ini terdiri atas 13 Bab dan 54 Pasal memiliki cakupan materi yang cukup luas, diantaranya adalah:

a. *Extraterritorial jurisdiction;*
b. Asas netral teknologi pengakuan informasi dan/atau dokumen elektronik (*certification authority*);
c. Penyelenggaraan sistem elektronik;
d. Nama domain;
e. Perlindungan hak pribadi;
f. Perbuatan yang dilarang; dan
g. Ketentuan pidananya.

UU ITE mendefinisikan informasi elektronik sebagai satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda,

angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Sedangkan transaksi elektronik sebagai perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau, media elektronik lainnya.

Ketika berbicara soal *cybercrime* maka kejahatannya akan berpotensi lintas teritorial atau universal. Pasal 2 UU ITE berbunyi "*Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.*" Implikasi dari pasal tersebut adalah UU ITE akan bersifat ekstrateritorial atau *extrateritorial jurisdiction*. Sehingga keberlakuan UU ITE tidak hanya berlaku kepada Warga Negara Indonesia saja, melainkan kepada setiap orang yang melanggar ketentuan UU ITE. Artinya, ketika ada Warga Negara Asing atau badan hukum asing melakukan perbuatan yang merugikan kepentingan Indonesia atau melanggar ketentuan UU ITE akan terkena sanksi dari undang-undang ini. Yang dimaksud dengan kepentingan Indonesia adalah meliputi, tetapi tidak terbatas pada, kerugian yang ditimbulkan terhadap kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia (Penjelasan Pasal 2).

Undang-undang ini juga mengatur kedudukan tanda tangan elektronik, dokumen elektronik, dan hasil cetakannya di mata hukum. Dalam Pasal 5 ayat (1) dikatakan bahwa ketiga entitas tersebut merupakan alat bukti hukum yang sah (selama memenuhi persyaratan yang terdapat pada Pasal 11). Namun demikian, secara praktik, ketentuan ini masih menuai kontroversi karena

bertentangan dengan beberapa peraturan yang sudah berlaku, yakni KUHPerdata dan UU Jabatan Notaris. Kedua aturan tersebut menyatakan bahwa akta notaris harus dibuat oleh atau dihadapan pejabat umum yang berwenang untuk itu ditempat akta itu dibuat. Sedangkan tanda tangan elektronik ataupun dokumen elektronik tidak sesuai dengan konsep tersebut karena bukan merupakan dokumen tertulis atau *non paperless* (Listyana, dkk, 2014).

Dalam Bab IV diatur terkait dengan penyelenggara sertifikasi elektronik dan sistem elektronik. Adapun tujuan diadakannya dua penyelenggara tersebut adalah untuk mewujudkan transaksi elektronik yang terpercaya, aman, dan andal. Oleh karena itu dalam Pasal 41 PP Penyelenggara Sistem dan Transaksi Elektronik dikatakan bahwa penyelenggaraan transaksi elektronik dalam lingkup atau privat yang menggunakan sistem elektronik untuk kepentingan pelayanan publik wajib menggunakan sertifikat keandalan dan/atau sertifikat elektronik. Sertifikat keandalan akan dimiliki pelaku usaha jika memenuhi beberapa persyaratan, seperti lolos standar perangkat keras, perangkat lunak, standar tenaga ahli, keamanan data, dan pengelola data (Setiawan, 2014).

Bab V mengatur tentang transaksi elektronik. Dalam Pasal 18 ayat (3) dikatakan bahwa jika para pihak hendak melakukan transaksi elektronik internasional maka hukum yang berlaku didasarkan pada asas hukum perdata internasional. Kemudian pada ayat (4) dan ayat (5) mengatur tentang kewenangan untuk menetapkan forum mana yang dipilih ketika terjadi sengketa. Namun, ketika gugatan berada dalam jangkauan hukum nasional maka akan dilakukan sesuai dengan peraturan perundang-undangan (Bab VIII). Selanjutnya, apabila timbul akibat hukum dalam pelaksanaan transaksi elektronik maka Pasal 21 ayat (2) mengatur sebagai berikut:

a. Jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab para pihak yang bertransaksi;
b. Jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pemberi kuasa; atau
c. Jika dilakukan melalui agen elektronik, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab penyelenggara agen elektronik.

UU ITE juga melindungi nama domain setiap penyelenggara negara, orang, badan usaha, dan/atau masyarakat yang telah didaftarkan. Perlindungan ini menggunakan prinsip pendaftar pertama atau *first come first serve*. Namun, apabila terdapat pihak yang menggunakan nama domain secara tanpa hak, pemilik nama domain dapat mengajukan gugatan pembatalan nama domain yang dimaksud. Selain itu, undang-undang ini menegaskan bahwa segala 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 (HKI) tetapi tetap memperhatikan ketentuan peraturan perundang-undangan.

Dalam perkembangannya, undang-undang ini sudah mengalami satu kali perubahan, yakni pada tahun 2016 saat Kominfo dipimpin oleh Rudiantara. Perubahan ini disahkan menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Terdapat tujuh poin perubahan yakni:

a. Untuk menghindari multitafsir terhadap ketentuan larangan mendistribusikan, mentransmisikan dan/atau memungkinkan informasi elektronik dapat diakses yang mengandung penghinaan dan/atau pencemaran nama

baik pada ketentuan Pasal 27 ayat (3), dilakukan tiga perubahan sebagai berikut:

1) Menambahkan penjelasan terkait istilah "mendistribusikan, mentransmisikan dan/atau memungkinkan informasi elektronik dapat diakses".
2) Menegaskan bahwa ketentuan tersebut adalah delik aduan, bukan delik umum.
3) Menegaskan bahwa unsur pidana pada ketentuan tersebut mengacu pada ketentuan pencemaran nama baik dan fitnah yang diatur dalam KUHP.

b. Menurunkan ancaman pidana dengan dua ketentuan, yakni:
   1) Pengurangan ancaman pidana penghinaan atau pencemaran nama baik dari pidana penjara paling lama enam tahun menjadi empat tahun. Sementara penurunan denda dari paling banyak Rp 1 miliar menjadi Rp 750 juta.
   2) Pengurangan ancaman pidana pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti dari pidana penjara paling lama 12 tahun menjadi empat tahun. Begitu juga dengan denda yang dibayarkan, dari paling banyak Rp 2 miliar menjadi Rp 750 juta.
c. Pelaksanaan putusan Mahkamah Konstitusi terhadap dua ketentuan sebagai berikut:
   1) Mengubah ketentuan Pasal 31 ayat (4) yang semula mengamanatkan pengaturan tata cara intersepsi atau penyadapan dalam Peraturan Pemerintah menjadi dalam Undang-Undang.
   2) Menambahkan penjelasan pada ketentuan Pasal 5 ayat (1) dan ayat (2) mengenai keberadaan informasi Elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah.
d. Melakukan sinkronisasi ketentuan hukum acara pada Pasal 43 ayat (5) dan ayat (6) dengan ketentuan hukum acara pada KUHAP, sebagai berikut:

1) Penggeledahan atau penyitaan yang semula harus mendapatkan izin Ketua Pengadilan Negeri setempat, kini disesuaikan kembali dengan ketentuan KUHAP.
2) Penangkapan penahanan yang dulunya harus meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu 1x24 jam, kini disesuaikan kembali dengan ketentuan KUHAP.

e. Memperkuat peran Penyidik Pegawai Negeri Sipil (PPNS) dalam UU ITE pada ketentuan Pasal 43 ayat (5):
   1) Kewenangan membatasi atau memutuskan akses terkait dengan tindak pidana teknologi informasi.
   2) Kewenangan meminta informasi dari Penyelenggara Sistem Elektronik terkait tindak pidana teknologi informasi.
f. Menambahkan ketentuan mengenai *right to be forgotten* alias hak untuk dilupakan pada ketentuan Pasal 26 yang terbagi atas dua hal, yakni:
   1) Setiap penyelenggara sistem elektronik wajib menghapus konten informasi elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
   2) Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik yang sudah tidak relevan.
g. Memperkuat peran pemerintah dalam memberikan perlindungan dari segala jenis gangguan akibat penyalahgunaan informasi dan transaksi elektronik dengan menyisipkan kewenangan tambahan pada ketentuan Pasal 40:
   1) Pemerintah wajib melakukan pencegahan penyebarluasan informasi elektronik yang memiliki muatan yang dilarang.
   2) Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada penyelenggara sistem elektronik untuk melakukan pemutusan akses

terhadap informasi elektronik yang memiliki muatan yang melanggar hukum.

3. **Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang**

Pasal 1 ayat (2) UU No. 5 Tahun 2018 mendefinisikan terorisme sebagai perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik, atau gangguan keamanan. Sejatinya, tindak pidana terorisme merupakan kejahatan yang sudah terorganisir. Dalam penjelasan umum UU No. 5 Tahun 2018 disebutkan bahwa tindak pidana ini bersifat klandestin yaitu rahasia, diam-diam, atau gerakan bawah tanah, lintas negara yang didukung oleh pendayagunaan teknologi modern di bidang komunikasi, informatika, transportasi, dan persenjataan modern sehingga memerlukan kerja sama di tingkat internasional untuk menanggulanginya.

Dalam rangka mengekspansi atau pun memperkuat jaringannya, organisasi terorisme sudah menggunakan teknologi informasi dan komunikasi. Misalnya jaringan ISIS di Indonesia, mereka menggunakan *youtube* (video berjudul "*Join the Ranks*") sebagai media propagandanya. Tokoh yang tampil di video tersebut adalah Abu Muhammad Al-Indonesi, dia mengajak umat Islam di Indonesia untuk melakukan jihat ke Irak dan Suriah (mendukung ISIS). Pemerintah merespon dengan langsung melarang peredaran paham ISIS di Indonesia dengan alasan tidak sesuai dengan ideologi Pancasila.

Abu Muhammad Al-Indonesi alias Bahrum Syah merupakan jaringan organisasi Al-Muhajirun (IPAC, 2014). Al-Muhajirun berusaha membentuk jaringan global dengan mengadvokasi kelompok-kelompok yang mendukung penegakan syariat Islam, bahkan dengan cara radikal (Rijal, 2017). Pusat Al-Muhajirun berada di Inggris, yang kemudian bernama "Islam4UK" atau "Sharia4UK". Sedangkan cabang di Indonesia sudah berdiri sejak tahun 2010 dengan nama "Sharia4Indonesia".

Tidak hanya berhenti dengan video *youtube*, simpatisan organisasi terorisme menggunakan media *online* untuk mengkampanyekan gerakannya. Kelompok Pro ISIS seperti M. Fachry, Bahrum Syah, dan Aman Abdurahman menggunakan *website* www.al-mustaqbal.net sedangkan kelompok Pro Al-Qaeda yang terdiri dari Abu Dujana, Zarkasih, Abu Tholut, Abu Jibriel menggunakan *website* www.arrahmah.com. (Bintar Mupiza, 2018).

Jika ditarik ke belakang, sebenarnya kelompok teroris di dunia sudah cukup *mainstream* dalam menggunakan teknologi informasi dan komunikasi. Sebelum tahun 1999, hampir 30 kelompok teroris ditemukan di internet oleh Departemen Pemerintahan Amerika Serikat (Banez, 2010). Puncaknya terjadi pada peristiwa 11 September 2001, kepemimpinan Al-Qaeda berusaha menyebarkan video dari persembunyian mereka di Pakistan melalui televisi Al-Jazeera tetapi mereka frustasi dengan segmen mereka yang sangat sedikit sehingga pesan bisa jadi disalah-persepsikan yang kemudian mereka beralih menggunakan internet untuk mengunggah secara lebih jelas dan detail tanpa adanya pengeditan (Gardner, 2013).

Barry Collin (1997) beranggapan munculnya fenomena tersebut sebagai akibat dari komputerisasi dalam berbagai bidang kehidupan manusia yang kemudian menciptakan kerentanan baru, sehingga ia menciptakan istilah iptakan istilah *cyber terrorism*. Dorothy E. Denning (2000) mendefinisikan *cyber terrorism* sebagai *unlawful attacks*

and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a goverment or its people in the furtherance of political or social objectives.

Konsep dari *cyber terrorism* adalah sebagai berikut (Rabiah dan Zahri, 2012):

a. Target: selain berfokus pada infrastruktur yang berbasis teknik informasi dan komunikasi (seperti jaringan *Critical National Information Infrastructure*), *cyber terrorism* juga menargetkan masyarakat sipil.
b. Motif: motif dari *cyber terrorism* bersifat sosial, politik, dan keyakinan terhadap suatu paham atau ideologi.
c. Metode penyerangan:
    1) Komputer dan jaringan internet sebagai senjata atau alat untuk melakukan *cyber attack*.
    2) Menjadi penyedia layanan informasi baik media elektronik maupun cetak. Dengan menjadi penyedia informasi, para *cyber terrorist* mampu untuk mengontrol tingkah laku atau respon dari orang-orang yang menerima informasi tersebut.
    3) Menyebarkan propaganda lewat media informasi. Seiring berkembangnya zaman kondisi penyebaran informasi menjadi semakin cepat, sehingga hal ini dimanfaatkan oleh cyber terroristuntuk melakukan propaganda tentang kegiatan teroris mereka.
d. Domain: *cyber terrorism* adalah konvergensi dari *cyber space* dan terorisme.
e. Tindakan pelaku: *cyber terrorist* melakukan tindakan melawan hukum dengan terencana untuk mengintimidasi atau memaksa pemerintah atau orang-orang dengan tujuan politik, sosial, atau tujuan ideologi yang dianut oleh mereka.
f. Dampak atau akibat: *cyber terrorism* dilakukan untuk menyebabkan kerusakan serius pada infrastruktur suatu negara maupun keamanan dalam skala internasional.

Jika menelisik instrumen hukum terorisme di Indonesia, pada Perppu No. 1 Tahun 2002 dan UU No. 15 Tahun 2003 sama sekali tidak ada pengaturan tentang *cyber terrorism*. Padahal, jaringan terorisme sendiri sudah sangat terorganisir secara rapi, mempunyai jaringan internasional yang kuat, memiliki dana yang besar, dan dalam melangsungkan operasinya kelompok teroris selalu menggunakan *hi tech technology* (Mahkamah Agung RI, 2007). Satu-satunya pasal yang memiliki kaitan dengan penggunaan teknologi informasi dan komunikasi dalam Perppu No. 1 Tahun 2002 jo. UU No. 15 Tahun 2003 adalah Pasal 27. Pasal tersebut mengatur tentang alat bukti pemeriksaan tindak pidana terorisme, yang mana menjadikan alat bukti elektronik (seperti data, rekaman, atau informasi yang terekam secara elektronik) sebagai alat bukti yang sah.

Pengaruh informasi global dalam bentuk propaganda di internet inilah yang merupakan potensi yang membahayakan sebelum perbuatan teror benar-benar terlaksanakan oleh teroris (Widianto, 2018). Untuk mengantisipasi hal ini, Pasal 12 B ayat (1) UU No. 5 Tahun 2018 mengatakan "*Setiap Orang yang dengan sengaja menyelenggarakan, memberikan, atau mengikuti pelatihan militer, pelatihan paramiliter, atau* ***pelatihan lain****, baik di dalam negeri maupun di luar negeri, dengan maksud merencanakan, mempersiapkan, atau melakukan Tindak Pidana Terorisme, dan/atau ikut berperang di luar negeri untuk Tindak Pidana Terorisme dipidana dengan pidana penjara paling singkat 4 (empat) tahun dan paling lama 15 (lima belas) tahun*." Maksud dari frasa **pelatihan lain** adalah seperti mengikuti pelatihan merakit bom menggunakan teknologi informasi. Apalagi di masa teknologi informasi dan komunikasi yang sudah berkembang dengan pesat, pelatihan semacam itu ataupun penyebaran doktrin melalui media *online* bukanlah suatu hal yang sulit.

Selain itu, UU No. 5 Tahun 2018 juga telah mengatur Badan Nasional Penanggulangan Teroris (BNPT). BNPT

menjadi pusat analisis dan pengendalian krisis yang berfungsi sebagai fasilitas bagi Presiden untuk menetapkan kebijakan dan langkah penanganan krisis, termasuk pengarahan sumber daya dalam menangani terorisme (Pasal 43 E ayat (2) UU No. 5 Tahun 2018).

Sebagai upaya menanggulangi *cyber terrorism*, BNPT (Deputi Bidang Penindakan dan Pembinaan Kemampuan) telah melakukan kerja sama dengan Direktorat Jenderal Aplikasi Informatika Kementerian Informasi dan Informatika pada tahun 2020. Adapun ruang lingkup kerja sama yang tertuang perjanjian kerja sama Nomor HK.01.00/24/2020 dan Nomor 20/KOMINFO/ DJAIHK.04/02/10/2020 meliputi pertukaran data dan informasi analisis dan *monitoring* evaluasi, penanganan konten yang dilarang yaitu informasi elektronik atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan, serta peningkatan kapasitas kelembagaan dan sumber daya manusia (BNPT, 2020).

Selain dengan Kemkominfo, BNPT juga melakukan kerja sama dengan Badan Siber dan Sandi Negara. Kepala BSSN Hinda Siburan (2010) mengatakan BSSN dapat mendukung BNPT dalam beberapa hal seperti pelaksanaan identifikasi kerentanan dan penilaian risiko, sistem dan infrastrukur teknologi informasi dan komunikasi, pengelolaan potensi ancaman siber dan pengawasan pemanfaatan ruang siber, bantuan penguatan *cyber security*, dan peningkatan kompetensi sumber daya manusia.

BAB VI
MASA DEPAN HUKUM MAYANTARA DI INDONESIA

A. MENAKAR PEMBENTUKAN HUKUM MAYANTARA MASA DEPAN

Saat ini, pesatnya kemajuan teknologi dan informasi telah membawa dampak yang cukup besar bagi kehidupan manusia. Hubungan serta aktivitas manusia yang semula terbatas dan memerlukan transaksi secara langsung menjadi hubungan dunia yang tanpa batas (*borderless*). Misalnya, seorang Warga Negara Indonesia (WNI) dari Jakarta dapat berkomunikasi dengan teman kuliahnya di New York, Amerika Serikat melalui aplikasi *video call* berbasis *Internet* dengan mudah dan praktis. Hal demikian dapat dimanfaatkan untuk berkontribusi dalam peningkatan kesejahteraan dan kemajuan peradaban manusia, sekaligus dimanfaatkan sebagai platform yang efektif untuk melakukan kejahatan seperti *hacking*, *carding, Data Leakage, Data Diddling* (Jati Kusuma, 2013). Bahkan untuk kejahatan yang semula konvensional dapat ditemukan perkembangan siber di dalamnya seperti *cyberwar*, terorisme, perdagangan ilegal, pornografi, dan lainnya.

Secara potensial, kemajuan ini berbanding lurus dengan tindakan *cybercrime* yang dapat merugikan sebagian bidang seperti, ekonomi, sosial, politik dan budaya yang menimbulkan dampak signifikan. Apalagi kejahatan tersebut cenderung tidak terlihat secara kasat mata dan bersifat transnasional.

Menurut pandangan dunia, Indonesia berada di peringkat 13 mengenai indeks keamanan siber global menurut *International Telecommunication Union* (ITU) dan *ABI Research* yang beranggotakan 193 negara di dunia. Dengan Amerika Serikat selaku puncak klasemen diikuti Kanada dan Australia yang menduduki peringkat tiga besar dunia (Ahmad Saudi, 2018). Selain itu, ID-SIRTII (Indonesia Security Incident Response Team on *I*nternet Infrastructure/CoordinationCenter)

dalam laporan tahunan keamanan siber dalam acara National Security Days di tahun 2014 mengemukakan bahwa Indonesia telah mendapat serangan siber lebih dari 42 juta sepanjang tahun 2014 dan cukup beresiko mengingat dampak dari keamanan siber yang lemah. Hal ini dijustifikasi dalam penyadapan pihak asing terhadap sejumlah pejabat Indonesia termasuk Presiden Susilo Bambang Yudhoyono. Melansir *New York Times*, penyadapan tersebut dilakukan oleh ASD (Australian Signals Directorate) dengan NSA (*No Such Agency*) dari Amerika Serikat untuk memberitahu NSA bahwa ASD telah melakukan pengawalan komunikasi antara pejabat Indonesia dengan salah satu firma hukum di Amerika Serikat (BBC News, diakses pada 13 April 2021). Hal demikian telah menimbulkan pernyataan sikap kekecewaan oleh Pemerintahan Indonesia terhadap Pemerintahan Australia saat itu. Bagi pertahanan dan keamanan negara, serangan siber pun tidak pilih kasih. Berkaca dari kejadian ini menjelaskan bahwa Indonesia adalah negara berkembang yang masih sedikit tertinggal dari segi penguasaan teknologi dan informasi sehingga menciptakan kekhawatiran mengenai resiko penyerangan siber sehingga membutuhkan penanganan yang khusus dari Pemerintah.

Selain itu ada pula kejahatan digital dalam bidang *e-commerce* yakni adanya dugaan bocornya data pribadi dari nasabah *KreditPlus*. Dugaan ini kemudian telah dikonfirmasi oleh pihak *KreditPlus* dengan menemukan jumlah data yang bocor menyentuh angka 890.000 data nasabah yang dijual dalam sebuah forum hacker dunia yang bernama *Raidforums*, dalam sebuah database berukuran 78 MB yang dijual seharga Rp. 50.000 dan diklaim telah bocor dari tanggal 16 Juli 2020 (Kompas, diakses pada tanggal 13 April 2021). Hal serupa dialami pengguna aplikasi *Tokopedia* yakni sebanyak 15 juta data pribadi penggunanya dijual di *Raidforums* dan sebanyak 91 juta data dijual di *Empire Market* senilai USD 5.000. (Kompas, diakses pada 12 April 2021).

B. GAGASAN HUKUM MAYANTARA

Dewasa ini, regulasi dasar yang dipergunakan untuk menangani segala permasalahan siber adalah Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dengan adanya UU ITE diharapkan dapat melindungi masyarakat dalam menggunakan teknologi informasi dan 'berselancar' di dunia siber. Disebutkan dalam Pasal 4 ayat (2) UU ITE bahwa 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. Namun dalam kebanyakan praktiknya, UU ITE digunakan dengan pendekatan politis-pragmatis untuk kepentingan seorang dan berujung kriminalisasi sepihak. Substansi dalam UU ITE masih perlu direvisi menggunakan pendekatan kebijakan publik yang inklusif bagi seluruh kalangan. Misalnya, unsur kelalaian yang telah diatur dalam KUHP namun belum diatur dalam UU ITE. Maka, pengaturan sejenis seperti KUHP, KUHAP, dan peraturan perundang-undangan lainnya masih belum mengatur secara komprehensif mengenai aktivitas masyarakat terutama perihal kejahatan di dunia digital. Oleh karenanya Indonesia masih memerlukan beberapa kajian dan inspirasi untuk menggagas sebuah pengaturan pidana atau *Penal Policy* (Wisnubroto, 1999) yang berkaitan pada dunia *cyberlaw*.

Dalam rangka memecahkan permasalahan siber maka perlu ada perencanaan kerja sama antar negara-negara dunia. Misalnya, NATO (North Atlantic Treaty Organization) yang menghimpun berbagai negara maju di dunia seperti Amerika Serikat, Belanda, Belgia, Britania Raya, Denmark, Islandia, Italia, Kanada, dan berbagai negara lainnya. NATO memiliki gagasan untuk memproteksi militer dan pasukan khusus dunia siber bagi anggotanya untuk menghindari ancaman siber mengenai pertahanan dan keamanan negara seperti kejadian

9/11 yang menimpa Amerika Serikat beberapa tahun lalu (Shawn Henry, 2018).

Sementara itu, konvensi internasional yang mengatur masalah *cybercrime* telah ada semenjak 2001 yang bernama Konvensi Budapest atau *Convention on Cybercrime* yang diadakan di Budapest, Hongaria. Konvensi ini bertujuan untuk menyatukan pandangan terhadap pengakuan dan penegakan hukum siber di seluruh dunia. Konvensi Budapest telah digagas oleh Uni Eropa namun tidak terbatas bagi negara manapun untuk menjalin kerjasama dalam perjanjian tersebut seperti Jepang, Filipina, dan Amerika Serikat (Akbar Kurnia, 2014). Namun definisi *cybercrime* menurut Kongres Perserikatan Bangsa-Bangsa (PBB) ke-10 di Wina pada bulan April 2000 hanya memfokuskan terhadap kejahatan yang berhubungan dengan komputer. Sehingga, Konvensi Budapest hanya mengatur secara khusus mengenai perlindungan data dari komputer saja.

Lanjutnya, konvensi ini diteruskan oleh negara-negara Eropa dengan mengadakan perjanjian lanjutan yakni *European Treaty Series* dengan Nomor 185. Substansi dari konvensi ini mencakup area yang cukup luas dengan mengatur *criminal policy* untuk melindungi masyarakat dari *cybercrime*, baik melalui peraturan perundang-undangan maupun kerjasama internasional. Hal ini dilakukan dengan penuh kesadaran mengenai tingginya intensitas digitalisasi, konvergensi, dan globalisasi dari pesatnya kemajuan teknologi informasi dan berpotensi untuk melakukan kejahatan di tanah Eropa.

Meskipun Konvensi Budapest dan *European Treaty Series* hanya memfokuskan kepada kejahatan komputer, hal ini tidak mengurangi manfaat dari adanya pengaturan tentang penanggulangan kejahatan digital di Indonesia. Hal ini dikarenakan pengaturan c*riminal policy*-nya yang cukup luas dan mencakup beberapa aspek modern sehingga dapat dijadikan pertimbangan dalam penjeratan suatu kejahatan siber. Adapun pengaturan utama dalam Pasal 2-5 Konvensi

Budapest diatur dalam UU ITE dengan beberapa substansi sebagai berikut:

1. Mengakses sistem komputer tanpa hak (*illegal acces*) (Pasal 27,28, 29 dan Pasal 30);
2. Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*) (Pasal 31);
3. Tanpa hak merusak data (*data interference*) (Pasal 32);
4. Tanpa hak mengganggu system (*system interference*) (Pasal 33);
5. Menyalahgunakan perlengkapan (*misuse of device*) (Pasal 34).

Adapun perjanjian regional sebagai upaya dalam pemberantasan *cybercrime* diatur juga dalam *ASEAN Convention on Counter Terorrism* atau Konvensi ASEAN mengenai pemberantasan terorisme termasuk masalah *cyberterrorism*. *Cyberterrorism* dalam hal ini merupakan penyebaran teror dengan penyebaran ideologi dan pencucian otak atau propaganda tentang paham negara melalui komunikasi secara aktif menggunakan teknologi *Internet* oleh kelompok radikalis. Salah satu contoh propaganda hitam yang terjadi di Indonesia adalah fenomena Masjid di Indonesia yang dikabarkan sebagai pertemuan anggota ISIS dan tersebar luas lewat platform *Youtube* (Marinda, 2020). Tidak hanya Indonesia, negara-negara anggota ASEAN seperti Filipina dan Malaysia menjadi sasaran penyebaran propaganda kelompok penyebar teror ISIS melalui media sosial, dengan mengunggah video *YouTube* dan mengklaim bahwa ISIS tengah mengumpulkan tentara-tentara muslim dari seluruh dunia. Dengan demikian, peningkatan hubungan dan komunikasi untuk menguatkan kerjasama antar negara sangat diperlukan. Hal ini dilakukan atas kekhawatiran kejahatan siber yang bersifat transnasional, anonim, dan dilakukan sangat cepat sehingga memerlukan dasar hukum yang mutakhir dalam bertindak preventif dan penanggulangan yang fleksibel antar negara mengenai kejahatan digital tersebut. Dan diperlukan bantuan hukum satu sama lain (mutual legal

assistance) untuk memudahkan aparat penegak hukum dalam pemberantasannya.

Di sisi internal negara, pengaturan hukum mengenai *cybercrime* masih tergolong belum komprehensif dan cenderung ketinggalan zaman. Peraturan perundang-undangan seperti KUHP, KUHAP, UU ITE, dan lainnya masih tergolong lawas sehingga menghambat para penegak hukum dalam menjalankan tugasnya. Sehingga modernisasi peraturan tersebut perlu diwujudkan dengan melakukan konstruksi hukum (Barda Nawawi Arief , 2003). Adapun model untuk melakukan konstruksi hukum terhadap hukum siber yakni sebagai berikut (Ni Luh Ketut Dewi Yani, 2020):

1. **Model Ketentuan Payung**

   Model ini digunakan untuk meningkatkan harmonisasi hukum dengan membuat aturan mengenai aktivitas di *cyberspace*. Adapun kelebihan dari gagasan ini adalah dapat menciptakan suatu pengaturan untuk menghimpun pemahaman yang beragam dari hal yang ingin diatur. Hal ini juga dapat dilakukan untuk menghindari kekosongan hukum sehingga dapat melibatkan pihak-pihak lain seperti konsumen, Pemerintah, penegak hukum, pengusaha, dan lainnya. Selain itu, konsep ini juga tidak menghapus ketentuan lama yang sekiranya masih relevan tanpa mengurangi kemanfaatannya. Namun, kekurangan dari ini adalah proses kajian serta penelitiannya yang relatif lama dalam rangka upaya sinkronisasi dan harmonisasi hukum.

2. **Model Triangle Regulations**

   Model ini diadakan untuk antisipasi dalam menghadapi pesatnya aktivitas *cyberspace*. Hal ini merupakan langkah baik dalam menertibkan permasalahan siber karena penegakannya yang bersifat efisien dan efektif terhadap permasalahan dengan spesifikasi yang khusus saja. Model ini dapat dibagi menjadi skala tiga prioritas regulasi, yakni:

a. Perihal aturan transaksi perdagangan Elektronika memuat *digital signature*, pembuktian, pajak, asuransi, serta perlindungan konsumen.
b. Untuk aturan mengenai perlindungan privasi terhadap pelaku bisnis dan konsumen, harus memuat perlindungan database elektronik dan catatan perusahaan individual.
c. Dalam aturan *cybercrime*, harus memuat yurisdiksi dan peradilan yang berkompeten dalam menangani kejahatan *cyberspace* seperti kejahatan penipuan, pemerasan, perdagangan anak, penghujatan, bahkan kejahatan seksualitas yang tidak pantas ditransmisikan. Oleh karena itu, dalam hal ini negara-negara dunia dihimbau untuk melaksanakan sosialisasi serta meningkatkan kegiatan kesadaran untuk menanggulangi *cybercrime*, dan juga mengharmonisasi segala Penal Policy antar negara disertai prosedur penegakannya. Mengingat cybercrime adalah kejahatan dunia yang melintasi berbagai negara, dibutuhkan pertimbangan untuk mengadopsi segala kebijakan mengenai perlindungan korban dan dapat pemidanaan pelaku yang berada di luar yurisdiksi dengan akulturasi ketentuan *cybercrime* dengan perjanjian ekstradisi antar negara.

Bila mengacu dua model diatas, maka pendekatan model pertama lebih direkomendasikan. Hal ini dikarenakan pengaturannya yang sistematis dan fleksibel terhadap perkembangan dunia siber yang sangat cepat. Karena apabila tidak adanya kerangka dasar serta peraturan perundang-undangan yang relevan, maka dikhawatirkan terjadinya unsinkronisasi atau tumpang tindih antar peraturan perundang-undangan.

Maka dari itu, Konvensi Budapest dan *Penal Policy* Indonesia masih tergolong minim dalam lingkup cakupannya. Dalam rangka upaya untuk mencegah dan

menanggulangi kejahatan siber kedepannya, diperlukan pengaturan dalam membuat kebijakan yang dijelaskan sebagai berikut:

a. Modernisasi hukum pidana serta peraturan perundang-undangan terkait;
b. Melakukan pengembangan dalam fasilitas *database* negara;
c. Menciptakan kepekaan terhadap masyarakat hingga badan penegak hukum terhadap urgensi cybercrime;
d. Memberdayakan pengembangan Sumber Daya Manusia, pemerintahan maupun swasta dalam mengawal aktivitas siber di Indonesia;
e. Melaksanakan filterisasi dan pelacakan konten jaringan *Internet* yang berkonotasi ancaman negara seperti terorisme, perdagangan manusia, dan sejenisnya;
f. Mengadakan kerjasama dengan pihak swasta pemilik badan hukum di jaringan *Internet* untuk memudahkan filterisasi dan pengawasan konten
g. Mengusung perlindungan korban dan fleksibilitas pemidanaan pelaku di lintas negara.

Selain itu untuk menegakkan hukum siber di Dunia maka perlu diadakan *Mutual Legal Assistance* (MLA) untuk mengoptimalisasi penindakan terhadap kejahatan siber lintas negara. Dengan adanya konsep MLA juga akanmeminimalisir ancaman negara baik dari eksternal seperti pengawasan oleh negara lain dan terorisme maupun dari pihak internal mengenai tindakan penyalahgunaan data pribadi oleh orang-orang yang tidak bertanggung jawab. Metode ini dianggap relevan dalam memberantas kejahatan siber di Indonesia dan negara-negara dunia lainnya. Hal ini juga menjadi langkah diplomatis untuk menjalin hubungan kenegaraan yang lebih erat dari sebelumnya.

BAB VII
PEMBENTUKAN BADAN KEAMANAN DAN KETAHANAN SIBER

A. URGENSI PEMBENTUKAN

Fakta lain yang cukup mengejutkan muncul dari perusahaan internet Akamai yang menyatakan bahwa kejahatan internet di Indonesia mengalami peningkatan dua kali lipat. Angka itu menempatkan Indonesia sebagai negara pertama yang berpeluang besar menjadi target dari *hacker,* menggantikan Tiongkok. Dari 175 negara yang telah diinvestigasi oleh lembaga tersebut, Indonesia menyumbangkan sebanyak 38 persen dari total sasaran *trafik hacking* di internet.

Menurut David Belson dari Akamai *Research,* kecepatan internet tidak memiliki keterkaitan dengan potensi besar kejahatan internet yang mengancam Indonesia. Aksi *hacking* lebih disebabkan ketiadaan sistem keamanan internet dan komputer yang di indonesia. Kerugian yang diakibatkan karena tindak kejahatan yang memanfaatkan dunia siber di Indonesia. Menurut data dari *Central Intelligence Agency* (CIA) telah mencapai 1,20 persen dari tingkat kerugian akibat *cyber crime* di dunia sebagaimana yang tampak dalam tabel berikut ini:

Kerugian akibat *cyber crime* di Indonesia mencapai angka USD 895 billion yang jika dijumlahkan mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat *cyber crime* secara global yang mencapai USD 71,620 billion. Dilansir dari laman Badan Siber dan Sandi Negara (BSSN) yang mencatat 88.414.296 serangan siber yang terjadi mulai 1 januari hingga 12 april 2020. Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada Februari tercatat 29.188.645 serangan lalu kemudian pada bulan Maret terekam 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan siber.

Tingginya angka tersebut mencapai puncak tepatnya di tanggal 12 Maret 2020 dimana angkanya mencapai 3.344.470, akan tetapi setelah hari itu jumlah serangan mengalami kemerosotan drastis akibat diberlakukannya aturan *work from home* (WFH) di segala tempat akibat adanya pandemi *covid*-19. Namun demikian, selama pemberlakuan kebijakan WFH telah berlangsung serangan siber yang memanfaatkan isu terkait dengan adanya *covid*-19. Adapun jenis serangan yang paling sering adalah *trojan activity* sebanyak 56% dan kemudian disusul oleh aktifitas *information gathering* (pengumpulan informasi) sebanyak 43% dari total keseluruhan serangan, sedangkan 1% sisanya ditempati oleh *web application attack* (BSSN, 2020).

Hal serupa juga diungkapkan dalam penelitian Frost dan Sullivan yang diprakrarsai oleh Microsoft pada tahun 2018. Dalam penelitian tersebut disebutkan kejahatan siber di Indonesia bisa menyebabkan kerugian mencapai Rp. 478,8 triliun atau 34,2 milliar dollar AS (Gewati, 2019). Pada hakikatnya kasus *cyber crime* hampir terjadi di setiap negara dan mereka mempunyai cara tersendiri dalam memerangi kejahatan tersebut. Misalnya Amerika Serikat(AS) telah mempunyai regulasi dan lembaga yang menangani kejahatan di dunia siber.

Respon AS terhadap kekuatan dunia maya dapat dilihat dalam garis besar politik luar negeri AS yang terangkum dalam QDPR 2010. Pemerintah AS telah memperlihatkan keseriusannya dalam membangun sistem keamanan informasi. Hal tersebut erat kaitannya dengan ketergantungan terhadap jaringan keamanan sistem informasi. Keamanan siber dijadikan prioritas untuk kebijakan politik AS karena keberadannya yang fundamental.

Berkaitan dengan hal tersebut, AS semakin memperkuat keamanan siber dengan mengesahkan dokumen "*International Strategy for Cyberspace*" pada tahun 2011. Siasat ini merupakan langkah pertama yang dikeluarkan AS yang menghubungkan dan mengikat AS dengan dunia siber yang sangat luas

jangkauannya. Langkah ini juga yang dijadikan rujukan AS dalam menghadapi resiko dunia siber. Maka dari itu, pada April 2015 Departemen Pertahanan AS membentuk lembaga "*The Departement Of Defense (DoD) Cyber Strategy*". Pembentukan lembaga ini bertujuan untuk mensukseskan tujuan dan prioritas sebagaimana termaktub dalam *International Strategy for Cyberspace* 2011. Berikut merupakan beberapa kebijakan AS terkait keamanan dan ketahanan siber dalam beberapa tahun terakhir (Triwahyuni, 2019):

Tabel Daftar Kebijakan Cyber Amerika Serikat

Tahun	Nama Dokumen	Lembaga Penerbit
2003	*The National Strategyto Secure Cyberspace*	Gedung Putih
2009	*Cyberspace policy Review*	Gedung Putih
2011	*International Strategy for Cyberspace*	Gedung Putih
2011	*Department of Defense Strategy for Operating Cyberspace*	Departemen Pertahanan Amerika Serikat
2015	*The Department of Defense Cyber Strategy*	Departemen Pertahanan Amerika Serikat
2016	*Department of State International Cyberspace Policy Strategy*	Departemen Luar Negeri Amerika Serikat

Dari tabel diatas terlihat jelas keseriusan pemerintah AS untuk mengamankan dunia siber. Berbagai kebijakan yang

dikeluarkan oleh pemerintah AS merupakan formulasi khusus yang dikeluarkan Gedung Putih sebagai *international code of conduct* AS untuk mengatasi permasalahan siber di ranah internasional. Beberapa negara yang berhasil dideteksi AS melalui strategi ini adalah Tiongkok dan Rusia.

Melalui strategi sebagaimana yang dipaparkan diatas, AS berfokus untuk menciptakan kebijakan internasional untuk ruang siber dan memberdayakan sejumlah inovasi untuk mendorong majunya ekonomi dan peningkatan hidup masyarakat AS. Sebagai langkah memastikan strategi tersebut berjalan lancar, maka secara teknis langkah strategis telah disusun oleh *Departement of Defense* (DoD) yang disebut sebagai strategi inisiatif. Strategi tersebut disusun untuk keamanan dunia siber yang menjadi tupoksi Departemen Pertahanan AS. Selain itu juga Departemen Pertahanan AS melaksanakan berbagai aktifitas diluar dunia siber untuk mengembangkan keamanan kolektif siber dan dalam rangka menjaga kepentingan nasional AS. Sebagai contoh, Dod menjalin kerjasama dengan agensi pemerintah, sektor privat, dan juga dengan lembaga internasional dalam ranah siber.

Jika melihat jauh kebelakang terdapat banyak sekali kasus terkait *cyber crime*, salah satunya tentang peretasan menggunakan perangkat komputer. Delapan tahun silam, tepatnya tanggal 9 Januari 2013 situs *www.presidensby.info* diretas. Saat situs tersebut diretas, halaman depan diganti dengan latar belakang warna hitam dengan tulisan hijau dibagian atas "Hacked by MJL007", sementara itu di bagian bawahnya tercantum sebuah logo dan tulisan "Jemberhacker Team" yang berwarna putih. Pelaku yang bernama wildan ditangkap setelah melakukan peretasan situs SBY yaitu *www.presidensby.info*.Wildan Yani S (22 th) yang merupakan pelaku peretasan situs SBY merupakan lulusan SMK tahun 2010, dan tidak melanjutkan ke pendidikan ke jenjang perguruan tinggi dikarenakan terhambat biaya (Hermawan, 2013).

Wildan sehari-hari bekerja sebagai operator internet di jember. Wildan setelah melancarkan aksinya langsung diringkus oleh pihak berwajib dan diancam melanggar pasal 50 *juncto* pasal 22 huruf b undang-undang nomor 36 tahun 1999 tentang telekomunikasi. Pelaku terancam hukuman pidana penjara paling lama 6 tahun penjara dan atau denda paling banyak Rp.600 juta.

Wildan juga dianggap menyalahi aturan yang termuat dalam pasal 46 ayat (1), (2), dan (3) *jo* pasal 30 ayat (1), (2), dan (3) serta pasal 48 ayat (1) *jo* pasal 32 ayat (1) undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Serangkain aturan tersebut mengancam pelaku dengan hukuman penjara 6 hingga 10 tahun serta denda mencapai Rp. 5 miliar. Namun, dari pihak kepolisian mengganggap motif pelaku hanya sebatas iseng mengganti tampilan situs tersebut tanpa termuat maksud politik.

Bahkan terdapat pernyataan menarik dari Bareskrim POLRI yang menyatakan Wildan akan direkrut sebagai staf *cyber crime* MABES POLRI. Penangkapan wildan ini menimbulkan kecaman dari suatu kelompok *hacker* internasional yang diketahui oleh banyak orang yaitu ANONYMOUS. Kelompok ini meminta Wildan dibebaskan dari segala tuntutan karena perbuatan Wildan tidak merusak sistem atapun data yang ada dalam situs tersebut tapi hanya bersifat menginformasikan dan mengingatkan bahwa pengelolaan situs penting milik pemerintah belum maksimal dari aspek keamanannya.

Kelompok ini juga mengatakan apabila tuntutannya tidak terpenuhi mereka menyatakan "perang" terhadap situs pemerintah republik Indonesia dengan menumbangkan situs-situs berdomaian "go.id". Adapun situs-situs yang telah berhasil dilumpuhkan antara lain beberapa sub domain di situs Komisi Pengawas Persaingan Usaha (KPPU), Badan Pusat Statistik (BPS), Kedutaan Besar Republik Indonesia (KBRI) Tashkent, Kementerian Hukum dan Hak Asasi Manusia (KEMENKUMHAM), Departemen Sosial (DEPSOS), dan

Kementerian Pariwisata dan Ekonomi Kreatif (KEMENPAREKRAF) bahkan Indonesia.go.id.

B. REFORMASI KELEMBAGAAN MELALUI PEMBENTUKAN BADAN KEAMANAN DAN KETAHANAN SIBER

Sampai dengan saat ini, Indonesia masih belum mempunyai aturan yang cukup untuk mengatasi keamanan dan ketahanan siber. Aturan yang ada masih memiliki banyak kelemahan dan kekurangan dalam menunjang perlindungan keamanan dan infrastruktur siber. Peraturan terkait keamanan dan ketahanan siber diantaranya tertuang di institusi Kementerian Pertahanan atau Tentara Nasional Indonesia dengan UU No. 3 Tahun 2002 tentang Pertahanan, UU No. 43 Tahun 2008 tentang Wilayah Negara, UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia, serta Peraturan Pemerintah Nomor 68 Tahun 2014 tentang Penataan Wilayah Negara.

Persoalan yang sama juga terdapat dalam institusi intelijen Indonesia. UU No. 17 Tahun 2011 tentang Intelijen masih terbatas untuk menindak ataupun melakukan respon atas serangan siber. Hal tersebut juga terlihat pada institusi Kementerian Komunikasi dan Informatika yang termuat dalam UU No. 32 Tahun 2002 tentang Penyiaran, UU No. 36 Tahun 1999 tentang Telekomunukasi, UU No. 14 tahun 2008 tentang Keterbukaan Informasi Publik, dan UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang masih ditemukan keterbatasan dalam konteks infrastruktur telekomunikasi, penyiaran dan informatika untuk pelayanan publik.

Sebenarnya aturan keamanan dan ketahanan siber sudah diakomodir oleh Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. Namun yang menjadi problematikanya adalah pedoman ini dibuat terbatas sebagai rujukan yang pemberlakuannya di ruang lingkup Kementerian Pertahanan dan Siber. Sangat disayangkan bahwa peraturan yang telah dibentuk masih bersifat parsial yaitu

hanya mengatur satu aspek tertentu dan belum komprehensif. Perlunya pengaturan yang berisi hak dan kewajiban pemerintah, pihak swasta, individu dan masyarakat terkait dengan perlindungan dan keamanan serta ketahanan siber, pengaturan preventif dan penindakan kejahatan di dunia siber, serta kordinasi antar lembaga ataupun instansi pemerintah yang terkait dengan dunia siber belum diatur secara jelas dan tegas.

Oleh karena itu, untuk mengatasi persoalan tersebut dibutuhkan pengaturan yang komprehensif melalui peraturan perundang-undangan. Undang-Undang yang diharapkan adalah perangkat hukum yang akomodatif terhadap perkembangan zaman serta preventif terhadap permasalahan, mencakup dampak negatif yaitu penyalahgunaan internet dengan berbagai motif yang dapat menimbulkan berbagai korban-korban bermunculan yang mengalami kerugian materi dan non-materi. Menurut Setiyadi, peraturan perundang-undangan termasuk *Cybercrime law* dibutuhkan karena beberapa faktor, diantaranya (Setiyadi, 2003):

1. Melindungi keamanan dan integritas pemerintah serta menjaga suatu reputasi suatu negara;
2. Membantu negara terhindar dari tuduhan sebagai tempat yang aman untuk menyimpan aplikasi dan melancarkan aksi kejahatan siber;
3. Meningkatkan perlindungan terhadap data yang dikategorikan khusus (*classified*), informasi pribadi, rahasia, data pengadilan kriminal, dan paling fundamental adalah data seluruh penduduk yang seyogianya dilindungi dan terjaga keamanannya;
4. Terjaminnya keamanan nasional dan mengurangi resiko aksi oleh teroris ataupun kejahatan lain yang menggunakan dunia siber.

Selain persoalan kebutuhan Undang-Undang, dalam tataran praktisnya terdapat hambatan mendasar yaitu kinerja kelembagaan masih belum terkordinasi dan terstruktur.

Lembaga-lembaga yang menjalankan tugas dan fungsi dalam penanganan siber di indonesia meliputi, Kementerian Komunikasi dan Informatika (Kemenkominfo), Badan Intelijen Negara (BIN), Kepolisian Republik Indonesia (Polri), Tentara Nasional Indonesia (TNI), dan Badan Siber dan Sandi Nasional (BSSN). Lembaga tersebut dalam menjalankan tupoksinya masing-masing merupakan satuan siber (*cyber force*) yang hingga saat ini mengelola keamanan dan pertahanan siber secara mandiri. Namun, terdapat sejumlah analisa yang menyatakan terdapat perbedaan tugas dan fungsi dalam mengatasi persoalan siber di Indonesia. Sinergi kelembagaan siber di Indonesia yang masih parsial dan kelemahan kordinasi yang disebabkan ego sektoral kelembagaan merupakan tantangan dan harus segera digagas solusi yang komprehensif.

Adapun kewenangan dari beberapa lembaga yang eksis menangani persoalan siber yakni sebagai berikut:

Institusi	Dasar Hukum	Kewenangan
Kementerian *Komunikasi dan Informatika (Kemenkominfo)*	*- UU No. 32 Tahun 2002 tentang Penyiaran,* *- UU No. 36 Tahun 1999 tentang Telekomunukasi* *- UU No. 14 tahun 2008 tentang Keterbukaan Informasi Publik* *- UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik*	Kewenangan Kemenkominfo terbatas konteks infrastruktur telekomunikasi, penyiaran dan informatika untuk pelayanan publik
Badan Intelijen Negara (BIN)	*UU No. 17 Tahun 2011 tentang Intelijen Negara*	Kemampuan untuk melakukan *cyber espionage* maupun untuk merespon

		cyber attack terbatas. Hal ini dikarenakan penyadapan hanya dapat dilakukan jika sudah mendapat penetapan dari ketua pengadilan dan adanya alat bukti yang cukup
Kepolisian Republik Indonesia (Polri)	*UU No. 2 Tahun 2002 tentang Kepolisian*	Dalam Undang-Undang tersebut wewenang pihak kepolisian hanya berfokus pada keamanan dan ketertiban masyarakat. Jadi, tidak ada wewenang khusus dalam ranah dunia siber.
Kementerian Pertahana/Tentara Nasional Indonesia (TNI)	- *UU No. 3 Tahun 2002 tentang Pertahanan* - *UU No. 43 Tahun 2008 tentang Wilayah Negara* - *UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia* - *Peraturan*	Tugas pertahanan negara mencakup tegaknya kedaulatan, keutuhan wilayah dan perlindungan bangsa. Namun, faktanya *Cyber space* belum menjadi wilayah pertahanan dan tugas nirmiliter TNI hanya sebagai

	Pemerintah Nomor 68 Tahun 2014 tentang Penataan Wilayah Negara	pendukung.
Badan Siber dan Sandi Nasional (BSSN)	- Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara - Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara	BSSN hanya diberikan wewenang untuk mengonsolidasikan semua unsur yang terkait dengan keamanan siber, dan fungsinya terbatas pada penyusunan, pemantauan, dan evaluasi kebijakan teknis, termasuk di dalamnya koordinasi dan kerjasama. BSSN bukanlah lembaga penegak hukum, dan tidak bisa melakukan penyeldikan dan penyidikan serta apabila menemukan suatu kasus mengenai *cyber crime* wajib mengkoordinasikan ataupun melimpahkan kepada pihak

		kepolisian.

Sumber: Materi Presentasi Direktorat Kebijakan Strategis Kementerian Pertahanan pada 5 Februari 2015 dan Perpres No.53 Tahun 2017 tentang Badan Siber dan Sandi Negara

1. **Menggagas Pembentukan Badan Keamanan dan Ketahanan Siber**

   Dalam praktiknya tak sedikit negara yang telah membuat peraturan tentang keamanan dan ketahanan siber, setidak-tidaknya dua negara tetangga yaitu Singapura dan Vietnam telah mempunyai Undang-Undang tentang Keamanan Siber. Singapura telah memiliki Undang-Undang yaitu *Cybersecurity Act* yang disahkan pada Februari 2018. Berdasarkan keterangan Strategi Keamanan Siber Singapura, UU ini berfokus untuk memberdayakan bisnis dan kemampuan masyarakat (Rahman, 2019).

   Jauh sebelum *Cybersecurity Act* diberlakukan, Singapura telah memiliki aturan yang bernama *Computer Misuse Act* yang berlaku tahun 1993 dan kemudian direvisi pada tahun 2007. Pada pokoknya kedua UU itu memperbolehkan untuk mengumpulkan informasi dari komputer atau perangkat manapun jika dirasa dapat mengancam keamanan dan stabilitas nasional. Di negara Vietnam pemberlakuan UU keamanan siber dimulai pada januari 2019. Pemerintah Vietnam menjelaskan dan menegaskan bahwa fungsi dari aturan ini untuk mendukung kemajuan ekonomi digital di negara mereka.

   Berkaca dari hal tersebut maka Indonesia memiliki suatu kewajiban untuk melindungi seluruh hak-hak penduduknya serta kedaulatan negara di zaman globalisasi saat ini dibutuhkan peraturan perundang-undangan yang mengaturnya secara tegas, jelas dan komprehensif.

   Indonesia sebagaimana yang disampaikan diatas sudah memiliki beberapa lembaga yang menangani siber namun masih terjadi tumpang tindih kewenangan antara satu dengan yang lainnya. Misalnya kewenangan BSSN

dalam melaksanakan tugasnya bersinggungan dengan kewenangan lain, seperti dalam penanganan kasus mesin sensor "konten negatif" seharga 200 milliar yang seharusnya diselesaikan oleh Kementerian Komunikasi dan Informatika (Kemenkominfo), pekerjaan menyelesaikan persoalan ujaran kebencian juga akan bersinggungan antara Kemenkominfo dan Kepolisian RI. Belum lagi, memburu penjahat digital (*cyber criminal*) yang sudah dilaksanakan oleh Unit *Cyber Crimes* Mabes Polri, dalam aspek pertahanan akan bentrok pula dengan kementerian pertahanan yang sudah memiliki *cyber operation center* (COC) (Mantra, 2018).

Jika kita menganalisa lebih mendalam, terdapat banyak sekali problematika seiring hadinya BSSN yang memicu tumpang tindih kewenangan diantaranya adalah beberapa pekerjaan dengan penanganan insiden keamanan informasi yang dimiliki Kementerian Luar Negeri, penanganan *fraud e-commerce* dengan Kementerian Perindustrian, Kementerian Perdagangan, dan Kemenkominfo. Hal serupa terjadi dalam penanggulangan teroris oleh Badan Nasional Penanggulangan Terorisme (BNPT), operasi intelligent dunia maya dengan Badan Intelijen Negara (BIN), kejahatan keuangan dan ekonomi digital oleh Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dan Komisi Pemberantasan Korupsi (KPK) serta kemungkinan masih terdapat lagi yang tumpah tindih kewenangannya.

Oleh karenanya dalam konteks pertahanan siber maka dibutuhkan *cyber security* dan *cyber defense* yang kokoh dan sinergis antara semua lembaga. Kementerian Komunikasi dan Informatika, Badan Intelijen Negara, Kepolisian Republik Indonesia, Tentara Nasional Indonesia, Badan Siber dan Sandi Nasional sebagai kepanjangan tangan dari negara harus mampu menciptakan sinergitas untuk menangkis, menangkal, dan mencegah serangan siber dari pihak tertentu atapun dari negara lain yang mencoba

untuk merusak kedaulatan dunia maya indonesia saat ini dan di masa depan.

Pengaturan dan penataan kelembagaan *cyber security* nasional yang kokoh merupakan salah satu prasyarat terbentuknya *cyber security* yang handal. Penanganan *cyber security* harus terintegrasi secara dan melibatkan semua pihak terkait. Sinergitas tersebut dapat diimplementasikan dalam unit kerja yang bernama Badan Keamanan dan Ketahanan Siber (BKKS). Konsep pembentukan unit kerja tersebut sejatinya hingga detik ini belum ada di Indonesia. Pembentukan unit kerja ini bertujuan untuk mengakomodasi seluruh persoalan yang tersebar di berbagai Kementerian/Instansi diselesaikan dalam satu atap lembaga.

Menurut hemat penulis, unit kerja ini akan mempunyai beberapa tupoksi untuk menyelesaikan persoalan *cyber crime* diantaranya:

a. BKKS mempunyai tugas melaksanakan keamanan dan ketahanan siber secara sinergis dan efektif.
b. BKKS bertugas mengharmonisasikan dan mengkoordinasikan dengan seluruh pihak terkait untuk menjalankan tugasnya.
c. BKKS melakukan kerjasama nasional, regional, dan internasional terkait keamanan dan ketahanan siber.
d. BKKS membentuk regulasi keamanan dan ketahanan siber yang memadai dan dapat melakukan pembaharuan apabila dianggap perlu sesuai mekanisme yang berlaku.
e. BKKS menyusun standart operasional prosedur (SOP) berkaitan tata cara pengoperasian siber dan kegiatan-kegiatan yang menggunakan perangkat teknologi.

Tentunya tupoksi yang diberikan kepada BKKS harus didukung dengan kewenangan yang dimiliki oleh unit kerja tersebut. Adapun kewenangan yang nantinya dipunyai adalah dapat mengambil tindakan hukum apabila menemukan seseorang/kelompok/organisasi yang

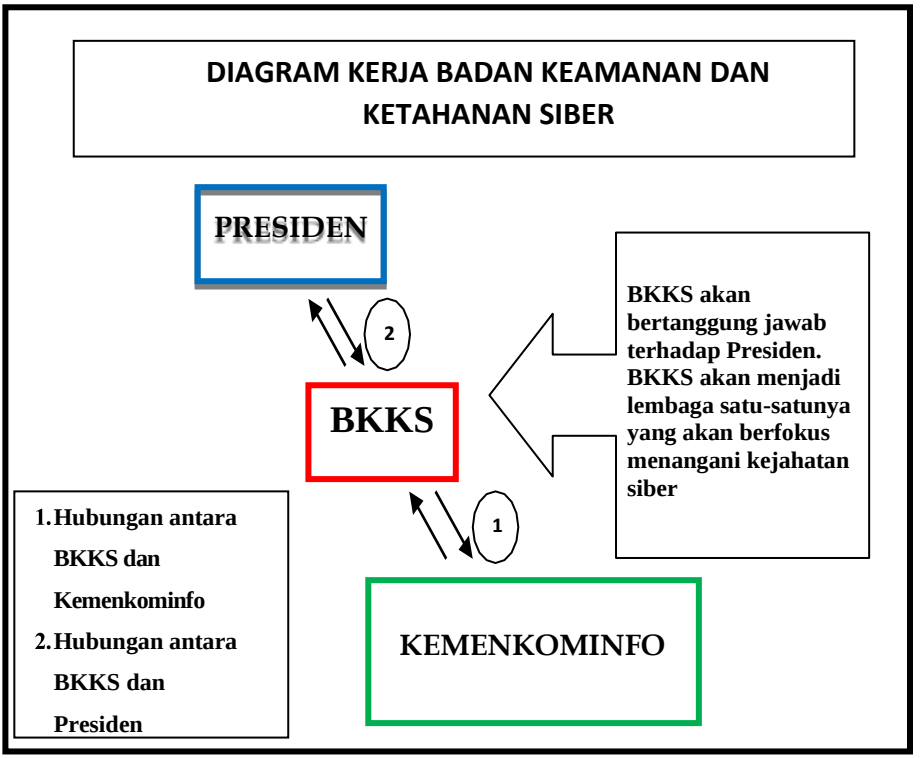
melakukan kejahatan di dunia siber dan selanjutnya diserahkan kepada pihak kepolisian. Selain itu BKKS berwenang sebagai pengatur tata kelola dunia siber di Indonesia yang akan mengkomandoi seluruh pihak terkait khususnya penanganan *cyber crime* dan *cyber space* pada umumnya. Selanjutnya dalam aspek penegakan hukumnya, unit kerja ini dapat memberikan sanksi bagi para pelaku kejahatan yang berupa pemblokiran, penghapusan situs dan melakukan peninjauan terhadap situs-situs yang dapat menimbulkan potensi kejahatan dunia siber.

Berkaitan dengan hal tersebut, unit kerja BKKS didesain sebagai Lembaga Pemerintah Non Kementerian (LPNK). Adapun alasan untuk menempatkan unit kerja ini termasuk dalam LPNK dikarenakan mempunyai tugas yang bersifat spesifik dan khusus diluar kewenangan kementerian. Hal tersebut sesuai dengan Laporan Akhir Lembaga Administrasi Negara yang menyatakan bahwasanya filosofi pembentukan LPNK sebenarnya dibentuk sebagai *special agency* yaitu melaksanakan tugas khusus dan perananannya juga sangat diperlukan dalam rangka mendukung melaksanakan tugas kementerian negara (Pusat Kajian Kinerja Kelembagaan Lembaga Administrasi Negara, 2019). Maka dari itu, idealnya untuk merumuskan kerangka kelembagaan diperlukan suatu aturan yang diejawantahkan dalam bentuk Peraturan Presiden. Selanjutnya unit kerja ini akan berada dibawah komando Kemenkominfo dan bertanggung jawab kepada kementerian tersebut serta bertanggung jawab juga kepada Presiden. Pengaturan tersebut dimaksudkan agar terciptanya sistem pelaporan dan pertanggungjawaban yang jelas dan efektif.

Kebutuhan adanya keamanan dan ketahanan siber di Indonesia tentunya bertolak dari realitas bahwa saat ini muncul banyak ancaman dalam dunia siber yang dapat merusak kedaulatan negara dan berimplikasi terhadap seluruh lini kehidupan masyarakat. Dalam hal ini gagasan yang penulis usung merupakan realisasi dari konsep sistem pertahanan

semesta. Dalam konteks ini, sistem pertahanan semesta sebagaimana termaktub dalam Undang-Undang No.3 Tahun 2002 tentang pertahanan negara, harus bisa diartikan sebagai semesta yang bersifat tidak hanyak fisik semata, melainkan non fisik, khususnya dalam dunia maya dan digital.

Badan yang memiliki ruang lingkup nasional dianggap sangat urgen di Indonesia sebagai langkah preventif agar sistem informasi negara tidak mengalami *shut down*. Keberadaan lembaga yang khusus menangani kejahatan siber penting karena setiap hari Indonesia menghadapi serangan siber dengan frekuensi yang masif. BKKS nantinya akan bekerja dalam proses penyelidikan yang berkaitan dengan kejahatan siber dan selanjutnya proses penyidikan dilakukan bersama dengan pihak kepolisian. Hal ini dimaksudkan agar lingkup kerja BKKS bersifat sistematis dan tidak terjadi tumpang tindih kewenangan dengan penegak hukum lainnya. Adapun pegawai BKKS merupakan gabungan dari seluruh pihak terkait yaitu Kemenkominfo, BIN, Polri, TNI, BSSN dan melalui proses seleksi yang ketat. BKKS juga akan bertanggung jawab kepada Presiden melalui Kemenkominfo. Mekanisme kerja tersebut tergambar dalam bagan di bawah ini.



Sumber: Kreasi Penulis

Selain itu dalam pembentukannya akan melibatkan seluruh pihak terkait dan nantinya dari setiap lembaga yang sudah ada mengirimkan personilnya untuk turut serta dalam pengelolaan unit kerja. Dengan adanya unit kerja ini dirasa akan mampu untuk menciptakan sinergitas diantara pihak-pihak terkait sehingga tidak akan terjadi konflik kepentingan dan persoalan klasik yaitu *misscomunication* yang berdampak ketidakharmonisan dan perpecahan pihak-pihak terkait.

Hadirnya unit kerja ini nantinya akan menjadi otoritas tunggal dalam pelaksanaan keamanan dan ketahanan siber di Indonesia. Dalam konteks Indonesia, pembentukan unit kerja tersebut harus ditempuh dengan jalan reformasi kebijakan yang mencakup dua hal. Pertama, mengatur pembentukan unit kerja

ini dalam peraturan perundang-undangan yaitu Peraturan Presiden. Pengaturan yang dimaksud adalah untuk memberikan dasar hukum yang kuat sekaligus merumuskan kerangka kelembagaan, disertai pemberian tugas pokok, fungsi, dan kewenangan yang kuat sebagai suatu pemegang otoritas tunggal dalam sistem keamanan siber. Kedua, melaksanakan penyesuaian kembali terhadap fungsi-fungsi yang dimiliki oleh lembaga atau instansi terkait sistem keamanan siber yang ada saat ini.

Pembentukan unit kerja ini disertai dengan penataan lembaga dan fungsi instansi lain yang serupa, sehingga tidak terjadi tumpang tindih kewenangan. Dalam hal ini, fungsi yang terkait dengan pelaksanaan keamanan dan ketahanan siber di lembaga-lembaga sebagaimana yang telah dipaparkan diatas harus dipindahkan dan dilimpahkan ke unit kerja baru ini. Dalam sistem ketatanegaraan, menurut hemat penulis akan sangat strategis dan efektif apabila unit kerja yang dibentuk untuk menangani persoalan keamanan siber berada di bawah naungan Kemenkominfo.

Dalam realisasi pelaksanaannya unit kerja BKKS membutuhkan personil yang ahli dan berkompeten demi menunjang kegiatan pemberantasan kejahatan siber. Hal tersebut dapat ditempuh dengan perekrutan tenaga ahli melalui mekanisme seleksi yang ketat disertai *capacity building* untuk memajukan sumber daya manusia yang mumpuni dan berkualitas dalam unit kerja BKKS. Sebagaimana yang dikatakan diatas bahwasanya dalam menghadapi kejahatan siber diperlukan sinergitas dari seluruh komponen untuk bersatu padu, sinergis, komunikatif dan koordinatif.

Kejahatan siber merupakan ancaman serius di era globalisasi saat ini dan membutuhkan satu persepsi untuk mensinergikan satu tindakan, satu kebijakan dan suatu rencana aksi yang utuh dan mantap. Kejahatan siber memerlukan partisipasi dari berbagai pihak terkait untuk menanggulanginya dalam satu kerangka kerja yang koordinatif. Ancaman serangan siber tidak bisa dilakukan

secara parsial semata, melainkan membutuhkan langkah penanganan secara terpadu, integral dan komprehensif. Maka dari itu, BKKS yang merupakan gabungan dari pihak terkait akan mampu menjadi suatu konstruksi perlindungan keamanan siber bersama bantuan dari seluruh komponen masyarakat.

DAFTAR PUSTAKA

BUKU

Adrian Sutedi, Tindak Pidana Pencucian Uang, Jakarta: Citra Aditya Bakti, 2008

Agus Rahardjo, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Adya, 1976

Al Wisnubroto, "Kebijakan Hukum Pidana Dalam Penanggulangan Komputer", Yogyakarta:Universitas Atmajaya, 1999

Alan Westin, *Privacy and Freedom*, New York: Atheneum, 1967.

Asshiddiqie, J., *Konstitusi dan Konstitusionalisme Indonesia,* Jakarta: Sinar Grafika, 2018.

Assidiq, Hasbi, Armelia Safira, and Siti Nurhalima Lubis. *Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional*. Makasar : Nas Media Pustaka, 2020.

Balbi, Gabriele, Paolo Magaudda. *A History of Digital Media : An Intermedia and Global Perspective*. Routledge : New York, 2018

Barda Nawawi Arief, "*Kapita Selekta Hukum pidana*", Bandung: PT Citra Aditya Bakti, 2003

_____, "Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia", Jakarta: PT. Rajagrafindo Persada, 2006

Bell, David, and Barbara Kennedy, eds. *The cybercultures reader*. London : Routledge, 2000.

Budiardjo M., *Aneka Pemikiran Tentang Kuasa dan Wibawa,* Jakarta: Sinar Harapan, 1986.

Chad Russel dan Shane Fuller, *GDPR for Dummies*, Britania Raya: John Wiley & Sons, Ltd, 2017.

Clark, David, *Thomas Berson, dan Herbert S. Lin. At the nexus of cybersecurity and public policy: Some basic concepts and issues*. The National Academies Press:Washington DC. 2014.

Dodge, Martin, and Rob Kitchin, *Mapping cyberspace*, London: Routledge, 2001.

Domrin N Alexander., *The Limits of Russian Democratisation Emergency Powers and State of Emergency,* London & New Yorks: Routledge, 2006.

Drs. Dikdik M. Arief Mansur, SH., MH, Elisatris Gultom, SH., MH, *CYBER LAW Aspek Hukum Teknologi Informasi*, Bandung: PT Refika Aditama, 2005

Drs.H Abdul Wahid, SH., MA, Mohammad Labib, SH, *Kejahatan Mayantara (Cyber Crime),* Bandung: PT Refika Aditama, 2005

Echols, John M., dan Hassan Shadily. *Kamus Inggris-Indonesia Cet. XXV* Jakarta: Gramedia Pustaka Utama, 2003

European Union Agency for Fundamental Rights and The Council of Europe. *Handbook on European Data Protection Law*. Inggris : European Union Agency. 2014

Fineman, M. *Faking It: Manipulated Photography before Photoshop*. New York: Metropolitan Museum of Art. 2012.

Graham Greeneaf, "*Asian Data Privacy Laws-Trade and Human Rights Perspective*", New York: Oxford University Press, 2014.

Hafner, Katie, and Matthew Lyon. *Where wizards stay up late: The origins of the Internet*. New York : Simon and Schuster, 1996

Hannah Arendt, *The Human Condition*, Chicago: The University of Chicago Press, 1958.

John Paul Filo. *Kent State Shootings*. Associated Press. 1970

John Vivian, *Teori Komunikasi Massa*, Jakarta: Penerbit Kencana, 2008.

Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*¸ Jakarta: PT Tatanusa, 2012.

Kelsen H., *Pure Theory of Law,* California: Berkeley University of California Press, 1978.

Kitchin, Rob, *Cyperspace: The World in the Wires*, Chichester: Wiley, 1998.

Kremling, J., & Parker, A. M. S. *Cyberspace, cybersecurity, and cybercrime*. London : SAGE Publications, 2017

M. Arsyad Sanusi, *Hukum Teknologi dan Informasi*, Bandung: Tim Kemas Buku, 2005.

Manthovani R, Problematika dan Solusi Penanganan Kejahatan Siber di Indonesia, Jakarta: Malibu, 2006

Nasrullah, Rulli. *Teori dan riset media siber (cybermedia)*. Jakarta : Kencana, 2016.

Naughton, John. *A Brief History of the Future: The Origins of the Internet*, London: Weidenfeld & Nicolson. 1998

Pangestuti, Dewi Cahyani. *Manajemen Keuangan Internasional*. Yogyakarta : Deepublish, 2020.

Paul Lambert, *Understanding the New European Data Protection Rules*, Amerika: CRC Press, 2018.

Powell, Anastasia, and Nicola Henry. *Sexual violence in a digital age*. Springer. 2017.

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), *Kajian Konvergensi Teknologi Informasi dan Komunikasi*, Jakarta:Pusat Teknologi Informasi dan Komunikasi BPPT,2007.

Schick, Nina. *Deepfake The Coming Infocalypse*. New York : Twelve Hachette Book Group 2020

Schmitt C., & Seitzer J, *Constitutional Theory*, Durham: Duke University Press, 2008.

Soedjono Dirdjosisworo, *Respon Terhadap Kejahatan, Introduksi Hukum Penanggulangan Kejahatan (Introduction To the Law Of Crime Prevention)*, Bandung: STHB Press, 2002.

Soemarno Partodihardjo, *Tanya Jawab Sekitar UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Jakarta: Gramedia Pustaka Utama, 2008.

Strong C.F., *Modern Political Constitution, an Intruction The Comparative Study of Their History and Existing Form*, London: Sidgwick & Jackson Limited, 1958.

Sudikno Mertokusumo & A. Pittlo, *Bab-Bab tentang Penemuan Hukum,* Bandung: PT Citra Aditya Bakti, 1993

Sue Titus Reid, *Crime and Criminology*, New York: CBS College Publishing, 1976

Sutanto, Hermawan Sulistiyo, dan Tjuk Sugiarto, *Cyber Crime - Motif dan Penindakan*, Jakarta: Pensil 324, 2005

Tongat, *Dasar-dasar Hukum Pidana Indonesia Dalam Perspektif Pembaharuan*, Malang: UMM Press, 2008.

Tubagus Irman, "Money Laundering: Hukum Pembuktian Pencucian Uang", Jakarta: Gramedia, 2017

Tubagus Ronny Rahman Nitibaskara, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*, Jakarta: Peradaban, 2001

Whittaker, Jason, *The Cyberspace Handbook*, London: Routledge, 2004.

Wibowo S., "Peran IP Address dan Domain Name Dalam Cyber Jurisdiction, *Tesis*, Universitas Gajah Mada, 2015.

JURNAL

Ahmad Budi Setiawan, 2014, *Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik,* Buletin Pos dan Telekomunikasi Volume 12 Nomor 2.

Ahmad Saudi, "KEJAHATAN SIBER TRANSNASIONAL DAN STRATEGI PERTAHANAN SIBER INDONESIA", *Jurnal Demokrasi Dan Otonomi Daerah* 16.3 (2018).

Akbar Kurnia Putra, "Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional", *Jurnal Ilmu Hukum Jambi* 5.2 (2014): 43297.

Bambang Hartanto, 2013, *Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding,* Jurnal Pranata Hukum Volume 8 Nomor 2.

Batty, Michael "*Virtual Geography*," Futures Vol. 29 No 4-5 (1997) 337– 352.

Batubara, Leo. "Memahami Pornografi Dari Sudut Pandang HAM", disampaikan dalam Semiloka RUU Anti Pornografi Dan Pornoaksi Dalam Perspektif HAM, Hotel Sheraton Media Jakarta, 27-28 (2006): 3-4

Bernadette Kamleitner dan Vince Mitchell, "*Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infrigements*", Journal of Public Policy & Marketing Vol. 38 (4), (2019): 437.

Brahma Astagiri, "Spamming dalam Perspektif Hukum Pidana", Yuridika Vol. 25, No. 1, (2010): 92.

Caren B. Goldberg, "*Relational Demography and Similarity-Attraction in Interview Assessments and Subsenquent Offer Decisions*", Sage Journals Vol. 30, Issue 6, (2005): 597-624.

Chen, Juan, Tao Ma, and Pei Jie Wei. "Study of Cyberspace Factors and Description Methods." *Applied Mechanics and Materials*. Vol. 427, (2013)

Cindy M. Rise, "*A Justification for the Prohibition of Spam in 2002*", North Carolina Journal of Law and Technology Vol. 3, Issue 2, (2002): 386.

Clare Chambers-Jones, "Virtual Economies and Financial Crimes", *Edward Elgar Publishing Limited: United Kingdom* (2012)

Clark, David. "Characterizing cyberspace: past, present and future." *MIT CSAIL, Version* 1 (2010): 2016-2028.

Dewi Puspasari, Achmad Nizar Hidayanto, dkk, "*Data Privacy, What Still Ned Consideration in Online Application System?*", Journal of Information Systems Vol. 16, Issue 1, (2020): 50.

Dian Eka Kusuma Wardani dan Maskun, 2019, *Kejahatan Skimming Sebagai Salah Satu Bentuk Cyber Crime*¸ Jurnal Jurisprudentie Volume 6 Nomor 1.

Dini Suka Listyana, dkk, 2014, *Kekuatan Pembuktian Tanda Tangan Elektronik Sebagai Alat Bukti yang Sah dalam Perspektif Hukum Acara di Indonesia dan Belanda*, Jurnal Verstek Volume 2 Nomor 2.

Dista Amalia Arifah, "Kasus Cyber Crime Di Indonesia", *Jurnal Bisnis dan Ekonomi* Vol.18, No 2, (2011): 185-195

Dorothy E. Denning, 2000, *Cyberterrorism: Testimony Before The Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives*, Focus on Terrorism Volume 9.

Fauzan Hanafi,"SERANGAN SIBER DI MASA PANDEMI: BANYAK AGRESI MINIM PROTEKSI", *JURNAL ALMISHBAH: Jurnal Ilmu Dakwah dan Komunikasi Vol. 17. No. 1* (2021)

Haleemah Bukola Adebayo, et al., "*Trajectories of University of Ibadan Undergraduates' Exposure to Cyber Pornography*", Journal of Social, Behavioral and Health Sciences 12, Issue 1, 2018.145.

Hardianto Djanggih, Nurul Qamar, "Penerapan Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime), *Jurnal Pandecta* Vol.13, no.1, (2018): 10-23

Heinegg W.H.V., "Legal Implications of Territorial Sovereignty in Cyberspace", 4th *International Conference on Cyber Conflict,* (2012): 7-19

Helmy Prasetyo Yuwinanto, "Privasi Online dan Keamanan Data", Journal Unair Vol. 2, No. 2, (2011): 1.

Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense", *Jurnal Pertahanan dan Bela Negara* Vol.7, no.2, (2017): 51-66

Institute for Policy Analysis of Conflict, *The Evolution of ISIS in Indonesia*, IPAC Report No. 13, 24 September 2014.

Jones, Steven G. "The Internet and its social landscape." *Virtual culture: Identity and communication in cybersociety* 1 (1997): 7-36

Kellerman, Aharon. "*Cyberspace classification and cognition: Information and communications cyberspaces*." *Journal of Urban Technology Vol* .1, No. 3 (2007): 5-32.

Kristyanto, Gregorius Hermawan, dan Anggie Rizky Kurniawan, "PENERAPAN METODE FOLLOWING THE MONEY DALAM PEMBUKTIAN PERKARA TINDAK PIDANA PENCUCIAN UANG HASIL TINDAK PIDANA PENGGELAPAN (Studi Perkara AN Terdakwa EKO EDI SUSANTO Pada Kejaksaan Negeri Semarang)", *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* 7.2 (2021)

Levitsky S., & Way LA., "The Rise of Competitive Authoritarianism", *Journal of Democracy, Vol 13 No 2,* (2002): 51-64

M Asrul Aziz, "Pengembangan Satuan Unit Cyber Crime", *Jurnal Litbang Polri* 22, no 1, (2019): 408-459

Maddocks, Sophie. "*A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political' deep fakes*", Porn Studies 7 no 4 (2020): 415-423.

Mahesa Jati Kusuma,"Perlindungan Hukum Terhadap Nasabah Bank yang Menjadi Korban Kejahatan ITE di Bidang Perbankan", *Al-Adl: Jurnal Hukum* 5.9 (2013).

Marcus Michaelsesn & Marlies Glasius, Authoritarian Practices in the digital age, *International Journal of Communication* 12(2018), 3788 -3794

Maria Minerva Kainama, Nuswantoro Dwi Warno, dan Joko Setiyono, "Pencegahan dan Penindakan Penggunaan Virtual Currency sebagai Sarana Kejahatan Pencucian Uang melalui Dunia Maya (Studi Kasus *Liberty Reserve*)", *Diponegoro Law Journal* 6.1 (2017)

Marinda, Fitrah, dan Rina Yulianti, "ASEAN AGAINST CYBER TERORRISM: UPAYA MENGATASI PROPAGANDA HITAM SEBAGAI KEJAHATAN SIBER TERORGANISIR", *Jurnal Legislatif* (2020): 106-123.

Md. Toriqul Islam dan Mohammad Ershadul Karim, "*A Brief Historical Account of Global Data Privacy Regulations and The Lessons for Malaysia*", Journal of History Departement, University of Malaya No. 28 (2), (2019): 171.

Menthe C.D., "Jurisdiction in Cyberspace: a Theory of International Spaces", *Mich. Telecomm. & Tech. L. Rev.* Vol 4, Issue 1, (1998): 69-103

Michelle Reed, "A Guide to US Data Protection", Trade Security Journal Issue 9, (2018): 6.

Morse, Margaret, and Elizabeth P. Seaton. "*Virtualities: television, media, art & cyberculture*." *Canadian Journal of Communication* Vol 24 No. 2 (1999): 298.

Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum Vol. 10, No. 2, (2019): 222.

Najamuddin Khairur Rijal, 2017, *Eksistensi dan Perkembangan ISIS: Dari Irak Hingga Indonesia*, Jurnal Ilmiah Hubungan Internasional Parahayang Center for Internasional Studies Volume 13 Nomor 1.

Nasrullah, Rulli. "Internet dan ruang publik virtual, sebuah refleksi atas teori ruang publik habermas." Jurnal Komunikator Vol 4 No.1 (2015).

Nazarudin Tianotak, 2011, *Urgensi Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan,* Jurnal Sasi Volume 17 Nomor 4.

Nguyen, Thanh Thi, dkk. "*Deep Learning for Deepfakes Creation and Detection: A Survey*." arXiv preprint arXiv 190911573. (2019).

Ni Luh Ketut Dewi Yani Putri, "KONSTRUKSI HUKUM DALAM PEMBUKTIAN TERHADAP KEJAHATAN MAYANTARA", *Kertha Semaya: Journal Ilmu Hukum* 8.8: 1202-1217. (2020)

Papacharissi, Zizi. "*The Virtual Sphere, The Internet as a Public Sphere*", dalam Jurnal New Media& Society, Vol 4. No.1. (2002) 9-27.

Piliang, Yasraf Amir. "*Cyberspace, Cyborg dan Cyber-Feminism*: Politik Teknologi dan Masa Depan Relasi Gender." *Jurnal Perempuan Vol* 18 (2001).

Radita Setiawan dan Muhammad Okky Arista, 2013, *Efektivitas Undang-Undang Informasi dan Transaksi Elektronik di Indonesia Dalam Aspek Hukum Pidana*, Jurnal Recidive Volume 2 Nomor 2.

Rana, M. S., & Sung, A. H. "*Deepfakestack: A deep ensemble-based learning technique for deepfake detection*". *IEEE* (2020). 70-75.

Rizki Dian Nursita, "Cyberspace: Perdebatan, Problematika, Serta Pendekatan Baru Dalam Tata Kelola Global", *Dauliyah Journal of Islamic and International Affairs* 4.1 (2019): 80-99.

Rudi Hermawan, "Kesiapan Aparatur Pemerintah Dalam Menghadapi Cyber Crime di Indonesia", *Jurnal Faktor Exacta* Vol. 6, No 1, (2013): 43-50

Rudi Natamiharja dan Stefany Mindoria, "Perlindungan Hukum atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Seluler), Jurnal Perundang-Undangan 7 (2), (2019): 4.

Rumampuk, Alfando Mario, "Tindak Pidana Penipuan Melalui Internet Berdasarkan Aturan Hukum Yang Berlaku Di Indonesia", *Jurnal Lex Crimen* Vol.6, no.3 (2015): 30-35

Samuel D. *Warren* dan Louis D. *Brandeis, "The Right to Privacy", Harvard Law Review Vol. 4, No. 5, (1890)*: *193-202*.

Shawn Henry dan Aaron F. Brantly, "Countering the Cyber Threat", *The Cyber Defense Review*, vol. 3, no. 1, 2018, pp. 47–56.

Shoup, Richard, "*Superpaint: An early frame buffer graphics system*," *IEEE Annals of the History of Computing* 23, no 2 (2001): 32-37.

Siti Yuniarti, "Perlindungan Hukum Data Pribadi di Indonesia", Jurnal Becoss Vol. 1, No. 1, (2019): 150.

Suci Utami, "TINDAK PIDANA PENCUCIAN UANG TERHADAP UANG VIRTUAL MONEY LAUNDERING ON VIRTUAL MONEY." *Al-Adl: Jurnal Hukum* 13.1 (2021)

Tanter R, Indonesia, Australia and Edward Snowden: Ambiguous and Shifting Asymmetries of Power, *The Asia Pasific Journal, (2018)*

Thaler, Michael. "*The "fake news" effect: An experiment on motivated reasoning and trust in news*." *Technical Report*. Working Paper, 2019.

Thies, Justus, dkk. "*Face2Face: Real-time Face Capture and Reenactment of RGB Videos*" Communications of the ACM 62, Issue 1 (2018): 96-104

Thomas K. Clancy, "*The Framers' Intent: John Adams, His Era, and the Fourth Amendment*", Indiana Law Journal Vol 86, Issue 3, (2011): 983.

Virtual Currencis Working Group, "Regulating Virtual Currencies", *France Ministry of Finance and Public Accounts, Paris* (2014)

Warren B. Chick, "*The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform*", Computer Law & Security Review Vol. 29, Issue 5, (2013): 6.

Yohanes Hermanto Sirait, "*General Data Protection Regulation* (GDPR) dan Kedaulatan Negara Non-Uni Eropa", Gorontalo Law Review Vol. 2 No. 2, (2019): 62.

Yunus Husein, "Tindak Pidana Pencucian Uang (Money Laundering) dalam Perspektif Hukum Internasional", *Jurnal Hukum Internasional (Indonesian Journal of International Law). Vol. 1. Nomor 2, Januari, Lembaga Pengkajian Hukum Internasional Fakultas Hukum Universitas Indonesia*, (2004)

Zahri Yunus dan Rabiah Ahmad, 2012, *A Dynamic Cyber-terrorism Framework*, Internasional Journal of Computer Science and Information Security Volume 10 Number 2.

Zuryatti Mohamed Yusoff, "*The Malaysian Personal Data Protection Act 2010: A Legislation Note*", New Zealand Journal of Public and Internasional Law Vol. 9, No. 1, (2011): 120.

Internet

Abu Hasan Banimal, Damar Juniarto, dan Ika Ningtyas, "*Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia*", SAFEnet, https://id.safenet.or.id/2020/12/riset-peningkatan-serangan-doxing-dan-tantangan-perlindungannya-di-indonesia/

Adam Satariano, "*Google is Fined $57 Million Under Europe's Data Privacy Law*", The New York Times, https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Adhi Wicaksono, "PPATK Sebut 'Virtual Currency' Bisa Mendanai Terorisme", CNN, www.cnnindonesia.com

Ali R. Hurson dan Hamid Sarbazi-Azad, "*Energi Efficiency in Data Centers and Clouds*", ScienceDirect,https://www.sciencedirect.com/topics/computer-science/big-data-processing

Aptika Kemkominfo, *Menilik Sejarah UU ITE*,Kominfo, https://aptika.kominfo.go.id/2019/02/menilik-sejarah-uu-ite-dalam-tok-tok-kominfo-13/

Arif Rahman, "*Inilah Perbandingan UU Kamsiber di Asia Tenggara*" Cyberr Threat, https://cyberthreat.id/read/771/Inilah-Perbandingan-UU-Kamsiber-di-Asia-Tenggara, diakses 1 Maret 2021

Asosiasi Penyelenggara Jasa Internet Indonesia; "*Laporan Survei Internet APJII 2019 - 2020 [Q2]*", APJII, https://apjii.or.id/survei.

Bagian Komunikasi Publik Biro Hukum dan Kerjasama BSSN, "*Rekap Serangan Siber (Januari-April 2020)*", BSSN, https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

BBC News, "*Dugaan penyadapan baru, Menlu kecam Australia*", https://www.bbc.com/indonesia/berita_indonesia/2014/02/140217_penyadapan_indonesia

Bill Clinten, "*KreditPlus Akui Kebocoran Data Pengguna*", Kompas, https://tekno.kompas.com/read/2020/08/05/06370007/kreditplus-akui-kebocoran-data-pengguna, diakses pada 13 April 2021

BNPT, *Waspadai Aktivitas Terorisme di Ruang Siber, Deputi Bidang Penindakan dan Pembinaan Kemampuan BNPT Sepakati Perjanjian Kerja Sama Dengan Direktorat Jenderal Aplikasi Informatika Kemkominfo,* BNPT, https://www.bnpt.go.id/waspadai-aktivitas-terorisme-di-ruang-siber-deputi-bidang-penindakan-dan-pembinaan-kemampuan-bnpt-sepakati-perjanjian-kerja-sama-dengan-direktorat-jenderal-aplikasi-informatika-kemkominfo

BSSN, *Cegah Terorisme, BSSN dan BNPT Jalin Kerja Sama Keamanan*, BSSN, https://bssn.go.id/cegah-terorisme-bssn-dan-bnpt-jalin-kerjasama-keamanan/

Cherri-Ann Beckles, "*From Ancient to Modern: The Changing Face of Personal Data*", *International Association of Privacy Professionals,* https://iapp.org/news/a/from-ancient-to-modern-the-changing-face-of-personal-data/

Daniar Supriyadi dan Selvy Annisa R, "*GDPR: Data Privacy Protection with Teeth*?", The Jakarta Post, https://www.thejakartapost.com/academia/2018/06/04/gdpr-data-privacy-protection-with-teeth.html

Frank Gardner, *How do Terorists Communicate?*, BBC News, https://www.bbc.com/news/world-24784756

Heru Soepraptomo, 2001, Kejahatan Komputer dan Siber serta Antisipasi Pengaturan Pencegahannya di Indonesia, Jurnal Hukum Bisnis vol. 12

IGN Mantra, *Tumpang Tindih Badan Siber dengan Lembaga Lain*, Komnfo, https://www.kominfo.go.id/content/detail/12355/tumpang-tindih-tugas-badan-siber-dengan-lembaga-lain/0/sorotan_media

Inside Privacy, "*Singapore to Introduce Data Protection Law*", Inside Privacy, https://www.insideprivacy.com/international/singapore-to-introduce-data-protection-law/

Interactive Constitution, https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv

Januta A., & Funakoshi M., "*Myanmar's Internet Suppression*", Graphics Reuters, http://www.graphics.reuters.com

Jonathan Stuart dan Adam Basker, "*Undefined by Data: A Survey of Big Data Definitions*", School of Computer Science, University of St Andrews, UK, 2013,https://arxiv.org/pdf/1309.5821.pdf

Judith DeCew, "*Privacy*", *The Stanford Encyclopedia of Philoshophy Archive*, https://plato.stanford.edu/archives/spr2018/entries/privacy/

Jürgen Stock, "*INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19*," *Interpol.Int*,https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Library of Congress; "*Sherman and his generals.*" https://www.loc.gov.

Lidya Julita Sembiring, "*Masih Banyak Kasus Pencucian Uang, Kapan RI Join FATF?*", CNN, www.cnbcindonesia.com

Matthew Rosenberg, Nicholas Confessore, dan Carole Cadwalladr, "*How Trump Consultans Exploited the Facebook Data of Millions*", The New York Times, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html,

Mawa Kresna, "*Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan*", Tirto.id, https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv,

Megan Garber, "*Doxing: An Etymology*", The Atlantic, https://www.theatlantic.com/technology/archive/2014/03/doxing-an-etymology/284283/, diakses 16 Februari 2021.

Mikhael Gewati, "*RI Rugi Rp.478,8 Triliun akibat Serangan Siber, DPR Siapkan RUU KKS*", Kompas https://nasional.kompas.com/read/2019/08/12/13454311/ri-rugi-rp-4788-triliun-akibat-serangan-siber-dpr-siapkan-ruu-kks?page=all

Nate Lord, "*What is a Data Protection Officer (DPO)*?", Digital Guardian, https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance

National Portrait Gallery. "*Sherman and His Generals*." https://npg.si.edu.

Peter Blume, "*Data Protection and Privacy – Basic Concepts in a Changing World*", Scandinavianlaw, https://www.scandinavianlaw.se/pdf/56-7.pdf

Shahbaz Adrian, "*Fake News, Data Collection, and the Challenge to Democracy*", Freedom House, http://www.freedomhouse.org

The New York Times, "*Libery Reserve Operators Accused of Money Laundering*", New York Times, http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?_r=0 ,

The White House, "*Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*", https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

Wahyudi Djafar dan M. Jodi Santoso, "*Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen*", Elsam, https://elsam.or.id/wp-content/uploads/2020/07/Policy-Paper-3_Otoritas-Independen-PDP.pdf,

Wahyudi Djafar, "*Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan*", https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf,

Wahyunanda Kusuma Pertiwi, "*Kasus Kebocoran Data Di Indonesia Dan Nasib UU Perlindungan Data Pribadi*", Kompas, https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all,

SKRIPSI/TESIS/DISERTASI

Bintar Mupiza, "Dampak Rivalitas Islamic State in Iraq and Syria (ISIS) dan Al-Qaeda Terhadap Gerakan Salafi Jihadi di Indonesia", Skripsi Program Studi Hubungan Internasional Fakultas Psikologi dan Ilmu Sosial Budaya Universitas Islam Indonesia, (2018).

Diptanala Dimitri, "Pelanggaran Hak Privasi (*Right to Privacy*) Oleh Pers Sebagai Dasar Perbuatan Melawan Hukum", Skripsi, Universitas Indonesia, (2011).

Erwin Kurnia N.M., "KESIAPAN SUMBER DAYA MANUSIA TEKNOLOGI INFORMASI (SDM-TI) KEMENTERIAN PERTAHANAN UNTUK MENGANTISIPASI CYBER WAREFARE", Tesis, Universitas Pertahanan Indonesia, (2015).

Iwan dkk, "KAJIAN STRATEGI KEAMANAN CYBER NASIONAL: DALAM RANGKA MENINGKATKAN KETAHANAN NASIONAL DI BIDANG KEAMANAN CYBER", Tesis, Universitas Pertahanan Indonesia, (2012).

Justin D Banez, "The Internet and The Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques", Tesis, Naval Postgraduate School, (2010).

Mohammad Haidar Ali, "cyber crime menurut undang-undang republik indonesia nomor 11 tahun 2008 tentang ite (perspektif hukum pidana islam)", tesis, uin alauddin makassar, (2012)

Ray William London, "*Comparative Data Protection and Security Law: A Critical Evaluation on Legal Standards*", Tesis, University of South Africa, (2013).

MAKALAH

Setiyadi, Mas Wigrantoro Roes, "Urgensi *Cybercrime Law* sebagai Perlindungan bagi Pengguna Teknologi Informasi" Pendekatan Kebijakan Publik Dalam Menjawab Kebutuhan Terhadap Perangkat Legal Untuk Memerangi Kejahatan Di Bidang Teknologi Informasi *(Cybercrime*), Makalah disampaikan pada Cybercrime Seminar 19 Maret 2003

Dan Lain-Lain

Erixon F., & Lee-Makiyama H., "Digital Authoritarianism: Human Rights, Geopolitics and Commerce", *Ecipe Occasional Paper,* No 5, 2011

Mahkamah Agung RI, 2007, *Naskah Akademis Undang-Undang Terorisme*, Badan Litbang Diklat Kumdil Mahkamah Agung RI.

Penjelasan Sekretaris Jenderal Kementerian Pertahanan Marsdya TNI Eris Haryanto pada seminar nasional keamanan Infrastruktur Internet yang diselenggarakan *Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI)* di Universitas Pertahanan di tahun 2011

Penjelasan Wakil Menteri Pertahanan Sjafrie Sjamsoeddin pada seminar nasional keamanan Infrastruktur Internet yang diselenggarakan *Indonesia Security Incident Response Team on Internet Infrastruktur (ID-SIRTI)* di Universitas Pertahanan di tahun 2011

We Are Social dan Hootsuite, "Essential Insight Into How People Around The World Use The *Internet*, Mobile Devices, Social Media, And Ecommerce", *Digitital 2020: Global Digital Overview* (2020)