INTELIGENSIA
INTRANS PUBLISHING

# KEAMANAN SIBER

## DAN PEMBANGUNAN DEMOKRASI DI INDONESIA

Editor : **Suwandi Sumartias**
Dosen Komunikasi Politik Fakultas Ilmu Komunikasi
Universitas Padjadjaran

KEAMANAN SIBER DAN PEMBANGUNAN DEMOKR

# KEAMANAN SIBER DAN PEMBANGUNAN DEMOKRASI DI INDONESIA

Editor:
Suwandi Sumartias

**Judul:**
Keamanan Siber dan Pembangunan Demokrasi di Indonesia

**Perpustakaan Nasional:**
Katalog Dalam Terbitan (KDT)
x+156 hlm.; 16 x 24 cm

**ISBN: 978-602-60367-2-8**
Cetakan Pertama, 2018

**Penulis:**
Prayudi
Ahmad Budiman
Aryojati Ardipandanto
Aulia Fitri

**Editor:**
Suwandi Sumartias

**Desain Sampul:**
Fajar Wahyudi

**Tata Letak:**
Tim Kreatif Lingkar Muda Mandiri

**Diterbitkan oleh:**
Pusat Penelitian Badan Keahlian DPR RI
Gedung Nusantara I Lt. 2
Jl. Jenderal Gatot Subroto Jakarta Pusat 10270
Telp. (021) 5715409 Fax. (021) 5715245

**Bekerjasama dengan:**
Inteligensia Intrans Publishing, Anggota IKAPI
Jl. Joyosuko Metro 42 Malang, Jatim
Telp. 0341- 573650 Fax. 0341-588010
redaksi.intrans@gmail.com
www.intranspublishing.com

# Pengantar Editor

Sejak reformasi, bangsa Indonesia teramat sibuk dengan urusan politik praktis dengan segala persoalan dan tantangannya. Kini di era industri 4.0 yang didukung teknologi komunikasi dan informasi yang sangat cepat, telah merubah tatanan sosial dan bisnis serta perilaku masyarakat, terutama masyarakat kota menengah ke atas. Era disrupsi komunikasi dan informasi bukan hanya menjadi tantangan, juga peluang yang membutuhkan jawaban dari semua elemen kebangsaan. Dalam dimensi politik dan atau demokratisasi, sedang terjadi gejala komunikasi yang luar biasa di dunia maya (media sosial). Salah satu efek negatif dari kebebasan ekspresi warga, kini disalurkan melalui media sosial dengan segala kontennya yang sangat mengancam keutuhan relasi kebangsaan. Media sosial (*twitter*, *instagram*, *youtube*, dlsb) seakan terbelah menjadi komunitas *lovers* dan *haters* yang berlebihan dan atau kebablasan. Kondisi ini menjadi "bom waktu" dalam membangun SDM yang berkualitas dan berkarakter di seluruh wilayah NKRI.

Salah satu artikel dari Crispin Thurlow, dkk. (2004) yang berjudul *Unwanted Cammmunication; Aggression and Abuse; Sexual Harassment; Ethical and Unethical Communication*"). Dia mengatakan bahwa media sosial *online* (media virtual) memiliki peran amat penting dan telah menjadi media alternatif bagi masyarakat, khususnya dalam berdemokrasi. Apresiasi tinggi masyarakat dalam penggunaan sistem jejaring sosial (*social-networking systems*) untuk berkomunikasi dan sekaligus menyalurkan, mengartikulasikan kepentingan secara *online* untuk hal yang bermanfaat ataupun merugikan. Dampak yang merugikan, para peneliti menemukan sejumlah pers populer telah mengingatkan kita tentang bahaya potensial yang tersembunyi dari *online* dan CMC (*Computer Mediated Communication*) yang tak

beretika. "*Online potential dangers lurking online and unethical CMC); Online harassment; hate speech online dan online ethics.*

Indonesia pengguna media sosial sungguh luar biasa. Menurut lembaga riset pasar *e-Marketer*, populasi netter tanah air mencapai 83,7 juta orang pada 2014. Angka yang berlaku untuk setiap orang yang mengakses internet setidaknya satu kali setiap bulan itu mendudukkan Indonesia di peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet. Pada 2017, *e-Marketer* memperkirakan netter Indonesia bakal mencapai 112 juta orang, mengalahkan Jepang di peringkat ke-5 yang pertumbuhan jumlah pengguna internetnya lebih lamban. Secara keseluruhan, jumlah pengguna internet di seluruh dunia diproyeksikan bakal mencapai 3 miliar orang pada 2015. Tiga tahun setelahnya, pada 2018, diperkirakan sebanyak 3,6 miliar manusia di bumi bakal mengakses internet setidaknya sekali tiap satu bulan. (*Kompas.com*)

Dengan dinamika yang sangat cepat di atas, tentunya antisipasi lembaga negara terkait sangat diperlukan tidak hanya pendekatan dan penegakkan formalitas yuridis melalui UU ITE, khususnya yang berkaitan dengan ujaran kebencian dan atau negatif di media sosial, juga terhadap dinamika gerakan *netizen* dan atau komunitas yang seringkali melakukan perlawanan sosial terhadap penyimpangan dari praksis demokrasi yang ditampilkan para elit politik. Aksi ini juga merupakan jalan terbaik untuk memperingatkan bahwa legitimasi dan optimalisasi fungsi demokrasi melalui lembaga-lembaga formal (eksekutif, legislatif, yudikatif) bentukan pemilu akan menjadi lembaga yang tak lagi memiliki legitimasi rakyat dan kehilangan makna dan kepercayaan di mata rakyatnya.

Untuk menjawab berbagai fenomena di atas, melalui buku Keamanan Siber yang ditulis para pakar di bidang media sosial sebagai hasil riset, tentunya menjadi menarik untuk disimak dan dikaji lebih dalam.

**Bagian I**, karya tulis Prayudi tentang Politik Siber dan Kedaulatan Negara yang menguraikan sub tema tentang: Politik Siber; Sentralisasi dan Desentralisasi Pemerintahan; Memudarnya Batas-Batas Teritorial Kedaulatan Negara; Masih Politik Partisan Jangka Pendek; dan Penyesuaian Kondisi Lapangan.

**Bagian II**, Ahmad Budiman menyajikan Tata Kelola *Cyber Security* Pemerintah Daerah dalam Upaya Meningkatkan Pelayanan Publik, dengan membahas sub tema: Pelayanan Publik Berbasis IT; ***Cyber Security* untuk Pelayanan Publik;** Tata Kelola *Cyber Security* di Pemerintah Daerah: Pelaksanaan di Sulawesi Tenggara, Pelaksanaan di Kalimantan Barat dan Pemutakhiran Tata Kelola *Cyber Security.*

**Bagian III**, Aryojati Ardipandanto menyajikan bahasan tentang Peran *Cyber Security* dalam Mencegah Konflik Politik Masyarakat di Daerah, dengan sub bahasan: Perkembangan Media Sosial dalam Demokrasi di Indonesia; Kasus HOAX; Sikap Pemerintah terhadap Dinamika Media Sosial; UU ITE, Apakah sudah Efektif?; *Cyber Security* di Indonesia; Daerah-daerah Rawan Konflik Akibat Lemahnya *Cyber Security* dan contoh kasus di Provinsi Sulawesi Tenggara dan Kalimantan Barat; Bagaimana Mengembangkan *Cyber Security* Sulawesi Tenggara dan Kalimantan Barat? Apa yang Perlu Diperbaiki?

**Bagian IV**, Aulia Fitri menyajikan pembahasan tentang Kebijakan Siber Nasional di Era Globalisasi Informasi, dengan sub tema tentang: Globalisasi Informasi; Kebijakan Siber di Berbagai Negara (Amerika Serikat; Australia; India; Singapura); Kebijakan Keamanan Siber di Indonesia; Problematika Kebijakan Siber di Indonesia dan Rekomendasi Implementasi Kebijakan Siber Nasional di Indonesia

Dengan uraian yang ada dalam buku ini, pentingnya *Cyber Security* dalam menata dan mengelola arus komunikasi dan informasi yang berkembang di masyarakat tentunya menjadi teramat penting

dan utama. Keberadaan lembaga formal yang serius, profesional dan berkelanjutan dalam bidang ini tentu menjadi tuntutan yang segera. Alih-alih kehadiran UU ITE No. 11 tahun 2008 masih belum dipahami dengan baik dan benar oleh para *netizen* atau warga masyarakat di seluruh pelosok negeri. Keadaan ini tentunya tidak bisa dibiarkan, karena pada gilirannya menjadi kontra produktif dalam mengawal dan mewujudkan karakter bangsa dan nasionalisme. Selamat menyimak.

Editor,

**Suwandi Sumartias**

*Dosen Komunikasi Politik Fikom Unpad*

# Daftar Isi

## BAGIAN 3
## PERAN *CYBER SECURITY* DALAM MENCEGAH KONFLIK POLITIK MASYARAKAT DI DAERAH

*Aryojati Ardipandanto*



## BAGIAN 4
## KEBIJAKAN SIBER NASIONAL DI ERA GLOBALISASI INFORMASI

*Aulia Fitri*

x

# Prolog
# "Keamanan Siber dalam Pembangunan Demokrasi di Indonesia"

## A. Perkembangan Teknologi Informasi

Pada era teknologi informasi modern dikenal internet dan komputer yang mampu mentransmisikan secara elektronis (komunikasi elektronis) segala bentuk data informasi secara cepat, tepat, efektif efisien serta *convenient* (nyaman, gampang). Bahkan para industri teknologi informasi mengklaim dapat pula menjamin kerahasiaan berita/ informasinya dalam sistem komunikasi yang umum dan terbuka itu. Perlu diamati lebih dalam dan tajam apakah "umum dan terbuka" itu benar-benar mampu melindungi kerahasiaan pada umumnya.[1]

Perkembangan teknologi informasi komunikasi (TIK) semakin pesat yang berimbas juga pada aktivitas pemerintahan daerah dan interaksi komunikasi di masyarakat. Komunikasi melalui saluran media maya (*cyber*), sesuai dengan perkembangan teknologi yang menyertainya juga harus berhadapan dengan potensi ancaman keamanan dalam pengelolaan (termasuk penyimpanan), serta penggunaannya. Pada sisi yang lain, kita tidak bisa memungkiri kemajuan TIK khususnya melalui saluran komunikasi maya (*cyber*) telah banyak digunakan dalam aktivitas pemerintahan atau interaksi di dalam masyarakat. Keamanan saluran media maya (*cyber security*) harus berhadapan dengan berbagai tantangan, baik yang bersifat umum maupun yang bersifat khusus di satu daerah.

---

[1] "*Persandian Indonesia*", http://www.lemsaneg.go.id/index.php/khasanah/persandian-indonesia/, diakses tanggal 12 Februari 2016.

Pilar *cyber security* di pemerintahan terdiri dari kebijakan, pelayanan, proses kerja, teknologi dan masyarakat. Untuk itu pemerintah perlu memperhatikan arsitektur pengelolaan *cyber security* yang meliputi:

a. *Definie and classify your requirements*
b. *Design for management requirements*
c. *Refini for business requirements*
d. *Overlay information architecture and manageability.*[2]

Tingginya penggunaan internet seiring dengan maraknya keterkaitan internet dengan kehidupan sehari-hari, mengakibatkan frekuensi serangan dan kejahatan *cyber space* semakin meningkat. Kejahatan-kejahatan *cyber space* atau yang dikenal dengan istilah *cybercrime* tersebut meliputi pencurian identitas dan data (sumber daya informasi), pembajakan *account* (*email, IM, social network*), penyebaran *malware* dan *malicious code, fraud, spionase industry*, penyanderaan sumber daya informasi kritis serta *cyber warfare* atau perang di dalam dunia maya.[3]

Keamanan saluran media maya (*cyber security*) juga diperlukan dalam rangka mengantisipasi terjadinya ancaman yang terkait dengan keamanan data dan informasi. *Cyber security* adalah aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *cyber crime.*[4]

Ancaman terhadap data dan informasi dapat dibagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif. Adapun ancaman aktif

---

[2] Dani Firmansyah, "*Cybersecurity for governance*", disampaikan pada FGD Proposal Penelitian Tata Kelola *Cyber Security* pada Pemerintahan Daerah, di Puslit BKD, 17 Maret 2017.

[3] Kementerian Komunikasi Informatika RI, *Buku Putih 2011 Komunikasi dan Informatika Indonesia*, 2011, hal. 22.

[4] Mochamad James Falahuddin, Sekilas Tentang *Cyber Crime, Cyber Security* dan *Cyber War*, https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war, diakses tanggal 26 Januari 2017.

antara lain, *pertama,* pencurian data, *kedua,* penggunaan sistem secara ilegal, *ketiga,* penghancuran data secara ilegal, *keempat,* modifikasi secara ilegal. Sedangkan ancaman pasif antara lain berupa, *pertama,* kegagalan sistem atau kegagalan *software* dan *hardware* yang dapat menyebabkan data menjadi tidak konsisten, transaksi tidak berjalan dengan lancar sehingga data menjadi tidak lengkap atau bahkan data menjadi rusak. *Kedua,* kesalahan manusia, yakni kesalahan dalam pengoperasian sistem yang dilakukan oleh manusia yang dapat mengancam integritas sistem dan data. *Ketiga,* bencana alam sumber daya pendukung sistem informasi menjadi luluh-lantak dalam waktu yang singkat.[5]

Namun dengan bertambahnya jumlah laporan insiden keamanan siber yang terus meningkat, ancaman siber tidak hanya membahayakan infrastruktur informasi penting yang ada, namun juga bisa mengancam kerahasiaan, keutuhan, dan ketersediaan informasi yang sensitif yang umumnya kita proses, kirim dan simpan secara *online.* Oleh karena itu, untuk memitigasi ancaman siber, pemerintah Indonesia berencana untuk lebih memperkuat dan memperluas kapasitas keamanan siber dalam hal struktur kelembagaan dan koordinasi terkait pengembangan keamanan siber nasional.[6]

## B. Fenomena Siber

Fenomena ruang siber menggambarkan sebuah realitas bahwa aktifitas kegiatan masyarakat modern saat ini sudah saling terkoneksi melalui ruang siber dan internet. Dari perspektif keamanan siber, pemanfaatan internet juga dimungkinkan untuk tujuan negatif atau destruktif oleh

---

[5] Paryati, *Keamanan Sistem Informasi,* http://repository.upnyk.ac.id/143/1/47_Keamanan_Sistem_Informasi.pdf, laman diakses pada Hari Selasa, 9 Agustus 2016, pukul 16.10 WIB.

[6] Peta Masa Depan Keamanan Siber Indonesia, http://aptika.kominfo.go.id/index.php/artikel/138-peta-masa-depan-keamanan-siber-indonesia, diakses tanggal 5-3-2017

pihak-pihak yang punya kemampuan baik dilakukan secara perorangan, kelompok hingga oleh negara.[7]

Penataan keamanan siber menjadi lebih relevan, terutama bila dikaitkan dengan kebijakan pemerintah dalam mengembangkan *e-government* terutama di pemerintah daerah (Pemda). Tata kelola keamanan siber ini sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan berbasis *online*. Pengembangan sistem *e-Government* tidak terlepas dari pengamanan siber, karena pengembangan *e-Government* dapat dimulai dengan pembangunan situs yang menyediakan peluang interaksi pelayanan publik dan penyimpanan data dan informasi.

Keamanan siber tidak hanya terkait dengan persoalan tata kelola keamanan siber utama yang terjadi di Pemda, namun juga terkait dengan permasalahan konten yang disebarluaskan melalui media *online* ini, seperti pada penerapan kehidupan demokrasi melalui kegiatan pemilihan umum utamanya yang terjadi di daerah. Dalam konteks tata kelola informasi dan kemanan informasi di era globalisasi informasi terutama pada era demokrasi pilkada, maka sistem persandian (*kriptografi*) sejatinya juga merupakan bagian integral yang tidak dapat dipisahkan. Tata kelola informasi dan keamanan informasinya bahkan menjadi lebih relevan jika dikaitkan dengan kebijakan pemerintah mengembangkan *e-gov* di lingkungan Pemda, termasuk aparatur sipil negara (ASN)-nya, karena dalam filosofis keamanan informasi diyakini bahwa *human factor is the weakest link*. Di lingkungan Pemda, tata kelola informasi dan keamanan informasi diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan yang prima.[8]

---

[7] Rudy Agus Gemilang Gultom, Membangun Tata Kelola Informasi dan Keamanan Informasi Pemerintahan Daerah di Era Globalisasi Informasi dalam Rangka Menjaga Keutuhan dan kedaulatan NKRI", disampaikan pada FGD Penelitian Tata Kelola *Cyber security* pada Pemerintahan Daerah, Puslit BKD, Jakarta, 17 Maret 2017.

[8] *Ibid.*

Keberadaan *cyber security* dalam konteks kehidupan demokrasi, tidak terlepas dari dinamika pemilu yang diselenggarakan. Ini biasanya dikaitkan dengan tahapan kampanyenya. Kampanye pemilu dan keberadaan media sangat kuat ditekankan dalam draft RUU Penyelenggara Pemilu 2016, tidak saja terkait proses penetapan hasil pemilu, tetapi juga di tahapan proses awal rekrutmen dan pengumuman kandidat penyelenggaranya, baik KPU maupun Bawaslu di tingkat nasional dan daerah. Pada rentang tahapan demikian, pemilu dan kampanye sangat kuat dipengaruhi oleh media dengan segala dinamika politik konten berita yang disebarkannya. Apalagi terdapat fenomena iklan politik yang mendorong budaya populer dalam politik, seperti logika seolah-olah bagi siapa saja anggota masyarakat yang berminat terjun ke dalam kompetisi politik tidak absah jika belum melakukan publikasi iklan politik. Ini berlaku nyaris jamak bagi setiap anggota masyarakat, apakah itu semula berprofesi kiai, santri, guru, artis, pengusaha, petani, dan lain sebagainya.[9]

Media yang penting bagi politisi dan partai tidak lagi sekedar pada konteks promosi melalui iklan diri secara terbuka, tetapi juga dapat dimanipulasi bagi sarana mendiskreditkan lawan atau saingan politik yang dilakukan secara tertutup. Sebaran manipulasi iklan politik semacam ini sangat terbuka peluang penggunaannya melalui media sosial yang nihil filter kebenaran atau akurasi konten pemberitaannya.

Peraturan KPU No. 12 Tahun 2016 tentang Kampanye Pilkada yang menjabarkan UU Nomor 10 Tahun 2016 tentang Pemilihan Gubernur, Bupati/Walikota hanya mengatur soal kewajiban pasangan calon (paslon) mendaftarkan akun resmi di media sosial kepada KPU setempat. Akun itu juga harus ditutup maksimal sehari setelah masa kampanye berakhir. Penggunaan media sosial saat pilkada serentak 101 daerah di tahun 2017, tidak hanya terjadi pada kasus di Jakarta. Tetapi penggunaannya juga marak berkembang di pilkada di daerah-daerah

---

[9] Sufyanto, *Selebrisasi Politik: Kajian Dramaturgi, Habitus dan Tindakan Komunikatif Aktor Pemilu*, Penerbit Nusa Media, Bandung, 2015, h. 17.

lainnya. Tanggung jawab dianggap menjadi penting dalam perkembangan pesat media sosial dalam pemilu dan pilkada, tidak sekedar pada konteks kendali atau pengawasan terhadap penggunaannya. Kalau terlampau prioritas pada aspek pengawasan penggunaan media sosial dalam momentum pilkada atau pemilu, maka dapat mengarah pada kekhawatiran adanya belenggu tertentu bagi kebebasan berekspresi dan memperoleh akses informasi publik.[10]

Kampanye pemilu yang mensyaratkan *fairness* sebagai fondasi bagi persaingan yang setara tidak akan terwujud maksimal, atau dapat diganggu oleh media sosial yang sifatnya sebaran beritanya dilakukan melalui genggaman individual. Bahkan, infiltrasi gangguan tidak saja di tingkat *fairness* kampanye, tetapi juga dapat menekan stabilitas politik dan jadi godaan bagi rezim penguasa melakukan tindakan represif. Tindakan represif diambil dengan alasan untuk menjaga kepentingan yang lebih besar dan stabilitas politik menjadi muatan kepentingan dimaksud. Kebijakan rezim Jokowi-Jusuf Kalla dalam mengendalikan media komunikasi masyarakat, terutama pada konteks media sosial, tampaknya tidak terlepas dari kontroversi media sosial dalam kampanye pemilu.

Media sosial sebagai sarana komunikasi menghadapi tantangan agar partisipasi publik dalam pemerintahan dapat berjalan dan menghasilkan substansi yang konstruktif. Ini menjadi tantangan, mengingat sumber dan topik berita bohong (*hoax*) yang paling sering diterima masyarakat adalah berita seputar isu politik. Produksi konten-konten negatif dari sektor ini sangat banyak karena melibatkan tim, mulai dari produser, penyokong, hingga pengikut. Gambaran betapa isu politik menjadi bahan perbincangan paling ramai di media sosial dapat terpantau dari hasil analisis perangkat *Social Topic Analysis*. Hanya dalam beberapa jam, khususnya di saat Pilkada DKI Jakarta hari pemungutan suara 15 Februari 2017, total *mentions* terhadap setiap paslon yang bersaing mencapai ratusan ribu. Pengamat sosial, Ismail Fahmi, berharap agar

[10] "Pengaturan Lebih Rinci Dibutuhkan", *Kompas*, 20 Februari 2017.

selain terhadap *facebook* yang menyaring konten-konten negatif dan meningkatkan literasi penggunanya, pemerintah, melalui Dewan Pers dan Kementerian Informasi dan Komunikasi, juga harus ikut andil dan tegas dalam membuat edukasi dan kriteria bagi situs-situs media yang sehat *vis a vis* yang tidak sehat.[11]

Ada 4 (empat) tulisan dalam buku yang sedang kita baca saat ini. Tulisan pertama berjudul "Politik Siber dan Kedaulatan Negara," ditulis oleh Prayudi. Konteks politik siber biasanya menyangkut persaingan kekuasaan dalam pemilu dan kesetiaan warga bangsa terhadap kepentingan nasional. Hal ini menyebabkan bahwa politik siber terkoneksi kuat dengan masalah kedaulatan negara. Kontestasi antar-peserta pemilu, pihak penyelenggara, dan masyarakat, dalam konteks politik siber juga tidak lepas dari pengaruh dunia internasional. Birokrasi negara seolah tertinggal langkahnya oleh kecepatan gerak politik siber dengan segala dimensi luas yang dimiliki oleh siber itu sendiri. Momentum politik tertentu memiliki konsekuensi bagi ikatan kebangsaan dalam konteks memudarnya kedaulatan negara. Masalahnya adalah, bagaimana regulasi siber di tengah semakin memudarnya batas-batas antar-kedaulatan wilayah negara saat ini? Bagaimana alternatif solusi yang dapat dilakukan dalam mengatasi dampak negatif dari fenomena siber di tengah semakin kaburnya batas teritorial antar negara?

Penulis kedua yaitu Ahmad Budiman yang membahas masalah "Tata Kelola *Cyber Security* Pemerintah Daerah dalam Upaya Meningkatkan Pelayanan Publik." Pada hakekatnya, keberhasilan pelayanan publik yang dilakukan oleh penyelenggara pelayanan publik kepada masyarakat sangat ditentukan oleh seberapa besar kemanfaatan pelayanan publik yang dapat dirasakan masyarakat. Semakin cepat masyarakat memperoleh pelayanan publik sesuai dengan kebutuhan yang dimilikinya, akan menjadi salah satu indikator dari telah dilaksanakannya pelayanan publik dengan baik. Untuk itu perlu dibangun sebuah sistem informasi yang dapat membantu meningkatkan pelayanan publik penyelenggara

[11] "Hoaks Politik Dominan", *Kompas*, 16 Februari 2017.

kepada masyarakat. Upaya untuk memberikan pelayanan publik berbasis internet, sesungguhnya sejalan dengan program pemerintah dalam mengembangkan *e-government* di semua kelembagaan baik di tingkat pusat hingga ke tingkat daerah. Untuk itu tata kelola keamanan siber sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam mendapatkan layanan publik dan layanan perijinan berbasis *online*. Hal inilah yang mendasari pertanyaan dalam tulisan ini, yaitu, bagaimana tata kelola keamanan siber dalam meningkatkan pelayanan publik kepada masyarakat?

Tulisan ketiga mengangkat judul "Peran *Cyber Security* dalam Mencegah Konflik Politik Masyarakat di Daerah" yang ditulis oleh Aryojati Ardipandanto. Media sosial seperti *Facebook, Twitter, Instagram,* dan lain-lain memang dapat membuat masyarakat semakin "melek" politik dan selalu dapat mengikuti perkembangan politik yang ada. Tetapi di sisi lain, kekuatan media sosial dapat dimanfaatkan untuk hal-hal berbahaya oleh pihak-pihak yang tidak bertanggung-jawab, terutama dalam momen menjelang Pemilu atau Pilkada. Hal yang berbahaya tersebut antara lain adalah bahwa media sosial dapat digunakan untuk menyebarkan *hoax* dalam perang kampanye di dunia maya. Bila masyarakat Indonesia tidak dibekali dengan kesadaran tentang pentingnya menggunakan media sosial dengan bijak dan hati-hati, tentunya ini akan sangat membahayakan kestabilan kehidupan bermasyarakat, berbangsa, dan bernegara. Hal ini dikarenakan *hoax* yang disebarkan di media sosial berdampak luas dan menimbulkan potensi konflik yang akibatnya bisa sangat menakutkan. Dalam memandang kondisi tersebut, tentunya logika kita akan mengarah pada pentingnya suatu sistem pengamanan arus informasi di media sosial. *Cyber security* yang dilaksanakan dengan profesional setidaknya akan menangkal dampak negatif dari penggunaan media sosial yang diarahkan pada timbulnya konflik oleh pihak-pihak tertentu yang memang ingin mengacaukan stabilitas politik negara.

Tulisan keempat ditulis oleh Aulia Fitri dengan judul tulisan "Kebijakan Siber Nasional di Era Globalisasi Informasi." Fenomena globalisasi informasi yang ditandai dengan pesatnya kemajuan teknologi, informasi, komunikasi dan interaksi lintas batas membawa dampak tersendiri terhadap keamanan suatu negara, khususnya di ruang siber. Perubahan ini juga mengakibatkan terjadinya pergeseran ancaman yang dihadapi oleh suatu negara, dari ancaman yang bersifat tradisional menjadi ancaman asimetris. Beberapa kasus mengenai serangan siber yang terjadi di beberapa negara termasuk Indonesia menandakan ketergantungan negara terhadap teknologi informasi membawa tantangan dan ancaman tersendiri. Besarnya potensi ancaman di ruang siber baik secara langsung maupun tidak langsung telah mendorong berbagai negara untuk melakukan penataan kebijakan di bidang siber. Indonesia belum memiliki kebijakan di bidang siber yang bersifat integratif, dengan kata lain kebijakan yang dijalankan masih bersifat sektoral. Oleh karena itu tulisan ini akan memetakan permasalahan kebijakan siber nasional di Indonesia dan merekomendasikan penerapan kebijakan siber yang terintegratif berdasarkan komparasi atas penerapan kebijakan siber dari berbagai negara di dunia.

Keempat tulisan dalam buku ini menjadi menarik untuk kita baca dan pahami isinya dengan cermat. Hal menarik dalam tulisan di buku ini yaitu adanya kesamaan pandangan dari semua penulis, bahwa siber dalam penerapannya di berbagai aspek akan dapat mempengaruhi pembangunan demokrasi di tanah air. Tentunya pembangunan demokrasi dimaksud adalah pembangunan demokrasi menuju pada arah yang lebih positif. Seberapa besar tujuan dari tulisan buku ini akan dapat tercapai, mari kita baca semua tulisan ini dengan seksama.

**Editor**

# BAGIAN 1
# POLITIK SIBER DAN KEDAULATAN NEGARA

*Prayudi*
*Peneliti Kepakaran Politik Pemerintahan Indonesia*
*Pusat Penelitian Badan Keahlian Dewan DPR RI*
*E-mail: prayudi_pr@yahoo.com*

## A. Politik Siber

Aktivitas manusia dan kelompoknya masing-masing di masa sekarang dan mendatang, tampaknya semakin super *mobile* dengan segala konsekuensinya. Di tengah aktivitas demikian kedaulatan negara menjadi semakin kabur (*borderless*), karena perangkat siber semakin memudahkan orang untuk bergerak tidak saja di lingkup mikro lokalitas seperti halnya dusun dan desa/kelurahan, atau sekedar daerah setempat dan regional hingga tingkat nasional, tetapi juga secara cepat mudah menjangkau hingga tingkat global.

Kedaulatan negara yang dipertaruhkan dalam politik siber mendorong pilihan kebijakan menyangkut siber itu sendiri memiliki arti strategis tersendiri bagi kepentingan bangsa Indonesia. Kebijakan yang diambil merupakan visi bagi kepemimpinan di negara bersangkutan dalam menghadapi segala konsekuensi yang menyertainya. Ikatan eksternal bagi negara menjadi kuat dalam konteks siber, manakala jaringan internet dan jasanya melalui organisasi APJII yang bergerak secara kelembagaan. APJII merupakan salah satu organisasi yang diberi kepercayaan untuk memiliki *National Internet Registry* (NIR), sehingga anggota APJII tidak perlu punya menyewa ke *Asia*

*Pacific Network Information Centre (APNIC)*.[1] Keterikatan regional antar-negara demikian menyebabkan adanya keterbatasan peran negara dalam mengelola siber yang berjaringan di kawasan kedaulatannya itu sendiri. Kondisi demikian tetap menyisakan catatan mengenai hal-hal tertentu seperti halnya pemasangan pipa jaringan kabel optik di dasar laut adalah menyewa pada provider satelit dan tetap memerlukan izin dari negara.

Konteks politik siber biasanya menyangkut persaingan kekuasaan dalam pemilu dan kesetiaan warga bangsa terhadap kepentingan nasional. Hal ini menyebabkan bahwa politik siber terkoneksi kuat dengan masalah kedaulatan negara. Kontestasi antar-peserta pemilu, pihak penyelenggara, dan masyarakat, dalam konteks politik siber juga tidak lepas dari pengaruh dunia internasional. Birokrasi negara seolah tertinggal langkahnya oleh kecepatan gerak politik siber dengan segala

dimensi luas yang dimiliki oleh siber itu sendiri.

Di lingkup lokal, siber juga sudah berpotensi bagi terjadinya perpecahan politik antar-pendukung saat pilkada dan bahkan bagi masyarakat setempat. Ini misalnya sebagaimana terjadi sejak saat

luar itu, masih ada 124 akun yang diawasi Polres Tulungagung, di samping itu juga dijalankan sosialisasi gerakan sehat bermedia sosial dengan para komunitas *netizen* yang ada di wilayah tersebut.[2]

Momentum politik tertentu memiliki konsekuensi bagi ikatan kebangsaan dalam konteks memudarnya kedaulatan negara. Masalahnya adalah, bagaimana regulasi siber di tengah semakin memudarnya batas-batas antar-kedaulatan wilayah negara saat ini? Bagaimana alternatif solusi yang dapat dilakukan dalam mengatasi dampak negatif dari fenomena siber di tengah semakin kaburnya batas teritorial antar-negara?

## B. Sentralisasi dan Desentralisasi Pemerintahan

Kata *cyber* berasal dari awalan "*cybernetic*" dari bahasa Yunani yang berarti kata sifat terampil. Istilah *cyber* digunakan untuk menggambarkan entitas yang ada (atau peristiwa yang terjadi) di dunia maya. Ini diwujudkan melalui jaringan komputer, sifatnya digital dan direpresentasikan dalam satuan bit, yang dalam perkembangannya teknologi informasi telah menciptakan "ruang baru" yang bersifat artifisial,[3] sekaligus memberikan pengaruh bagi masyarakat dan bahkan kedaulatan negara. Teknologi mendorong terjadinya konvergensi media yang menyebabkan tidak lagi sekedar pada media konvensional semata, tetapi juga hubungan interaktif antar-berbagai kalangan yang lebih luas. Masyarakat bukan lagi sekedar sebagai konsumen berita, tetapi juga sekaligus dapat berperan sebagai produsen berita itu sendiri. Mc Quil menjelaskan soal ini, bahwa: "konsep budaya konvergen (*convergence culture*) barangkali pertama kali disebutkan Jenkins (2004), tetapi telah dikenal secara luas sebelumnya. Istilah ini merujuk

---

[2] "Polisi Awasi 240 Akun Media Sosial di Pilkada Tulungagung", *Koran Tempo*, 12 April 2018, h. 10.

[3] Nudirman Munir, *Pengantar Hukum Siber Indonesia*, Rajawali Press, Depok, 2017, edisi ketiga, h. 193.

pada serangkaian fenomena yang berhubungan dan bermula serta sepertinya disebabkan oleh konvergensi teknologi secara murni.[4] Munculnya perkembangan media yang merupakan konsekuensi teknologi dengan segala dampak publiknya, dapat dilihat pada tabel berikut:

**Tabel 1. Perbedaan Antara Media Pertama dan Kedua**

| Era Media Pertama (*Broadcast*) | Era Media Kedua (*Interactivity*) |
|---|---|
| Tersentral (dari satu sumber ke banyak khalayak) | Tersebar (dari banyak sumber ke banyak khalayak) |
| Komunikasi terjadi satu arah | Komunikasi terjadi timbal balik atau dua arah |
| Terbuka peluang sumber atau media untuk dikuasai | Tertutupnya penguasaan media dari bebasnya kontrol terhadap sumber |
| Media merupakan instrumen yang melanggengkan strata dan ketidaksetaraan kelas sosial | Media memfasilitasi setiap khalayak (warga negara) |
| Terfragmentasinya khalayak dan dianggap sebagai massa | Khlayak bisa terlihat sesuai dengan karakter dan tanpa meninggalkan keragaman identitasnya masing-masing |
| Media dianggap dapat atau sebagai alat mempengaruhi kesadaran | Media melibatkan pengalaman khalayak baik secara ruang maupun waktu |

Sumber: Rulli Nasrullah, *Teori dan Riset Media Siber (Cybermedia)*, (2016), h. 14

[4] Denis Mc Quill, *Teori Komunikasi Massa*, Penerbit Salemba Humanika, Jakarta, 2011, h. 71.

Perkembangan di atas menyebabkan ruang siber pelaku pelanggaran menjadi sulit dijerat karena hukum dan pengadilan Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan yang terjadi mengingat bersifat transnasional, ironisnya justru berdampak pada implikasi bagi negara bersangkutan. Konsekuensi atas siber yang ironis demikian di tengah kedaulatan negara bisa dilihat dari pendekatan teritorial yang merupakan kelanjutan atas pendekatan yurisdiksi bagi siber.[5] Sehubungan sifatnya yang demikian lintas batas negara, penting bagi negara untuk menjaga kedaulatannya untuk mengaturnya lebih lanjut, termasuk dari aturan terkait selama ini, dan selanjutnya mencari solusi atas kemungkinan konflik yang harus dihadapi.

Siber memiliki konsekuensi besar bagi masyarakat dan negara, mengingat pengaruh dalam mendekonstuksi teori klasik komunikasi politik mengenai aliran komunikasi dua arah dan pengaruhnya dalam pengambilan kebijakan. Ini ditandai dengan kehadiran media sosial yang tidak saja pada konteks makro di kalangan para aktor dan kelembagaan suprastruktur, tetapi juga terhadap cara kerja dan proses di internal mikro industri dan komunitas.[6] Dengan ruang kebebasan bagi penggunanya yang bisa mengangkat isu tertentu sebagai pilihan acuan utama publik *follower* atau populer disebut viral, maka "keunikan" atau bahkan "kekejaman" dari isu yang diangkat dapat memiliki pengaruh politik signifikan.

*Cyber war* adalah semua tindakan yang dilakukan secara sengaja dan terkoordinasi dengan tujuan mengganggu kedaulatan sebuah negara. *Cyber war* bisa berupa *cyber attack*, *cyber terrorism*, maupun *cyber espionage* yang mengganggu keamanan nasional.[7]

---

[5] Nudirman Munir, *Op.cit.*, h.292.

[6] Bruce E. Drushel, "Social Media versus Madmen: Notes from Frontlines of a Digital Insurgency", dalam Glenn W. Richardson Jr (editor), *Social Media And Politics: A New Way To Participate in the Political Process*, Preager, California, 2017, h. 211-212.

[7] Draft Naskah Akademik RUU Siber, PUU Badan Keahlian DPR RI, per-tanggal 28 Mei 2018, h. 17.

Penyalahgunaan siber yang berdampak kedaulatan negara, tidak saja pada konteksnya yang menyangkut kemasyarakatan antar-segmen sosialnya, tetapi di tingkat infrasruktur politik negara bersangkutan. Kasus pemanfaatan media sosial *Facebook* bagi pemenangan kandidat pemilu misalnya, belum lama berselang, menjadi contoh kongkret penyalahgunaan siber dimaksud. Kasus ini semakin menghangat pada saat penyelidik dari badan pengawas data Inggris menggeledah kantor *Cambridge Analytica* di London, Inggris. Perusahaan konsultan ini menambang data pribadi 50 juta pengguna *Facebook* untuk membantu memenangkan Donald Trump dalam Pemilihan Presiden AS tahun 2016.[8] Kasus kejahatan ini dengan memanfaatkan data pengguna *Facebook* terkait produk dan layanannya, sementara pengguna sendiri tidak mengetahui pihak konsultan perusahaan tadi melalui jaringannya menggunakan untuk kepentingan bisnis dan sekaligus politik. Dugaan keterlibatan perusahaan konsultan ini juga terjadi pada beberapa kasus pemilu di negara lainnya, termasuk di Malaysia yang berbuntut pada dugaan korupsi.

Teknologi informasi komunikasi (ICT) tidak saja membawa nilai terkait baik secara hukum atau legal, maupun ekonomi, tetapi juga menyangkut nilai demokrasi (*democratic values).* Dari kategorisasi yang ada, kiranya tabel berikut menunjukkan muatan nilai dari masing-masing ranah yang dipengaruhi oleh ICT dimaksud.

[8] Kasus ini telah memicu krisis besar bagi perusahaan *Facebook* antara lain dengan jatuhnya nilai saham pasarnya hingga 14 persen dan menyebabkan hilangnya lebih dari 50 miliar dollar AS pada nilai sahamnya. CEO *Facebook* Mark Zuckerberg telah meminta maaf secara terbuka sekaligus mengakui telah terjadi pembobolan besar kepercayaan. Lihat "Cambridge Analytica Diusut", *Kompas*, 25 Maret 2018.

**Tabel 2. Nilai Legal, Ekonomi dan Demokrasi dalam Administrasi Publik**

| | Nilai Legal | Nilai Ekonomi | Nilai Demokrasi |
|---|---|---|---|
| Contoh Nilai-Nilai: | *Rule of laws*, legalitas; Legal equity, netralitas Ketidakpastian, penurunan | Efektivitas, efisiensi Orientasi pelanggan Fleksibilitas | Keterbukaan Transparansi Akuntabilitas |
| Mekanisme Kordinasi | Hirarki | Pasar | Kesamaan sosial jaringan |
| Instrumen Kordinasi | Aturan & Regulasi | Uang & harga | Komunikasi & informasi |
| Perspektif warga negara | Subordinat | Pelanggan | Partner |

Sumber: Kris Snijkers, "*E-Government: ICT From A Public Management Perspective*", *13th Annual NISPAcee Conference, 19-21 Moscow State University, Moscow, Russia*, h.4

Lintasan demokrasi yang luas tidak saja secara teknis teknologi instrumen, tetapi juga di aspek-aspek kehidupan lainnya mencipatakan pola komunikasi politik tidak lagi sekedar konvensional pada ruang lingkup regional kawasan tertentu saja. Itu sebabnya pola komunikasi baik antar-elit maupun elit dengan masa adalah perlu dilihat perbandingannya pada setiap negara, tidak sekedar pada kepentingan politik partisan yang berlaku terbatas pada mengukur popularitas tokoh dari hasil survai dan *polling*.[9] Langkah perbandingan demikian diharapkan dapat menemukan pola komunikasi yang terjadi di antara

[9] Barbara Pfest, *Political Communication in the Era New Technologies*, Berlin (tanpa tahun), h.193.

negara dan kelompok kawasan secara lintas kepentingan lebih luas dan memperoleh karakteritsik demokrasi modern digital yang berbeda dengan demokrasi lama.

Penyebaran gagasan dan gerakan demokrasi di berbagai negara tidak lagi sebatas pada kanal komunikasi konvensional, tetapi sudah merambah pada skala kecepatan luar biasa hitungan perdetik pengaruhnya dalam lintasan regional antar-kawasan dan negara, bahkan hingga tingkat global. Pada beberapa kasus sebagaimana dialami kawasan Timur Tengah, ini melahirkan fenomena politik *Arab Spring* yang melanda beberapa negara sekitar dan meruntuhkan rezim lama yang berkuasa. Meskipun fenomena politik di beberapa kasus itu tidak selalu berujung keberhasilan pada konsolidasi demokrasi, tetapi beberapa gejala dari runtuhnya rezim lama di Timur Tengah sudah menjadi inspirasi gerakan serupa diperkuat eskalasinya di kawasan lain. Siber melalui kehadiran instrumen digital telah menjadi nilai dalam politik yang strategis dan tidak lagi sekedar teknis prosedural pengelolaan pemerintahan dan sukar dibendung pengaruhnya dalam kehidupan setiap negara. Bahkan di lingkup internal partai pun, dikembangkan teknologi serupa dalam hal pengelolaan data dan sumber daya awal bagi pengembangan kelembagaan demokrasi untuk dapat menggerakan partisipasi masyarakat terhadap kebijakan-kebijakan yang diambil pemerintahan setempat.

Dalam konteks internal partai dimaksud, era digital sebagai penanda kekuatan aspek politik siber menjadi tantangan tersendiri. Partai dituntut untuk beradaptasi dengan era baru ini, dirinya harus melakukan transformasi kelembagaan dan sumber daya yang ada di lingkup kepemilikannya. Kalau partai tidak melakukan transformasi, maka partai bersangkutan oleh lajut perkembangan teknologi digital dalam pengelolaan manajemen partai.

Mengandalkan semata pada cara manual tidak lagi dapat dipertahankan, meskipun bukan berarti perlu dihilangkan sama sekali penggunaan cara manual itu sendiri. Kampanye, sosialisasi, kaderisasi

partai harus menggunakan teknologi digital sebagai perangkatnya. Generasi muda dan pemilih pemula sebagai segmen baru partai dalam persaingan dan dukungan politik, sangat perlu didukung siber terkait perangkat digital pengelolaan kelembagaan partai. Melalui siber yang berperan dalam aspek politik, maka visi digital tata kelola partai mendorong era baru e-politik kepartaian yang berbasis jaringan teknologi komunikasi dan bersifat terintegrasi antar-elemennya dalam kondisi *real time* dan kekinian perkembangan setiap tempatnya.

Siber telah mendorong politik sebagai konsekuensi dari saling terkoneksi dan interdependesi dalam apa yang disebut sebagai *global village.* Meskipun diakui, bahwa akses dari komunitas dan orang yang berada di wilayah setiap negara saling berbeda satu sama lain, dihitung dari besaran persentasenya, tetapi sekitar 6 miliar penduduk bumi menggunakan teknologi komunikasi dan informasi (ICT) untuk kepentingan produksi dan konsumsi berbagai hal.[10] Kasus di beberapa negara Amerika Latin, menunjukkan bahwa ICT memiliki konsekuensi tidak sekedar mengenai pembiayaan dan prioritas yang harus ditetapkan, tetapi juga dapat dimanfaatkan bagi alat untuk mengerahkan secara terkoordinasi terhadap sumber daya yang dimiliki. Dari apa yang disebut sebagai "kerangka keraja cube" yang diadopsi pada beberapa kejadian di tingkat lokal, nasional, hingga ke tingkat antar -negara. Ini merupakan konsekuensi atas peran pembangunan ICT yang berusaha keras untuk bersifat menyeluruh, dan membangun konsep yang dapat diandalkan. Pada tahun 2003, PBB melalui *United Nations Regional Commision for Latin America and Carribean* (UN-ECLAC) mengusulkan tiga dimensi sebagai model peralihan menuju masyarakat sebagai pengguna dan sekaligus arena permainan di antara teknologi, kebijakan dan perubahan sosial. Ini merupakan akar teoritis Joseph Schumpeter mengenai inovasi teknologi.

---

[10] Namik K. Pak, "The Impact of ICT Revolution In Turkey: Tunneling Trough Barriers", *Journal of International Affairs* Vol VI Number 1, March-May 2001, h. 2.

Hal ini dilakukan pada setiap tingkatan siklus kebijakan dengan mengidentifikasi wilayah dan memprioritaskan bagi para pelaku dan pemangku kepentingan sebagai pihak yang mengeksekusinya di lapangan, melakukan koordinasi terhadap para pelaku dan pemangku kepentingan dimaksud, serta memonitor atau sekaligus mengawasi kemajuan masyarakat informasi. Dari hasil tabulasi silang secara horizontal Pembiayaan Public ICT di Cile di tahun 2003 dengan perhitungan persentasenya secara total, tabel berikut menggambarkan potensi atas koordinasi di antara pelaku dan pemangku kepentingan yang dapat dijalankan. Hal yang penting dicatat bahwa Cile adalah salah satu pioner dalam agenda *setting* nasional bagi pembangunan digital di negara-negara berkembang. Generasi pertama perencanaan pembangunan digital Cile 2003-2006 disebut *Digital Agenda Cile*, sedangkan perencanaannya di tahun 2007-2012 disebut *Digital Strategy.*[11]

**Tabel 3. Tabulasi Silang Pengeluaran Biaya ICT di Cile (antar simbol), Tahun 2003 (%)**

| Simbol | Regulasi | Insentif | Total |
|---|---|---|---|
| Infrastruktur (horizontal | 12% | 4% | 16% |
| *Generic Service* (horizontal) | 35% | 18% | 52% |
| *Capacities and Skill* (horizontal) | 16% | 5% | 20% |
| Administrasi Proyek (diagonal) | 11% | 0% | 12% |
| Total | 73% | 27% | 100% |

Sumber: Martin Hilbert (2012) h. 251

Pembiayaan dari ICT membutuhkan langkah desentralisasi dan melibatkan banyak pendekatan lintas sektor. Ini dalam rangka menciptakan dukungan bagi negara bersangkutan bagi pembangunan

[11] Martin Hilbert, "Toward a Conceptual Framework for ICT for Development: Lessons Learned from Latin American "Cube Framework", h.1, dalam *http:itdjournal.org.*,diakses 11 Mei 2018.

ICT secara luas dengan melibatkan pembagian beban penganggarannya di antara masing-masing kelembagaan. Langkah demikian membentang mulai dari soal mikro seperti halnya antara lain soal kurikulum sekolah, sistem layanan kesehatan, hingga persoalan makro sebagaimana halnya tentang keamanan negara, digitalisasi warisan budaya, dukungan legislasi, dan lain-lain. Inilah yang secara potensial dapat dibebankan pada penggunaan instrumen "kerangka kerja *cube*" dalam rangka langkah berikutnya dari pembangunan ICT. Langkah berikut dimaksud adalah terkait koordinasi antar-sumber daya yang tersedia dan pembagian beban dari setiap instansi pemerintah. Sampel contoh berikut menunjukkan pembagian beban pembiayaan ICT dan koordinasi yang potensi dapat dikembangkan antar-lembaga pemerintah.

**institusi pemerintahan) (persentase)**

| Kementrian Jumlah | Kementrian | Kementrian | Kementrian | Kementrian | Kementrian | |
|---|---|---|---|---|---|---|

perkembangan paham kapitalisme modern terkait posisi para korporat raksasa dan menengah dalam menjaga kepentingan sektoral dan sekaligus berbagi beban pembiayaan ICT di tengah tuntutan perubahan yang dihadapi pembangunan negara-negara bersangkutan.

Konteks masyarakat dalam kasus bocornya data media sosial di tengah kemajuan teknologi komunikasi tetap memiliki arti yang penting bagi kedaulatan negara. Ini harus dilihat pada tataran yang saling berinteraksi secara positif antara kedaulatan negara itu sendiri dengan partisipasi masyarakat. Walaupun secara teoritis, disebutkan: "...pada negara yang mendasarkan diri pada prinsip kedaulatan negara, juga terdapat patokan dasar yang ditaati dalam menyusun aturan-aturan hukum selanjutnya, sebagaimana posisi penting dari kebebasan menyatakan pendapat atau berpartisipasi dalam negara demokrasi. Hanya saja sumber kekuasaannya bagi kedaulatan negara adalah berasal dari negara. Sedangkan dalam negara demokrasi tadi adalah kemauan rakyat. Dalam prinsip kedaulatan negara, arah hubungan rakyat dan penguasa akan berlainan dengan negara yang menganut kedaulatan negara. Sehingga ini dimengerti kalau yang dibutuhkan adalah aturan yang menjamin kebebasan menyatakan pendapat oleh rakyat. Selanjutnya, yang justru dijaga adalah agar tidak ada isi aturan hukum yang berakibat merongrong atau mengurangi wibawa negara. Ini sering dinamakan dengan tidak merongrong atau mengurangi wibawa pemerintahnya, karena pemerintah (kepala negara, raja, atau *despot*) adalah lambang konkretisasi negara.[12]

Di Indonesia, informasi tentang bocornya data pribadi pengguna *facebook* muncul dari pengakuan mantan kepala riset *Cambridge Analytica*, Cristopher Wylie, Maret 2018, yang menyebutkan sejumlah peneliti di lembaganya mengumpulkan data pribadi 87 juta akun *Facebook* dengan menggunakan aplikasi survei kepribadian. Data ilegal tersebut telah dijual pada Cambridge Analytica yang kemudian dimanfaatkan bagi dasar penyusunan dan pembuatan iklan politik bagi

[12] Marsillam Simanjuntak, *Pandangan Negara Integralistik*, Jakarta, Grafiti, 1994, h. 2.

tim kampanye Donald Trump saat menjadi calon Presiden AS tahun 2016. Pihak Polri memeriksa petinggi perusahaan media sosial *Facebook* dalam kasus bocornya data pengguna di Indonesia. Direktorat Tindak Pidana Siber Badan Reserse Kriminal Polri sudah memulai penyelidikan atas perkara pencurian data lebih dari 1 juta akun facebook di Indonesia oleh firma *Cambridge Analytica* tadi. Menyikapi perkembangan demikian, DPR melalui Komisi 1 sudah membentuk Panitia Kerja (Panja) Perlindungan Data Pribadi. Namun panja ini beranjak dari persoalan dugaan penyalahgunaan data pribadi dalam proses registrasi nomor telepon seluler. Kasus bocornya data pengguna *Facebook* di Indonesia hanya menjadi pelengkap materi panja tersebut, saat bertemu dengan instansi, lembaga atau badan hukum.[13] Selama ini Indonesia menggunakan Undang-Undang Informasi dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi untuk upaya penegakkan hukum atas kejahatan *cyber.*

Pada kasus *Facebook*, salah satu pintu masuk pengambilan data pribadi penggunanya adalah melalui aplikasi *This is Your Digital Life* berbentuk kuis yang berisi sejumlah pertanyaan untuk menguji kepribadian seseorang. Peneliti Universitas Cambridge, Inggirs, Alexander Kogan, bersama perusahaannya, *Global Science Research*, memperkenalkan kuis itu di media sosial pada tahun 2013. Pada Desember 2015, berdasarkan laporan *The Guardian*, Alexander Kogan diduga membagikan data pribadi pengguna aplikasi *This is Your Digital Life* kepada *Cambridge Analytica Life.* Data itu digunakan untuk kepentingan kampanye bakal calon Presiden AS Partai Republik, Ted Cruz. Melihat hal itu, *Facebook* memerintahkan Kogan dan *Cambridge Analytica* menghapus seluruh data pengguna *Facebook.* Akan tetapi perintah itu tidak dilaksanakan, bahkan pada Maret 2018, salah satu pendiri *Cambridge Analytica*, Christopher Wylie, mengungkapkan data itu digunakan oleh kandidat Presiden AS dari

[13] "Polisi Periksa Petinggi Facebook Pekan Ini", *Koran Tempo*, 10 April 2018, h. 7.

Partai Republik, Donald Trump, untuk memasang iklan di Facebook saat kampanye pemilu presiden.[14] Meskipun secara statistik hanya digunakan 270.000 akun, berdasarkan data *Facebook*, Cambridge Analytica telah menghimpun 87 juta pengguna *Facebook*. Hal itu dimungkinkan karena *This is Your Digital Life* tidak hanya menghimpun data akun peng-*install* aplikasi tersebut, tetapi juga seluruh teman dari setiap akun itu. Skema ini dimungkinkan karena aplikasi tersebut menggunkan platform yang disediakan *Facebook* yaitu *open graph API (application programming interface)*. Sejak diluncurkan pada 2010, platform itu menghasilkan berbagai aplikasi kuis dan *game* yang populer, di antaranya *FarmVille* dan *TraVian*.

Menjelang pilkada serentak 2018 dan pemilu serentak pileg dan pilpres 2019, sejumlah partai politik di Indonesia semakin intensif menggunakan jasa konsultan untuk menganalisis data di media sosial guna menyusun strategi kampanye. Mereka memastikan data itu diperoleh dengan cara legal dan dapat dipertanggungjawabkan. Analisis politik melalui pembacaan perilaku pengguna media sosial menjadi fenomena yang sedang berkembang di dunia politik. Data yang didapat dari media sosial menjadi bahan untuk menyusun strategi kampanye yang efektif karena sasarannya akan lebih bersifat spesifik. Kondisi ini membuat sejumlah partai politik mulai menggunakan konsultan guna menganalisis data di media sosial. Direktur Eksekutif Charta Politika, Yunarto Wijaya, mengatakan, analisis politik dan perumusan strategi kampanye saat sekarang telah bergeser ke aspek mempelajari perilaku pemilih. Untuk masyarakat urban, metode yang paling tepat untuk mengetahui hal itu dengan mengamati perilaku pemilih di media sosial. Apalagi, ketika selisih jumlah pemilih yang riil dengan pengguna media sosial semakin mendekati 100 persen, maka perilaku pengguna yang tampak di media sosial dapat dibaca sebagai preferensi politik mereka yang sebenarnya.[15]

---

[14] "Ancaman Tersembunyi Zaman Siber", *Kompas*, 22 April 2018.

[15] "Data Medsos Jadi Sumber", *Kompas*, 18 April 2018, h. 2.

## C. Memudarnya Batas-Batas Teritorial Kedaulatan Negara

Tantangan kedaulatan negara manakala desentralisasi pemerintahan berkembang pesat di berbagai negara dan sentralisasi cenderung meredup atau kalau tidak dikatakan bangkrut perannya. Peran demikian dihadapkan pada kompleksitas tantangan dan aspirasi masyarakat yang berkembang dalam sistem politik negara bersangkutan. Kendali negara terhadap siber jelas berpengaruh di tengah gejala memudarnya sentralisasi pemerintahan. Desentralisasi pemerintahan di era reformasi menghadapi tantangan siber yang sukar dikendalikan dinamika dan implikasi tertentu di tengah masyarakat. Ini menjadi catatan, manakala terorisme dalam dunia maya merebak melalui peluang bagi pergerakan informasi yang disebarkannya. NIIS dengan segala aktivitasnya tidak perlu melakukan interaksi langsung dalam proses penyebaran gagasan, rekrutmen kader dan simpatisan hingga penyiapan operasi di lapangan targetnya.[16]

Muhammad AS Hikam menulis:

> *"In Indonesia, support for ISIS initailly began from the links which a young Indonesian activist, Tuah Febriansyah (also known as Muhammad Fachry), had with the al Muhajiroun, founded by Omar Bakri in 1983, is a branch of Hizb ut Tahrir (HT), an international organization campaigning for the return of the caliphate system and global enforcement of Islamic law. Al Muhajiroun believes that violence is permissible to further its cause, a view supported by all its followers. In addition, Al Muhajiroun brands fellow Muslims as dibilievers if they disagree with the imposition of Islamic law. Al Muhajiroun has built a presence in Indonesia through the internet since early 2005, when Muhammad Fachry found acess to the organization via the website www.paltak.com. From then on, he regularly engaged in online discussions with Omar Bakri.*[17]

Celakanya, gerakan politik siber dalam mendiseminasi gagasan dan langkah perekrutan sekaligus indoktrinasi ideologi yang dibawanya pada

---

[16] "Antisipasi Terorisme Dunia Maya", *Kompas*, 23 Februari 2018.

[17] Muhammad AS Hikam, *Deradicalization: Engendering Indonesian Civil Society Organizations in Curbing Radicalism*, Kompas Publisher, Jakarta, 2016, h. 9-10.

konteks radikalisasi, seringkali menggunakan label "Islam" yang justru bisa bias dalam pemahaman konteksnya. Peneliti Pusat Pengkajian Islam dan Masyarakat, Jakarta, Dirga Maulana, mengacu pada Penelitian Pusat Studi Budaya dan Perubahan Sosial (PSBPS) Universitas Muhammadiyah dan Pusat Pengkajian Islam dan Masyarakat (PPIM) UIN Jakarta, menguraikan bahwa situs organisasi Islam arus utama (*NU Online* dan *Suara Muhammadiyah*) sering memproduksi narasi-narasi yang menekankan pentingnya integrasi umat, pesan yang menyejukkan dan membawa pesan Islam yang rahmat bagi semua. Adapun organisasi Islam kontemporer (*Hidayatullah.com* dan *Suara Islam*) menarasikan persoalan kelompok dan cenderung diam pada fenomena radikalisme agama. Sedangkan situs organisasi Islam non-afiliasi (*Eramuslim.com* dan *VOA-Islam.com*, sering memproduksi narasi-narasi yang mendukung sikap dan tindakan intoleran, dan bahkan radikal). Penelitian ini juga menyebutkan bahwa situs-situs organisasi Islam non-afiliasi itu justru paling populer di kalangan warganet Indonesia. Data menunjukkan dari pengunjung selama Juli-September 2017 misalnya, total pengunjung *Eramuslim.com* sekitar 9,5 juta lebih, *Islam.id* 8,3 juta lebih, dan *VOA-Islam.com* 5 juta lebih. Bandingkan dengan pengunjung *NU Online* yang 6,5 juta lebih dan *Suara Muhammadiyah* sekitar 388 ribu lebih.[18]

Agus Sudibyo menulis mengenai ironi dari siber, khususnya media sosial terkait soal terorisme: "Facebook, Twitter, Youtube *hidup dari iklan-iklan yang menargetkan pengguna media sosial berdasarkan konten di halaman yang mereka kunjungi. Ketika kelompok teroris mengunggah video pada suatu halaman media sosial, perusahaan media sosial bukan hanya membiarkan video tersebut ditayangkan di platform mereka, tetapi juga menempatkan iklan-iklan yang mungkin bersimpati pada video tersebut atau disukai oleh pengunjung halaman tersebut. Meski mungkin tidak sengaja, proses komodifikasi video teror di sini semestinya melahirkan konsekuensi atau tanggung jawab. Seringkali*

[18] Dirga Maulana,"Dominasi Situs-situs Radikal", *Koran Tempo*, 15 Maret 2018.

*bukan pengiklan yang menentukan di mana iklan digital akan dipasang. Perusahaan media sosial yang memutuskan penempatan iklan itu pada suatu halaman yang menentukan penempatan iklan itu pada suatu halaman yang mengkombinasikan antara konten buatan pengguna dan iklan berdasarkan pada data tentang minat dan kebutuhan pengakses konten tersebut."*[19]

Selanjutnya ilustrasi dari situasi ironis dari kehadiran siber khususnya media sosial, lebih lanjut Agus Sudibyo menulis dan diakhiri dengan pertanyaan yang sangat menggugah nurani: "*Dalam konteks ini, banyak pengiklan besar dunia kelabakan karena produk-produk iklan mereka secara otomatis muncul di video-video yang diunggah NIIS. Ansheur-Busch, Procter & Gamble, Johnson & Johnson, dan beberapa produsen besar di AS menarik iklan mereka dan mengajukan protes keras kepada* Youtube. *Di Eropa, produsen mobil Audi,* Mc Donald's *UK, dan* L'Or'Eal *juga pernah menarik iklan digital mereka dari* Google *dengan alasan yang sama. Pernahkah kita membayangkan iklan bedak bayi* Johnson & Johnson *tiba-tiba nongol di video* Youtube *tentang pemenggalan kepala sandera oleh NIIS di Suriah?"*[20]

Kelenturan pencapaian sebaran informasi yang menjadi sasaran, dunia siber dipermudah dengan adanya media sosial. Dengan keleluasaan teks yang dimiliki, siber memiliki salah satu karakteristik yaitu tidak dibatasi oleh ukuran-ukuran seperti waktu dan ruang. Selagi ada akses terhadap internet, informasi yang diinginkan pengguna akan selalu tersedia. Kerja internet yang menghubungkan ribuan, bahkan jutaan komputer sebagai pangkalan data yang juga perangkat itu hidup selama 24 jam tanpa hasil memungkinkan pengguna untuk mengakses internet.[21]

---

[19] Agus Sudibyo, "Memanggungkan Terorisme di Media Sosial", *Kompas,* 21 Juni 2018, h. 6.

[20] Agus Sudibyo, *Ibid.*

[21] Rulli Nasrullah, *Media Sosial: Perspektif Komunikasi, Budaya dan Sosioteknologi,* Simbiosa Rekatamamedia, Bandung, 2016 ,h..64.

Siber telah melahirkan generasi milenial yang sangat tinggi tingkat adaptasinya terhadap berbagai informasi yang dihadirkan melalui dunia maya. Ini tidak saja terjadi bagi negara industri maju, tetapi juga sudah merambah hingga ke negara berkembang. Negara seolah menjadi desa di antara berbagai warga yang berlainan etnis dan latar belakang sosial ekonomi dengan saling lebur identitasnya, manakala warga *netizen* generasi milenial menjadi sasaran paling rentan bagi adanya kekaburan identitas negara bersangkutan. Itu sebabnya menjadi ironi di saat teknologi siber mempermudah aktivitas umat manusia, justru di saat bersamaan dinilai menjadi ancaman bagi kedaulatan negara.

Kepolisian RI memperketat pengawasan terhadap kelompok teroris, terutama dari kalangan perempuan. Kepala Divisi Humas Mabes Polri, Irjen (Pol) Setyo Wasisto mengatakan kepolisian telah memiliki data mengenai mereka yang tergabung dalam Negara Islam Irak dan Suriah (ISIS) di Indonesia. Kebanyakan dari jaringan *Jamaah Ansharud Daulah* (JAD). Peran perempuan dalam jaringan teroris di dalam negeri selama beberapa tahun terakhir cenderung meningkat. Sebelumnya, mereka lebih banyak berperan sebagai pendukung. Namun sejak tahun 2016, mereka mulai aktif terlibat langsung dalam aksi teror. Dari catatan yang ada menunjukkan bahwa keterlibatan perempuan dalam teroris semakin meningkat. Dari 172 terduga teroris yang ditangkap tahun 2017, 10 orang adalah perempuan. Mereka berkomunikasi melalui media sosial atau aplikasi pesan singkat, seperti hal *facebook, telegram, twitter, whatsApp*. Kelompok-kelompok paham radikal yang menggunakan jaringan komunikasi media sosial dimaksud, adalah *Baqiyah United Grup*, pembuatnya adalah (1) Aisyah Lina Kamelya yaitu saat September 2015. Keanggotannya meliputi kalangan internasional, termasuk dari Indonesia, India, Kenya, Filipina, Mesir, dan Libya; (2) Grup Pembela Tauhid, di mana pembuatnya adalah seorang perempuan berinisial NJ, jaringannya dibuat tahun 2014, dengan keanggotaan 850 orang; (3) *Channel Taaruf*: pembuatnya, seorang perempuan berinisial NJ, dengan keanggotaan 941 orang, merupakan kanal khusus

untuk sarana perjodohan antar-pendukung ISIS; (4) Info Manfaat, dibentuk pada tahun 2014, dengan Administrator: *Syuhada Uhud, Jihadis online*; Anggota: ratusan, termasuk puluhan buruh migran di Hongkong yang terpapar paham radikal; (5) *Mawar Berduri*, dibentuk tidak diketahui, administratornya tidak diketahui, dengan keanggotannya, setelah diblok kanal ini berubah nama menjadi *Penghias Hati*, kemudian berganti lagi menjadi *Mawar Berduri Anti Propaganda Thogut NKRI*; (6) *Jamaah Amaliyah Akhwat*, waktu dibentuknya tidak diketahui, administratornya tidak diketahui, jumlah anggota sekitar 30 orang dari Jakarta, Bekasi, Depok, Subang, Solo, Jambi dan Palembang. Dibubarkan setelah sempat berdiskusi untuk melakukan penyerangan dan setiap anggotanya harus bersumpah setia pada ajaran *Daulah Islamiah*. Kelompok-kelompok percakapan media sosial ini pada dasarnya isi percakapannya: seputar doktrin cara berpakaian; sarana perjodohan; ajang berjualan *online* sesama anggota; penggalangan dana untuk aksi terorisme dan berusaha menyebarkan video terorisme. Cara bergabung yang digunakan dalam kelompok-kelompok ini adalah menggunakan *link* yang memiliki masa berlaku terbatas.[22]

Pancasila sebagai ideologi negara adalah panduan bagi Bangsa Indonesia dalam menjaga identitas atau jati diri kewarganegaraan dan relasi antar-komunitas yang beragam di Tanah Air. Pancasila sebagai ideologi negara merupakan landasan folosofis kehidupan berbangsa dalam pelaksanaan agenda pembangunan di tengah interkoneksi antara pihak yang semakin erat dalam era globalisasi saat ini. Siber sebagai perangkat interkoneksi dalam kehidupan antar-manusia bukan lagi sekedar bermuatan teknik dalam kemajuan teknologi informasi, tetapi juga memiliki nilai-nilai yang sangat mendasar bagi sikap dan perilaku manusia itu sendiri sebagai pemangku kepentingan dari siber. Untuk penuangan regulasi siber penting dijaga konteksnya dalam ikatan nilai-nilai Pancasila yang sudah tentu merupakan satu kesatuan utuh dari

[22] "Polisi Waspadai Kelompok Teroris Perempuan", *Koran Tempo*, 31 Mei 2018, h. 1.

*Pembukaan* yang ada di dalamnya dan ke lima sila yang ada. Kelima sila sebagai nilai dasar bangsa Indonesia itu adalah: (1) Ketuhanan Yang Maha Esa; (2) Kemanusiaan yang adil dan beradab; (3) Persatuan Indonesia; (4) Kerakyatan yang dipimpin oleh hikmat kebijaksanaan dalam permusyawaratan/perwakilan; dan (5) Keadilan sosial bagi seluruh rakyat Indonesia.

Dalam kerangka Pancasila sebagai ideologi negara di tengah interkoneksi globalisasi yang semakin erat antar-berbagai pihak di atas, maka tujuan pengaturan terhadap siber bertujuan:

a. Mendukung persatuan dan kesatuan bangsa, sekaligus tetap memberikan perlindungan maksimal bagi kearifikan lokal yang beragam di wilayah Indonesia;
b. Meningkatkan kesejahteraan rakyat secara adil dan merata dengan membuka ruang yang luas dan secara bertanggung jawab bagi adanya partisipasi masyarakat;
c. Mendukung kehidupan ekonomi dan kegiatan pemerintah;
d. Meningkatkan hubungan antar-bangsa yang saling menguntungkan;
e. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
f. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
g. Meningkatkan efektivitas dan efisensi pelayanan publik;
h. Membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab, dan;
i. Memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara siber.

Tujuan pengaturan terhadap siber di atas, merupakan penegasan Pancasila yang merupakan dasar utama kesepakatan berdirinya bangsa

dan merupakan bagian dari Pembukaan UUD 1945. Bahkan, kedudukan Pancasila sebagai landasan ideologis dan sekaligus filosofis pengaturan siber menegaskan mengenai kaidahnya sebagai penuntun dari pengguna dan penyelenggara yang ada di dalamnya. Kedudukan Pancasila tersebut semakin memperkuat apa yang disebut sebagai sistem hukum yang bersifat khas bagi bangsa Indonesia yaitu Sistem Hukum Pancasila. Sistem Hukum Pancasila menciptakan rambu-rambu dan melahirkan kaidah penuntun dalam politik hukum yang dianut. Rambu yang paling umum adalah larangan bagi munculnya hukum yang bertentangan dengan nilai-nilai ketuhanan dan keagamaan yang berkeadaban, tidak diperkenankannya hukum yang bertentangan nilai-nilai kemanusiaan dan hak asasi manusia (HAM), merusak keutuhan ideologi dan teritori bangsa dan negara Indonesia, melanggar kedaulatan rakyat, serta larangan bagi adanya pelanggaran terhadap nilai-nilai keadilan sosial.[23]

Perkembangan teknologi komunikasi dan informasi siber dengan mengandalkan infrastruktur digital semaksimal mungkin harus diatur dalam kerangka mendatangkan kemaslahatan bangsa Indonesia. Potensi yang dimilikinya diletakkan dalam pengaturan Sistem Hukum Pancasila yang mencerminkan benang merahnya sebagai dasar negara. Ini merupakan konsekuensi dari apa yang disebut sebagai dasar filsafat negara (*philosophische grondslag)* dan ideologi negara (*staatside*).[24] Dalam hal ini, Pancasila dalam konteks pengaturan siber menjadi dasar menjalankan pemerintahan negara dan aktivitas di tingkat masyarakat

---

[23] Moh. Mahfud MD, *Konstitusi dan Hukum dalam Kontroversi Isu*, Rajawali Press, Jakarta, 2009, h. 37-38

[24] Filsafat/falsafah (*philosophy*) dan dasar negara atau *Weltanschauung* (pandangan hidup/ pandangan dunia) tidak selalu sebangun. Filsafat berkonotasi sebagai pemikiran saintifik dan rasional dengan klaim validitas universalnya. Adapun *Weltanschauung* berkonotasi sebagai pandangan yang lebih personal, eksistensial, dan historikal. Filsafat ada dalam lingkungan manusia, sedangkan *Weltanschauung* ada dalam lingkungan hidup. Filsafat sebagai filsafat tidak otomatis menjadi *weltanschauung*. Dengan berfilsafat orang berhasrat memerlukan memandang realitas sedalam-dalamnya. Untuk menjadi *Weltanschauung*, pemikiran filsafat itu harus dijadikan sikap dan pendiran orang/kelompok orang tentang dunia kehidupan. Pemikiran yang abstrak beralih menjadi pendirian hidup, yang kemudian pendirian itu diterima dan dijalankan. Sebaliknya, *Weltanschuung* tidak selalu didahului dan melahirkan filsafat.

pada umumnya dengan segala keberagaman yang melatarinya. Penjabaran lebih lanjut bahwa Pancasila sebagai dasar negara dituangkan dalam norma hukum yang harus berpuncak pada UUD 1945.

Tantangan dalam konteks pengaturan siber dengan panduan Pancasila sebagai dasar negara, adalah mengingat dalam pelaksanaannya bisa atau sangat dimungkinkan terjadinya interpretasi yang beragam. Bahkan bisa saja terdapat kontradiksi dari interpretasi nilai itu sendiri dari Pancasila sebagai landasan filosofis dan sekaligus dasar negara. Dalam lingkup mikro, nilai-nilai dalam Pancasila juga dianggap bisa mengandung kontradiksi, misalnya kemanusiaan yang menekankan kebebasan dengan persatuan yang menekankan kebersamaan. Pada tataran praktis muncul perbedaan dalam interaksi relasi-relasi sosial (ideologi) dalam menentukan interpretasi (pendekatan dan tujuan tindakan) untuk merumuskan implementasi nilai-nilai Pancasila dalam dunia kehidupan.[25] Dengan adanya kebutuhan untuk memahami secara mendalam atas Pancasila sebagai panduan bagi setiap tingkatan regulasi yang berpuncak pada UUD 1945 sebagai landasan konstitusi bernegara RI, maka interpretasi yang beragam atas nilai-nilai Pancasila melalui ke lima sila yang dikandungnya, menjadi tantangan tersediri. Tantangan demikian juga dipastikan akan dihadapi dalam perumusan norma-norma mengenai siber dengan segala kecepatan dinamika kemajuan teknologinya yang sangat tinggi agar benar-benar sejalan dengan tujuan pengaturan siber itu sendiri bagi bangsa Indonesia. Di samping itu, perumusan norma-norma Siber dalam regulasi di tingkat kebijakan dan aturan operasional dituntut untuk menjaga identitas atau jati diri dari bangsa Indonesia dengan segala kearifan lokal yang dimilikinya.

---

Di dalam berbagai kearifan lokal atau tradisional berbagai suku di Indonesia, terkandung adanya *Weltanschauung*, tetapi pada umumnya tanpa rumusan filsafat. Selain itu, ada pula Weltanschauung yang melahirkan rumusan filsafat, dan filsafah berbuah *Weltanschauung*. Lihat: Yudi Latif, *Revolusi Pancasila*, Mizan, Jakarta, 2017, h. 34

[25] Mhd. Halkis, *Konstelasi Politik Indonesia: Pancasila dalam Analisis Fenomenologi Hermeneutika*, Yayasan Pustaka Obor, Jakarta, 2017, h.9.

## D. Masih Politik Partisan Jangka Pendek

Politik siber memiliki kitan erat dengan masalah kedaulatan negara yang berawal dari kesadaran bangsa. Bahkan, menurut Benedict G. Anderson, bangsa merupakan "sebuah komunitas politis dan dibayangkan terbatas secara inheren dan memiliki kedaulatan". Bangsa disebutnya sebagai komunitas terbayang *(imagine communities)* yang memang mustahil bagi individunya untuk saling mengenal dan berinteraksi secara fisik atau langsung. Kesadaran berbangsa demikian disebutnya sebagai akibat perkembangan percetakan massal media yang memungkinkan peran bahasa bukan lagi mempersatukan antar-berbagai kelompok dalam konteks administrasi, tetapi juga perannya secara politik.[26] Konteks komunitas berbayang sebagai bangsa yang menjadi landasan kedaulatan negara demikian, artinya memang tidak lepas dari kemajuan teknologi informasi. Ruang bagi berperannya dukungan kemajuan teknologi informasi dalam kondisi saat ini ditrasformasikan bukan lagi secara cetakan fisik, tetapi sudah lebih canggih dengan instrumen digital.

Pendekatan lembaga pemerintah terhadap keamanan siber selama ini berfokus pada ancaman nasional dan perlindungan infrastruktur nasional kritis. Terdapat dua kementerian di era pemerintahan Jokowi-Jusuf Kalla hasil Pemilu 2014, yang bertanggung jawab mengelola keamanan siber, yaitu Kementerian Politik, Hukum dan Keamanan, dan Kementerian Komunikasi dan Informatika. Selain kedua kementerian tersebut, TNI, BIN dan Kementerian Luar Negeri, dan ketika itu juga melalui Lembaga Sandi Negara yang turut berkontribusi membahas persoalan di sekitar keamanan siber. Kementerian Komunikasi dan Informatika (Kemenkominfo) saat menghadapi tuntutan bagi strategi keamanan internet pada tahun 2007, pernah membentuk ID-SIRTII. ID-SIRTII adalah melaksanakan pemantauan (*monitoring*), memelihara sistem deteksi dan peringatan dini terhadap

[26] Benedict G. Anderson, Imagine Communities*: Komunitas-Komunitas Berbayang*, Insist, Yogyakarta, 2014.

ancaman di jaringan telekomunikasi, serta menangani tindakan hukum dalam sengketa *cybersecurity*. ID-SIRTII juga bertanggung jawab untuk menciptakan lingkungan yang aman untuk komunikasi berbasis internet di Indonesia, serta berfungsi sebagai pusat koordinasi isu-isu terkait *cybersecurity*. Pada tahun 2010, Kementerian Kominfo membentuk Direktorat Keamanan Informasi untuk membantu merumuskan dan melaksanakan kebijakan terkait keamanan siber, beserta norma, standar, prosedur dan kriteria di ranah keamanan informasi. Direktorat Keamanan Informasi diintegrasikan ke dalam struktur Kominfo, sementara ID-SIRTII bertindak sebagai lembaga negara independen.[27]

Kementerian Koordinator Politik, Hukum dan Keamanan juga memiliki divisi keamanan sibernya yang tersendiri, yang bertujuan menangani dan mengelola keamanan siber nasional. Jika Kominfo menjadi lembaga utama (*leading sector*) dalam keamanan siber sipil, maka Kemenko Polhukam bertanggung jawab atas ancaman terkait keamanan nasional. Divisi siber lembaga ini juga pernah menginisiasi sebuah Forum *Cybersecurity*, yaitu sebuah kelompok informal untuk mendiskusikan isu-isu yang terkait dengan serangan siber dan tata kelola siber. Kelompok informal ini terdiri dari para aktor yang menangani kasus kejahatan siber, yang meliputi perwakilan unsur pebisnis, kepolisian, hingga pihak masyarakat sipil.[28]

Melalui Perpres No. 133 Tahun 2017 yang merupakan perubahan tehadap Perpres No. 53 Tahun 2017, pemerintahan Joko Widodo-Jusuf Kalla (Jokowi-JK) tampaknya mencoba memformulasikan ulang tatanan Badan Siber dan Sandi Negara atau disingkat BSSN. Meskipun rentang penguatan coba dilakukan dalam tatanan kelembagaannya, tetapi kurun waktu menjelang Pilkada serentak 2018 dan Pemilu serentak 2019 sangat kuat pertimbangan politiknya. Dengan dilantiknya

---

[27] Donny B.U, et.al (editor), *Kebijakan* Cybersecurity *dalam Perspektif Multistakeholder*, seri literasi digital, ICT watch dan Kominfo, Jakarta, 2018, h. 12.

[28] *Ibid.*, h. 13.

Mayjen Djoko Setiadi sebagai Kepala Badan Siber dan Sandi Negara, yang sebelumnya adalah Kepala Lembaga Sandi Negara (Lemsaneg) melalui Keppres No. 130/P Tahun 2017, maka resmilah operasional tatanan BSSN yang baru saja diformulasikan ulang tadi.

Meskipun ada beberapa hal internal keorganisasian yang masih dilanjutkan kerja-kerja manajerialnya, tetapi secara politis BSSN yang berlandaskan Perpres No. 113 Tahun 2017 adalah merupakan bagian absah dalam sayap pemerintahan Jokowi-JK. Ruang keabsahan ini diperluas karena BSSN adalah lembaga pemerintah yang berada di bawah dan bertanggung jawab kepada Presiden. Presiden memiliki mata dan telinga secara langsung terhadap akses siber dan sandi negara melalui BSSN, yang berbeda saat masih di bawah Perpres No. 53 Tahun 2017, karena semula BSSN berada di bawah dan bertanggung jawab kepada Presiden melalui Menko Polhukam.

Konsekuesi atas politik siber yang secara kelembagaan masih partisan dan jangka pendek, adalah menyebabkan kerentanan Indonesia terhadap serangan siber menjadi hal yang tetap mengkhawatirkan. Ini tidak akan menjawab kebebasan publik digital yang dapat menggerus kapasitas demokrasi suatu negara dalam mengantisipasi dan merespons tantangan yang muncul. Padahal, demokrasi digital menggabungkan antara konsep perwakilan dan partisipatif dengan penekanan pada perangkat teknologi digital. Ini merupakan model revolusi terhadap politik sebagai karakteristik demokrasi digital. Bahkan, kecepatan perubahan dari politik demikian tidak saja pada konteks ruang dan waktu, tetapi juga pada konteksnya di lintasan komunikasi global.[29]

[29] Fayakhun Andriadi, *Partispasi Politik Virtual: Demokrasi Netizen di Indoensia*, RIMBooks, Jakarta, 2017, h.11.

## Tabel 1: Kondisi Saat Ini: Koordinasi dan Kewenangan Kelembagaan Siber

| No. | KEWENANGAN | KOORDINASI | | | |
|---|---|---|---|---|---|
| | | US | LEGAL | IND | LEGAL |
| 1. | Cyber Military Intelligent | CIA | Cyber Inteligent Agency Act | BAIS | UU Intelijen, UU TNI<br>UU Pertahanan Negara |
| 2. | Cyber Non-Military Intelligent | NSA | Natl. Security Act | BIN | UU Intelijen, Perpres BIN, Inpres Penanganan Gangguan DN |
| | | FBI | | POLRI | UU Polri, UU ITE |
| 3. | Cyber Crime | DEPT. Of JUSTICE | Computer Fraud & Abuse Act | KEJAKSAAN | UU Kejaksaan, UU ITE |
| 4. | Information Secure | US-CERT | Federal Information Security Management Act | LEMSANEG | Keppres 103/2001, Perka 122/2007 |
| | | GENERAL SVC Adm | Freedom of Information Act | | |
| 5. | Public Cyber Security | DHS | Homeland Security Act | ? | ? |
| 6. | Cyber Defense | DOD | National Defence Authorization Act | KEMHAN | UU TNI,<br>UU Pertahanan Negara |
| | | USCYBERCOM | | ? | ? |
| 7. | Cyber Regulation & Standard | NIST | Federal Information Security Management Act | KOMINFO | UU Pos, UU KIP, UU ITE, UU Penyiaran, UU Pers, UU Telekomunikasi |
| | | | | KEMENLU | UU Hub. LN |
| 8. | Cyber Diplomacy | DEPT. Of STATE | - | POLHUKAM cq. DK2ICN | SK Menko Polhukam 24/2014 jo. 5/2015 |

Sumber: Sekolah Tinggi Sandi Negara, "Diskusi Strategi Keamanan Siber Nasional", Badan Keahlian DPR RI, Jakarta, 23 Februari 2018, h.8

Hal yang mengkhawatirkan adalah serangan siber pada khususnya dan kejahatan dunia maya pada umumnya, bagi Indonesia belum ditangani secara terintegrasi di antara kelembagaan yang ada. Kerawanan demikian tercermin dalam dokumen *Global Cyber Security Index 2017* yang diterbitkan oleh ITU D, Indonesia memperoleh nilai 0,424 dan berada diposisi nomor 69 dari 164 negara. Ini diberikan status *Maturing* (sedang menuju kesiapan), dibandingkan misalnya terhadap Singapura yang memimpin di nomor 1 dengan nilai 0,925 dan Malaysia di nomor 3 dengan nilai 0,893.[30] Peretasan menjadi

[30] Komponen-komponen yang masih mendapatkan penilaian merah adalah *Computer Emergency Response Team (CERT)* sektor, standar organsiasi, strategi keamanan siber, *good practice*, program edukasi, institusi dalam negeri, perjanjian bilateral, perjanjian multilateral, dan kerjasama pemerintah-swasta. Lihat, Satriyo Wibowo, "BSSN dan Peta Keamanan Siber Indonesia", dalam *detiknet../*dikutip 10 Maret 2018.

ancaman terhadap keamanan siber di Indonesia. Peretas mampu membobol secara otodidak berbagai sistem dan situs. Kemampuan meretas dipelajari dari berbagai komunitas peretas yang mempunyai kelompok diskusi di dunia maya. Kasus anggota *Surabaya Black Hat* (SBH) yang ditangkap polisi Maret 2018 karena meretas 3000 sistem elektronik dan situs di 44 negara, misalnya, antara lain ada yang dimaksudkan sekedar menunjukkan kelemahan pada sistem. Pihak dimaksud mengaku tidak pernah meminta uang dalam jumlah tertentu, tetapi ada pemilik sistem yang membayarnya.[31] Kemajuan teknologi seringkali tidak diimbangi dengan regulasi yang memadai dan kelemahan sistem, membuat peretasan bisa menimbulkan efek sangat besar bagi negara. Ini tidak saja secara sosial dan kerugian ekonomi yang dialami, tetapi juga bagi ancaman kedaulatan negara, bagi musuh dari infiltrasi dalam negeri dan kekuatan yang berasal dari luar negeri.

Dari segi regulasi, kelemahan dunia siber di Indonesia tidak terlepas dari kurangnya pengaturan mengenai siber sehingga menimbulkan kerancuan di tengah masyarakat. Dunia siber tidak mengenai batas kedaulatan negara, baik secara kepemilikan wilayah maupun hingga tingkatan individu mengakibatkan timbulnya konflik di tengah masyarakat itu sendiri. Keberadaan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) tidak dapat menjangkau sedemikian jauh pengaruh dari dunia siber yang disebut sebagai *cyber law*. Walaupun UU ITE tersebut telah dibantu dengan keberadaan UU No. 39 Tahun 1999 tentang Telekomunikasi, tetapi tetap banyak hal yang tidak terpecahkan masalah dari *cyber law*.[32] Terdapat gagasan kejelasan pidana siber dan pengelolaan keamanan siber terkait melewati batas kedaulatan negara, menjadi penting. Bahkan ini secara politis bisa memberikan kepastian bagi negara guna mengelola siber dan penerapan pidana siber dalam konteks kepastian hukum.

---

[31] "Peretas di 44 Negara Belajar Otodidak", *Kompas*, 16 Maret 2018.

[32] Nudirman Munir, dalam *Op.cit.*, h. 27.

Kerentanan Indonesia terhadap serangan keamanan siber justru berbanding terbalik dengan kondisi melipahnya isu berita bohong atau menyesatkan yang masuk melalui media sosial. Dengan luasnya limpahan berita-berita demikian dan segala dampak yang harus ditanggung, maka diperlukan upaya penanganannya yang dianggap memadai di tengah segala keterbatasan yang ada. Ini menjadi pemikiran awal dan jangka pendek, manakala instrumen koersif lebih dikedepankan dalam menangani kasus-kasus yang bermuatan berita bohong dan ujaran kebencian melalui langkah hukum penangkapan pelaku oleh pihak kepolisian. Tetapi pada kurun waktu jangka panjang, pendekatan yang lebih mengedepankan penyadaran literasi dan bahkan adanya majelis yang melibatkan berbagai kalangan tehadap rumusan berita bohong dan mekanisme pengajuan banding, tetap harus menjadi upaya kongkret untuk segera dan secara serius diwujudkan.[33]

Kerentanan demikian menjadi sangat serius, karena ranah politik juga diwarnai oleh spektrum informasi melalui siber yang saling bersaing antar-tokoh pada saat momentum strategis bagi negara. Ini ditandai oleh momentum pemilu dan pilkada, di mana partai atau gabungan partai, apalagi para calon atau tokoh yang bersaing saling memanfaatkan siber untuk komunikasi politik dan kampanyenya. Media sosial sebagaimana halnya *Facebook* dan *Twitter*, misalnya, tidak terlepas dari para komunitas atau tim yang bekerja di belakang layar, guna mengapampanyekan pada tokoh atau calon yang didukungnya. Ini misalnya, dilakukan oleh Gatot Nurmantyo, mantan Panglima TNI, ketika pada saat pensiun dari dinas militer, dirinya justru sudah memiliki tim yang mengelola akun *twitter*, *facebook*, dan *instagram*, sebagai konskuensi dari tiga media sosial yang dianggap paling banyak penggunanya. Ini artinya, siber memiliki arti strategis bagi politik partisan pemenangan pemilu di antara para tokoh yang bersaing. Dalam konteks ini, menjadi sangat penting bagi kendali politik siber yang

[33]Lihat misalnya "RI Darurat Hoaks", *Kompas*, 14 Maret 2018.

jangan sampai terjebak pada manuver politik partisaan demi kepentingan elit atau kelompok terbatas. Sebaliknya, politik siber harus benar-benar dimanfaatkan pada kepentingan nasional, sebagaimana halnya menjaga soliditas kedaulatan negara.

## E. Penyesuaian Kondisi Lapangan

Pengguna gawai di Indonesia cenderung semakin meningkat dan hingga bulan Maret 2018 mencapai tidak kurang dari 351,6 juta kartu prabayar yang melakukan registrasi ulang. Ini berarti jumlah tersebut telah melebihi jumlah penduduk Indonesia. Padahal, data itu belum termasuk jumlah pengguna kartu pascabayar yang tidak mendaftar ulang karena data pengguna otomatis sudah ada di operator saat mereka mendaftar. Kondisi tersebut dimanfaatkan para kontenstan pilkada untuk membentuk opini sebagai strategi pemasaran politik melalui media sosial yang mudah diakses melalui telepon pintar (*smart phones*). Laporan indeks kerawanan pilkada 2018 yang disusun oleh Badan Pengawas Pemilihan Umum (Bawaslu) menyebutkan 12 dari 17 provinsi yang akan menyelenggarakan pilkada serentak tahun 2018, termasuk dalam kategori tingkat kerawanan tinggi terkait penggunaan media sosial oleh masyarakat. Provinsi dimaksud adalah: Sumatera Utara, Riau, Sumatera Selatan, Kalbar, Kaltim, Jawa Barat, Jawa Timur, Bali, Nusa Tenggara Barat, Sulawesi Tenggara, Maluku dan Maluku Utara. Penilaian Bawaslu itu didasarkan pada aspek penggunaan media sosial yang mencakup dua indikator, yaitu materi kampanye dan relasi kekerabatan politik para kontestan yang diwacanakan di media sosial.[34]

Berkembangnya media sosial memang mengubah cara manusia berkomunikasi, dari komunikasi lisan secara langsung menjadi komunikasi melalui berbagai aplikasi percakapan dan media sosial. Perubahan itu memang menjadi mudah, tetapi juga dianggap

[34] "Mewaspadai Kegaduhan di Dunia Maya", *Kompas*, 16 April 2018.

melahirkan banyak masalah baru. Dalam komunikasi lisan melalui tatap muka langsung, otak kiri dan kanan manusia akan bekerja bersama. Otak kiri merupakan tempat memproses bahasa verbal, baik lisan maupun tulisan. Sementara otak kanan tempat memproses bahasa non-verbal, seperti halnya intonasi suara, tatapan mata, mimik muka, hingga gerak tubuh. Dalam komunikasi digital, hanya otak kiri manusia yang aktif. Namun, komunikasi langsung lebih mudah menimbulkan kelelahan, karena dua sisi otak manusia membutuhkan banyak energi untuk bekerja. Masalahnya, kecenderungan otak bekerja adalah dengan menghindari hal-hal yang melelahkan dan memerlukan banyak energi. Akibatnya, manusia lebih menggemari komunikasi melalui tulisan dibandingkan bertemu secara langsung. Wajar jika akhirnya banyak orang sangat aktif di media sosial, tetapi justru bungkam di saat bertemu langsung.[35]

Penggunaan satu sisi otak dalam komunikasi digital juga membuat berbohong lebih mudah dilakukan dalam komunikasi di dunia maya dibandingkan jika komunikasi secara langsung. Dalam pesan tulisan, orang memang akan lebih sulit menilai bahasa nonverbal yang disampaikan seseorang bersamaan dengan bahasa verbal yang disampaikan. Kondisi itu juga membuat kebohongan lebih mudah disebarkan dalam komunikasi digital. Di samping itu, karakter media sosial yang memungkinkan penyebaran informasi secara cepat dan masif, juga akan membuat kebohongan dan berita bohong lebih mudah menyebar. Masalahnya, adalah meskipun berita bohong itu sudah diklarifikasi dengan berita yang benar, informasi yang benar tetap sulit menyebar. Kondisi ini diperparah dengan kecenderungan manusia menilai sebuah informasi yang sering dipengaruhi efek kebenaran ilusi (*illusory truth effect).* Dalam efek itu, suatu informasi akan dipercaya kebenarannya jika sesuai logikanya atau pernah mendengar informasi sebelumnya. Keadaan itu membuat sebuah berita bohong akan lebih mudah dipercayai

[35] "Media Sosial Mengubah Otak dan Jiwa", *Kompas*, 3 Juni 2018.

dibanding informasi yang benar. Selain itu, berita bohong yang diulang terus menerus lama lama akan dianggap sebagai kebenaran.[36]

Pentingnya penyadaran literasi berbanding lurus dengan ancaman terhadap kedaulatan negara yang bersifat ideologis. Panglima TNI, Marsekal Hadi Tjahjanto mengatakan, era revolusi industri 4.0 saat ini ditandai dengan lahirnya inovasi, distruptif, terutama di bidang teknologi, yaitu informasi digital dan transportasi, telah mengubah tatanan lama menjadi hal yang baru dengan segala dampaknya yang sukar diprediksi. Dalam konteks tertentu, dampak tersebut dapat bertransfomasi menjadi ancaman baru bagi kedaulatan negara. Contohnya, kemajuan teknologi informasi digital membuka peluang lahirnya berbagai industri kreatif. Tetapi ini juga dapat disalahgunakan sebagai sarana indoktrinasi terhadap individu-individu hingga siap melakukan teror demi agenda kelompok tertentu. Disebutkan pula, ancaman nyata terhadap keutuhan bangsa adalah kemunculan fenomena hiperrealitas, yaitu fakta yang bersilang sengkarut dengan rekayasa. Prinsip-prinsip kebenaran, kepalsuan, keaslian, isu dan realitas membaur menjadi satu. Akibatnya, sebagian masyarakat akan kebingungan untuk mencerna mana yang benar dan mana yang palsu.[37]

Kebocoran data pemerintahan di Indonesia sebagai tindakan pembajakan sudah terjadi berulang kali. Terakhir adalah peristiwa data kependudukan yang bocor setelah diberlakukan kebijakan registrasi bagi pemilik *handphone* dengan masing-masing providernya. Harian *The Jakarta Post* edisi tgl 15 Maret 2018 menulis: "*In its annual report, the Indonesian Security Incident Response Team on Intrenet Infrastructure (ID SIRTII/CC) found more than 79.000 cases of data spills sourced from dozens of government websites with the go.id domain in 2017. The breaches were caused by malware, hacking or misconfiguration.*".[38] Jumlah yang signifikan data pemerintah yang

---

[36] *Ibid.*, h. 5.

[37] "Pengamanan Pancasila Jadi Syarat", *Kompas*, 21 Maret, 2018.

[38] "*Government Websites Prone to Data Theft*", *The Jakarta Post*, 15 Maret 2018.

mengalami kebocoran ini jelas menjadi rawan bagi negara terkait kejahatan terhadap negara dan bahkan menjadi ancaman bagi kedaulatan negara. Pada konteks pendaftaran nomor pengguna telepon *mobile* misalnya, data kependudukan terkait NIK dan KK jelas adanya kebocoran data tersebut bisa menjadi ancaman tidak saja bagi potensinya munculnya aksi kriminal di tingkat individu dan/atau kelompok, tetapi juga serangan terhadap kepentingan negara. Pengalaman kebocoran data semacam ini, menimbulkam pentingnya perlindungan siber bagi data pemerintahan dan kemasyarakatan. Ini di antaranya adalah pentingnya program *e-system* sebagai langkah meningkatkan keamanan data. Program *e-ID* sudah diluncurkan pada tahun 2009 untuk mengatasi pencurian data, penghindaran pajak, manipulasi pengadaan barang/jasa, dan kebocoran sebagai akibat pembajakan jaringan.

Dalam UU No. 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana diubah menjadi UU No. 24 Tahun 2013 terdapat ketentuan bahwa negara berkewajiban untuk menyimpan dan melindungi data penduduk. Bahkan di Pasal 85 Undang-Undang tersebut terdapat ketentuan yang secara spesifik mengatur mengenai data pribadi:

(1) Data pribadi penduduk yang wajib disimpan dan dilindungi oleh negara;
(2) Ketentuan lebih lanjut mengenai penyimpanan dan perlindungan terhadap Data Pribadi Penduduk itu diatur lebih lanjut melalui Peraturan Pemerintah;
(3) Data pribadi penduduk harus dijaga dan dilindungi kerahasiaannya oleh Penyelenggara dan Instansi Pelaksana sesuai dengan ketentuan peraturan perundang-undangan.

Pelanggaran atas perlindungan data pribadi penduduk dan tindakan penyebarluasan atau manipulasi data pribadi penduduk memiliki konsekuensi pidananya dalam UU Adminduk, sebagaimana disebutkan dalam Pasal 94 dan Pasal 95 A. Masalahnya, hingga kini pemerintah belum memiliki payung hukum terkait perlindungan data

pribadi, padahal pelanggaran kejahatan siber yang melanggar manipulasi atau perlidungan data pribadi cukup berkembang luas di masyarakat. Sejak Maret-April 2018, Kepolisian Daerah Metro Jaya menelusuri asal-usul ribuan data yang diperjualbelikan di situs *Temanmarketing.com* dan muncul dugaan bahwa jaringan pembocor data nasabah melibatkan "orang dalam" bank. Penjualan data nasabah bukan hanya terjadi di tahun 2018, sebelumnya yaitu di tahun 2017, Badan Reserse Kriminal Mabes Polri juga pernah mengungkap kasus serupa. Sejumlah situs yang terlacak menjual data rahasia nasabah saat itu telah diblokir. Ahli digital forensik, Ruby Alamsyah mengatakan, kasus jual beli data nasabah yang dapat berulang kejadiannya biasanya berawal dari proses tukar menukar data antar-tim pemasaran bank. Pertukaran data jamak terjadi ketika data nasabah di suatu bank telah habis dihubungi, sementara target untuk mendapat nasabah baru belum tercapai. Saling tukar data antar-petugas bank yang saling berbeda, secara perlahan tumbuh menjadi luas dan berkembang menjadi pola.[39]

Koordinator Forum Keamanan Siber dan Informasi, Gidas Lumy mengingatkan, pemerintah dan DPR harus lebih serius melindungi data pribadi warga di ruang maya. Kegagalan dalam melindungi data dapat berdampak luar biasa seperti halnya terkait usaha mengarahkan preferesi pemilih di pemilu dan mengancam persatuan nasional. Ketidakmampuan dalam melindungi data privat warga di ruang maya berpotensi menimbulkan dampak luar biasa, sehingga negara harus lebih hadir untuk menjaga kedaulatan negara di ruang digital. Langkah negara ini adalah melalui regulasi atau kemauan politik yang kuat untuk menegakkan hukum (*law enforcement*). Terungkapnya kasus *Cambridge Analytica*, konsultan politik yang diduga "menambang" data pribadi sekitar 50 juta pengguna *Facebook* untuk memenangkan Donald Trump pada pemilihan Presiden AS tahun 2016, hanya puncak gunung es persoalan perlindungan data privasi pengguna internet.

---

[39] "Polisi Usut Jaringan Penjual Data Nasabah", *Koran Tempo*, 19 April 2018, h. 6.

Kondisi serupa, bahkan bisa lebih parah menimpa Indonesia yang tingkat perlindungan data pribadi lebih rendah dari negara-negara maju. Terkait media sosial, adalah penting bagi setiap penggunanya untuk "melek" perlindungan data pribadi. Selama ini masyarakat masih kurang literasi atau bahkan abai terhadap keamanan data pribadinya. Media sosial bisa berubah menjadi "binatang buas" yang menerkam siapa saja yang ada di dalamnya. Masyarakat perlu selalu memahami konsekuensi atas apa yang diunggahnya melalui media sosial dan bagi pemerintah ini memerlukan kerja keras dan cepat bergerak mengatur siber agar tidak lepas kendali yang menghancurkan kedaulatan negara.

Indonesia dengan kekayaan informasi sedemikian besar sangat memerlukan tindakan-tindakan yang bersifat preventif maupun defensif terhadap ancaman siber. Di samping hal ini untuk melindungi negara, juga untuk melindungi kepentingan warga negaranya atau organisasi di bawah negara. Tindakan-tindakan ini tidak cukup hanya berupa kebijakan atau peraturan perundang-undangan, tetapi juga perlu disikapi melalui tindakan dalam bentuk kegiatan secara semesta yang melibatkan seluruh potensi dan komponen bangsa. Pada hakikatnya, "Pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah NKRI dan keselamatan bangsa dari segala bentuk ancaman. Ancaman terhadap sebagian wilayah merupakan ancaman terhadap seluruh wilayah NKRI dan menjadi tanggung jawab seluruh rakyat Indonesia." Penyelenggaraan sistem pertahanan semesta melibatkan seluruh warga negara, wilayah dan sumber daya nasional lainnya serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah dan berlanjut untuk menegakkan kedaulatan negara, keutuhan wilayah dan keselamatan segenap bangsa dari segala bentuk ancaman.[40]

Kondisi kewilayahan di Indonesia menunjukkan keragaman yang tidak dapat diterapkan pola pendekatan kebijakan siber yang

[40]Djoko Setiadi, "Membangun Kerangka *Cyber* Indonesia", dalam *Jurnal Negarawan*, Kementerian Sekretariat Negara RI, No. 31, Tahun 2014. Seh. 10-11

menyeragamkan antar-segmennya. Ini bisa dilihat pada kondisi kewilayahannya pada segmen budaya komunitas, geografis, kelembagaan yang terlibat, dan dukungan jaringan infrastruktur. Pola pendekatan demikian mengungkapkan pentingnya kemajuan teknologi informasi dan dimensi global juga dibarengi oleh penempatan dimensi kearifan lokalnya secara tepat. Muatan kearifan lokal dalam muatan kebijakan siber menjadi bersifat mendasar, karena keterbatasan sumber daya fisik dan literasi mudah ditemui di tengah komitmen pemerintah bagi realisasi jaringan infrastruktur pembangunan daerah secara terintegrasi dalam konteks nasional.[41] Hal ini disadari juga pada saat penanganan segala dampak siber, seperti halnya penggunaan media sosial, mengalami eskalasi tidak saja menghadapi momentum politik tertentu, seperti halnya pilkada maupun pemilu, tetapi juga dalam relasi sosial sehari-hari.

Di Provinsi Maluku misalnya, Dinas Kominfo Pemprov setempat mengakui bahwa daerahnya kemajuan teknologi dan pengelolaan siber belum terkelola dengan baik. Mereka menilai bahwa hal ini sebagai akibat dari belum adanya Undang-undang atau peraturan pemerintah khususnya mengatur soal siber yang merupakan payung hukum acuan bagi pelaksanaan lebih lanjut kebijakan pemerintah daerah. Ini disadari meskipun kewenangan persandian sebagai Urusan Wajib yang berkategori non-pelayanan dasar sudah diakomodasi di UU No. 23 Tahun 2014 tentang Pemda. Padahal, payung hukum Undang-Undang dan perangkat aturan di bawah UU terkait Siber sangat diperlukan bagi provinsi Maluku yang memiliki total luas wilayah dengan kawasan lautannya mencapai 93,29 persen dan luas daratan hanya sebesar 6,71 persen. Secara administrasi pemerintahan, provinsi ini memiliki 2 kota dan 9 kabupaten.[42] Dengan rentang wilayah yang luas secara geografis

---

[41] Diungkapkan dalam kunjungan Tim Penyusunan NA dan RUU Siber saat dialog dengan Reskrimsus Pola Maluku, KPU Maluku, Prodi Ilmu Hukum Universitas Patimura, dan Dinas Kominfo Pemprov Maluku, Ambon, 26-28 Maret 2018.

[42] Dinas Kominfo Pemprov Maluku, "Masukan Tertulis bagi Badan Keahlian DPR RI tentang Penyusunan Naskah Akademik Draft RUU Siber", Ambon, Maluku, Maret 2018.

kepulauan dan sebarannya yang berbatasan dengan negara-negara tetangga, seperti halnya Timor Leste, Australia, dan Papua New Guinea (PNG, hingga tahun 2018 masih ditemui beberapa titik *blank spot* dan memerlukan pembangunan menara jaringan BTS. Dukungan pemerintah pusat untuk bergerak secara nasional dan merealisasikan pembangunan jaringan telekomunikasi dan menara BTS jelas menjadi urgen dan memiliki arti strategis bagi upaya menjaga keutuhan kedaulatan negara RI.

Di tengah keterbatasan infrastruktur siber menjad hal yang *crusial*, awal Mei 2018 muncul gugatan arbitrase internasional, yaitu di *London International Court of Arbitration*, dari perusahaan satelit dari Inggris, *Avanti Communications Group*. Gugatan tersebut merupakan akibat dari penilaian terhadap pemerintah Indonesia yang dianggap gagal memenuhi pembayaran kontrak perjanjian sewa satelit milik Avanti yang bernama Artemis atau *Advance Relay and Technology Mission*. Pemerintah Indonesia, dalam hal ini Kementerian Pertahanan, saat itu baru membayar US $ 13,2 juta dari total kontrak US $ 30 juta, atau masih menyisakan pembayaran US $16,8 juta. Gugatan ini sudah dimasukkan melalui Pengadilan Internasional London sejak Agustus 2017. Menhan Ryamizard Ryacudu telah menyatakan kesiapan pemerintah Indonesia menghadapi gugatan tersebut dan bahkan dinilainya bukan merupakan persoalan besar. Persoalan dengan perusahaan satelit *Avanti Communications* muncul karena Pemerintah Indonesia masih menunggak pembayaran sewa satelit yang nilainya mencapai 30 juta *US Dollar*. Penyewaan satelit ini dilakukan sebagai akibat dari upaya mengganti peran satelit Garuda 1 yang telah mengorbit sejak tahun 2000 di orbit 123 BT (Bujur Timur) yang "melenceng" dari lintasannya sejak tahun 2015. Padahal, penempatan satelit di titik orbit dimaksud sangat penting untuk mengawasi kedaulatan wilayah RI. Orbit 123 BT dapat diisi oleh satelit jenis L-band yang beroperasi di ketinggian 36 ribu kilometer. Satelit Artemis semula direncanakan akan dioperasikan sampai dengan tahun 2020,

yang kemudian diharapkan akan diganti alat baru yang benar-benar dimiliki pemerintah Indonesia. Adapun Orbit 123 BT akan ditempati satelit pasokan *Airbus Defence and Space*. Rencana itu terancam gagal terlaksana setelah kasus gugatan *Avanti Communications* muncul di publik. Kegagalan pemerintah RI membayar sisa biaya sewa satelit, disebabkan oleh pencairan dananya yang tidak bisa disetujui oleh Kementerian Keuangan. Kementerian Keuangan tidak mencairkan anggaran yang dijadwalkan usulan tahun 2017, karena Badan Pengawas Keuangan dan Pembangunan (BPKP) menilai studi kelayakan proyek pembiayaan satelit dimaksud tidak memadai. Kementerian Keuangan menilai adanya perbedaan atau belum dibangun kesamaan rencana strategis (Renstra) ihwal penyewaan satelit antara TNI dengan pihak Kemenhan.[43] Setelah menggugat pemerintah Indonesia, *Avanti Communications* menghentikan operasional satelit yang dimulai sejak November 2017. Akibatnya, orbit 123 BT strategis bagi kendali kedaulatan wilayah RI tidak lagi diisi oleh satelit antariksa apapun. Pemerintah Indonesia melalui pihak Kejaksaan Agung sebagai Jaksa Pengacara Negara menjanjikan akan menyelesaikan kasus ini melalui jalur di luar persidangan (non-litigasi), meskipun pemerintahan Indonesia tetap membayar sisa tunggakan sewa satelit.

Keterbatasan jaringan telekomunikasi juga menjadi isu politik yang rawan pada saat bersamaan kedaulatan RI atas wilayah udara yang menaunginya, justru tidak berlaku penuh. Sejak 1946, wilayah udara Indonesia di sekitar Riau dan Kepulauan Riau dikendalikan oleh Singapura. Bukan rahasia lagi, hal itu seringkali menimbulkan kegeraman di pilot-pilot TNI AU di wilayah itu. Mereka harus meminta izin ke Singapura jika ingin menerbangkan pesawatnya untuk latihan atau tugas lain. Pengambilalihan FIR (*flight information region*) adalah amanat UU No. 1 Tahun 2009 tentang Penerbangan. Presiden Jokò Widodo juga sudah menyatakan keinginannya untuk mengambil-alih

[43] "Dibalik Kasus Gugatan Sewa Satelit yang Menyeret Pemerintah", *https//tirto.id.*, dikutip 7 Mei 2018.

FIR di atas wilayah udara Riau dan Kepulauan Riau saat bertemu Wakil Perdana Menteri merangkap Menteri Koordinator Keamanan Nasional Republik Singapura, Teo Chee Hean, November 2015. Kendala utama pengambilalihan FIR berada di dalam negeri, yaitu meliputi: pertama, belum ada kesamaan persepsi tentang FIR. Kementerian Perhubungan dan Kementerian Luar Negeri cenderung melihat FIR sebagai masalah teknis operasional untuk keselamatan dan efisiensi penerbangan. Terdapat dua alasan yang disampaikan mengapa Indonesia tidak segera mengambil alih FIR. Pertama, Indonesia belum memiliki kemampuan teknis untuk mengatur wilayah udara. Namun hasil audit *ICAO (International Civil Aviation Organization)* pada 2017 mengatakan skor Indonesia untuk *Air Navigation Service* mencapai 86 persen, di atas rata-rata global 60,7 persen. Pencapaian pelaksanaan protokol udara keselamatan penerbangan juga telah mencapai 81,15 persen di atas rata-rata global yang hanya sebesar 64,71 persen. Adapun alasan kedua, FIR dianggap tidak terkait kedaulatan negara, tetapi lebih ditempatkan pada aspek keselamatan udara negara. Padahal, alasan yang terakhir ini cenderung tidak lagi sesuai dengan perkembangan zaman, karena banyak ancaman terhadap keselamatan negara bisa terjadi melalui udara. Sementara saat kondisi damai, wilayah udara dapat menjadi alat diplomasi dan bahkan langkah mendatang pemasukan devisa.[44]

Kasus penanganan angkutan daring sudah membuktikan dampak lain pula secara sosial dan ekonomi dari siber yang berkonsekuensi lanjutan secara politis bagi hubungan pusat-daerah. Pemerintah daerah tampaknya tidak berdaya menghadapi lonjakan luar biasa *stake holder* dan individu pengguna dan penyedia moda transportasi daring. Sehingga secara politik siber, muncul tuntutan atau desakan agar pemerintah pusat sesegera mungkin menerapkan kebijakan guna mengatur angkutan dalam jaringan (daring) baik ojek maupun taksi.

[44] "Saat F-16 Mengawal Panglima TNI", *Kompas*, 29 April 2018.

Lonjakan penyedia layanan transportasi daring dimaksud berkembang sangat luas dan memicu masalah di kota-kota di Indonesia. Hal substansi secara politik siber dari masalah yang muncul ini, adalah sudah terbukti intervensi pemerintah daerah tidak mampu menanggulangi efek berkelanjutan dari maraknya transportrasi daring. Ini misalnya, dicontohkan saat di Bogor diberlakukan Peraturan Walikota setempat nomor 21 Tahun 2017 tentang pengaturan operasi motor atau mobil sewa daring, di mana aturan itu tidak terlalu efektif mengatasi persoalan terkait angkutan daring. Bahkan, perusahaan cenderung tidak menggubris aturan tadi.[45]

## F. Alternatif Solusi

Politik siber dalam konteks hubungan pusat-daerah dan antar-kelembagaan secara nasional jelas membutuhkan sinergi secara baik di antara pemangku kepentingan, karena dimensi persoalan siber tidak hanya mengenai soal teknis IT, tetapi lebih luas dan memiliki dampak bagi negara. Bahkan, ruang yang demikian terbuka atas siber dengan segala batasan dan perangkat pengamanan persandian sekalipun, memiliki potensi tersendiri bagi keutuhan kedaulatan negara atas wilayah dan masyarakatnya. Di lingkup media, kehadiran media siber berpotensi mengurangi kepercayaan publik terhadap media konvensional. Apalagi, media konvensional diduga memiliki agenda tertentu terhadap seluruh informasi yang diproduksi dan didistribusikan bahwa seringkali media menganggap apa yang dianggap penting oleh khalayak. Di samping itu, di tingkat media massa tersebut juga terjadi perbedaan antar-institusi media. Survei yang dilakukan oleh *YouGov* untuk *prospect magazine*, sebagaimana dilaporkan Guardian edisi 23 September 2010, menemukan bahwa kepercayaan terhadap liputan BBC menurun dari 81 persen dan di tahun 2010 menjadi 33 persen,

[45] "Intervensi Pusat Dinanti", *Kompas*, 3 April 2018.

kemudian terhadap 3 surat kabar *The Times*, *Daily Telegraph*, dan *The Guardian* menurun 24% menjadi 40 persen. Hal yang sama juga terjadi pada *Daily Mail* dan *Daily Express* turun dari 35% tingkat kepercayaan menjadi tinggal 21 %, serta terhadap *The Sun*, *Daily Mirror* dan *Daily Star* ditahun 2003 memperoleh 14% tetapi di tahun 2010 turun menjadi 10%. Meskipun penelitian tentang menurunnya tingkat kepercayaan dan tidak dapat dijadikan satu-satunya sumber untuk menyatakan ada pergeseran akses warga terhadap media dalam hal memperoleh informasi, tetapi kehadiran media siber memberikan alternatif bagi warga.[46]

Tingkat kepercayaan masyarakat bagi media konvensional yang dipertaruhkan di tengah semakin kuatnya peran media alternatif siber menempatkan kedaulatan negara tidak lagi bersifat mutlak. Ini menegaskan bukan saja fenomena globalisasi, tetapi juga sekaligus bisa menjadi ancaman tersendiri kalau penetrasi informasi yang tidak terkendali dapat mengikis kedaulatan negara. Media siber perlu dimanfaatkan bagi kepentingan nasional semaksimal mungkin tanpa harus menimbulkan konflik dengan negara atau pihak lain. Kebutuhan pemerintahan dan kemasyarakatan dalam pemanfaatan ruang publik jangan sampai disalahgunakan atau bahkan menjadi instrumen intervensi pihak asing. Kelengahan dalam pemenuhan kebutuhan demikian, pemanfaatannya bisa merugikan kepentingan nasional dan bahkan diisintegrasi bangsa.

Lemahnya regulasi dan adanya beberapa *blank spot* akibat masih terbatasnya jaringan telekomunikasi menara BTS, terutama di kawasan terpencil atau perbatasan dengan negara lain, bukan tidak mungkin digunakan untuk mengambil peluang melakukan intervensi dimaksud. Ini juga tidak saja dikelilingi oleh keterbatasan masyarakat dalam hal akses media, tetapi juga dari aparat sendiri yang kelembagaan

[46]Rulli Nasrullah, *Teori dan Riset Media Siber/ (Cybermedia)*, Prenada Media Group, Jakarta, 2016, h. 40-41

pemerintahan daerahnya masih belum diterpa tekanan informasi *online* atau digital secara maksimal. Kesadaran yang dibangun oleh masyarakat dan pemerintahan setempat perlu perjuangan berat dan dukungan dari pusat secara serius dalam rangka menciptakan literasi digital yang kuat terhadap berbagai informasi yang masuk dan menyampaikan pesan tertentu ke ruang publik. Ini sekaligus penting bagi agenda pembentukan regulasi siber yang tetap mampu menjaga keseimbangan antara kepentingan keamanan negara di satu sisi dan kepentingan privat individu sebagai bagian dari hak asasi manusia (HAM) di sisi lain. Pentingnya keseimbangan ini disampaikan, karena ketika politik siber diterjemahkan hanya dari perspektif keamanan, maka sangat berpotensi bagi terjadinya kemunduran demokrasi sebagai konsekuensi tertinggalnya langkah bagi penguatan perlindungan hak privat, sebagaimana contoh terhadap data pribadi dalam soal e-KTP. Intervensi asing yang berpeluang sebagai akibat dari kelengahan kelembagaan yang tidak sinergis terkait kebijakan siber dan keterbatasan sumber daya dalam negeri dalam hal infrastruktur teknologi komunikasi, merupakan agenda yang penting untuk ditangani dengan tahapan kerja dan waktu yang jelas.

## G. Penutup

Politik siber merupakan cerminan dari lanskap akibat pengaruh digital yang tidak lagi sekedar teknis kemajuan teknologi yang memudahkan interaksi manusia, tetapi juga konstruksi persaingan di tingkat kekuasaan yang semakin kuat desakan transparansi publiknya. Itu sebabnya, politik siber menjurus pada konteks semakin melemahnya batas-batas teritorial kedaulatan negara. Otonomi negara tidak lagi menjadi mutlak adanya dan siber membuat jarak antara segmen penguasa dan rakyat dan di antara segmen elit atau komunitas menjadi lebih dekat atau bahkan akrab. Tetapi di tengah mendekatnya jarak interaksi di antara segmen tersebut menyimpan potensi yang penting

dikelola secara hati-hati agar benar-benar maksimal diusahakan membawa kebaikan bagi bangsa. Dalam konteks ini, regulasi siber benar-benar ditujukan bagi kepentingan nasional yang mampu menghargai keragaman di setiap level lokal, regional, dan pusat, menjadi harus mampu diwujudkan.

Tantangan politik siber yang erat bagi penguatan integrasi bangsa harus dijawab dengan komitmen melahirkan regulasi siber di tingkat peraturan perundang-undangan yang sejalan dengan iklim globalisasi. Pada titik inilah, ketentuan yang tertuang dalam regulasi siber diharapkan benar-benar dapat diandalkan dalam rangka menjaga kedaulatan negara dan sekaligus menjaga hak privasi individu sebagai bagian dari demokrasi. Sehubungan ini beberapa langkah kongkret penting dilakukan.

Pertama, memperkuat kelembagaan BSSN sebagai badan siber dan sandi negara yang benar-benar mengabdi pada kepentingan bangsa dan bukan sekedar basa-basi bagi altruisme kekuasaan. BSSN harus mampu menjadi penjuru bagi koordinasi dari setiap kelembagaan siber di pemerintahan dan menghilangkan ego sektoral di antara pihak-pihak yang terlibat. Penjuru posisional koordinasi ini menjadi penting agar penguatan kerahasiaan data-data pribadi dan informasi krusial bagi kedaulatan negara tetap mampu dijaga.

Kedua, penyesuaian di lapangan yang penting dilakukan, mengingat siber secara bertahap semakin merembes pada relung kehidupan masyarakat. Tidak saja pada ranah fasilitasi bagi menjamurnya komunitas peduli siber yang semakin meningkat di setiap daerah, tetapi juga dinamika siber di daerah harus diletakkan pada substansinya bagi partisipasi masyarakat. Itu sebabnya regulasi siber harus mampu memadukan dua titik ekstrim dari dunia digital, yaitu di satu pihak pengaturannya terhadap segala dampak dari teknologi komunikasi di satu sisi dan kemampuannya menjaga kearifan lokal di sisi lain. Kemampuan itu tidak mudah dirumuskan dan bahkan kalau sampai di tingkat operasional, tetapi ini bukan mustahil diwujudkan, sekali

lagi, kalau sinergi partisipasi masyarakat dan pemerintah daerah dapat ditransformasikan sebagai energi lokal bagi kepentingan nasional.

Ketiga, karakter media siber sebagai generasi media baru yang begitu terbuka dan luang untuk dimanfaatkan setiap data atau informasi, penting diisi oleh setiap instansi pemerintahan dalam mengajukan informasi yang positif. Tanpa pengisian yang intensif informasi semacam ini, maka dikhawatirkan ruang siber justru dimanfaatkan oleh pihak yang tidak bertanggung jawab, termasuk antara lain dalam kasus pemanfaatan media sosial oleh terorisme. Pemerintah di tengah membanjirnya informasi, termasuk informasi sampah atau muatan terorisme atau sekedar radikalisme, jangan sampai berfikir untuk menutup siber. Langkah yang tepat adalah dilakukan pengaturan secara tegas dalam pengelolaan siber agar media digital digunakan sebagai bentuk kemajuan bangsa dalam pengelolaan kedaulatan negara secara kondusif melalui kehadiran pemerintahan yang baik (*good governance*).

## DAFTAR PUSTAKA

**Buku**

AS Hikam, Muhammad (2017), *Deradicalization: Engendering Indonesian Civil Society Organizations in Curbing Radicalism*, Kompas Publisher, Jakarta.

B.U, Donny, et.al (editor) (2018), *Kebijakan Cybersecurity dalam Perspektif Multistakeholder*, seri literasi digital, ICT watch dan Kominfo, Jakarta.

Halkis, Mhd. (2017), *Konstelasi Politik Indonesia: Pancasila dalam Analisis Fenomenologi Hermeneutika*, Yayasan Pustaka Obor, Jakarta.

Latif, Yudi (2017), *Revolusi Pancasila*, Mizan, Jakarta.

Mahfud MD, Moh. (2009), *Konstitusi dan Hukum dalam Kontroversi Isu*, Rajawali Press, Jakarta.

Munir, Nudirman (2017), *Pengantar Hukum Siber Indonesia*, Rajawali Press, Depok.

Nasrullah, Rulli (2016), *Teori dan Riset Media Siber/ (Cybermedia)*, Prenada Media Group, Jakarta.

Pfest, Barbara (tanpa tahun), *Political Communication in the Era New Technologies*, Berlin (tanpa tahun).

Quill, Denis Mc (2011), *Teori Komunikasi Massa*, Penerbit Salemba Humanika, Jakarta.

Richardson Jr, Glenn W (editor) (2017), *Social Media And Politics: A New Way To Participate in the Political Process*, Preager, California.

Simanjuntak, Marsilam (1994), *Pandangan Negara Integralistik*, Jakarta, Grafiti.

**Koran:**

*Koran Tempo*, 15 Maret 2018.

_____,12 April 2018.

_____, 10 April 2018.

_____, 19 April 2018.

*Kompas*, 25 Maret 2018.

_____, 23 Februari 2018.

_____, 3 April 2018.

_____,14 Maret 2018

_____, 21 Maret 2018.

_____, 29 April 2018.

_____, 16 April 2018.

_____, 18 April 2018.

_____, 22 April 2018.

_____, 3 Juni 2018.

*The Jakarta Post*, 15 Maret 2018.

**Jurnal:**

*Journal of International Affairs* Vol VI Number 1, March-May, 2001

*Jurnal Negarawan*, Kementerian Sekretariat Negara RI, No. 31, Tahun 2014.

**Dokumen:**

Draft Naskah *Koran Tempo*, 10 Aprl 2018Akademik RUU Siber, PUU Badan Keahlian DPR RI, per tanggal 28 Mei 2018

Laporan Tim Kerja Penyusunan Naskah Akademik dan draft RUU Siber Dalam Diskusi dengan Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII).

Dinas Kominfo Pemprov Maluku, "Masukan Tertulis bagi Badan Keahlian DPR RI tentang Penyusunan Naskah Akademik Draft RUU Siber", Ambon, Maluku, Maret 2018.

Catatan Tim Penyusunan NA dan RUU Siber saat dialog dengan Reskrimsus Pola Maluku , KPU Maluku, Prodi Ilmu Hukum Universitas Patimura, dan Dinas Kominfo Pemprov Maluku, Ambon 26-28 Maret 2018.

**Situs Internet:**

*https//tirto.id.*, dikutip 7 Mei 2018.

*http:itdjournal.org.*,diakses 11 Mei 2018.

**Makalah:**

Sekolah Tinggi Sandi Negara, "Diskusi Strategi Keamanan Siber Nasional", Badan Keahlian DPR RI, Jakarta, 23 Februari 2018.

Snijkers, Kris,"E-Government: ICT From A Public Management Perspective", 13th Annual NISPAcee Conference, 19-21 Moscow State University, Moscow.

# BAGIAN 2
# TATA KELOLA *CYBER SECURITY* PEMERINTAH DAERAH DALAM UPAYA MENINGKATKAN PELAYANAN PUBLIK

*Ahmad Budiman*
*Peneliti Kepakaran Komunikasi Politik*
*Pusat Penelitian Badan Keahlian DPR RI*
*E-mail: a.budiman69@gmail.com*

## A. Pelayanan Publik Berbasis IT

Pertimbangan filosofis tentang mengapa masyarakat perlu mendapatkan pelayanan dengan baik, karena negara berkewajiban melayani setiap warga negara dan penduduk untuk memenuhi hak dan kebutuhan dasarnya dalam kerangka pelayanan publik yang merupakan amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Selanjutnya pelayanan publik dalam terminologi regulasi sebagaimana termuat dalam Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (UU Pelayanan Publik) diartikan sebagai kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundang-undangan bagi setiap warga negara dan penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.[1] Sedangkan penyelenggara pelayanan publik diartikan sebagai setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan undang-undang untuk kegiatan pelayanan publik, dan

[1] Pasal 1 angka 1 Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.

badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik.[2]

Pada hakekatnya, keberhasilan pelayanan publik yang dilakukan oleh penyelenggara pelayanan publik kepada masyarakat sangat ditentukan oleh seberapa besar kemanfaatan pelayanan publik yang dapat dirasakan masyarakat. Semakin cepat masyarakat memperoleh pelayanan publik sesuai dengan kebutuhan yang dimilikinya, akan menjadi salah satu indikator dari telah dilaksanakannya pelayanan publik dengan baik. Untuk itu perlu dibangun sebuah sistem informasi yang dapat membantu meningkatkan pelayanan publik penyelenggara kepada masyarakat. Sistem ini termuat dalam sistem informasi pelayanan publik yang diartikan sebagai rangkaian kegiatan yang meliputi penyimpanan dan pengelolaan informasi serta mekanisme penyampaian informasi dari penyelenggara kepada masyarakat dan sebaliknya dalam bentuk lisan, tulisan latin, tulisan dalam huruf *braile*, bahasa gambar, dan/atau bahasa lokal, serta disajikan secara manual ataupun elektronik[3].

Penyelenggara berkewajiban mengelola Sistem Informasi yang terdiri atas sistem informasi elektronik atau nonelektronik, sekurang-kurangnya meliputi profil Penyelenggara, profil Pelaksana, standar pelayanan, maklumat pelayanan, pengelolaan pengaduan, dan penilaian kinerja. Penyelenggara berkewajiban menyediakan informasi kepada masyarakat dengan secara terbuka dan mudah diakses. Hal penting lainnya yaitu dokumen, akta, dan sejenisnya yang berupa produk elektronik atau nonelektronik dalam penyelenggaraan pelayanan publik dinyatakan sah sesuai dengan peraturan perundang-undangan[4].

Mencermati panduan normatif sebagaimana termuat dalam UU Pelayanan Publik dapat kita pahami, bahwa pelayanan publik yang prima akan dapat terlaksana bila tersedia sistem informasi yang memadai

dari penyelenggara pelayanan publik. Mengapa demikian? Hal ini disebabkan bentuk awal dari terselenggaranya pelayanan publik yang baik adalah karena telah disediakannya informasi yang dibutuhkan oleh masyarakat. Informasinya harus selalu dekat dan cepat didapat sesuai dengan kebutuhan masyarakat. Kedekatan informasi dan kecepatan masyarakat dalam mendapatkan informasi, perlu dibangun dalam sebuah sistem informasi yang menggunakan teknologi informasi komunikasi berbasis internet.

Upaya untuk memberikan pelayanan publik berbasis internet, sesungguhnya sejalan dengan program pemerintah dalam mengembangkan *e-government* di semua kelembagaan baik di tingkat pusat hingga ke tingkat daerah. Tuntutan global,[5] pada akhirnya mengarahkan pemerintah termasuk juga pemerintah daerah untuk menyediakan sistem pemerintahan yang efisien dan efektif yang diantaranya melalui sistem pemerintahan elektronik (*e-government*). Tujuan pengembangan *e-government* sebagaimana disebutkan dalam Kepres Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *e-government* yaitu merupakan upaya untuk mengembangkan penyelenggaraan kepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan *e-government* dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup 2 (dua) aktivitas yang berkaitan yaitu:

(1) Pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis;

---

[5] Ketidakmampuan menyesuaikan diri dengan kecenderungan global tersebut akan membawa bangsa Indonesia ke dalam jurang "*digital divide*", yaitu keterisolasian dari perkembangan global karena tidak mampu memanfaatkan informasi. Oleh karena itu penataan yang tengah kita laksanakan harus pula diarahkan untuk mendorong bangsa Indonesia menuju masyarakat informasi.Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-Government*.

(2) Pemanfaatan kemajuan teknologi informasi agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat di seluruh wilayah negara.

Seluruh kegiatan pemerintahan yang berbasis elektronik dapat menghemat dan mengefisienkan biaya penyelenggaraan pemerintahan.[6] Manfaat *e-government* untuk Indonesia, data negara bisa terdokumentasi dengan baik, membuat masyarakat menjadi lebih mudah mengakses data, efektifitas dan efisiensi surat menyurat menjadi lebih mudah dan cepat serta pelayanan publik menjadi lebih dekat antara pemerintah dan masyarakat.[7]

Dampaknya, kita tidak bisa memungkiri kemajuan TIK khususnya melalui saluran komunikasi maya (*cyber*) telah banyak digunakan dalam aktivitas pemerintahan atau interaksi di dalam masyarakat. Keamanan saluran media maya (*cyber security*) harus berhadapan dengan berbagai tantangan, baik yang bersifat umum maupun yang bersifat khusus di satu daerah.

Tingginya penggunaan internet seiring dengan maraknya keterkaitan internet dengan kehidupan sehari-hari, mengakibatkan frekuensi serangan dan kejahatan *cyber space* semakin meningkat. Kejahatan-kejahatan *cyber space* atau yang dikenal dengan istilah *cybercrime* tersebut meliputi pencurian identitas dan data (sumber daya informasi), pembajakan account (*email, IM, social network*), penyebaran *malware* dan *malicious code, fraud, spionase industry*, penyanderaan sumber daya informasi kritis serta *cyber warfare* atau perang di dalam dunia maya.[8]

---

[6] *Kemenpan-RB pantau implementasi "e-government" instansi daerah*, http://www.antaranews.com/berita/508938/kemenpan-rb-pantau-implementasi-e-government-instansi-daerah, diakses tanggal 23-5-2016

[7] *Menpan RB: E-Government Korea Paling Bagus di Dunia*, http://news.okezone.com/read/2016/03/02/337/1325739/menpan-rb-e-government-korea-paling-bagus-di-dunia, diakses tanggal 25-5-2016

[8] Kementerian Komunikasi Informatika RI, *Buku Putih 2011 Komunikasi dan Informatika Indonesia*, 2011, hal. 22.

Sudah banyak pemerintah daerah (Pemda) yang menerapkan pelayanan publik berbasis internet. Keperluan bagi Pemda dalam penggunaan IT untuk keperluan perijinan dan pelayanan publik. Jaringan kerja perijinan atau pelayanan publik telah mampu dikoneksikan antara satu dinas dengan dinas lainnya. Untuk mempermudah layanan bagi masyarakat, maka bentuk layanan di satu tempatkan pada dinas yang mengelola pelayanan terpadu satu pintu. Selanjutnya untuk mengontrol jalanannya pelayanan terpadu kepada masyarakat, pada umumnya dibuat ruangan pengawasan layanan publik, yang di dalamnya juga tersedia database dari berbagai informasi yang memiliki keterkaitan dengan layanan publik di maksud. Kondisi ini di setiap daerah pada umumnya dibantuk dalam *command center*, seperti contoh yang sangat baik dilaksanakan oleh Pemkot Bandung atau Pemkot Surabaya. Keberadaan *commod center* di kedua Pemda ini sangat membantu dalam memberikan kemudahan bagi masyarakat dalam memperoleh pelayanan Pemdanya. Lebih dari itu, Pemda juga telah mampu menyimpan keseluruhan data yang terkait dengan pelayanan publik atau perijinan kepada masyarakat.

Fenomena ruang siber menggambarkan sebuah realitas bahwa aktifitas kegiatan masyarakat modern saat ini sudah saling terkoneksi melalui ruang siber dan internet. Dari perspektif keamanan siber, pemanfaatan internet juga dimungkinkan untuk tujuan negatif atau destruktif oleh pihak-pihak-pihak yang punya kemampuan baik dilakukan secara perorangan, kelompok hingga oleh negara.[9] Penataan keamanan siber menjadi lebih relevan, terutama bila dikaitkan dengan kebijakan pemerintah dalam mengembangkan *e-government* terutama di pemerintah daerah (Pemda). Tata kelola keamanan siber ini sangat diperlukan untuk tetap menjaga kepercayaan masyarakat dalam

[9] Rudy Agus Gemilang Gultom, Membangun Tata Kelola Informasi dan Keamanan Informasi Pemerintahan Daerah di Era Globalisasi Informasi dalam rangka menjaga keutuhan dan kedaulatan NKRI", disampaikan pada FGD Penelitian Tata Kelola *Cyber security* pada Pemerintahan Daerah, Puslit BKD, Jakarta, 17 Maret 2017.

mendapatkan layanan publik dan layanan perijinan berbasis *online*. Hal inilah yang mendasari pertanyaan dalam tulisan ini, yaitu bagaimana tata kelola keamanan siber dalam meningkatkan pelayanan publik kepada masyarakat?

## B. *Cyber Security* untuk Pelayanan Publik

Internet yang berasal dari kata "*interconnection*" dan "*network*" merupakan jaringan yang dibentuk dari kerjasama jaringan-jaringan komputer yang saling terhubung/terkoneksi. Internet merupakan hasil konvergensi teknologi telekomunikasi, komputer, dan informasi yang terhubung melalui jaringan secara global.[10] Internet juga diartikan sebagai *interconnection of networks* yang menghubungkan jaringan-jaringan di bidang bisnis, universitas, pemerintah dan organisasi lainnya.[11]

Internet sebagai konsep teknologi yang umum terdiri atas tiga perangkat pokok: perangkat keras (*hardware*), perangkat lunak (*software*) dan perangkat otak manusia (*brainware*). Yang pertama berwujud peranti, kedua berupa program komputer yang beragam, dan ketiga berada di otak manusia, pamakai, pengguna atau pelaku komunikasi yang memanfaatkan teknologi tersebut.[12]

Aktivitas empat komponen di dalam internet yang menunjukkan adanya konvergensi yaitu:

a. *Content*

   Keberadaan isi atau substansi dari data dan atau informasi yang merupakan *input* dan *output* dari penyelenggaraan informasi.

---

[10] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber*, Bandung, Penerbit PT Refika Aditama, 2012, h. 81.

[11] Ibid., h. 82.

[12] Ahmad Muntaha, Berpisah-Menyatu dan Berbagi ruang Rindu di Media Baru: Pengalaman Komunikasi Online Tiga *Nettie-Family* Indonesia, dalam Heri Budianto (ed), *Ilmu Komunikasi Sekarang dan Tantangan Masa Depan*, Jakarta: Penerbit Kencana, 2013, h. 484.

b. *Computing*

Keberadaan sistem pengolah informasi yang berbasiskan sistem komputer yang merupakan jaringan sistem informasi.

c. *Communication*

Keberadaan sistem komunikasi yang merupakan perwujudan interkoneksi sistem informasi atau jaringan komputer.

d. *Community*

Keberadaan masyarakat, baik sebagai pelaku usaha, profesional penunjang maupun pengguna sistem tersebut.[13]

Sesuai terminologinya, *cyber security* adalah aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *cyber crime*. Dan seperti juga *cyber crime*, spektrum dari aktivitas *cyber security* ini juga sangat luas. Sebuah proses peningkatan keamanan (*security hardening*), umumnya meliputi masalah teknis, seperti pengamanan dari sisi jaringan, sistem operasi, keamanan data dan *source code* aplikasi. Institusi keuangan dan telekomunikasi secara rutin menyewa konsultan keamanan untuk melakukan kegiatan '*penetration testing*'.[14]

*Cyber security* adalah kumpulan alat, kebijakan, konsep dan keamanan, perlindungan keamanan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

---

[13] Edmon Makarim, *Pengantar Hukum telematika, Suatu Kompilasi Kajian*, Jakarta, Penerbit PT Raja Grafindo Persada, h. 11

[14] Disari dari Sekilas Tentang *Cyber Crime, Cyber Security* dan *Cyber War, https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war, diakses tanggal 22-9-2017*

*Cyber security* merupakan upaya untuk memastikan pencatatan dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap resiko keamanan yang relevan dalam lingkungan siber. Tujuan keamanan umum terdiri dari ketersediaan, integritas, termasuk di dalamnya keaslian dan keunggulan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.

Ruang lingkup *cyber security* dimulai dari *install, harden* atau keamanan terkait dengan perangkat keras yang digunakan dalam mengoperasikan internet, monitor yang menyebabkan terjadinya insiden atau kejadian dan insiden itu dapat pula berasal dari serangan atau *cyber attact* yang membutuhkan penanganan terhadap insiden tersebut dengan melakukan uji forensik sebagai pembuktian dalam menegakan hukum terhadap terjadinya *cybercrime.*

Prinsip-prinsip keamanan siber telah dikembangkan, misalnya dalam bidang *software security*, Microsoft membuat panduan *Security Development Lifecycle* (SDL) yang memasukkan unsur-unsur keamanan siber dalam pengembangan perangkat lunak. Dalam SDL milik Microsoft ini, proses audit keamanan siber terintegrasi sepanjang proses pengembangan aplikasi mulai dari titik awal hingga ke titik akhir proses. Untuk keperluan pemodelan ancaman (*threat*), Microsoft mengembangkan model STRIDE, yakni pengelompokan ancaman menjadi 6 bagian[15]:

- *Spoofing identity* (pencurian identitas)
- *Tampering with data* (pengubahan data secara tidak sah)
- *Repudiation* (transaksi yang tidak disetujui oleh pihak asal)
- *Information disclosure* (pembocoran informasi)
- *Denial of service* (penghentian layanan)
- *Elevation of privilage* (peningkatan hak akses secara tidak sah)

---

[15] *The Unknown Unknown* Pada *Cyber Security*, https://kriptologi.com/2017/05/16/the-unknown-unknown-pada-cyber-security/, diakses tanggal 3-10-2017

Tata kelola pengamanan siber dipentingkan dalam rangka memaksimalkan pelayanan publik terhadap kemungkinan terjadinya ancaman terhadap ketersediaan data dan informasi yang dimilikinya. Ancaman dimaksud akan mengarah pada tindak pidana terhadap *confidentiality*, *integrity*, dan *availability* data atau sistem komputer seperti *hacking*, *cracking*, *phreaking*, *viruses*, dan lain-lain.[16]

Hal utama yang mendasari perlunya dilakukan tata kelola keamanan siber karena ancaman dan atau tindak pidana siber berdimensi transnasional dan interkoneksi secara global. Setiap perbuatan khususnya yang dilakukan dengan menggunakan internet akan selalu melekat sifat transnasional karena berkaitan dengan interkoneksi sistem jaringan global dari internet tersebut.[17]

## C. Tata Kelola *Cyber Security* di Pemerintah Daerah

### 1) Pelaksanaan di Sulawesi Tenggara

Harus diakui, tata kelola *cyber security* di Sulawesi Tenggara (Sultra) belum dapat dikatakan maju, mengingat kelembagaan Pemda yang bertugas khusus untuk masalah ini memang baru saja terbentuk. Dinas Komunikasi dan Informatika (Infokom) baru saja terbentuk pada bulan Januari 2017. Unit kerja yang tergabung dalam Dinas Infokom sebelumnya tergabung dalam Biro Humas Pemda Sultra dan Dinas Perhubungan Sultra. Saat ini bagian yang tergabung dalam Dinas Infokom yaitu Bidang Informasi Publik, Bidang Teknologi Informasi Komunikasi, Bidang Pengelolaan *Data Center*, Bidang Sandi Telekomunikasi dan Bagian Tata Usaha[18].

Meski baru saja terbentuk, namun rencara strategis telah disusun sebagai pegangan bagi dinas dalam melakukan tata kelola informasi dan komunikasi di provinsi ini. Kebijakan strategis yang ditetapkan

---

[16] Sigid Suseno., Op.cit., h. 2

[17] Ibid., h. 7

[18] Wawancara dengan Kepala Dinas Infokom, Kusnadi, 4-4-2017.

diskominfo yaitu membenahi jaringan *website* dan membenahi jaringan data informasi, serta menyusun pusat data *online* (*command center*). Melalui konsep *command center* ini masyarakat bisa mengakses seluruh data dan informasi yang dihasillan oleh seluruh SKPD Pemda. Hal dimaksudkan menciptakan efisiensi dan efektivitas pelayanan publik yang dilakukan Pemda kepada masyarakat. Walaupun kendala utama yang harus diatasi dalam membangun jaringan di provinsi ini yaitu SDM yang menguasai masalah IT masih terbatas, ketersedian data yang akan dimasukan dalam pusat data masih dimiliki oleh masing-masing SKPD, dan kondisi jaringan masih terpengaruh oleh kondisi alam.

Konsep pengamanan jaringan nantinya masuk ke dalam bidang tugas Dinas Kominfo, meski sekarang ini belum banyak upaya dilakukan untuk itu. Dari pemantau Dinas Kominfo, hingga saat ini aktivitas *hacker* belum begitu banya dan mengganggu aktivitas kerja *website* Pemda. Konsep pengamanan terhadap berita *hoax* dilakukan dengan melibatkan semua unsur SKPD dan Dinas Kominfo sebagai adminnya. Selanjutnya pengamanan isi pesan yang disampaikan melalui *online* dilakukan melalui sistem persandian, meliputi informasi kenegaraan, kedaerahan, informasi dikecualikan dan memo kepala daerah. Selain itu pengamanan informasi juga dilakukan dalam bentuk *jammer* informasi yang berada di suatu ruangan.

Tata kelola *cyber security* juga perlu dilakukan di tataran penyelenggara pemilu di daerah. Hingga saat ini KPU Provinsi Sultra telah memiliki *website* resmi yang digunakan untuk menyampaikan informasi resmi dari KPU terkait dengan kegiatan atau tahapan serta hasil kegiatan pemilu. KPU Provinsi juga telah memiliki PPID dan memasukan folder PPID dalam website KPU[19].

Kebijakan dalam meng-*update* website KPU dimaksudkan untuk mengajak semua komisioner KPU untuk menyajikan informasi melalui *website* resmi dan memberikan segala bentuk laporan kerja atau tahapan

[19] Wawancara dengan Natzir Komisioner KPU Sultra Divisi Sosialisasi dan Iwan Komisioner KPU Sultra Divisi IT, 7-4-2017.

kegiatan pemilu melalui *website* KPU. Harapannya agar masyarakat mengetahui seluruh tahapan kegiatan pemilu dan kinerja KPU. Indikator keberhasilannya ditentukan oleh sudah seberapa banyak data dan informasi diinput ke *website* KPU dan terpenuhinya kebutuhan masyarakat akan informasi publik yang dimiliki oleh KPU yang pelayanannya dilakukan oleh PPID KPU.

Hal yang sama juga dilakukan oleh KPU Kota Kendari. Penggunaan aplikasi kepemiluan dilakukan dengan menggunakan aplikasi dari KPU pusat. Beberapa aplikasi terpusat yang juga digunakan di tingkat daerah yaitu SITAP (Sistem informasi tahapan pemilu), SIDALI (Sistem Informasi Data Pemilih), SITUNG (SIstem Informasi Pemungutan Suara). Sedangkan untuk pengamanan data IT dari sistem terpusat di KPU pusat ditambah dengan bentuk pdf dan identifikasi logo KPU.[20]

Badan Pengawas Pemilu (Bawaslu) Provinsi Sultra menilai masalah *cyber security* harus ditangani oleh pemerintah pusat dalam konteks pemerintahan, termasuk kepemiluan. Pengamanan dilakukan terhadap gangguan terhadap penggunaan media *online* baik jaringan maupun kontennya.

Pengamanan secara sistematis telah dilakukan Bawaslu terkait dengan data yaitu melalui *google drive* (Bawaslu Pusat dan Provinsi), dilengkapi dengan akses terbatas, WA Bawaslu Provinsi dan Kabupaten/ Kota, email resmi seluruh Bawaslu, program *gowaslu* di mana setiap orang bisa melaporkan dan melihat sampai di mana aduannya ditindaklanjuti oleh bawaslu.[21]

Secara politis, DPRD Sultra menilai Pemda telah melakukan tata kelola menuju *cyber security*. Pemda sudah melaksanakan berbagai program yang mengarah pada pembentukan *e-gov* dan sistem pengamanannya, misalnya dengan membuat aplikasi *e-lelang*. Hingga

---

[20] Wawancara dengan KPU Kota Kendari, Zainal Abidin Komisioner KPU Kota Kendari Divisi Teknis dan Hubungan Partisipasi Masyarakat, 5-4-2017.

[21] Wawancara dengan Bawaslu Sultra, Mushir Salam Komisioner Bawaslu, 4-4-2017

saat ini memang tidak pernah ada keluhan dari ancaman penggunaan *website* di Sultra. Masalah justru bersifat teknis terkait dari masih terbatasnya kualitas pita frekuensi yang digunakan di sini.[22]

Khusus untuk pelaksanaan tugas Dewan, telah dimiliki *website* DPRD yang pengelolaannya dilakukan oleh Sekretariat Dewan. Isi web memang sangat tergantung pada isu yang beredar di acara dewan dan hasil kerjanya. Walau harus diakui web DPRD belum terlalu aktual, dan masyarakat juga belum terlalu intens menggunakan web untuk memaknai hasil kerja dewan. Untuk membantu kelancaran tugas dewan, di komisi I telah dibuat WA Komisi I yang berisi semua pimpinan, anggota dewan, dan sekretariat. Isi WA terkait dengan agenda acara, proses pembahasan dan hasil kerja serta pandangan setiap anggota.

Pandangan korektif dilakukan oleh media *Kendari Post* terhadap persoalan tata kelola *cyber security* di Pemda. Tata kelola *cyber security* di Pemda belum ada yang melakukannya. Media sendiri belum memiliki gambaran atau pengetahuan tentang bagaimana tata kelola *cyber security* di provinsi ini, sedangkan perkembangan medsos di provinsi ini cukup marak terutama di daerah perkotaan.[23]

Hingga sekarang ini banyak pihak menyatakan kesulitan untuk mendapatkan informasi yang berasal dari *website* Pemda. hal ini disebabkan tenaga SDM Pemda yang belum terbiasa untuk menulis berita di media sosial, sehingga berita-berita tersebut bisa diakses banyak pihak. Sebetulnya aktifnya Pemda dalam menulis informasi di *website* Pemda, akan mampu mencegah terjadinya berita bohong di masyarakat yang terkait dengan aktivitas Pemda.

Kritikan kepada Pemda juga disampaikan LSM AJI mengenai belum berhasilnya program pusat informasi yang dilakukan oleh Pemda.

---

[22] Wawancara dengan DPRD Sultra, H Bustam F Gerindra, 3-4-2017

[23] Wawancara dengan Kendari Post, Arief Budmangka (redaksi pelaksana) Abdi (redpel), Arial Padli (redaksi olah raga), Inu Saputra (Redpel), Hasrudin (Redaksi metropolitan), La Ode Iman (redpel harian dan portal online), Indri (Litbang), Emilia (redaksi ekonomi), Sartianti (redaksi politik), 7-4-2014

Pusat Informasi kurang berhasil karena etos kerja PNS yang tidak terbiasa dalam penggunaan *online*. Mereka malas dalam bekerja. Anggaran banyak namun kurang efektif untuk digunakan dalam konteks ini dan kurang serius dalam melaksanakan program dimaksud.[24]

### 2) Pelaksanaan di Kalimantan Barat

Organisasi Dinas Komunikasi dan Informatika (Diskominfo) masih sangat baru, setelah sebelumnya tergabung dalam Dinas Perhubungan Komunikasi dan Informatika. Selama ini pengelolaan infokom dilakukan di dalam bidang dinas tersebut. Diskominfo memang memiliki rencana untuk menyusun tim yang mengelola keamanan siber khusus di provinsi ini. Kerja awal dari tim ini nantinya terkait dengan memfilter konten medsos yang mengarah pada pertentangan SARA. Alasan dari berdirinya tim ini adalah menindaklanjuti dari berdirinya BSSN di pusat dan secara konten terkait dengan adanya potensi konflik etnis di Kalbar. Tim akan bekerja pada pencegahan konflik lewat medsos.[25]

Fungsi proteksi sistem jaringan bisa dilakukan, namun saat ini terkendala masalah infrastrukturnya belum ada. Demikian halnya dengan SDM yang akan melakukan kerja pengamanan jaringan tersebut, saat belum belum sesuai kompetensinya dan sangat terbatas jumlahnya. Untuk melakukan koordinasi penanganan berita *hoax*, Diskominfo melakukan koordinasi dengan SKPD terkait berita dimaksud untuk memastikan apakah berita tersebut benar atau tidak. Jadi memang tindakannya adalah pasif yaitu memberikan klarifikasi atas berita yang sudah beredar. Selanjutnya yang menjawab atas berita tersebut bisa berasal dari SKPD terkait atau oleh Diskominfo. Sedangkan kewenangan untuk merahasiakan atas informasi yang bisa diakses publik

---

[24] Wawancara Aliansi Jurnalistik Independen (AJI), Pandi, 5-4-2017

[25] Wawancara Dinas Infokom Kalbar, Aswin Khatib (Sekretaris Dinas), Agustian (Kabid Penyelenggaraan e-gov, Kurniasari (Kabid Pengelolaan Layanan Informasi Publik), Iskandar (Kasie Operasional Pengamanan Persandian), FB Anugrah (Kasie Keamanan Informasi e-gov). 9-8-2017

tidak menjadi kewenangan Diskominfo. Hal ini karena penentuan atas informasi masuk dalam kategori dirahasiakan masuk dalam kewenangan Komisi Informasi Publik.

Tata kelola persandian dilakukan oleh diskominfo terhadap berbagai materi surat dinas di provinsi atau atas permintaan SKPD di provinsi. Hanya sayangnya hal ini hanya dilakukan oleh satu orang tenaga sandiman yang harus menangani sekian banyak surat dinas. Selain itu ketersediaan alat peralatan persandian juga masih sangat kurang jumlahnya. Sedangkan keamanan jaringan di provinsi belum dilakukan Server masih dimiliki oleh masing-masing SKPD, walaupun ada juga yang menitipkan servernya di Diskominfo.

Terkait dengan pengelolaan aktivitas politik dan kebangsaan di Kalbar, Kesbangpol Kalbar menjelaskan berbagai kegiatan komunikasi yang digunakan untuk membangun kesempahaman mengenai kesatuan kebangsaaan dan politik, dilakukan melalui komunikasi langsung seperti dialog demokrasi, dialog pilkada, sosialisasi pilkades dan forum komunikasi umat beragama (FKUB). Deteksi dini disampaikan Polda untuk diketahui oleh semua pemangku kepentingan untuk digunakan masing-masing instansi. Hingga saat ini tidak ada program link jaringan antara Kesbangpol dengan semua pemangku kepentingan karena dari pusat belum selesai diputuskan aturannya. Kendala ini juga terjadi karena di pusat juga belum ada koordinasi dalam pengelolaan link jaringan. Sedangkan solusinya dilakukan melalui pengelolaan secara manual.[26]

DPRD Kalbar menilai kesadaran Pemda untuk mengamanankan data memang belum dapat dikatakan maksimal. Hal ini juga terkait dengan keterbatasan sarana prasarana, serta SDM yang melakukan pengamanan data dimaksud. Data masih dikelola secara manual. Hingga saat ini data manual masih aman karena selalu dilengkapi dengan data pembanding yang dimiliki oleh instansi lain. Kesungguhan Pemda dalam

[26] Wawancara Dinas Kesbangpol Kalbar, Tarmidji Sayub, 8-8-2017.

menyajikan data kegiatannya di dalam website Pemda tentunya akan membantu DPRD dalam mendapatkan data yang dibutuhkan dan juga memberikan kemudahan bagi masyarakat untuk mengakses data.[27]

Penilaian DPRD terhadap kinerja diskominfo memang belum bisa dikatakan bekerja secara maksimal, mengingat masih merupakan SKPD baru yang merupakan pecahan dari dinas perhubungan. Dinas masih kurang aktif untuk mengantisipasi keamanan data dan berita *hoax* dan mengarah pada potensi konflik. Pemda kurang aktif untuk melakukan pemantauan terhadap medis sosial yag beredar di masyarakat. namun pihak Kepolisian dan TNI telah mampu bekerja secara lebih cepat mengatasi masalah ini, karena telah memiliki berbagai perangkat IT yang canggih dan didukung oleh tenaga SDM yang memadai.

Terkait dengan informasi kepemiluan khususnya di KPU Kalbar, penggunaan media *online* yang digunakan oleh KPU Kalbar dalam menyimpan dan mengelola informasi kepemiluan yaitu di jaringan website KPU Kalbar yang terkoneksi oleh KPU pusat, jaringan JDIH (jaringan dokumentasi informasi hukum), dan jaringan PPID (pejabat pengelola informasi dokumentasi) yang dikelola oleh KPU Kalbar. Manfaat yang dirasakan KPU dalam menggunakan jaringan komunikasi *online* yaitu pelayanan informasi kepemiluan melewati jaringan menjadikan proses komunikasi berlangsung dengann mudah dan cepat, penyimpanan data kepemiluan menjadi aman, dan data dikecualikan disimpan tersendiri agar tak bisa diakses oleh masyarakat.[28]

Namun kendala yang ditemui terkait dengan pengelolaan komunikasi melalui jaringan yaitu kualitas jaringan telekomunikasi internet yang sering kali tidak optimal sehingga mempengaruhi kecepatan transfer data, juga keterbatasan anggaran operasional KPU yang ditujukan untuk menyelenggarakan kegiatan komunikasi siber.

---

[27] Wawancara DPRD Kalbar, Lucanus Lucas Pasalima SH, F Gerindra, Anggota Komisi I DPRD Kalbar, 10-8-2017

[28] Wawancara dengan KPU Kalbar, Umi Rifdiawati (Ketua KPU Kalbar) dan Misrawi (Anggota KPU Kalbar Divisi Sosialisasi dan Partisipasi Masyarakat), 8-8-2017

Saat ini penyimpanan informasi kepemiluan dilakukan pada server milik KPU Kalbar yang manajemen penyimpanannya disesuaikan dengan pola kerja keterbukaan informasi publik. Aplikasi SIDALIH dikoordinasikan dengan Disdukcapil dan KPU pusat. Namun kendalanya terletak pada masih kurang maksimalnya jaringan yang digunakan.

Jaringan KPU pernah di-*hack* di mana tampilannya diubah, namun tidak diganggu datanya. Namun dengan cepat dapat diatasi. Memang hingga kini belum ada SOP yang disusun oleh pusat untuk digunakan di daerah dalam mengatasi masalah gangguan keamanan data di jaringan. KPU daerah masih menunggu arahan dari pusat. Kebijakan penyimpanan data kepemiluan sebelum adanya aplikasi SIDALIH, disimpan di arsip daerah secara manual. Namun sekarang disimpan dalam bentuk arsip digital.

Kebijakan tata kelola informasi kepemiluan di KPU Kalbar juga hampir sama dilakukan di KPU Pontianak. Tampilan *website* dan pengembangannya dilakukan secara terus menerus dan dilakukan secara terbuka, kecuali untuk data kepemiluan yang tersifat tertutup atau masih berproses. Data final selanjutnya diserahkan ke arsip daerah. Pengamanan data dan informasi yang ada di *website* KPU kota menggunakan sistem aplikasi dan ketentuan yang berasal dari KPU pusat.[29]

Kebijakan tata kelola siber yang dilakukan oleh Bawaslu Kalbar yaitu melakukan jaringan terintegrasi Baswaslu RI. Antisipasi untuk pilkada 2018 yaitu lakukan sosialisasi kepada masyarakat tentang kampanye lewat medsos, sosialisasi kepada pemilih pemula dan *stakeholders* terkait.[30]

Berkaitan dengan tata kelola informasi publik, KIP Kalbar menjelaskan sinkronisasi kerja layanan informasi publik dan pelayanan publik, seharusnya dapat dilakukan oleh badan publik untuk

---

[29] Wawancara dengan KPU Kota Pontianak, Sujadi Ketua KPU Kota Pontianak, 8-8-2017

[30] Wawancara dengan Bawaslu Kalbar, Kristanto Komisoner Bawaslu Kalbar Divisi Pencegahan dan Hubungan Lembaga. 7-8-2017

mempermudah masyarakat mendapatkan informasi publik dan pelayanan publik. Namun hingga saat ini belum dapat dilaksanakan oleh SKPD. Hal ini disebabkan juga karena belum adanya kesadaran dari pimpinan daerah untuk melakukannya, belum didukung oleh ketersediaan saran prasaran IT, anggaran operasional yang terbatas dan kemampuan SDM pengelola IT yang terbatas.[31]

Media menilai Pemda sudah mulai beralih menggunakan menyediakan informasi yang dimilikinya melalui *website* Pemda yang dimilikinya. Hal ini juga dilakukan dengan penggunaan media sosial untuk berkomunikasi dengan masyarakat, misalnya yang dilakukan oleh Pemkot Pontianak. Walikota sudah sering menyajikan hasil kerjanya lewat media sosial seperti lewat *facebook*. Beberapa kegiatan pelayanan masyarakat juga sudah dilakukan berbasis IT, misalnya pelayanan masyarakat yang ingin membuat paspor.[32]

Pemkot Pontianak sudah cukup cepat melakukan *up-date* informasi di *website*-nya. Pemda sudah aktif memasukan data yang dimilikinya ke dalam pusat data. Kinerja Pemda juga ditampilkan lewat android di mana melalui aplikasi ini masyarakat bisa langsung mengadukan seluruh keadaan yang benar terjadi. Pemda juga harus memberikan jawaban segera setelah adanya pengaduan dimaksud dan dilanjutkan dengan melakukan eksekusi atas temuan masyarakat dimaksud.

## D. Pemutakhiran Tata Kelola *Cyber Security*

Kehadiran media sosial adalah perwujudan dari demokrasi baru karena dapat mendorong partisipasi aktif dari sebagian besar elemen masyarakat. Potensi melalui *e-democracy* ini memudahkan pendekatan kepada warga, memudahkan cara berkomunikasi, mengefektifkan komunikasi, dan mengubah perilaku *silent majority* ke perilaku yang lebih menunjukkan

---

[31] Wawancara dengan KIP Kalbar, Rospita Vici Paulyn, ST Ketua KIP Kalbar, 8-8-2017

[32] Wawancara dengan Pontianak Post Ari (*Webcontent Pontianak Post*), Salman (Penanggungjawab *Website Pontianak Post*), 9-8-2017

kapasitas demokrasi mereka. *E-democracy* adalah salah satu upaya untuk mewujudkan *e-government, on line administration, e safety, regulation, e voting*. Secara keseluruhan hal ini dipandang sebagai tranformasi dalam komunikasi politik dan mobilisasi politik.[33]

Jika bercermin dari hasil penelitian, pada satu sisi ada negara yang menunjukkan adanya kaitan antara dinamika politik dengan kemajuan media sosial (Norris, 2001; Kedzi, 1997). Tetapi, di Cina dan Kuba justru 'sukses' dengan membatasi internet lewat strategi reaktif dan proaktif (Kalathil dan Boaz, 2001). Dalam memperkuat politik yakni melalui penguatan lembaga politik dan negara, bukan melalui pengembangan teknologi. Karena itu, sudah sewajarnya agar penggunaan media sosial secara benar baik dari sisi fungsi dan struktur akan memilah keuntungan dan kerugian. Seberapa kecilnya, media sosial mempunyai kontribusi terhadap pengembangan demokrasi. Di sisi lain, seberapa kecilnya juga mempunyai efek negatif. Namun, dengan membendung secara habis-habisan penggunaan media sosial, juga bukan pilihan yang bijak. Karena itu, teknologi yang tepat dan demokrasi yang tepat merupakan salah satu jalan terbaik.

Bila ditelusuri penggunaan siber dalam penyelenggaraan pemerintahan daerah di Sulawesi Tenggara masih termasuk dalam kategori minim. Hal ini seperti yang disinyalir pada penilaian Inovasi Administrasi Negara (INAGARA) oleh LAN (2016), bahwa pemerintah daerah baik provinsi maupun kabupaten di Sulawesi Tenggara masih kurang memiliki inovasi siber dalam pelayanan publik. Padahal penggunaan *cyber* melalui aplikasi layanan informasi memberi kontribusi yang sangat besar dalam mewujudkan tata kelola pemerintahan yang baik.[34]

---

[33] Disari dari makalah Eka Suaib, Lektor Kepala UHO Kendari, "MENIMBANG PEMANFAATAN MEDIA SOSIAL DALAM *E-DEMOCRACY*", FGD *Cyber Security*, Kendari, 7 April 2017

[34] Disari dari makalah Sartono, Dosen Adminstrasi Publik UHO, TATA KELOLA *CYBER SECURITY* PADA PEMERINTAHAN DAERAH Penggunaan Media Sosial Dalam Tata

Minimnya penggunaan siber atau belum berkiblatnya pemerintah daerah di Sulawesi Tenggara disebabkan oleh masih rendahnya komitmen pimpinan daerah terhadap pemanfaatan media sosial dalam tata kelola pemerintahan daerah. Hal ini dapat dilihat dari kebijakan pemerintah daerah terkait optimalisasi penggunaan siber yang masih sangat kurang. Ini bukan sebuah justifikasi yang tidak berdasar, namun faktanya seperti ini. Rangkaiannya dapat juga kita lihat dari kesiapan sumber daya aparatur yang rendah, perangkat keras maupun perangkat lunak, anggaran dan sebagainya, *e-gov* baru sekedar slogan.

Oleh karena itu, diperlukan regulasi pemerintah yang mengatur untuk mengoptimalkan penggunaan siber dalam tata kelola pemerintahan daerah dan pada sentra-sentra layanan publik. Komitmen kepala daerah di Sulawesi Tenggara terhadap penggunaan media sosial dalam tata kelola pemerintahan dan layanan publik, maupun dalam pemilu kepala daerah, relatif rendah, sehingga siber belum menjadi pilihan atau menu utama dalam tata kelola organisasi perangkat daerah.

Masalah keamanan sistem informasi merupakan salah satu aspek yang sangat penting bagi suatu organisasi. Namun, sangatlah disayangkan jika masih banyak organisasi (lembaga publik/Pemda) yang yang kurang dapat memberikan perhatian secara khusus mengenai pentingnya aspek tersebut. Dalam perkembangannya seiring dengan perkembangan teknologi komputer dan telekomunikasi semakin pesat, keamanan informasi saluran media maya *(cyber security)* sangat diperlukan guna menangkal terjadinya ancaman keamanan data dan informasi bagi setiap organisasi/lembaga publik[35].

Keamanan Sistem Informasi Internal bertujuan untuk menjaga, *pertama* kerahasiaan. Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan

[35] Disari dari makalah Djumadi, Ph.D dan Dr Martoyo, Dosen dan Direktur Pasca Sarjana Untan Paontianak, dalam FGD tanggal 11-8-2017

sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi. *Kedua,* ketersediaan. Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. *Ketiga,* integritas. Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Satu fakta yang mengejutkan datang dari perusahaan *monitoring internet* Akamai yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini menempatkan Indonesia di posisi pertama negara berpotensi menjadi target *hacker,* menggantikan Tiongkok.

Berdasar data *Global Threat Intelligence Report* (GTIR) 2017, sebelumnya, ancaman *cyber* bagi sektor pemerintahan pada 2015 hanya berporsi 7 persen dari semua ancaman siber di dunia. Tahun 2016, porsi itu meningkat menjadi 14 persen atau dua kali lipat. Begitu juga halnya dengan ancaman *cyber* di industri keuangan dan perbankan telah mengalami peningkatan secara signifikan.

Pengaturan dan penataan kelembagaan *cyber security* nasional dan di daerah yang kuat merupakan salah satu prasyarat terwujudnya *cyber security* yang handal. Penangganan *cyber security* harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait yaitu intelejen, penegak hukum, Kementerian Pertahanan, TNI, Kominfo, dan Lembaga Sandi Negara. Kebijakan yang diperlukan adalah dengan menempatkan *cyber security.*

Tidak bisa dipungkiri, kemanfaatan yang akan didapatkan dalam

ketersediaan SDM, perangkat kerja dan infrastruktur siber. Faktor lain juga dipengaruhi oleh keseriusan sosok kepala daerah dalam memimpin jajaran organisasi di bawahnya untuk melakukan pengelolaa siber.

Hal ini tentunya sejalan dengan kemanfaatan yang dapat dihasilkan apabila Pemda secara serius melakukan tata kelola siber di wilayah kerjamya. Di samping dalam rangka pengamanan data dan informasi, juga dimaksudkan memberikan kelancaran komunikasi yang digunakan dalam pelayanan publik menjadi lebih cepat terselenggara, bila dibandingkan dengan komunikasi tatap muka. Komunikasi melalui saluran internet memiliki daya tarik berupa kapasitas yang lebih besar dari pada arsitektur jaringan lainnya. Kapasitas ini juga membisakan kemungkinan timbal balik canggih dengan cara menggantikan mode-mode timbal balik dalam hubungan tatap muka. Komunikasi yang dimediasi komputer, fokus pada keunikan dari peristiwa dalam *cyberspace*. Lebih terkait dengan interaksi dari pada integrasi yaitu seluk-beluk berbagai interaksi individu. Lebih tertarik pada faktor ekternal yang mempengaruhi peristiwa komunikasi. dan terkahir lebih mengarah pada integrasi informasi.

Komunikasi yang efektif yang mempersyaratkan dibangun dalam dua arah dan adanya umpan balik, dapat dimutakhirkan dengan mempergunakan sarana siber. Namun di balik kecanggihannya tersebut, komunikasi siber juga perlu diperhatikan hal-hal yang bersifat spesifik dalam penanganannya. Komunikasi anonim di internet dapat dilihat pada kenyataan bahwa perlu adanya kebijakan untuk menangani masalah tersebut. Sementara banyak orang percaya bahwa komunikasi anonim di internet tidak hanya bisa diterima tetapi juga memiliki nilai positif, orang lain justru menilai resikonya karena pengguna anonim tidak bertanggung jawab atas perilaku mereka. Akibatnya, anonimitas dapat menyembunyikan atau bahkan mendorong perilaku kriminal atau anti-sosial. Tata kelola siber diperlukan untuk tidak hanya mengamankan data dan informasi yang dimiliki Pemda, tetapi lebih penting dari itu yaitu menjaga

otentisitas data dan informasi serta memperlancar pelayanan publik kepada masyarakat.

Hal ini sejalan dengan terminologi *cyber security* yang merupakan aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *cyber crime*. Sebuah proses peningkatan keamanan (*security hardening*), umumnya meliputi masalah teknis, seperti pengamanan dari sisi jaringan, sistem operasi, keamanan data dan *source code* aplikasi. Institusi keuangan dan telekomunikasi secara rutin menyewa konsultan keamanan untuk melakukan kegiatan '*penetration testing*'. Totalitas dalam pengelolaan siber di kedua provinsi ini memang belum dapat dikatakan maksimal. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya belum tertata dalam satu kesatuan sistem yang berorientasi kepada pelayanan publik. Pengelolaannya masih dilakukan terpisah-pisah oleh organisasi di daerah. Bahkan beberapa organisasi di daerah, harus mengikuti ketentuan tata kelola yang ditetapkan dari pusat, seperti yang terjadi di KPU Daerah dan Bawaslu. Walaupun ada juga SKPD yang belum melakukan mengelolaan pengamanan data melalui jaringan, karena pengamanan data masih dilakukan secara manual yang di-*print* dan diarsipkan pada arsip daerah.

Masih sangat kurangnya tenaga SDM yang memiliki kemampuan dan jumlahnya yang terbatas, menjadi salah faktor ancaman bagi maraknya serangan data dan informasi melalui siber. Kemampuan SDM dalam bidang siber ini diidentifikasikan ke dalam kemampuannya dalam melakukan analisis keamanan jaringan memetakan potensi ancaman keamanan, lalu memberikan rekomendasi untuk mitigasi terhadap potensi ancaman tersebut. Kemampuan berikutnya terkait dengan kemampuan untuk melakukan spesialisasi forensik untuk bisa mencari dan memetakan jejak-jejak yang ditinggalkan oleh pelaku, untuk bisa

melacak dan menemukan pelaku. Dan yang tidak kalah pentingnya terkait dengan kemampuan dalam hal *hacker* atau peretas, yaitu istilah yang diberikan kepada orang-orang yang memiliki kemampuan untuk melakukan tindakan eksploitasi terhadap sistem telematika melalui berbagai cara.

Kondisi yang terjadi pada dua daerah provinsi ini menunjukkan masalah siber belum dilakukan penataan yang pada akhirnya dapat berdampak pada upaya peningkatan pelayanan publik kepada masyarakat. Baru sebagian kecil saja, komponen dalam melakukan penataan siber tersedia di dua daerah ini. Perlu waktu yang cukup untuk melakukan penataan keamanan siber, agar bisa terpenuhi berdasarkan standar yang keamanan yang optimal. Keamanan siber yang optimal memang mempersyaratkan adanya kebijakan, alat, perlindungan keamanan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi dan aset pengguna.

Pada bidang tugas yang stategis seperti Kesbangpol, belum dilakukan upaya untuk melakukan keamanan jaringan data. Padahal data dan informasi yang dimilikinya masuk dalam kategori informasi yang bersifat rahasia yang hanya boleh diketahui oleh beberapa orang saja. Pemanfaatan teknologi informasi dalam rangka penyimpanan data dan informasi akan sangat membantu proses komunikasi yang bersifat terbatas ini untuk dikirim dan diterima oleh pihak yang dimaksud. Untuk itu setiap fase yang dilewati harus benar-benar dijamin keamanannya. Titik pengamanan dimaksud berawal dari pihak yang menyampaikan informasi, pengelolaan informasi, penerima informasi, dan penyimpanan informasi. Kesemua titik dimaksud memerlukan sistem keamanan, agar data dan informasi tersebut tetap berada dalam kondisi yang asli dan valid.

Tata kelola siber pada sistem pengamanan informasi yang dilakukan secara terpusat, seperti KPU dan Bawaslu memang memiliki kelebihan pada tataran implementasinya. Pengguna sistem informasi di daerah

tidak perlu lagi memikirkan bagaimana sistem pengamanan informasi dibangun dan dipelihara. Daerah hanya cukup menyediakan SDM yang memiliki kemampuan untuk menjalankan sistem keamanan dimaksud. Organisasi dan aset pengguna dalam *cyber security* termasuk perangkat yang terhubung komputasi, infrastruktur, aplikasi layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/ atau disimpan dalam lingkungan maya, dipersiapkan secara maksimal oleh pusat.

Meski demikian ancaman terhadap keamanan siber untuk tata kelola sistem keamanan informasi seperti ini juga perlu diwaspadai. Ketidakpuasan peserta pemilu maupun pemilukada di tingkat daerah, bisa menjadi ancaman serius bagi keamanan siber terpusat seperti ini. Potensi konflik di suatu wilayah baik yang disebabkan oleh masalah kepentingan atau masalah SARA, juga merupakan bentuk ancaman terhadap keamanan siber bagi interaksi penataan sistem informasi kepemiluan.

Masih belum optimalnya Pemda dalam melakukan tata kelola pengemanan siber, perlu segera dicarikan solusinya. Pemda perlu memastikan data dan informasi yang dikirimkan dari seluruh SKPD dapat berlangsung dengan aman dan cepat. Data dan informasi disampaikan melalui jaringan-jaringan komputer yang saling terkoneksi. SKPD terkoneksi dengan Diskominfo sebagai admin dari komunikasi di daerah yang juga bertugas untuk membangun sistem keamanannya. Tata kelola sistem keamanan siber perlu dibangun mulai dari informasi tersebut dihasilkan di masing-masing SKPD, informasi di sampaikan SKPD kepada Diskominfo, pelayanan informasi publik kepada masyarakat, dan pengamanan sistem penyimpanan informasi tersebut. Pengamanan juga perlu dilakukan dalam rangka melaksanakan aktivitas koneksi jaringan baik dengan pemerintah pusat maupun dengan pemerintah daerah di wilayah kabupaten/kota.

Pada konteks pelayanan publik, sistem keamanan dilakukan tidak hanya pada informasi yang masuk dalam kategori informasi yang dikecualikan, namun juga kepada informasi publik. Pada intinya,

keamanan siber ditujukan kepada upaya untuk tetap menjaga otentisitas atas informasi yang dimilikinya. Sedangkan masalah kerahasiaan hanyalah merupakan bagian terkecil yang hanya berkaitan dengan jenis informasi dikecualikan.

Untuk itu Pemda perlu membangun sistem keamanan jaringan yang terhubung ke internet dengan perencanaan yang baik, dalam rangka melindungi investasi dan sumber daya di dalam jaringan tersebut. Pemda perlu mengetahui secara tapat tingkat ancaman yang harus diatasinya. Kalau ancaman berasal dari kemungkinan untuk terjadinya konflik di masyarakat, maka Pemda perlu membangun sistem pengamanan yang mampu mengatasi kemungkinan pengerusakan sistem yang dilakukan oleh pihak yang berkonflik, termasuk juga menghadapi atau menghindari resiko yang akan dihadapi.

Pemda Sultra dan Pemda Kalbar memang belum memiliki kebijakan yang dimaksudkan untuk mengatasi ancaman terhadap jaringan. Pada kebijakan keamanan jaringan perlu menyediakan kerangka-kerangka untuk membuat keputusan yang spesifik. Kebijakan keamanan juga merupakan dasar untuk mengembangkan petunjuk pemrograman yang aman untuk diiukti user maupun bagi administrator sistem. Faktor-faktor yang berpengaruh terhadap keberhasilan kebijakan keamanan antara lain:

1. Komitmen dari pengelola jaringan
2. Dukungan teknologi untuk menerapkan kebijakan keamanan tersebut
3. Keefektifan penyebaran kebijakan tersebut
4. Kesadaran semua user jaringan terhadap keamanan jaringan.[36]

Beda halnya dengan instansi vertikal dengan pusat yang telah memiliki sistem pengamanan pada jaringan *website*-nya. Tidak ada lagi

---

[36] Onno W Purbo dan Tony Wiharjito, *Keamanan Jaringan Internet*, Jakarta: Alex Media Komputindo, 2002, h. 6

persoalan komitmen, dukungan IT, keefektifan kerja siber. Semuanya telah terbangun dari pusat, di mana daerah hanya ditugaskan untuk menjalankan dan melaporkan bila mana ditemui adanya ancaman yang menderanya. Daerah hanya cukup memberikan laporan terhadap KPU maupun Bawaslu Pusat sudah membuat sistem pengamanan yang berlaku untuk seluruh Indonesia.

Enkripsi dapat digunakan untuk melindungi data baik pada saat ditransmisikan maupun pada saat disimpan. Keuntungan menggunakan enkripsi adalah bila metode lain untuk melindungi data berhasil dirusak oleh pihak lain, maka data yang dirusak tersebut tidak lagi memiliki arti pada perusak tersebut.[37]

Upaya Pemda untuk membangun sistem keamanan siber di wilayahnya, tidak boleh dilakukan hanya untuk mengatasi suatu masalah atau dilakukan untuk waktu yang besifat sementara saja. Tata kelola keamanan sistem harus dipandang sebagai sebuah aktivias yang berjalan secara kontinu dan terus dimutakhirkan. Untuk itu keberadaaan SDM yang memiliki kompetensi khusus sangat diperlukan untuk menjamin sistem dapat tetap berjalan dengan aman.

Pemda perlu benar-benar menyadari, bahwa sistem keamanan siber tidak hanya terkait dengan keamanan teknologi informasinya saja, namun juga melingkupi pelaku dan proses pengamanannya. Kerja sistem keamanan siber senatiasa dilandasi dengan adanya risiko terhadap sistem pengamanan tersebut.

## E. Penutup

Tata kelola sistem keamanan siber di daerah pada hakekatnya dimaksudkan untuk membangun sistem keamanan informasi secara terpadu di daerah tersebut. Meskipun demikian pada penelitian ini, didapatkan fakta bahwa di Pemda Provinsi Sultra dan Pemda Provinsi Kalbar, upaya untuk

[37] Ibid., 97.

melakukan penataan keamanan siber belum dapat dikatakan optimal. Hal ini disebabkan organisasi perangkat daerah yang secara khusus dibentuk untuk ini, baru saja mengalamai perubahan struktur dan tugas pokoknya.

Hal ini menyebabkan SKPD yang khusus menangani bidang ini belum bisa melakukan tugasnya secara maksimal, meskipun landasan kerja yang disusun dalam bentuk rencana kerja strategis sudah disusun. Selain itu kurangnya SDM serta infrastruktur penunjang teknologi pengamanan siber, juga belum dipenuhi secara maksimal. Kondisi-kondisi inilah yang menyebabkan penanganan keamanan siber di daerah masih sering dilakukan secara sektoral di masing-masing institusi.

Pada hakikatnya tata kelola keamanan siber ditujukan untuk membangun keamanan sistem informasi baik di tingkat daerah, maupun saat berintegrasi dengan sistem di tingkat nasional. Keamanan Sistem Informasi Internal bertujuan untuk menjaga, *pertama* **kerahasiaan**. Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi. *Kedua,* **ketersediaan**. Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. *Ketiga* **Integritas**. Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Untuk itu perangkat organisasi yang bertugas menangani keamanan siber di daerah perlu segera melakukan penataan keamanan siber dengan melengkapi beberapa hal yang masih dinilai kurang seperti, menambah SDM yang kompeten, meningkatkan anggaran yang diperuntukan pada pembangunan sistem keamanan siber, serta menyediakan perangkat teknologi yang modern. Hal lain yang diperlukan yaitu pada skala nasional perlu segera dibentuk peraturan terkait dengan sistem keamanan siber yang bisa dijadikan dasar hukum bagi pengelolaan siber di tingkat nasional dan dasar pembentuk hukum di tingkat daerah.

# DAFTAR PUSTAKA

Ahmad Muntaha, *Berpisah-Menyatu dan Berbagi Ruang Rindu di Media Baru: Pengalaman Komunikasi Online Tiga Nettie-Family Indonesia*, dalam Heri Budianto (ed), *Ilmu Komunikasi Sekarang dan Tantangan Masa Depan*, Jakarta: Penerbit Kencana, 2013.

Edmon Makarim, *Pengantar Hukum telematika, Suatu Kompilasi Kajian*, Jakarta, Penerbit PT Raja Grafindo Persada.

Kementerian Komunikasi Informatika RI, Buku Putih 2011 Komunikasi dan Informatika Indonesia, 2011.

Onno W Purbo dan Tony Wiharjito, *Keamanan Jaringan Internet*, Jakarta, Penerbit Alex Media Komputindo, 2002.

Sigid Suseno, *Yuridiksi Tindak Pidana Siber*, Bandung, Penerbit PT Refika Aditama, 2012.

Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik.

Instruksi Presiden Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government.

*Kemenpan-RB pantau implementasi "e-government" instansi daerah*, http://www.antaranews.com/berita/508938/kemenpan-rb-pantau-implementasi-e-government-instansi-daerah, diakses tanggal 23-5-2016

*Menpan RB: E-Government Korea Paling Bagus di Dunia*, http://news.okezone.com/read/2016/03/02/337/1325739/menpan-rb-e-government-korea-paling-bagus-di-dunia, diakses tanggal 25-5-2016

The Unknown Unknown Pada Cyber Security, https://kriptologi.com/2017/05/16/the-unknown-unknown-pada-cyber-security/, diakses tanggal 3-10-2017

Disari dari Sekilas Tentang *Cyber Crime, Cyber Security* dan *Cyber War, https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war, diakses tanggal 22-9-2017*

Rudy Agus Gemilang Gultom, Membangun Tata Kelola Informasi dan Keamanan Informasi Pemerintahan Daerah di Era Globalisasi Informasi dalam rangka menjaga keutuhan dan kedaulatan NKRI", disampaikan pada FGD Penelitian Tata Kelola Cyber security pada Pemerintahan Daerah, Puslit BKD, Jakarta, 17 Maret 2017.

Makalah Eka Suaib, Lektor Kepala UHO Kendari, "Menimbang Pemanfaatan Media Sosial Dalam *E-Democracy",* FGD Cyber Security, Kendari, 7 April 2017

Makalah Sartono, Dosen Adminstrasi Publik UHO, "Penggunaan Media Sosial Dalam Tata Kelola Pemerintahan dan Kampanye Pemilu/ Pemilukada Di Provinsi Sulawesi Tenggara", FGD 7-4-2017

Makalah Djumadi, Ph.D dan Dr Martoyo, Dosen dan Direktur Pasca Sarjana Untan Paontianak, dalam FGD tanggal 11-8-2017

# BAGIAN 3
# PERAN *CYBER SECURITY* DALAM MENCEGAH KONFLIK POLITIK MASYARAKAT DI DAERAH

*Aryojati Ardipandanto*
*Peneliti Kepakaran Ilmu Politik*
*Pusat Penelitian Badan Keahlian DPR RI*
*E-mail: aryojati.ardipandanto@gmail.com*

## A. Perkembangan Media Sosial dalam Demokrasi di Indonesia

Perkembangan media sosial di Indonesia, khususnya, tentunya memberikan warna dan dinamika yang beragam dalam kehidupan demokrasi. Menurut Andreas Kaplan dan Michael Haenlein, media sosial merupakan sebuah kelompok aplikasi berbasis internet yang membangun di atas dasar ideologi dan tekonologi *web 2.0* yang memungkinkan penciptaan dan pertukaran *user-generated content.* Secara sederhananya media sosial ini merupakan ruang di mana antar-pengguna dapat saling berinteraksi secara langsung meskipun dalam ruang dan waktu yang berbeda. Ruang interaksi yang mampu dibangun oleh media sosial tersebut lantas dikembangkan oleh banyak para politikus di dunia sebagai ruang berdialog dengan konstituen, termasuk juga dengan para politikus di Indonesia. Sebut saja bapak Ganjar Pranowo (Gubernur Jawa Tengah) dan bapak Ridwan Kamil (Walikota Bandung), keduanya seringkali memakai akun media sosial untuk berinteraksi dengan masyarakatnya. Interaksi tersebut sengaja dibuka oleh keduanya untuk menampung aspirasi dari masyarakat.

Hal tersebut sangat masuk akal karena media sosial kini menjadi salah satu *platform* paling efektif dalam membangun hubungan politik antara pemimpin dengan masyarakat. Hal ini salah satunya merujuk pada data dari Intrans (2016) yang mengatakan bahwa terjadi kenaikan 10% bagi netizen aktif media sosial, yang sebelumnya hanya 71,9 juta jiwa pada tahun 2015 kini sudah mencapai 88 juta jiwa. Kenaikan tersebut juga dipengaruhi oleh kenaikan konsumen *smartphone* yang sudah mencapai 326,3 juta jiwa.

Dengan demikian, dapat dikatakan bahwa media sosial menjadi kebutuhan yang esensial yang harus dipenuhi di masyarakat. Derasnya arus informasi yang beredar di media sosial dan mudahnya sebuah isu berkembang disana (viral) secara tidak langsung telah membentuk perilaku di masyarakat. Masyarakat menjadi mudah peka dan sadar terhadap isu-isu sensitif yang mampu menjadi viral.

Salah satu isu yang pernah menjadi viral adalah tagar *#ShameOnYouSBY* pada September 2014. Isu yang dilatarbelakangi berubahnya Undang-Undang Pemilihan Kepala Daerah dari langsung menjadi tidak langsung sempat menjadi isu panas yang bergulir di media sosial.

Dari peristiwa tersebut dapat disimpulkan bahwa masyarakat saat ini melalui media sosial menjadi lebih peka dan sadar terhadap isu-isu yang beredar. Hal ini kemudian dimanfaatkan oleh para politikus termasuk para pejabat daerah dan pejabat negara untuk membangun interaksi guna mewadahi aspirasi masyarakat. Arena berdialog yang efektif dan efisien pun terwujud sebagai bentuk demokrasi baru.

Media sosial seperti *Facebook, Twitter, Instagram,* dan lain-lain memang dapat membuat masyarakat semakin "melek" politik dan selalu dapat mengikuti perkembangan politik yang ada. Tetapi di sisi lain, kekuatan media sosial dapat dimanfaatkan untuk hal-hal berbahaya oleh pihak-pihak yang tidak bertanggung-jawab, terutama dalam momen menjelang Pemilu atau Pilkada. Hal yang berbahaya tersebut antara lain adalah bahwa media sosial dapat digunakan untuk

menyebarkan *HOAX* dalam perang kampanye di dunia maya. Bila masyarakat Indonesia tidak dibekali dengan kesadaran tentang pentingnya menggunakan media sosial dengan bijak dan hati-hati, tentunya ini akan sangat berbahaya kestabilan kehidupan bermasyarakat, berbangsa, dan bernegara. Hal ini dikarenakan *HOAX* yang disebarkan di media sosial berdampak luas dan menimbulkan potensi konflik yang akibatnya bisa sangat menakutkan.

Dalam memandang kondisi tersebut, tentunya logika kita akan mengarah pada pentingnya suatu sistem pengamanan arus informasi di media sosial yang dilakukan oleh lembaga atau badan khusus yang menangani masalah *cyber*. Dengan kata lain, isu *cyber security* menjadi titik sentral untuk mengimbangi perkembangan media sosial sebagai sarana interaksi sosial masyarakat di dunia maya, terlebih lagi pada masa-masa Pemilu atau Pilkada.

*Cyber Security* yang dilaksanakan dengan profesional setidaknya akan menangkal dampak negatif dari penggunaan media sosial yang diarahkan pada timbulnya konflik oleh pihak-pihak tertentu yang memang ingin mengacaukan stabilitas politik negara. Hal itu bisa diimplementasikan dengan dukungan terhadap penegakan aturan-aturan perundang-undangan terkait Informasi Publik, tentang Komunikasi, dan tentang aturan-aturan pelaksanaan Pemilu dan Pilkada. *Cyber Security* yang lemah akan menyebabkan informasi-informasi yang bersifat mengadu domba masyarakat akan "tumbuh secara liar", tak terkendali, dan sulit ditangani secara hukum.

Kita dapat melihat fenomena "perang kampanye" di media sosial setiap menjelang Pemilu atau Pilkada. Kita dapat melihat bahwa sebagian kalangan masyarakat semakin berani dan seakan-akan tidak takut akan hukum ketika beropini dan menjelek-jelekkan tokoh politik yang tidak disukainya dan memprovokasi masyarakat untuk tidak menyukainya pula. Hal itu semakin membahayakan di mana kondisi masyarakatnya masih kurang terdidik dan cenderung langsung "menelan mentah-mentah" informasi-informasi yang bertebaran di

media sosial tanpa melalui proses *filter* terlebih dahulu. Tentu saja kondisi seperti ini akan menimbulkan konflik sosial yang bila tidak diantisipasi, akan bersifat luas dan *massive.*

Tampaknya memang media sosial benar-benar dimanfaatkan oleh masyarakat Indonesia untuk dapat menyalurkan opini-opini politiknya, baik yang bersifat bertanggung jawab maupun yang bersifat *black campaign.* Hal ini bisa jadi sebagian karena adanya kekecewaan masyarakat terhadap media-media massa konvensional yang seringkali dinilai berpihak pada kandidat-kandidat tertentu pada momen Pemilu atau Pilkada. Beberapa fakta yang terjadi di Indonesia dapat kita lihat. Pada tahun 2014 pernah dilakukan penelitian tentang keberpihakan televisi menjelang Pemilu Presiden 2014. Penelitian ini dicantumkan dalam Buku "Independensi Televisi Menjelang Pemilu Presiden 2014".[1] Inti hasil Penelitian tersebut adalah bahwa media massa di Indonesia menjadi partisan ketika Pemilihan Umum. Media yang semula kerap disebut sebagai pilar keempat demokrasi seolah-olah lenyap pada Pemilihan Umum 2014 lalu. Dengan begitu, peran media yang mulanya menginformasikan, mengedukasi, wadah diskursus, dan institusi advokasi demokrasi menjadi hilang dan yang terjadi adalah realitas dikonstruksi sedemikian rupa hingga menjadi informasi yang manipulatif.

Hilangnya fungsi media sebagai pilar keempat demokrasi tersebut lantas digantikan dengan keberadaan media sosial. Meskipun media sosial tetap memiliki ketergantungan dengan media massa, namun setidaknya fungsi-fungsi media massa dapat dilaksanakan. Seperti yang diungkapkan oleh Habermas mengenai ruang publik, di mana ruang publik didefinisikan sebagai ruang mandiri yang terpisah dari pasar (*market*) dan negara (*state*). Media sosial hadir sebagai ruang publik baru di tengah minimnya "ruang publik" yang memberikan wadah untuk warga berdialog dan membangun opini.

---

[1] Adhnia Adzkia, Heychael, Muhamad. 2014. *Independensi Televisi Menjelang Pemilu Presiden 2014.* Jakarta (Remotivi)

Konstruksi realitas yang sifatnya manipulatif akibat media yang partisan dapat di-dialog-kan sedemikian rupa oleh masyarakat di media sosial. Segala bentuk informasi yang semula sifatnya jauh dari kredibel dapat diperdebatkan keabsahannya dalam "ruang publik" virtual (media sosial). Sehingga pada akhirnya media sosial pada momen ini hadir sebagai solusi di tengah kekecewaan masyarakat terhadap media massa yang partisan dan manipulatif.

Namun sayangnya, penyaluran aspirasi masyarakat ke media sosial itu justru dalam sebagian kasus membuat praktek demokrasi menjadi "kebablasan". Seringkali sebagian masyarakat terlalu emosi dalam menuangkan opini-opininya, khususnya dalam konteks politik. Akibatnya, faktor etika dalam berkomunikasi menjadi terabaikan dan adu argumentasi menjadi terkesan kurang beradab. Pembuatan meme-meme yang mengarah pada tokoh atau partai politik tertentu seringkali tampak vulgar dan membuat yang melihatnya seringkali "geleng-geleng kepala" karena timbul pertanyaan dalam diri mereka, apakah para pembuat meme-meme tersebut tidak takut pada konsekuensi hukum terkait pencemaran nama baik dan pelanggaran atas UU ITE?

Maka tidak heran bahwa Presiden Jokowi pernah mengatakan penyesalannya akan praktik demokrasi yang sudah "bablas". Menurut beliau, demokrasi yang bablas ini telah membuka peluang terjadinya artikulasi politik yang ekstrem seperti liberalisme, fundamentalisme, sektarianisme, radikalisme, dan terorisme. Presiden juga menyebut bahwa penyimpangan praktik demokrasi itu telah mengambil bentuk nyata dalam bentuk politisasi SARA. Jika terus menerus dibiarkan, maka praktik ini akan menjurus pada perpecahan bangsa Indonesia.[2]

---

[2] "Wiranto : Demokrasi Kebablasan Bisa Picu HOAX": https://kumparan.com/@kumparannews/wiranto-demokrasi-kebablasan-bisa-picu-hoax : diakses 20 Mei 2018.

## B. Kasus *HOAX*

Contoh kasus *HOAX* yang sangat berbahaya melalui media sosial adalah penyebaran ujaran kebencian, fitnah, dan berita bohong oleh Kelompok Saracen dan *Muslim Cyber Army* (MCA). MCA mirip dengan kelompok Saracen dalam konteks membuat berita hoax yang kemudian diviralkan. Namun, perbedaannya, Saracen terbukti menerima pesanan dan mendapat bayaran. Saracen juga memiliki struktur organisasi, seperti ketua, sekretaris, dan koordinator daerah. Adapun MCA, merupakan organisasi tanpa bentuk di dunia maya. Anggota MCA bisa mencapai ribuan karena komunitas tersebut sangat cair dan terbuka sehingga orang dengan mudah menjadi anggota atau *follower*. Jumlah *follower*-nya yang banyak kemudian mengerucut pada tim inti yang disebut *Family* MCA. MCA Indonesia ini menginduk ke *United* MCA, jaringan internasional yang telah berhasil memecah belah Suriah dan Irak.[3]

Kasus HOAX lain di daerah misalnya ada sebanyak 20 kasus penyerangan ulama (terutama oleh PKI) muncul dan tersebar di media sosial. Tapi dari sekian banyak kasus itu, hanya dua yang benar-benar terjadi. Sisanya, sebanyak 18 kasus, adalah berita palsu. 18 belas berita palsu itu dapat dikategorikan menjadi tiga jenis. Pertama, berita palsu yang mendompleng kejadian kriminal biasa. Contohnya, berita penyerangan ulama oleh orang sakit jiwa di Bogor dan pembunuhan muazin di Majalengka. Kedua, berita palsu yang diciptakan oleh pengunggah. Contoh, perusakan masjid oleh pengidap sakit jiwa di Bandung dan pengeroyokan anak santri oleh enam orang pengidap sakit jiwa di Garut. Ketiga, berita palsu yang sama sekali tidak ada kejadiannya, tapi mereka menciptakan peristiwanya. Contoh, pengidap sakit jiwa yang masuk ke sebuah pondok pesantren di Cimahi, lalu membacok orang. Padahal, tidak ada kejadian apapun di Cimahi,

---

[3] "Polisi : Berita HOAX *Muslim Cyber Army* 'Bermuatan Politik'": http://www.bbc.com/indonesia/indonesia-43221362 : diakses 1 Juni 2018.

sementara fotonya yang juga diunggah diketahui sumbernya dari sebuah kejadian di luar negeri.[4]

Polisi menyatakan bahwa fenomena maraknya penyebaran informasi bohong atau *HOAX* yang bernuansa suku, agama, ras, dan antargolongan atau SARA, sebenarnya murni tindak kejahatan. Namun, fenomena itu dilatarbelakangi pertentangan keras seputar Pilkada DKI Jakarta pada 2017. Titik awalnya adalah dari Pilkada DKI. Hal itu bermula dari polemik pernyataan Basuki Tjahaja Purnama alias Ahok, calon gubernur Jakarta waktu itu, yang dianggap menodai agama Islam. Dari situ berkembang pesat akun-akun penyebar fitnah yang bernuansa agama.[5]

Contoh kejadian akibat HOAX selanjutnya adalah terkait isu penyebaran ajaran komunisme oleh PKI yang dikatakan kembali muncul. Salah satu isu yang disebarkan melalui media sosial adalah bahwa Yayasan Lembaga Bantuan Hukum Indonesia (YLBHI) melakukan kegiatan-kegiatan yang disusupi oleh PKI. Massa yang terprovokasi mendatangi Kantor YLBHI pada dini hari tanggal 17 September 2017, menuntut agar YLBHI tidak mengakomodasi acara-acara yang mengandung unsur misi komunisme PKI. Pihak Polres Jakarta Pusat ketika itu datang dan mengklarifikasi, memeriksa, dan mengawasi langsung ke dalam gedung, tapi bukti-bukti yang menunjukkan acara tersebut berkaitan dengan PKI, tak ditemukan sedikitpun. Meski pihaknya sudah menjelaskan, tapi massa memilih tidak percaya dan malah melawan aparat. Akibatnya terjadi bentrok antara polisi dan massa. Sekitar pukul 02.00 WIB, massa baru bisa dipukul mundur setelah polisi menyemprot *water canon* dan gas air mata. Sementara di dalam YLBHI sendiri tak kalah mencekam. Banyak tamu acara yang histeris, panik, bahkan sampai pingsan. Masalahnya

---

[4] *Ibid.*

[5] Penjelasan Direktur Tindak Pidana Siber Bareskrim Polri, Brigadir Jenderal Polisi Fadil Imran, dalam program *Indonesia Lawyers Club tvOne* pada Selasa malam, 6 Maret 2018.

orang-orang yang ada di sana nggak cuma pemuda-pemuda saja, melainkan juga para lansia.[6]

Tingkat pemahaman sebagian masyarakat yang belum baik tentang pentingnya menggunakan media sosial secara bijak menyebabkan bahaya yang serius bila dihadapkan dengan maraknya HOAX. Lebih berbahaya lagi karena kecenderungan sebagian orang yang justru merasa paling tertarik kepada berita-berita yang aneh, unik, dan sensasional. Bila kondisi ini dipicu dengan stimulus konflik yang bernuansa SARA, terutama agama, maka daya picu konflik horizontalnya sangat besar.

## C. Sikap Pemerintah terhadap Dinamika Media Sosial

Akhir-akhir ini, Presiden Joko Widodo semakin serius dalam menangani masalah penyebar-luasan kebencian dan pemicu konflik melalui media sosial. Sebagai upaya mengantisipasi bertebarannya berita bohong, Presiden meminta agar Staf Kepresidenan memiliki Satuan Tugas (Satgas) Media Sosial. Satgas ini bertugas mengantisipasi propaganda dan berita bohong di media sosial. Pihak Presiden juga telah menyiapkan langkah perbaikan komunikasi publik. Termasuk cara untuk menampung dan merespon keluhan publik. Keluhan dari publik akan disampaikan kepada kementerian dan lembaga terkait agar segera ditindaklanjuti. Disampaikan bahwa komunikasi Lembaga Pemerintah harus berubah. Bagaimana merespon keluhan, pendapat masyarakat itu harus dilakukan terobosan-terobosan, sehingga masyarakat menjadi lebih bisa memahami dan menerima apa yang dikeluhkan dan bisa ditangani keluhan itu.[7]

---

[6] "*HOAX* Kian Merajalela Memecah Belah Negeri Ini : Beberapa Kasus Hoax Bahkan Sampai Makan Korban" : https://www.hipwee.com/feature/ : diakses 7 Mei 2018.

[7] "Demokrasi Kebablasan Dimaksud Jokowi Terkait Banyak Berita HOAX" : https://www.merdeka.com/peristiwa/demokrasi-kebablasan-dimaksud-jokowi-terkait-banyak-berita-hoax.html : diakses 20 Mei 2018.

Pihak internal kepresidenan juga menyarankan agar humas-humas kementerian bersinergi dalam merespons gagasan dan aspirasi masyarakat. Di lembaga pemerintahan, masing-masing humasnya juga melakukan sinergi bagaimana merespons secara cepat. Di tiap kementerian, Bagian Humas akan melakukan klarifikasi jika ada berita atau isu bohong di jagad dunia maya. Selain itu, Kemenkominfo juga akan memverifikasi dan memberikan klarifikasi melalui *website* Jaringan Pemberitaan Pemerintah (JPP).[8]

Hal tersebut memang sudah seharusnya dilakukan oleh Pemerintah, karena tampaknya regulasi atau peraturan perundang-undangan yang ada belum optimal "menjerat" para pelaku HOAX dengan cepat. UU ITE belum optimal terimplementasikan dalam kasus-kasus HOAX di media sosial. Demikian pula dalam konteks pelaksanaan Pemilu dan Pilkada, seringkali Penyelenggara Pemilu tidak bisa memberikan tindakan hukum yang jelas karena dasar hukumnya belum jelas dan tegas.

Contoh masalah yang dihadapi dialami oleh POLRI. Pada awal-awal tahun 2017, Badan Reserse Kriminal Polri (Bareskrim Polri) kesulitan menyelidiki dan menindak penyebar ujaran kebencian (*hate speech*) di *Facebook*. Perbedaan regulasi menjadi tantangan POLRI dalam kaitannya dengan pemilik *Facebook* di Amerika Serikat. Hal ini disampaikan oleh Kepala Subdit II Direktorat Siber Bareskrim Polri Kombes Pol Himawan Bayu Aji. Seringkali terjadi, Polisi telah mendeteksi sejumlah pemilik akun *Facebook* yang membagikan ujaran kebencian, namun kesulitan meminta informasi mengenai pelaku ke layanan jejaring sosial yang berkantor pusat di California, Amerika Serikat itu. Pihak *Facebook* tidak akan memberikan data karena di AS *hate speech* adalah hal yang lumrah.[9]

---

[8] *Ibid.*

[9] "Penyebar Kebencian Sulit Ditindak Karena *Facebook* Tak Mau Bantu": https://koransulindo.com/penyebar-kebencian-sulit-ditindak-karena-facebook-tak-mau-bantu/ : diakses 22 Mei 2018.

Karena itu, Polisi menangani kasus ujaran kebencian di *Facebook* dengan pemulihan keadilan, meminta pelaku meminta maaf, menghapus konten, dan meminta mereka menerapkan etika penggunaan teknologi informasi di dunia maya. Ketika pelaku men-*share*, belum menjadi viral, Polisi akan melakukan *restore justice*, meminta pelaku melakukan permintaan maaf, menghapus konten, lalu meminta pelaku mensosialisasikannya ke komunitasnya.

Penegakan hukum saja dalam kasus seperti itu tidak efektif 100%. Ketika Polisi menangkap satu, muncul tiga pelaku. Polisi menangkap tiga, muncul sepuluh pelaku. Upaya pemulihan keadilan semacam itu dilakukan karena personel kepolisian yang menangani tindak pidana itu masih terbatas. Kepolisian juga menggandeng sejumlah komunitas siber untuk meluruskan berita-berita bohong yang beredar di media sosial.

Hal ini merupakan masalah yang serius karena konten berisi ujaran kebencian merupakan jenis tindak pidana yang paling banyak diadukan masyarakat ke polisi pada 2016. Pada 2015, jumlah laporan yang masuk berkaitan dengan ujaran kebencian sebanyak 671 laporan. Tahun 2016, jumlah laporan mengenai hal itu juga tinggi. Tertinggi pada 2016 itu adalah *hate speech* terkait SARA. Ujaran kebencian itu meliputi pencemaran nama baik, pelecehan, fitnah, provokasi, dan ancaman. Dari besaran laporan itu, yang ditangani per Maret 2017 baru 199 kasus. Banyaknya laporan tersebut, khususnya untuk ujaran kebencian, tak terlepas dari maraknya berita *HOAX*. Sebuah konten biasanya dibuat mulanya untuk iseng. Pembuatnya tak menyadari bahwa ada pasal pidana yang bisa menjerat mereka. Cara yang dilakukan untuk menindaklanjuti kasus-kasus tersebut salah satunya dengan menutup akun yang menyebarkan *HOAX*.

Pada akhir 2016, data yang dipaparkan oleh Kementerian Komunikasi dan Informatika menyebut ada sebanyak 800 ribu situs di Indonesia yang terindikasi sebagai penyebar berita palsu dan ujaran kebencian (*hate speech*). Untuk situs, Menkominfo Rudiantara mengatakan pemerintah bisa langsung melakukan pemblokiran.

Namun untuk media sosial, kerjasama dengan penyedia layanannya harus dilakukan terlebih dahulu. Khusus ujaran kebencian yang tersebar di media sosial, konten yang ada di dalamnya menjadi prioritas. Siapapun pihak yang menyebarkan itu lebih dulu maka dialah yang akan diincar paling awal.

Sementara cara untuk mencari pemilik akun media sosial yang mempublikasikan ujaran kebencian atau berita hoax bisa berdasarkan laporan warga ataupun pengawasan. Jika ada akun media sosial yang tertangkap atau ketahuan menyebarkan berita *hoax*, maka bisa langsung mengambil tindakan tanpa harus ada pelaporan. Dengan kata lain, situs yang berindikasi menyebarkan ujaran kebencian dan *hoax* akan diblokir, sedangkan pada medium media sosial akun-akun yang bertanggung jawab tersebut akan ditutup. Lebih lanjut, jika ada akun media sosial yang sudah masuk ranah hukum maka urusannya akan dipegang langsung oleh penegak hukum terkait.[10]

## D. UU ITE: Apakah Sudah Efektif?

Kian maraknya ujaran kebencian di media sosial belum optimal diikuti oleh regulasi dan kesiapan aparat penegak hukum. Advokat Todung Mulya Lubis mengungkapkan, banyak sekali potensi ujaran kebencian di media sosial yang tidak ditindaklanjuti. Untuk itu, ia menyampaikan perlunya pembenahan regulasi. Pendapat lainnya adalah dari Direktur Imparsial, Al Araf, yang menyampaikan bahwa aturan di Indonesia seperti KUHP dan UU ITE masih belum menjelaskan secara rigid menyangkut ujaran kebencian. Dengan begitu, aturan tersebut menjadi multitafsir yang kemudian mengakibatkan penerapannya sangat sulit.[11]

---

[10] "Ada 800 Ribu Situs Penyebar HOAX di Indonesia" : https://www.cnnindonesia.com/teknologi/20161229170130-185-182956/ada-800-ribu-situs-penyebar-hoax-di-indonesia: diakses 5 Mei 2018.

[11] "Perlu Pembenahan Regulasi untuk Atasi Ujaran Kebencian: http://mediaindonesia.com/read/detail/94190-perlu-pembenahan-regulasi-untuk-atasi-ujaran-kebencian : diakses 4 Juni 2018.

Pasal 28 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") menyatakan, "Setiap orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."[12] Perbuatan yang diatur dalam Pasal 28 ayat (1) UU ITE merupakan salah satu perbuatan yang dilarang dalam UU ITE. UU ITE tidak menjelaskan apa yang dimaksud dengan "berita bohong dan menyesatkan".

Terkait dengan rumusan Pasal 28 ayat (1) UU ITE yang menggunakan frasa "menyebarkan berita bohong", sebenarnya terdapat ketentuan serupa dalam Pasal 390 Kitab Undang-Undang Hukum Pidana ("KUHP") walaupun dengan rumusan yang sedikit berbeda yaitu digunakannya frasa "menyiarkan kabar bohong".[13] Menurut buku Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal yang ditulis oleh R. Soesilo, terdakwa hanya dapat dihukum dengan Pasal 390 KUHP, apabila ternyata bahwa kabar yang disiarkan itu adalah kabar bohong. Yang dipandang sebagai kabar bohong, tidak saja memberitahukan suatu kabar yang kosong, akan tetapi juga menceritakan secara tidak betul tentang suatu kejadian.[14] Melihat hal tersebut, bisa dikatakan bahwa penjelasan ini berlaku juga bagi Pasal 28 ayat (1) UU ITE. Suatu berita yang menceritakan secara tidak betul tentang suatu kejadian adalah termasuk juga berita bohong.

Selanjutnya, dari sisi kriminalitas, Direktur *Cyber Crime* Mabes Polri Komisaris Besar Fadil Imran mengakui, bahwa persoalan yang ada di ruang sosial masyarakat saat ini sudah masuk ke dalam ruang-ruang siber. Laporan yang masuk mulai dari fitnah maupun pencemaran nama baik biasanya lebih kepada hubungan personal,

---

[12] UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[13] KUHP.

[14] Soesilo, R. 1991. Kitab Undang-Undang Hukum Pidana (KUHP) : Serta Komentar-Komentarnya Lengkap Pasal demi Pasal : Bogor : Politeia Bogor. Hal.269.

misalnya antarteman atau karyawan dengan atasan. Lebih lanjut dikatakan pula bahwa, sumber daya manusia, alat, dan peraturan masih menjadi kendala. Terkait peraturan, perlu ada batasan yang lebih rinci mengenai ujaran kebencian. Pihak Polri menyampaikan bahwa pihaknya akan terus mempelajari hal-hal mana saja yang merupakan ujaran kebencian dan mana yang bukan.[15]

Isu *hoax* (kabar palsu) yang beredar melalui media elektronik khususnya di media sosial memang sangat gencar, khususnya menjelang saat-saat Pilkada dan Pemilu. Selama ini upaya Kepolisian RI memburu penyebar isu *hoax* menggunakan UU ITE 2008 yang disempurnakan pada tahun 2016. Dalam ketentuan umum UU ITE, kata "menyebarkan" lebih dapat dimengerti sebagai pelaku pertama yang mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi. Intinya, pelaku dalam hal ini adalah orang atau pihak yang pertama sekali memproduksi informasi. Mengolah dari bukan informasi menjadi informasi. Kalau hanya untuk pelaku pertama dikenakan pasal ini, maka jelas UU ITE sangat lemah.

Karena pasal-pasal UU ITE sangat lemah, maka pola kejahatan penyebaran informasi bohong pun dapat didesain sedemikian rupa. Dalam konteks *Proxy War*, tumbal disiapkan yakni pelaku pertama. Dan itu sah-sah saja. Setelah pelaku pertama memproduksi informasi, pelaku-pelaku berikutnya dengan sengaja atau tidak sengaja mengeroyok "tombol *share*" sehingga orang-orang yang tidak tahu menjadi tahu. Senjata yang telah terbukti mampu memecah-belah bangsa Indonesia adalah *"devide et impera"*. Ini telah terbukti memampukan Belanda menjajah Indonesia selama 350 tahun. Kemudahan rakyat Indonesia dihasut sudah diketahui oleh dunia sebelum kita-kita yang sedang membaca ini lahir. Oleh karena itu, kita pun tidak tahu kalau kelemahan ini dimanfaatkan untuk menghancurkan kita.

---

[15] http://mediaindonesia.com/read/detail/94190-perlu-pembenahan-regulasi-untuk-atasi-ujaran-kebencian. *Opcit.*

## E. *Cyber Security* di Indonesia

Sebenarnya bagaimana posisi *Cyber Security* di Indonesia saat ini? Berdasarkan laporan *The Global Cybersecurity Index* 2017 yang dirilis oleh UN *International Telecommunication Union* (ITU), Indonesia digambarkan masih lemah *Cyber Security*-nya. Posisi Indonesia berada di peringkat ke 70 dari 195 negara dengan skor 0,424 dalam hal keamanan siber. Menurut Menteri Komunikasi dan Informatika Rudiantara, posisi keamanan siber Indonesia hampir serupa dengan negara-negara di Amerika Selatan, seperti Brasil. Indonesia masuk peringkat 10 besar negara yang terkena serangan siber setiap saat.[16]

Serangan siber di Indonesia memang cukup luar biasa. Data dari *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) menunjukkan bahwa sejak bulan Januari hingga Juli 2017 saja, sebagai contoh, telah terjadi 177,3 juta serangan siber terhadap Indonesia, di mana serangan itu biasanya berupa *fraud* dan *malware*. Ini berarti kurang lebih ada 836.200 serangan siber terjadi setiap harinya. Kondisi ini disikapi Pemerintah dengan menerbitkan Peraturan Presiden Nomor 53 Tahun 2017 tentang Pembentukan Badan Siber dan Sandi Negara (BSSN).[17] Selain itu, Pemerintah juga akan terus mengedukasi masyarakat agar lebih memiliki budaya keamanan siber, karena budaya ini dilihat masih rendah, contohnya masih lemahnya masyarakat memproteksi akun-akun atau data-data pribadinya, seperti masih jarang atau bahkan tidak pernah mengganti nomor PIN dan *password* pribadi pada email, ATM, dan lain-lain. Padahal, bila itu dilakukan oleh setiap masyarakat, maka akan memberikan kontribusi yang kuat bagi *National Resiliance* dan

---

[16] Singapura berada di posisi puncak, disusul oleh Amerika Serikat di peringkat kedua, dan Malaysia di posisi ketiga dengan skor 0,893. Lihat : " Hati-Hati di Dunia Maya; Keamanan Siber Indonesia Masih Lemah : https://biz.kompas.com/read/2017/11/30/112934928/hati-hati-di-dunia-maya-keamanan-siber-indonesia-masih-lemah : diakses 9 Juni 2018.

[17] "Hati-hati di Dunia Maya ; Keamanan Siber Indonesia Masih Lemah". *Ibid.*

*National Cyber Security.*[18] Jadi, tampak jelas bahwa Indonesia membutuhkan sinergitas antara Pemerintah dengan warga negaranya untuk sama-sama mendukung terwujudnya *Cyber Security* yang kuat.

## F. Daerah-Daerah Rawan Konflik Akibat Lemahnya *Cyber Security*

Contoh daerah-daerah yang rawan konflik antara lain Provinsi Sulawesi Tenggara. Di provinsi ini, potensi konflik cukup rentan dalam hal pertambangan, di mana ada persinggungan yang masih menjadi ajang "pertarungan" antara para pengusaha tambang dengan sebagian masyarakat yang adalah masalah perizinan usaha. Seringkali terjadi izin usaha tambang menjadi isu yang menjadi inti konflik karena dianggap menyerobot tanah adat rakyat Sulawesi Tenggara.[19] Apabila konflik itu dikembangkan oleh pihak-pihak yang tidak bertanggung jawab di media sosial, maka tingkat kerawanan konflik akan meningkat signifikan.

Berdasarkan pengalaman, masa-masa Pemilu dan Pilkada di Sulawesi Tenggara juga rentan konflik. Tahun politik 2018 pun diingatkan pihak Polda Sulawesi Tenggara adalah rawan konflik, terutama konflik antar-sesama pendukung dan Tim Sukses. Tim Pemenangan pasangan calon kepala daerah untuk berhati-hati mengelola akun media sosial (medsos), sebab Polda Sulawesi Tenggara dalam menghadapi masa-masa Pilkada 2018 akan menggencarkan patroli *Cyber*. Targetnya adalah untuk memberantas kejahatan dunia maya dan kampanye hitam di medsos.[20]

---

[18] Lihat : "Menkominfo: Masyarakat Indonesia Budaya *Cyber Security* Masih Lemah" : https://telko.id/14407/menkominfo-masyarakat-indonesia-budaya-cyber-security-masih-lemah/ : diakses 13 Juni 2018.

[19] Penjelasan Kapolda Sulawesi Tenggara Brigjen Pol. Iriyanto. Lihat : "Sulawesi Tenggara Rawan Potensi Konflik" : https://www.viva.co.id/berita/politik/1034596-sulawesi-tenggara-rawan-potensi-konflik : diakses 2 Juni 2018.

[20] "Berantas Kejahatan Dunia Maya dan Kampanye Hitam Polda Sultra Gencarkan Patroli Cyber: : http://kendaripos.co.id/2018/02/23/ : Diakses 4 Juni 2018.

Kapolda Sulawesi Tenggara, Brigjen Pol Andap Budhi Revianto mengatakan tim *cyber* akan terus memantau potensi kejahatan dunia maya di Sulawesi Tenggara. Bagi calon kepala daerah di Sulawesi Tenggara yang sudah siap melakukan kampanye melalui media sosial, diharapkan bersikap santun. Kejahatan media sosial kata Brigjen Andap Budhi Revianto menjadi perhatian publik. Sebab, kejahatan seperti itu dapat memecah belah dan memantik konflik antarkubu. Dalam konteks Pilkada, biasanya tim pasangan calon dan tim pasangan lain akan saling menjatuhkan dengan cara membuat akun palsu lalu menebar ujaran kebencian di media sosial. Hal-hal seperti ini yang dipantau oleh tim *cyber*. Hal seperti itulah yang akan dipantau dan akan diatasi secara cepat bila terjadi potensi konflik.[21]

Brigjen Andap Budhi Revianto menyampaikan bahwa kejahatan media sosial harus diatasi sedini mungkin. Kalau bisa, sebelum terjadi harus segera dicegah lebih dulu. Ini untuk menjaga proses jalannya Pemilihan Kepala Daerah yang akan diselenggarakan di Sulawesi Tenggara. Brigjen Andap Budhi Revianto juga sudah meminta anak buahnya agar memberikan peringatan kepada oknum yang kedapatan menebar ujaran kebencian secara berulang-ulang. Jika masih diabaikan maka akan ditindak dengan proses hukum, karena perkataan yang berulang-ulang melalui media sosial itu bisa dianggap sebagai kebenaran. Hal itu mempengaruhi persepsi orang. Brigjen Andap Budhi Revianto juga berpesan agar warga Sulawesi Tenggara dan calon kepala daerah yang akan bertarung di kontestasi Pilkada untuk santun berkampanye di media sosial.[22]

Contoh daerah selanjutnya yang rawan konflik adalah Provinsi Kalimantan Barat. *Strategic Assessment* pada akhir 2017 pernah menyatakan bahwa di Kalimantan Barat rawan konflik yang disebabkan oleh penggunaan media sosial yang tidak bertanggung jawab, terutama

---

[21] *Ibid.*

[22] *Ibid.*

dalam menyulut konflik terkait SARA, menyulut kebencian, dan saling menjatuhkan dalam masa kampanye Pilkada. Survey menunjukkan bahwa Kalimantan Barat berada dalam posisi ketiga dalam hal kerawanan pada masa Pilkada. Hal ini disebabkan karena kampanye di Kalimantan Barat didasarkan atas dasar identitas suku dan agama, bukan kampanye program.[23]

Di Kalimantan Barat, *HOAX* bahkan telah menelan korban jiwa. Pernah terjadi di Kabupaten Mempawah, seorang pria tewas dianiaya masyarakat karena diduga menjadi pelaku penculikan anak, di mana isu penculikan anak tersebut sebelumnya ramai menjadi isu yang disebarkan di media sosial. Hal seperti ini akan lebih berbahaya lagi bila HOAX diarahkan ke isu SARA di Kalimantan Barat.[24]

Pihak Polda Kalimantan Barat juga mengingatkan hal serupa. Dikatakan bahwa Kalbar merupakan satu diantara provinsi paling rawan konflik etnis. Sejak tahun 1952-2016, setidaknya telah terjadi 17 peristiwa konflik antar-etnis. Di era Orde Baru ada 13 peristiwa. Di era Reformasi ada lima persitiwa. Dari semua konflik tidak ada satupun pihak yang merasa menang, semuanya merugi. Stabilitas terganggu, proses belajar-mengajar terganggu, distribusi sembako terhambat dan berbagai dampak lainnya. Semua pihak pasti akan dirugikan.[25]

---

[23] Disampaikan Jumadi, Dosen Ilmu Sosial dan Ilmu Politik Universitas Tanjungpura, dalam Diskusi yang diselenggarakan Pokja Rumah Demokrasi dan KNIP Kalimantan Barat bertema 'Memotret Titik Rawan Pilkada 2018' pada Desember 2017. Lihat: "Media Sosial Bisa Menjadi Kerawanan Politik Pilkada di Kalimantan Barat : https://www.centerofrisk-sia.com/ : diakses pada 3 Juni 2018.

[24] Penjelasan Kepala Dinas Komunikasi dan Informatika (Diskominfo) Provinsi Kalimantan Barat. Lihat : "Waspada *HOAX*: Masyarakat harus Belajar dari Pengalaman Konflik Berbagai Negara : http://pontianak.tribunnews.com/2018/05/08/ : diakses 3 Juni 2018.

[25] Penjelasan Kasubdit Kermaditbinmas Polda Kalbar, AKBP Harjito. Lihat: "Polda Kalbar: Berita HOAX Berpotensi Timbulkan Konflik SARA": http://pontianak.tribunnews.com/2017/04/23/ : diakses pada 3 Juni 2018.

## G. Fakta di Provinsi Sulawesi Tenggara dan Kalimantan Barat

### 1. Sulawesi Tenggara

Berdasarkan hasil wawancara dengan pihak Diskominfo, didapat informasi bahwa Diskominfo masih menghadapi masalah SDM dalam menerapkan sistem *online.* Adapun terkait *HOAX,* Untuk menghadapi, sudah dibentuk tim untuk menangkisnya. Fungsi Tim ini adalah untuk meluruskan berita dan memberikan sosialisasi kepada masyarakat mengenai *HOAX.* Tim ini dibentuk melihat kecenderungan bahaya *HOAX* secara nasional, sehingga perlu dibentuk tim untuk mengantisipasinya, sambil menunggu rencana pembentukan Badan *Cyber.* Di sisi lain, yang cukup membesarkan hati adalah bahwa konflik yang dipicu melalui media sosial atau internet tidak mengemuka di Sulawesi Tenggara.

Terkait memberikan kesadaran mengenai pentingnya menggunakan internet secara bijak kepada masyarakat agar tidak mudah terprovokasi oleh *HOAX* dan adu domba melalui media sosial terkait SARA, Diskominfo senantiasa melakukan sosialisasi mengenai penggunaan internet secara baik dan bertanggung jawab kepada masyarakat, walaupun masih dilakukan secara insidentil. Belum terlalu difokuskannya masalah pendidikan internet kepada masyarakat karena pertama, Diskominfo baru terbentuk Januari 2017, setelah sebelumnya bergabung dengan Dinas Perhubungan. Kedua, saat ini Diskominfo masih berfokus pada membangun infrastruktur jaringan untuk kepentingan pelayanan publik secara *online.*

Pihak selanjutnya yang diwawancarai adalah pihak Bawaslu. Menurut pihak Bawaslu Provinsi Sulawesi Tenggara, masalah potensi konflik melalui internet harus menjadi perhatian Pemerintah karena selama ini tidak terkontrol. Sebenarnya KPU harus lebih berperan dalam mengontrol konten-konten terkait kampanye pemilu di internet. KPU harus memberikan koridor yang tegas tentang siapa yang berhak

melakukan postingan-postingan kampanye pemilu di internet atau media sosial. Walaupun dalam UU dikatakan bahwa situs-situs terkait kampanye pemilu harus didaftarkan ke KPU sebagai situs resmi kandidat/calon dalam pemilu, tapi selama ini terlihat bahwa KPU tidak cukup punya kekuatan untuk mengontrol konten-konten kampanye pemilu di internet.

Untungnya, masyarakat Sulawesi Tenggara tidak mudah terprovokasi oleh pemicu konflik yang bersifat SARA. Hal ini selain karena sifat dasar masyarakatnya yang tidak mudah terprovokasi, juga karena sinergi antara Pemerintah Daerah dan para penyelenggara pemilu dalam memberikan pemahaman-pemahaman tentang bahayanya hal-hal yang dapat memicu konflik di internet atau media sosial kepada masyarakat Sulawesi Tenggara.

Kasus konflik antara masyarakat Bugis dengan Moronene yang pernah terjadi dapat dengan segera diredam sehingga tidak meluas atau merembet ke "perang" di internet atau media sosial. Jadi, bila ada sesuatu konflik, itu biasanya masih dalam tataran di dunia nyata, belum sampai merambah ke dunia maya. Hal ini karena Pemerintah Daerah, Penyelenggara Pemilu, dan seluruh aparat terkait bertindak sigap untuk menanggulanginya.

Dalam hal memberikan pemahaman kepada masyarakat, Bawaslu senantiasa melakukan sosialisasi tentang cara menggunakan dan memanfaatkan media sosial dalam kampanye pemilu yang sehat dan bertanggung-jawab. Sosialisasi ini selalu dihadiri oleh semua pihak terkait, termasuk dari pihak media massa, tokoh-tokoh agama atau organisasi di masyarakat. Kegiatan ini juga dilakukan dengan berinovasi dalam konteks *online.* Ketika wawancara dilakukan, Bawaslu sedang merancang program pengawasan pemilu secara *online* yang dinamakan program GO-WASLU, yang terinspirasi dari GO-JEK.

Pandangan selanjutnya adalah dari Asosiasi Jurnalis Indonesia (AJI) Provinsi Sulawesi Tenggara. Menurut pihak AJI Provinsi Sulawesi Tenggara, intensitas potensi konflik dalam media sosial, terutama ketika

masa pemilu, adalah sangat tinggi, terutama pada Pilkada 2015, dan muatan-muatannya banyak yang bersifat HOAX dan kampanye hitam. Namun, penggunaan internet atau media sosial masih kurang dapat diakses oleh penduduk di daerah perkampungan karena jaringan internet belum tersedia secara memadai. Dengan demikian, gesekan dalam pemilu, misalnya dalam Pilpres dan Pileg, lebih bersifat di dunia nyata. Kampanye tidak hanya yang bersifat hitam, tetapi juga yang bersifat kritik sosial atau hukum.

Di Kabupaten Muna Barat, konflik di media sosial cukup tinggi. Pernah terjadi saling lapor ke Polisi karena masalah serang-menyerang secara pribadi. Tapi konflik ini tidak sampai pada tahap konflik fisik. Sebenarnya potensi konflik terkait SARA adalah sangat rentan. Di Provinsi Sulawesi Tenggara, kumpulan komunitasnya heterogen. Daerah-daerah yang rentan antara lain adalah Kota Kendari, Kabupaten Tolaki, Muna, Buton (ada 42 suku), dan Bugis (sebagai suku dominan). Seringkali konflik dalam pilkada disamakan dengan konflik yang memuat simbol kesukuan. Konflik yang terjadi antara Bugis dengan Moronene tidak sampai melebar ke media sosial, karena mudah diredam dan diatasi secara cepat.

Untuk menyosialisasikan agar masyarakat tidak mudah terprovokasi melalui informasi-informasi di media sosial, biasanya yang diundang adalah tokoh-tokoh masyarakat dan pihak-pihak dari media, lalu pihak media akan memberitakannya. Untuk mengatasi konflik di media sosial, peraturan perundang-undangan yang ada harus dipertegas, karena UU Pemilu dan ITE belum cukup. Perlu digarisbawahi bahwa potensi konflik SARA di Provinsi Sulawesi Tenggara memang ada.

Selanjutnya dijelaskan bahwa sebelum media sosial *booming,* konflik yang bernuansa SARA biasanya terjadi di kampus-kampus. Hal ini dapat dilihat dalam bentuk sentimensi kesukuan misalnya pada pemilihan Ketua BEM. Ini berarti konflik komunal di kampus-kampus sangat tinggi. Sementara itu, konflik yang bersifat anti-Cina dan yang bersifat agama termasuk rendah di Sulawesi Tenggara. Di Kendari bahkan ada 5 masjid yang berhadapan letaknya dengan gereja.

Dari pihak KPU Kota Kendari, diketahui bahwa untuk meminimalisir terjadinya potensi konflik dalam pilkada, paslon dan para pengusung sejak awal diberikan sosialisasi tentang bagaimana menyikapi sistem kampanye *online* atau melalui media sosial secara bijak dan bertanggung jawab.

Sebelum diberlakukannya UU ITE, serang-menyerang dalam pilkada di media sosial, terutama di FB sangat liar. Di dunia nyata, orang pura-pura baik dan tidak ada pertentangan, tetapi di media sosial, terlihat lah aslinya. Namun demikian, isu SARA di media sosial tidak terlalu tinggi dalam memunculkan potensi konflik. Dalam konflik kampanye hitam di media sosial, *counter*-nya terjadi secara alami, yaitu dilakukan oleh pihak yang tidak setuju dengan materi kampanye hitam yang disebarkan oleh pihak lawan politik.

Selanjutnya, dari pihak Akademisi Universitas Halu Oleo (UNHO), didapat informasi bahwa pemanfaatan *cyber* di Provinsi Sulawesi Tenggara masih termasuk rendah. Yang sudah baik baru di Pemkot [illegible]

pemanfaatan media sosial untuk berkampanye tergolong minim. Masyarakat masih menyukai model kampanye konvensional.

Isu-isu SARA tidak pernah terjadi sebagai potensi memunculkan konflik di masyarakat. Grup Sulawesi Tenggara *Watch* di media sosial

Dalam konteks pemilu, pengawasan "pertarungan liar" kampanye media sosial oleh KPU belum maksimal dapat dilakukan pada seluruh kasus, karena sesuai dengan Peraturan KPU Nomor 6 Tahun 2016 Pasal 41, 46, 48, yang diawasi adalah akun-akun di media sosial yang terdaftar. Inilah kelemahannya, karena justru akun-akun yang tidak terdaftar lah yang seharusnya diawasi dan diberi sanksi. Dalam konteks ini, BAWASLU juga masih kesulitan karena regulasi untuk mengawasinya belum mendukung. Jadi, penyelenggara pemilu perlu diberi kewenangan yang lebih besar dan lebih luas untuk mengontrol atau mengawasi, dan menindak akun-akun yang menimbulkan konflik di media sosial, yang pada akhirnya akan menimbulkan konflik di masyarakat.

Regulasi yang diperlukan sebagai patokan untuk mengatasi konflik di media sosial adalah:

1) Konten-konten terkait: Apakah memperkuat atau memperlemah integrasi bangsa? Banyak ajaran-ajaran radikalisme yang harus difilter. Perangkat Kementerian harus tegas. Polisi *Cyber Crime* juga harus lebih tegas.
2) Rumuskan fungsi-fungsi yang ada di media sosial: untuk penyebaran info atau pendidikan politik.
3) Bagaimana resolusi/memediasi konflik: dengan aktor-aktor penengah, memperhatikan akar atau sumber konfliknya.

**2. Kalimantan Barat**

Dari pihak *Pontianak Post*, didapatkan informasi bahwa sistem pelayanan Pemda di Provinsi Kalbar ada yang sudah berorientasi *online* dan ada yang belum memfokuskan pada sistem *online.* Di Pemkot Pontianak sudah memakai sistem *online,* walaupun masih ada beberapa SKPD yang masih menggunakan sistem manual. SKPD yang sudah melakukan sistem *online,* melakukan posting-posting di media sosial secara cukup aktif. Hal ini dilakukan untuk mengimbangi karakteristik

masyarakat yang masih cenderung mudah terpancing oleh informasi-informasi yang belum jelas kebenarannya. Adapun di sisi lain, Pemprov Kalbar belum berorientasi pada sistem *online* dalam pelayanannya. *Website* Pemprov Kalbar kurang optimal di-*update.* Bahkan, tampaknya SDM yang ada di Pemprov Kalbar belum memadai untuk diterapkannya sistem *online.*

Sebenarnya masyarakat Kalbar kurang peduli dengan perpolitikan di dunia nyata. Tetapi di media sosial mereka sangat eksis. Mereka rawan terprovokasi dengan mudah, apalagi bila ada isu yang terkait SARA. Info semacam ini cepat menyebar dan rawan menimbulkan konflik. Namun demikian, di kalangan anak-anak muda justru seringkali dapat memilah mana berita-berita yang sifatnya HOAX, sehingga mereka lebih waspada.

Pada Pemkot Pontianak, rata-rata pejabat-pejabatnya mempunyai akun media sosial masing-masing. SKPD juga ada yang menyediakan *Media Center.* Sistem *online* Pemkot Pontianak juga sudah cukup maju, contohnya dengan adanya aplikasi android yang terkait pengaduan masyarakat. Jadi bila ada hal-hal di lapangan yang ingin disampaikan atau diadukan masyarakat kepada Pemda, masyarakat tinggal memfotonya dan mengirimkannya ke akun Walikota Pontianak di Instagram, dan lain-lain. Tiap SKPD Pemkot Pontianak terintegrasi secara *online.* Kalau di Pemprov Kalbar, yang menjadi "corong" pemberitaan Pemda adalah Bagian Humas, dan ini menyebabkan *high cost.*

*Booming*-nya media sosial memang harus sangat diwaspadai di Kalbar. Di Kalbar sudah pernah terjadi 12 perang antar-suku. Bahkan ke depan, ada seorang Ahli Sejarah yang "meramalkan" akan ada perang suku yang lebih besar lagi. Di Sambas, sampai sekarang konflik masih ada. Oleh karena itu, dengan adanya era internet, terutama media sosial saat ini, penggunaan dunia maya harus dilakukan dengan sangat hati-hati. Dalam kaitannya dengan ini, pihak media massa, termasuk *Pontianak Post* melakukan setiap pemberitaan dengan pemilihan kata-

kata/kalimat-kalimat (diksi) secara hati-hati, dengan tujuan sedapat mungkin menghindari potensi konflik yang terkait SARA. Contohnya, bila terjadi suatu peristiwa kerusuhan, maka pihak media massa akan menyebutkan nama besar wilayah tempat terjadinya kerusuhan tersebut sebagai pemberitaannya. Jadi tidak dengan menyebut ke detail wilayah kecilnya, karena bila wilayah kecil itu adalah dominan suku tertentu, yang *vis a vis* mengalami konflik dengan pihak di luar suku itu dalam peristiwa kerusuhan tersebut, maka sudah dipastikan akan terjadi konflik yang mengalami perluasan secara cepat, karena melalui media internet, hal itu akan cepat tersebar dan berita-beritanya pun akan semakin "dibumbui" oleh pihak-pihak yang memperkeruh suasana dengan isu-isu SARA yang dilebih-lebihkan. Sayangnya, pihak Pemda di Kalbar kurang jeli dalam hal-hal seperti ini. Pihak Pemda harus lebih berhati-hati dalam melakukan pemberitaan yang dapat menimbulkan kerawanan konflik, terutama yang terkait SARA.

## H. Bagaimana Mengembangkan *Cyber Security* Sulawesi Tenggara dan Kalimantan Barat?

Dari fakta-fakta di atas, tampaknya ada beberapa poin penting yang dapat dijadikan dasar analisa: pertama, potensi konflik SARA di Provinsi Sulawesi Tenggara dan Kalbar memang ada, dan tampaknya lebih tinggi potensinya di Kalbar. Kedua, di Sulawesi Tenggara, fokus membangun *cyber security* belum optimal karena di sana justru sedang menitikberatkan pada pembangunan sistem *online*-nya, termasuk sedang membangun jaringannya. Jadi, di Sulawesi Tenggara adalah dalam tahapan membangun pondasi *online* nya. Belum pada tahap bagaimana cara mengembangkan *cyber security.* Sistem penyeimbang bila terjadi potensi konflik yang terpicu oleh *hoax* atau provokasi di media-media sosial justru didapat dari keaktifan pihak masyarakat itu sendiri, khususnya mereka yang telah "melek politik", di mana berita-berita *hoax* atau provokasi yang mengancam SARA di-*counter* oleh mereka

dengan cara memberikan informasi-informasi yang sebenarnya, dan menyadarkan bahwa apa yang diterima masyarakat adalah *HOAX* yang akan membahayakan persatuan dan kesatuan masyarakat Provinsi Kalbar.

Adapun di Provinsi Kalbar, kesadaran *cyber security* memang lebih tinggi dan lebih maju langkahnya daripada di Provinsi Sulawesi Tenggara. Namun sayangnya, kesadaran ini belum menyeluruh pada Pemda. Yang memiliki dan menerapkan kesadaran *cyber security* adalah baru di tataran Pemkot Pontianak, sementara di Pemprov Kalbar belum dilakukan sebagai suatu prioritas untuk diimplementasikan.

Dengan demikian, kunci untuk mengembangkan *cyber security* di Sulawesi Tenggara adalah 'menuntaskan infrastruktur *online* dan mempersiapkan SDM nya, Setelah itu dituntaskan, barulah Pemda Sulawesi Tenggara akan mampu menata diri bagi pengembangan *cyber security.* Sementara ini, yang bisa dilakukan Pemda Sulawesi Tenggara untuk mencegah berkembangnya potensi konflik di Sulawesi Tenggara adalah dengan bekerja sama dengan kalangan masyarakat yang selama ini menjadi penyeimbang dalam meredam konflik yang terjadi, khususnya melalui provokasi di media sosial. Biasanya, salah satu dari kalangan masyarakat tersebut adalah dari pihak LSM. Perlu diidentifikasi mana LSM yang selama ini peduli pada pencegahan konflik di masyarakat dan giat beraktifitas dalam konteks mencerdaskan masyarakat Sulawesi Tenggara agar bijak dalam bermedia sosial.

Hal tersebut perlu dilakukan secepatnya oleh Pemda Sulawesi Tenggara, karena salah satu unsur demokrasi adalah adanya keseimbangan dalam pemberian informasi kepada masyarakat. Informasi yang bersifat hoax harus diimbangi dengan informasi yang berdasarkan fakta atau sumber yang dapat dipertanggungjawabkan. Ini tentunya membutuhkan pendidikan politik yang baik kepada masyarakat, di mana harus ada kerja sama yang erat antara Pemda dengan masyarakat itu sendiri agar hal itu dapat terimplementasi.

Adapun di Kalbar, Pemprov harus memacu diri untuk menjadikan Pemkot Pontianak sebagai percontohan dalam penerapan sistem pemerintahan berbasis *online.* Hanya dengan kemajuan dalam dunia maya lah maka perang *cyber* dapat ditangani oleh Pemda. Serangan-serangan dari pihak-pihak yang tidak bertanggung jawab dalam dunia *cyber* yang mengedepankan sistem memecah-belah persatuan dan kesatuan masyarakat Kalbar harus diimbangi dengan kemampuan Pemda dalam menguasai teknologi *online,* terutama *cyber security.* Tanpa itu, tentu Pemda akan menjadi "bulan-bulanan" dari para kriminal *cyber* yang demi kepentingan pribadi atau golongannya semata, bisa menghancurkan kerukunan antar-warga di Provinsi Kalbar.

Pemprov Kalbar harus mengesampingkan rasa "gengsi" untuk mau belajar dari Pemkot Pontianak. Ego sektoral harus dibuang jauh-jauh bila ingin kehidupan bermasyarakat di Kalbar tetap damai dan penuh dengan toleransi SARA. Bila Pemprov Kalbar tidak mau menundukkan ego sektoralnya, maka jangan harap potensi konflik SARA terutama yang dipicu oleh *hoax* dan provokasi di Kalbar dapat menurun, terlebih lagi dapat dihapuskan. Hanya dengan sinergitas antara Pemprov dan Pemkot, maka *cyber security* dapat efektif menghadapi serangan provokasi bernuansa SARA melalui media sosial.

*Political will* adalah kata kuncinya, baik bagi Pemprov Sulawesi Tenggara maupun Kalbar. Dari sisi masyarakat yang selama ini menjadi penyeimbang terhadap *hoax* dan provokasi di media sosial, harus disadari bahwa selain mereka perlu terus berjuang mencerdaskan masyarakat di daerahnya masing-masing, mereka juga harus senantiasa mengajak Pemda masing-masing untuk mengembangkan sistem pemerintahan berbasis *online* dengan akselerasi penuh, agar *cyber security* dapat segera dapat diwujudkan. Pemda perlu disadarkan bahwa tanpa membangun sistem pemerintahan berbasis *online* dengan kecepatan tinggi, kekuatan untuk mengatasi potensi konflik yang muncul di media sosial hanyalah akan menjadi *utopia.*

Pemerintah Pusat harus memperhatikan permasalahan-permasalahan di atas. Pemerintah Pusat bersama-sama dengan DPR RI harus merumuskan regulasi yang dapat menjadi pegangan bagi Pemda dan Penyelenggara Pemilu untuk meredam konflik yang terjadi karena "keganasan" pertarungan informasi di media sosial. Hendaknya diperhatikan poin-poin dalam membuat regulasi itu, sebagaimana yang disampaikan oleh kalangan akademisi, yaitu bahwa pertama, regulasi yang diperlukan sebagai patokan untuk mengatasi konflik di media sosial adalah konten-konten terkait, di mana yang menjadi acuannya adalah perlu adanya klasifikasi atas konten-konten dengan kategori memperkuat atau memperlemah integrasi bangsa? Kedua, rumuskan fungsi-fungsi yang ada di media sosial, yaitu untuk penyebaran info sekaligus untuk pendidikan politik. Ketiga, rumuskan bagaimana metode untuk membuat resolusi atas suatu konflik atau memediasinya, dengan memperhatikan akar atau sumber konfliknya.

Regulasi tersebut sangat mendesak untuk dibentuk karena contohnya dalam konteks pemilu atau pilkada, aparatur penyelenggara pemilu atau pilkada belum bisa memberikan penindakan yang efektif terhadap situs-situs atau orang-orang yang memposting konten-konten bernuansa mengadu-domba atas dasar SARA, sehingga situs-situs yang memprovokasi atau yang khusus (spesialis) menyebarkan *hoax* tumbuh dengan lebih subur tak terkendali. KPU dan Bawaslu akan tetap menjadi "macan ompong" bila tidak dibekali dengan "amunisi" berupa regulasi atau perundang-undangan yang dapat memberi mereka "taring" untuk menindak provokator-provokator di media sosial. Ini juga dalam rangka mendukung *cyber security,* terutama bagi daerah yang sistem *online*-nya baru mulai dibangun dan belum menjadikan *cyber security* sebagai salah satu unsur prioritas.

# I. Apa yang Perlu Diperbaiki?

Mengingat akan berbahayanya potensi berita *hoax* bagi kerukunan berbangsa dan bernegara serta melihat masih lemahnya implementasi UU ITE terhadap pelaku *hoax* di masyarakat, maka yang dapat direkomendasikan dalam tulisan ini adalah dengan melakukan perbaikan dan penyempurnaan serta pengawasan dalam implementasi UU ITE itu sendiri oleh legislatif. Kemudian di ruang publik, pemerintah harus lebih banyak melakukan kegiatan literasi media terhadap masyarakat agar tak mudah termakan oleh berita *hoax* yang menyesatkan.

Literasi media adalah pendidikan yang mengajari khalayak media agar memiliki kemampuan menganalisis pesan media, memahami bahwa media memiliki tujuan komersial/bisnis dan politik sehingga mereka mampu bertanggung jawab dan memberikan respon yang benar ketika berhadapan dengan media. Sejak kemudahan berinteraksi disediakan oleh TIK, kedudukan manusia terhadap pesan yang dibawa media berubah, tidak hanya sebagai konsumen, tetapi juga sebagai produsen dan distributor. Kedudukan sebagai produsen dan distributor sekaligus idealnya dapat dimanfaatkan untuk mengendalikan laju informasi.

Dengan masifnya informasi menerpa seseorang, seharusnya manusia sebagai individu merdeka mampu mengontrol pesan atau informasi yang menerpa. Yang menjadi pengontrol pesan adalah khalayak. Pemakaian teknologi komunikasi selalu melahirkan perubahan sosial dalam masyarakat; pemakaian komputer untuk komunikasi telah menyebabkan orang lebih percaya pada informasi yang ada di komputer daripada kenyataan yang sebenarnya. Ketika mencari informasi di internet, mereka menciptakan alasan untuk mencari informasi yang baru lagi dan lagi. Mereka menyerahkan sebagian, kalau tidak seluruh, otoritas diri mereka pada internet. Seorang individu pengguna teknologi komunikasi harus tahu persis apakah kelak perilakunya baik dan responnya proporsional. Dengan melek terhadap informasi yang dibawa

teknologi komunikasi, manusia akan memiliki otoritas dirinya, dan tidak akan terombang-ambing oleh ketidakpastian informasi yang saat ini banyak beredar. Seorang pengguna yang melek media akan berupaya memberi reaksi dan menilai suatu pesan media dengan penuh kesadaran dan tanggung jawab.

Karena itu, literasi media adalah kegiatan yang bisa mengurangi ekses negatif dari masifnya penyebaran berita *hoax* di masyarakat. Inilah yang harus dipahami baik oleh Pemprov Kalbar maupun Sultra. Dengan demikian, tidak hanya sistem *Cyber Security* di dalam tubuh Pemda saja yang diperbaiki, tetapi juga itu harus diimbangi dengan pemberian pendidikan kepada masyarakat tentang pentingnya memperhatikan koridor-koridor hukum dalam memanfaatkan atau menggunakan internet.

## DAFTAR PUSTAKA

Adzkia, Adhnia, dan Heychael, Muhamad Heychael. 2014. Independensi Televisi Menjelang Pemilu Presiden 2014. Jakarta (Remotivi)

Plato. 2017. "Repulik; Ed Revisi 2017". Yogyakarta. Pustaka Narasi.

Soesilo, R. 1991. Kitab Undang-Undang Hukum Pidana (KUHP): Serta Komentar-Komentarnya Lengkap Pasal demi Pasal: Bogor: Politeia Bogor.

Tamburaka, Apriadi. 2013. *Literasi Media.* Jakarta. Rajawali Pers.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Kitab Undang-Undang Hukum Pidana

Peraturan KPU Nomor 6 Tahun 2016

"Wiranto : Demokrasi Kebablasan Bisa Picu HOAX": https://kumparan.com/@kumparannews/wiranto-demokrasi-kebablasan-bisa-picu-hoax : diakses 20 Mei 2018.

"Polisi : Berita HOAX *Muslim Cyber Army* 'Bermuatan Politik'": http://www.bbc.com/indonesia/indonesia-43221362: diakses 1 Juni 2018.

"HOAX Kian Merajalela Memecah Belah Negeri Ini: Beberapa Kasus Hoax Bahkan Sampai Makan Korban" : https://www.hipwee.com/feature/ : diakses 7 Mei 2018.

"Demokrasi Kebablasan Dimaksud Jokowi Terkait Banyak Berita HOAX" : https://www.merdeka.com/peristiwa/demokrasi-kebablasan-dimaksud-jokowi-terkait-banyak-berita-hoax.html: diakses 20 Mei 2018.

"Penyebar Kebencian Sulit Ditindak Karena *Facebook* Tak Mau Bantu": https://koransulindo.com/penyebar-kebencian-sulit-ditindak-karena-facebook-tak-mau-bantu/ : diakses 22 Mei 2018.

"Ada 800 Ribu Situs Penyebar HOAX di Indonesia": https://www.cnnindonesia.com/teknologi/20161229170130-185-182956/ada-800-ribu-situs-penyebar-hoax-di-indonesia: diakses 5 Mei 2018.

"Perlu Pembenahan Regulasi untuk Atasi Ujaran Kebencian: http://mediaindonesia.com/read/detail/94190-perlu-pembenahan-regulasi-untuk-atasi-ujaran-kebencian: diakses 4 Juni 2018.

" Hati-Hati di Dunia Maya; Keamanan Siber Indonesia Masih Lemah: https://biz.kompas.com/read/2017/11/30/112934928/hati-hati-di-dunia-maya-keamanan-siber-indonesia-masih-lemah: diakses 9 Juni 2018.

"Menkominfo: Masyarakat Indonesia Budaya *Cyber Security* Masih Lemah": https://telko.id/14407/menkominfo-masyarakat-indonesia-budaya-cyber-security-masih-lemah/: diakses 13 Juni 2018.

"Sulawesi Tenggara Rawan Potensi Konflik": https://www.viva.co.id/berita/politik/1034596-sulawesi-tenggara-rawan-potensi-konflik: diakses 2 Juni 2018.

"Berantas Kejahatan Dunia Maya dan Kampanye Hitam Polda Sultra Gencarkan Patroli Cyber:: http://kendaripos.co.id/2018/02/23: Diakses 4 Juni 2018.

"Media Sosial Bisa Menjadi Kerawanan Politik Pilkada di Kalimantan Barat: https://www.centerofrisk-sia.com/: diakses pada 3 Juni 2018.

Masyarakat harus Belajar dari Pengalaman Konflik Berbagai Negara: http://pontianak.tribunnews.com/2018/05/08/: diakses 3 Juni 2018.

Berita HOAX Berpotensi Timbulkan Konflik SARA": http://pontianak.tribunnews.com/2017/04/23/: diakses pada 3 Juni 2018.

# BAGIAN 4
# KEBIJAKAN SIBER NASIONAL DI ERA GLOBALISASI INFORMASI

*Aulia Fitri*
*Calon Peneliti Kepakaran Pertahanan*
*Pusat Penelitian Badan Keahlian DPR RI*
*E-mail: auliarosadi@gmail.com*

## A. Globalisasi Informasi

Perkembangan teknologi informasi yang semakin pesat di era globalisasi telah membuka aliran arus informasi tanpa mengenal batas-batas negara. Di satu sisi, pesatnya perkembangan tersebut dinilai menguntungkan masyarakat yang dapat mengakses informasi dan perkembangan dunia terbaru dengan mudah. Namun di sisi lain juga merupakan sebuah ancaman apabila dilihat dari persepsi kedaulatan negara, mengingat semakin terbatasnya kontrol negara atas arus informasi yang masuk sebagai dampak dari globalisasi. Persepsi terhadap kekuatan suatu negara tidak lagi dipandang dari seberapa besar kekuatan militer atau ekonomi tetapi juga dari penguasaan teknologi informasi.

Perubahan ini juga mengakibatkan terjadinya pergeseran ancaman yang dihadapi oleh suatu negara, dari ancaman yang bersifat tradisional menjadi ancaman asimetris atau *asymmetric threat.*[1] Ancaman di era globalisasi yang semakin kompleks tentunya berdampak pada pertahanan negara. Buku Putih Pertahanan mengolongkan ancaman berupa ancaman militer dan ancaman nonmiliter. Ancaman militer

[1] Dorman Andrew, Smith Mike, and Uttley Matthew, *The Changing Face of Military Power*, Palgarave, 2002

adalah ancaman yang bersifat membahayakan kedaulatan dan keutuhan wilayah negara, dengan menggunakan kekuatan bersenjata. Sedangkan ancaman nirmiliter adalah ancaman terhadap ketahanan ideologi, politik, ekonomi, sosial budaya, teknologi dan informasi suatu bangsa dan negara.[2]

Salah satu wujud ancaman nirmiliter adalah ancaman keamanan siber. Tidak dapat dipungkiri, pesatnya perkembangan ilmu pengetahuan dan teknologi informasi dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan yang dapat membahayakan keamanan negara, contohnya serangan siber (*cyber-attack*). Serangan siber didefinisikan sebagai serangan yang dilakukan baik oleh aktor negara atau non-negara menggunakan jaringan komputer, internet di ranah dunia maya (*cyber space*) dengan tujuan melakukan gangguan, pencurian data atau membuat kerusakan sistem komputer dan jaringan suatu negara ataupun suatu kelompok atau organisasi.[3] Adapun bentuk-bentuk dari serangan *cyber* di antaranya adalah; *hacking, cracking* atau peretasan, yaitu tindakan penerobosan terhadap jaringan komputer tanpa sepengetahuan pemilik atau bersifat ilegal dengan tujuan melakukan tindakan perusakan seperti memberikan virus, mencuri bahkan mengunci data; *cyber sabotage,* gangguan, perusakan atau penghancuran terhadap sistem jaringan komputer dengan menyusupkan suatu *logic bomb*, virus ataupun program sehingga data dan sistem jaringan komputer tidak dapat digunakan atau tidak berjalan sebagaimana mestinya atau berjalan sesuai kehendak pelaku; *spyware/malware*, penginstalan program pada sistem komputer yang bertujuan untuk mengumpulkan berbagai informasi untuk dikirimkan ke lokasi tertentu tanpa sepengetahuan user.[4]

---

[2] Buku Putih Pertahanan Indonesia. 2015.

[3] Thornton, Rod. *Asymmetric Warfare: Threat and Response in the 21st Century.* Cambridge: Polity Press.2006

[4] Ineu Rahmawati, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan* Cyber Defense. Jurnal Pertahanan & Bela Negara. 2017. Vol 2.

Setidaknya terdapat lima kasus serangan siber terbesar yang pernah terjadi di dunia. Pertama, *Wannacry*, serangan *ransomware* yang melanda 150 negara di dunia pada tahun 2017 yang menargetkan komputer yang senjalankan sistem operasi *Microsoft Windows* dengan mengenkripsi data dan menuntut pembayaran tebusan berupa *bitcoin cryptocurrency*.[5] Kedua, pemilu Amerika Serikat 2016, di mana *hacker* Rusia berhasil menembus sistem komputer Partai Demokrat dan membocorkan serangkaian email dan dokumen manajer kampanye Hillary Clinton, John Podesta selama masa kampanye hingga hari pemilihan.[6] Ketiga, serangan Stuxnet yang melumpuhkan reaktor nuklir Iran, Bushehr, dengan virus *worm* pada tahun 2010.[7] Keempat, *Operation Buckshot Yankee*, yaitu serangan terhadap Pusat Komando Amerika Serikat (AS) melalui sebuah USB Flash pada tahun 2008 yang memuat kode berbahaya hasil pengembangan intelijen asing yang menyebar melalui sistem komputer Departemen Pertahanan AS yang terjadi di markas militer AS di Timur Tengah, yang mengakibatkan terkirmnya data-data penting ke server asing.[8] Kelima, gelombang serangan siber yang terjadi di Estonia pada tahun 2007 yang melumpuhkan segenap infrastruktur internet dan sistem pemerintah negara tersebut selama dua minggu.[9]

Sebagai salah satu negara dengan pengguna internet terbesar di dunia, Indonesia juga rentan akan serangan siber. Di Indonesia, terdapat beberapa kasus serangan siber yang juga terjadi. Pertama, peretasan situs KPU pada pilkada serentak 2018, serangan siber dilakukan

---

[5] Bill Gertz. iWar: *War and Peace in the Information Age. An Imprints of Simon & Schuster.* New York. 2017

[6] ibid

[7] Cyber warfare: A different way to attack Iran's reactors. https://edition.cnn.com/2011/11/08/tech/iran-stuxnet/index.html

[8] Secret US military computers 'cyber attacked' in 2008 https://www.bbc.com/news/world-us-canada-11088658

[9] Mohan B. Gazula. Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology. 2017

dengan cara membanjiri situs web atau suatu jaringan dengan permintaan yang tinggi dan dalam waktu bersamaan sehingga melumpuhkan server. Dalam konteks Indonesia, pada Pilkada serentak 2018, Indonesia belum memakai sistem pemungutan suara berbasis internet atau *e-voting*, namun aksi peretas pada situs web Pemilu akan berdampak pada akses publik terhadap segala informasi dari penyelenggara Pemilu.[10] Kedua, serangan *ransomware wannacry* yang melumpuhkan sistem komputer beberapa rumah sakit dan perusahaan-perusahaan besar di Jakarta serta ribuan alamat IP lainnya. Serangan yang berlangsung pada bulan Maret 2018 tersebut melumpuhkan 54 juta sistem komputer di Indonesia dan menjadikan Indonesia sebagai negara dengan serangan *wannacry* terbesar kedua di dunia setelah Rusia.[11] Ketiga, kasus penyadapan komunikasi pribadi Presiden RI pada tahun 2013 oleh Australia berdasarkan dokumen yang dibocorkan oleh Edward Snowden, mantan anggota *National Securiy Agency* Amerika Serikat.[12] Keempat, *cyber terrorism*, penyalahgunaan internet oleh kelompok jaringan teroris Imam Samudra untuk menyebarkan propaganda, paham-paham radikal, melakukan *hacking, cracking* dan *carding* untuk mengumpulkan dana dan melakukan rekrutmen anggota.[13] Ancaman yang terjadi di ruang siber didominasi oleh aktor non-negara yang juga dapat mengancam keamanan negara. Ancaman tersebut tidak hanya ditujukan untuk menyerang instansi pemerintah tetapi dapat mengancam seluruh aspek kehidupan manusia.

Beberapa kasus mengenai serangan siber yang terjadi di beberapa negara termasuk Indonesia menandakan ketergantungan negara terhadap teknologi informasi membawa tantangan dan ancaman tersendiri.

---

[10] Mengenal DDoS, Teknik Peretasan yang Melumpuhkan Situs KPU https://tirto.id/mengenal-ddos-teknik-peretasan-yang-melumpuhkan-situs-kpu-cNn7

[11] Serangan WannaCry di Indonesia Terbesar Kedua di Dunia. https://inet.detik.com/security/d-4007294/serangan-wannacry-di-indonesia-terbesar-kedua-di-dunia

[12] BIN: Australia menyadap Indonesia sejak 2007. https://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia

[13] Indonesia Pertama Kali Bongkar Kasus "Cyber-Terrorism" https://www.antaranews.com/berita/42142/indonesia-pertama-kali-bongkar-kasus-cyber-terrorism

Teknologi informasi menjadi sebuah titik sentral yang memiliki potensi kerusakan masif terhadap berbagai sektor yang terkait dengan ruang siber.[14] Serangan terhadap ruang siber tidak dapat dipungkiri merupakan sebuah konsekuensi dari semakin pesatnya perkembangan era teknologi informasi. Ruang siber merupakan sektor yang bersifat kompleks karena memiliki interkonektivitas dengan sektor-sektor lainnya. Keterkaitan itulah yang menjadi tantangan dalam melawan ancaman di ruang siber.

Besarnya potensi ancaman di ruang siber baik secara langsung maupun tidak langsung telah mendorong berbagai negara untuk melakukan penataan kebijakan di bidang siber. Dalam konteks ini, Indonesia belum memiliki kebijakan di bidang siber yang bersifat integratif, dengan kata lain kebijakan yang dijalankan masih bersifat sektoral. Oleh karena itu tulisan ini akan memetakan permasalahan kebijakan siber nasional di Indonesia dan merekomendasikan penerapan kebijakan siber yang terintegratif berdasarkan komparasi atas penerapan kebijakan siber dari berbagai negara di dunia.

## B. Kebijakan Siber di Berbagai Negara

Perkembangan teknologi informasi telah membawa perubahan yang signifikan terhadap konsep ancaman yang tidak hanya dibatasi ancaman di ruang fisik tetapi meluas ke ruang siber. Ruang siber menampilkan realitas virtual yang mengaburkan batas-batas negara dengan menghilangkan dimensi ruang, waktu dan tempat yang memungkinkan warga negara untuk terhubung dengan dunia luar tanpa mengenal jarak dan waktu. Menurut Bruce Sterling, ruang siber, meski bukan ruang yang terlihat, tetapi segala sesuatu yang terjadi disana memiliki konsekuensi yang sangat nyata.[15]

---

[14] Susan W. Brenner, Cyber-threats and the Limits of Bureaucratic Control, 14 Minn. J.L. Sci. & Tech. 137 (2013)

[15] Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books. Hal 21

Serangan siber yang terjadi terhadap beberapa negara di dunia telah dipandang sebagai sebuah ancaman yang nyata. Kebutuhan akan keamanan siber menjadi semakin nyata dan mendesak karena dampaknya dapat berpotensi mengganggu kehidupan manusia, negara dan seluruh dunia. Dunia telah sejak lama menaruh kepedulian terhadap isu keamanan siber. Pada kongres PBB ke 10 tentang *Prevention of Crime and the Treatment of Offenders* di Wina Austria tahun 2000, salah satu topik yang dibahas adalah mengenai kejahatan terkait jaringan komputer. Berbagai negara telah mengimplementasikan kebijakan siber nasional (*National Cyber Security Policy*), sebagai respon dari ancaman keamanan di ruang siber yang semakin kompleks.[16] Pada bagian ini akan dijelaskan mengenai implementasi kebijakan siber nasional yang diterapkan oleh beberapa negara di dunia.

### 1. Amerika Serikat

Amerika Serikat (AS) merupakan salah satu negara yang memprioritaskan keamanan siber dalam kebijakan politik domestiknya. Pemerintah AS membangun sistem keamanan informasi sebagai konsekuensi dari ketergantungan penggunaan jaringan sistem informasi dalam menjalankan pemerintahan seperti sistem keamanan informasi dalam bidang militer, agraria, sistem pengaturan lalu lintas, air dan sanitasi, energi dan transportasi. Pemerintah AS membentuk *Executive Branch Cybersecurity Coordinator* (Koordinator Eksekutif Urusan Keamanan Siber) yang berperan sebagai garda pertahanan terdepan atas berbagai potensi ancaman siber.[17] AS juga memiliki *The Departement Of Defense Cyber Strategy,* yakni strategi dalam

---

[16] United Nations Office on Drugs and Crime. Crimes Related to Computer Networks - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Retrieved from United Nations Office on Drugs and Crime: https://www.unodc.org/document s/congress//Previous_Congresses/1 0th_Congress_2000/017_ACONF.1 87.10_Crimes_Related_to_Comput er_Networks.pdf

[17] Rachma Fitriarti, Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara. 2014. Jakarta. Universits Pertahanan Indonesia.

menjalankan prioritas dalam menghadapi tantangan keamanan teknologi informasi dalam ruang siber. Prioritas tersebut antara lain;[18] pertama, menjaga infrastruktur dan sistem informasi penting negara dari ancaman siber. Kedua, meningkatkan kemampuan untuk mengindentifikasi dan melaporkan peristiwa-peristiwa siber agar dapat merespon di waktu yang tepat. Ketiga, mempromosikan *internet freedom* dan membangun dukungan keterbukaan ruang siber. Keempat, mengamankan jaringan pemerintah pusat dengan menyusun target keamanan yang jelas dan menempatkan agen pemerintah yang akuntabel untuk dapat memenuhi target tersebut. Kelima, menjalin kemitraan dengan sektor privat dalam membentuk kekuatan siber.

Sebagai penguatan atas prioritas-prioritas yang telah ditetapkan, Departemen Pertahanan AS menyusun lima strategi inisiatif. Pertama, memperlakukan ruang siber sebagai sebuah wilayah operasional yang harus dikelola, dilatih dan dilengkapi sehingga Departemen Pertahanan AS dapat memanfaatkan potensi dari ruang siber itu sendiri. Kedua, mengembangkan sistem operasi pertahanan baru untuk melindungi sistem dan jaringan Departemen Pertahanan AS. Ketiga, Bermitra dengan departemen/ agen-agen pemerintah maupun dengan sektor swasta untuk melaksanakan seluruh strategi ruang siber. Keempat, membangun hubungan yang kuat dengan para sekutu AS dan partner internasional lainnya untuk memperkuat keamanan siber kolektif. Kelima, mengembangkan inovasi teknologi.

Pemerintah AS juga merumuskan tiga misi utama Departemen Pertahanan AS untuk ranah siber; 1) Menjaga jaringan, sistem dan informasinya sendiri. Departemen pertahanan harus dapat mengamankan jaringannya dari serangan dan memulihkan sistem secara cepat jika pengamanan gagal; 2) Departemen Pertahanan harus mempersiapkan diri untuk menjaga AS dan semua kepentingannya

[18] The Departement of Defense Cyber Strategy. United State's Departement of Defense. 2015.

melawan serangan siber yang memberikan dapak signifikan; 3) Dengan dipimpin oleh Presiden dan Menteri Pertahanan, Departemen Pertahanan harus mampu untuk menciptakan kapabilitas siber yang terintegrasi untuk mendukung operasi militer dan rencana-rencana yang akan dicapai ke depannya. Departemen Pertahanan AS juga memiliki *Cyber Mission Force* (CMF) yang terdiri dari elemen militer dan sipil yang bertujuan untuk melindungi dan membela kepentingan nasional AS. Departemen Pertahanan AS juga mengintegrasikan CMF ke dalam keseluruhan perencanaan dan pengembangan operasi pengamanan ruang siber.

Serangkaian misi tersebut dapat dicapai melalui lima tujuan strategis, antara lain: 1) Untuk dapat beroperasi secara efektif di dunia siber, Departemen Pertahanan membutuhkan dukungan tenaga individual dan tentara yang terlatih dengan standar tinggi. Untuk itu Departemen Pertahanan harus melakukan investasi besar dengan memberikan pelatihan kepada tentara, membangun organisasi yang efektif. 2) Departemen Pertahanan harus memulai dengan melakukan identifikasi, membuat prioritas dan mempertahankan jaringan dan data terpenting sehingga dapat melaksanakan tujuan misi dengan efektif. Departemen Pertahanan harus terus mengembangkan teknologi untuk tetap lebih terdepan dalam menghadapi ancaman dengan memperbesar kemampuan pertahanan siber. 3) Departemen Pertahanan harus bekerja antar-patner, mulai dari sektor swasta, dan aliansi termasuk dengan patner negara lain untuk menangkal dan jika dibutuhkan melumpuhkan serangan siber yang memberikan dampak signifikan atas kepentingan AS. 4) Departemen Pertahanan harus membangun sistem pertahanan siber yang berkelanjutan dan terintegrasi dengan rencana-rencana lembaga yang berkaitan. Departemen Pertahanan akan mengembangkan kemampuan siber untuk mencapai tujuan dari keamanan kunci. 5) Ketiga misi Keamanan siber Departemen Pertahanan membutuhkan kolaborasi dengan sekutu asing dan patner lainnya. Dalam keterikatan dengan dunia siber internasional, Departemen

Pertahanan harus membangun kapasitas kerjasama dalam keamanan dan pertahanan siber.[19]

Tujuan strategis di atas didasari suatu kesadaran bahwa keamanan siber yang efektif membutuhkan kerjasama yang baik antara pemerintah pusat, pemerintah negara bagian, industri dan sekutu internasional. Tercapainya keamanan siber memerlukan pendekatan yang menyeluruh mengingat banyaknya stakeholder yang terlibat, aliran arus informasi yang melintasi batas internasional, melalui pembagian tanggung jawab dan wewenang terhadap keseluruhan sektor. Untuk menjamin keberhasilan misi keamanan siber, Departemen Pertahanan AS terus mengembangkan proses dan koordinasi operasi siber di negaranya.

## 2. Australia

Australia menempatkan keamanan siber sebagai program strategis pemerintah. Strategi keamanan siber yang dijalankan oleh pemerintah Australia didasarkan pada potensi-potensi ancaman dunia maya yang terjadi tidak hanya di lingkup nasinoal tetapi juga lingkup internasional. Negara yang sedang membangun kekuatan eknomi digital ini memandang penting antisipasi terhadap potensi serangan siber. Pemerintah Australia menyadari bahwa penyelenggaraan ekonomi digital memiliki ancaman dan sangat rentan dari gangguan keamanan siber. Oleh karena itu pemerintah Australia berkomitmen untuk meningkatkan inovasi, pertumbuhan dan kesejahteraan bagi seluruh warga negara melalui keamanan siber yang kuat. Hal ini sejalan dengan agenda pemerintah Australia untuk menciptakan perekonomian abad 21 yang dinamis dan modern.

Terdapat lima program prioritas strategis dijalankan Pemerintah Australia untuk meningkatkan tingkat keamanan siber yang ditargetkan tercapai pada 2020.[20] Pertama, kemitraan siber nasional. Pemerintah

---

[19] Alexander Klimburg. The Darkening Web: The War for Cyberspace. Penguin Press. New York. 2017

[20] Australia's Cyber Security Strategy. Commonwealth of Australia. 2016.

Australia bersama dengan sektor bisnis berkomitmen untuk bersama-sama mendorong keamanan siber Australia dengan menetapkan agenda strategis melalui pertemuan keamanan siber tahunan. Pertemuan ini diselenggarakan oleh Perdana Menteri dengan melibatkan sektor bisnis dan komunitas riset dan ditujukan untuk menyelaraskan strategi dan inisiatif dalam penanganan masalah keamanan siber. Tata kelola keamanan siber Pemerintah Australia didasarkan pada pembagian tanggung jawab pada badan-badan pemerintah persemakmuran Australia. Lebih lanjut, Pusat Keamanan Siber Australia akan memfasilitasi kerjasama pemerintah dengan sektor swasta untuk efektifitas tujuan keamanan siber. Pemerintah Australia juga berkomitmen untuk mensponsori kegiatan penelitian, khususnya mengenai penanganan resiko keamanan siber.

Kedua, penguatan pertahanan siber. Pemerintah Australia berkomitmen untuk terus meningkatkan kapabilitas pertahanan siber nasional khususnya kemampuan merespon dan mengantisipasi resiko ancaman. Dalam hal ini pemerintah Australia bekerja sama dengan sektor swasta dalam pertukaran informasi mengenai potensi ancaman siber dan berbagi portal siber *online*. Pelatihan peningkatan respon terhadap ancaman serangan siber juga terus ditingkatkan dengan optimalisasi kemampuan Direktorat Sinyal Australia untuk mendeteksi kerentanan keamanan siber. Selain itu, kapabilitas sumber daya manusia juga terus ditingkatkan dengan menambahkan personil spesialis deteksi ancaman, serta analis teknis kejahatan siber dari Polisi Federal Australia. Pemerintah Australia juga meningkatkan standar kinerja keamanan siber baik di sektor publik maupun privat. Pemerintah, sektor bisnis dan komunitas riset juga bersama-sama merancang panduan keamanan siber untuk menciptakan standar bersama yang diaplikasikan di berbagai sektor.

Ketiga, pengaruh dan tanggung jawab global. Selain pada lingkup domestik, Australia juga bekerja sama dengan negara-negara asing khususnya untuk mengatasi ancaman keamanan siber. Pemerintah

Australia telah menunjuk duta besar siber yang akan mengidentifikasi peluang kerjasama internasional dan mempromosikan pengaruh Australia dalam permasalahan siber internasional. Australia memberi dukungan ruang siber bagi negara-negara yang mematuhi hukum internasional serta membangun kepercayaan bersama untuk mengurangi resiko konflik. Pemerintah Australia akan menjalin kerjasama dengan penegak hukum internasional, badan intelejen serta tim tanggap darurat komputer untuk membangun kapasitas pengamanan siber serta mencegah potensi ancaman serangan siber. Dalam menyebarkan pengaruh global, Pemerintah Australia juga menawarkan kerjasama bantuan pengembangan kapasitas kelembagaan untuk mengatasi ancaman keamanan siber, khususnya di wilayah Indo Pasifik.

Keempat, pengembangan dan inovasi. Komitmen pemerintah Australia untuk keamanan siber salah satunya adalah dengan mendukung pengembangan dan inovasi teknologi siber di berbagai bidang. Untuk memanfaatkan pasar global untuk layanan keamanan siber, Pemerintah Australia mendukung sektor keamanan siber untuk memperluas dan mempromosikan kemampuan mereka ke pasar global. Di dalam negeri, layanan keamanan siber yang kuat akan mendorong kepercayaan diri kapabilitas siber nasional. Dengan penelitian dan pengembangan keamanan siber yag lebih terfokus dalam merespon kebutuhan pemerintah dan industri, Australia akan menghasilkan investasi dalam peningkatan keamanan siber nasional. Hal tersebut juga akan menjadikan Australia sebagai tujuan investasi bisnis dunia. Pemerintah Australia juga berkomitmen untuk menempatkan negaranya sebagai pusat inovasi keamanan siber dengan mendirikan *Cyber Security Growth Center* atau Pusat Pengembangan Keamanan Siber. Lembaga ini akan menyatukan pemerintah Australia, sektor bisnis dan komunitas riset untuk menentukan dan memprioritaskan tantangan siber dan menjadikan Australia sebagai yang terdepan untuk menghasilkan solusi permasalahan keamanan siber.

Kelima, negara *cyber-smart*. Strategi ini adalah komitmen pemerintah Australia untuk menyetarakan kemampuan dan kesadaran digital masyarakatnya, dengan tujuan untuk membangun negara berbasiskan sains dan teknologi. Pemerintah Australia bersama dengan akademisi, komunitas riset dan pebisnis merancang bersama pusat kajian akademik keamanan siber di berbagai universitas untuk menghasilkan pakar-pakar ahli bidang siber. Pusat Kajian yang berada di bawah Pusat Pengembangan Keamanan Siber ini akan bekerja sama dengan pusat-pusat kajian akademik lainnya di seluruh dunia untuk membahas antisipasi ancaman siber beserta pengembangan inovasinya. Pemerintah Australia bersama dengan sektor bisnis dan akademisi juga bekerja sama untuk meningkatkan kapabilitas pengetahuan siber dengan menginisiasi pendidikan siber di lingkungan sekolah, dan melakukan pengembangan kapabilitas keterampilan siber untuk seluruh lapisan masyarakat dan jenjang karir. Pemerintah Australia juga terus meningkatkan kesadaran akan keamanan siber dan memastikan seluruh warga negara Australia memahami manfaat dan resiko serta mengetahui cara melindungi informasi pribadi secara *online* melalui kampanye inisiatif pembangunan kesadaran publik.

### 1. India

Pemerintah India mendefinisikan keamanan siber sebagai aktifitas perlindungan informasi dan sistem informasi dengan prosedur dan ukuran keamanan teknologi yang tepat. Kebijakan keamanan siber pemerintah India memiliki visi untuk membangun ketahanan dan keamanan ruang siber untuk masyarakat, bisnis dan pemerintahan. Sedangkan misi yang ingin dicapai adalah untuk melindungi informasi dan infrastruktur ruang siber, membangun kapabilitas untuk mencegah dan merespon ancaman keamanan siber, mengurangi kerawanan dan meminimasi kerusakan insiden siber melalui kombinasi struktur institusional, sumber daya manusia, proses, teknologi dan kerjasama.

Adapun tujuan strategis Pemerintah India dalam perlindungan keamanan siber dirumuskan sebagai berikut:[21]

1. Menciptakan lingkungan siber nasional yang aman, menghasilkan kepercayaan terhadap sistem dan transaksi IT yang akan meningkatkan pengaplikasian IT di seluruh sektor ekonomi.
2. Menciptakan kerangka kebijakan keamanan siber dan meningkatkan kepatuhan terhadap standar kemanan siber global berdasarkan praktik terbaik.
3. Memperkuat kerangka peraturan untuk memastikan keamanan ruang siber.
4. Menciptakan mekanisme pengamanan siber 24 jam di tingkat nasional dan sektoral dalam rangka merespon, resolusi dan menerapkan manajemen krisis terkait ancaman infrastruktur teknologi informasi melalui tindakan prediktif, preventif, protektif, tanggap dan menerapkan pemulihan yang efektif.
5. Meningkatkan perlindungan dan ketahanan infrastruktur informasi strategis negara dengan mengoperasikan Pusat Perlindungan Infrastruktur Penting Nasional (NCIIIPC) serta mewajibkan praktik keamanan infomasi berdasarkan pengembangan, penggunaan dan pengoperasian sumber daya informasi.
6. Mengembangkan teknologi keamanan siber nasional yang sesuai melalui penelitian teknologi yang berorientasi pada solusi, konsep, pengembangan, percontohan, transisi, difusi dan komersialisasi yang mengarah pada penyebarluasan produk teknologi informasi yang aman untuk menangani permasalahan keamanan siber nasional.
7. Meningkatkan visibilitas integritas produk dan layanan teknologi informasi dengan membangun infrastruktur untuk pengujian dan validasi produk keamanan siber.

---

[21] *National Cyber Security Policy. Ministry of Electronics & Information Technology. Government of India.* 2013

8. Menciptakan tenaga kerja sebanyak 500.000 profesional yang terampil dalam keamanan siber dalam jangka waktu 5 tahun melalui pengembangan kapasitas, pengembangan keterampilan dan pelatihan.
9. Memberikan manfaat fiskal bagi sektor bisnis dalam penerapan praktik dan proses keamanan siber.
10. Memberikan perlindungan informasi dalam proses, penanganan, penyimpanan dan transit untuk melindungi data pribadi warga negara dan untuk mengurangi kerugian ekonomi akibat pencurian data.
11. Melakukan pencegahan yang efektif, penyelidikan dan penuntutan kejahatan siber dan meningkatkan kapasitas penegakan hukum melalui intervensi legislatif yang sesuai.
12. Menciptakan budaya keamanan dan privasi siber yang memungkinkan terciptanya tanggung jawab perilaku dan tindakan pengguna melalui strategi komunikasi dan promosi yang efektif.
13. Mengembangkan kemitraan publik yang efektif dan keterlibatan kolaboratif melalui kerjasama dan kontribusi teknis dan operasional untuk meningkatkan keamanan siber.
14. Meningkatkan kerjasama global dengan mempromosikan pemahaman bersama dan peningkatan hubungan untuk penanganan masalah keamanan siber.

## 2. Singapura

Strategi keamanan siber Singapura bertujuan untuk menciptakan ruang siber yang aman dan terpercaya.[22] Pemerintah Singapura beranggapan bahwa ruang siber yang aman memungkinkan terealisasinya manfaat teknologi untuk masa depan yang lebih baik bagi warga negara Singapura. Pemerintah Singapura mengembangkan ruang siber yang

[22] Clarke, R. A., & Knake, R. *Cyber War: The Next Threat to National Security and What to Do About It* (1st Edition ed.). New York: Harper Collins Publishers. 2010

terdiri dari tenaga profesional, perusahaan berteknologi maju dan lembaga riset yang mendukung kebutuhan keamanan siber Singapura dalam tujuan pertumbuhan ekonomi. Selain pada lingkup nasional, mengingat bahwa ancaman siber tidak mengindahkan batas-batas kedaulatan negara, pemerintah Singapura juga berkomitmen dalam meningkatkan kemitraan internasional. Pada sektor bisnis, pemerintah Singapura melakukan mobilisasi dan membangun komunitas untuk menciptakan ruang siber yang lebih aman dengan melawan ancaman siber dan memaksimalkan perlindungan data pribadi.

Dalam memperkuat keamanan siber nasional, Pemerintah Singapuara memiliki empat pilar strategi sebagai berikut:[23]

1. Membangun ketahanan infrastruktur

   Dalam rangka mengamankan ruang siber di mana seluruh aspek kehidupan, khususnya ekonomi yang sudah terdigitalisasi, Pemerintah Singapura bekerja sama dengan para pemangku kepentingan untuk memperkuat keamanan siber nasional melalui lima langkah utama. Pertama, peningkatan manajemen resiko ancaman siber secara sistematis di semua sektor penting. Kedua, peningkatan respon dan pemulihan dengan mengadakan simulasi keamanan siber lintas sektor untuk mempersiapkan diri akan kemungkinan serangan siber. Ketiga, memperkuat sumber daya keamanan siber nasional seperti Tim Tanggap Bencana Siber Nasional (NCIRT) dan Pusat Keamanan Siber Nasional (NCSC). Kelima, memperluas upaya pengamanan sistem dan jaringan pemerintah untuk melindungi data pribadi warga negara.

2. Menciptakan ruang siber yang lebih aman

   Pemerintah Singapura menyadari bahwa ruang siber yang aman adalah tanggung jawab kolektif pemerintah, bisnis, perorangan dan masyarakat. Dalam rangka menghadapi ancaman keamanan siber secara efektif, Pemerintah Singapura meluncurkan *National*

[23] *Singapore's Cybersecurity Strategy. Cyber Security Agency of Singapore*, 2016.

*Cybercrime Action Plan.* Dalam hal ini, Pemerintah Singapura meningkatkan posisi negaranya sebagai pusat pembinaan data yang terpercaya. Kerjasama internasional juga dijalankan antara lain dengan lembaga global, negara lain dan penyedia layanan internet untuk dapat mengidentifikasi segala bentuk ancaman serangan siber dengan lebih cepat tanggap. Komunitas keamanan dan sektor bisnis juga memainkan peran pembinaan mengenai pemahaman permasalahan keamanan siber dan mendorong penerapan praktik yang baik.

3. Mengembangkan lingkungan siber yang prima

   Ruang siber pada saat yang bersamaan adalah sebuah tantangan dan kesempatan. Singapura dengan infrastruktur canggih dan tenaga kerja IT yang kompeten, sudah memiliki posisi yang baik untuk membangun ruang siber yang hidup. Pemerintah Singapura terus meningkatkan kapabilitas profesional di bidang keamanan siber dengan menjalin kolaborasi dengan industri mitra di bidang pengembangan kapabilitas teknologi siber, termasuk mendorong para profesional bidang teknologi informasi dan keamanan siber untuk terus memperdalam kemampuan mereka. Perkembangan bisnis berbasis teknologi yang semakin pesat juga didampingi dengan peningkatan kapabilitas layanan keamanan siber yang memadai. Pemerintah Singapura juga berkomitmen untuk terus memperkuat kemitraan dengan akademisi dan industri untuk memanfaatkan riset dan pengembangan solusi keamanan siber yang semakin terarah untuk menghasilkan solusi efektif akan ancaman keamanan siber, juga untuk menjadikan Singapura berasa di garis depan dalam hal inovasi keamanan siber.

4. Penguatan Kemitraan Internasional

   Isu keamanan siber adalah masalah global. Ancaman serangan dunia maya tidak memandang batas-batas kedaulatan. Serangan siber yang dihadapi oleh satu negara dapat mengakibatkan efek *spill-over* yang serius pada negara lain seperti halnya

interdependensi yang kian meningkat melalui kerjasama perdagangan dan pasar keuangan global.[24] Pemerintah Singapura berkomitmen untuk memperkuat kolaborasi kolektif global dalam penanganan ancaman keamanan siber. Selain itu, Pemerintah Singapura juga secara aktif bekerja sama dengan komunitas internasional, khususnya ASEAN dalam permasalahan keamanan siber transnasional dan kejahatan siber. Melalui kerjasama internasional, Pemerintah Singapura bertujuan untuk membangun kapasitas ruang siber yang aman dengan memfasilitisasi diskusi mengenai norma-norma dan aturan siber internasional.

## C. Kebijakan Keamanan Siber di Indonesia

Kebijakan keamanan siber Indonesia dimulai pada tahun 2007, setelah dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.KOMINFO/5/2007 tentang Keamanan Penggunaan Jaringan Telekomunikasi Berbasis Protokol Internet, yang kemudian diperbaharui dengan Peraturan Menteri Komunikasi dan Informatika No. 29 Tahun 2010.[25] Aspek penting dalam regulasi ini adalah pendirian ID-SIRTII (*Indonesia Security Incident Response Team on Internet and Infrastructure*) yang bertugas melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. ID-SIRTII memiliki tugas pokok melakukan sosialisasi dengan pihak terkait tentang keamanan sistem informasi, melakukan pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam

[24] Ghernaouti-Hélie, S. *Cybersecurity Guide for Developing Countries* (Enlarged Edition ed.). Geneva: International Telecommunication Union. 2009

[25] Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2017 Tentang Perubahan Keempat Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 26/Per/M.Kominfo/5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

tindakan pengamanan pemanfaatan jaringan, mengembangkan dan *database log file* serta statistik keamanan Internet di Indonesia.[26]

Dalam menangani kejahatan siber, pemerintah Indonesia memberlakukan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Walaupun Undang Undang ini membentuk landasan regulasi keamanan siber, tetapi ruang lingkupnya terbatas karena masih membutuhkan undang-undang lain untuk melengkapinya. Karena keterbatasan ini, penanganan kasus terkait kejahatan siber diproses dengan UU Perlindungan Konsumen No. 8/1999, UU Hak Cipta No. 19/2002 atau UU Anti-Pornografi No. 44/2008. Di bawah kepemimpinan Tifatul Sembiring, Kementrian Komunikasi dan Informatika menerapkan Peraturan No. 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif untuk mempromosikan penggunaan internet sehat. Melalui peraturan menteri ini, pemerintah memberikan prosedur hukum untuk memblokir 'situs negatif,' adapun 'situs negatif' didefinisikan sebagai mengandung materi pornografi atau ilegal berdasarkan undang-undang.[27] Adapun beberapa undang-undang lain yang mendukung penerapan keamanan siber, antara lain UU No. 36 tahun 1999 tentang Telekomunikasi, dan UU No. 14 tahun 2008 tentang Keterbukaan Informasi Publik, UU No.8 Tahun 1999 tentang Perlindungan Konsumen, UU No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, UU No. 3 2002 tentang Pertahanan Negara, UU No. 34 Tahun 2004, tentang Tentara Nasional Indonesia, UU No. 25 tahun 2009 tentang Pelayanan Publik.[28]

Dari segi regulasi, Indonesia belum memiliki kebijakan keamanan siber yang komprehensif dan integratif untuk menghadapi berbagai ancaman siber. Kemampuan dan daya tangkal siber Indonesia masih

---

[26] ibid

[27] Leonardus K. Nugraha And Dinita A. Putri. Mapping the Cyber Policy Landscape: Indonesia. Global Partners Digital. 2016

[28] Muhammad Rizal & Yanyan M. Yani. Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*, Vol. 4, No. 1.2016

lemah sehingga rentan terhadap serangan yang masif. Berangkat dari kesadaran akan perlunya suatu sistem terpadu yang bisa menangkal serangan-serangan siber, pemerintah Indonesia meresmikan Badan Sandi dan Siber Negara (BSSN) pada tahun 2017. BSSN merupakan revitalisasi Lembaga Sandi Negara (Lemsaneg) dengan tambahan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (Kemkominfo). BSSN berfungsi untuk mendeteksi, mencegah, dan menjaga keamanan siber. Selain membangun ekosistem ranah siber Indonesia yang kuat dan aman, BSSN juga menjadi penyelenggara dan pembina persandian negara dalam menjamin keamanan informasi dengan tujuan untuk menjaga keamanan nasional.[29]

Meskipun lemah dari segi regulasi, Indonesia cukup tangguh dalam hal teknis dan prosedural terkait penanganan ancaman keamanan siber. Indonesia menerapkan beberapa standar dan program yang diharapkan mampu menjadi pendorong utama untuk meningkatkan kemampuan dari tiap sektor yang ada dalam bidang keamanan ruang siber. Adapun standar dan program yang telah dilakukan oleh Pemerintah Indonesia antara lain; Perumusan Standar Nasional Indonesia mengenai sistem manajemen informasi keamanan, pelaksanaan program internet aman dan sehat, *Internet Devices Health & Safe for Children Indonesia* (Perisai), Nawala Project.[30]

Program *capacity building* juga dilakukan melalui instrumen seperti Standar Kompetensi Kerja Sektor Keamanan Informasi Nasional Indonesia (SKKNI). Instrumen ini digunakan untuk meningkatkan kapasitas sumber daya manusia dalam area keamanan informasi. Terdapat pula instrumen yang disebut sebagai Indeks KAMI (Indeks Keamanan Informasi) yang digunakan untuk mengukur tingkat keamanan ruang siber oleh lembaga-institusi-agensi pemerintah. Dalam

---

[29] Pengantar Strategi Keamanan Siber Indonesia. https://bssn.go.id/strategi-keamanan-siber-nasional/

[30] Muhammad Rizal & Yanyan M. Yani, op. cit

bidang kerjasama pengamanan *cyber space*. Indonesia telah menjadi anggota dari APCERT FIRST (*Forum for Incident Responses and Security Team*) Asia Pasifik. Indonesia anggota penuh sekaligus pendiri dari OIC CERT (*Organisasi Konferensi Islam Computer Emergency Response Team*). Beberapa prinsip utama menjadi basis mendasar strategi siber nasional, yaitu: (1) kepemimpinan, (2) pembagian tanggung jawab, (3) *partnership*, (4) kerjasama internasional, serta (5) manajemen risiko.[31]

Dari segi aktor, terdapat beberapa aktor penting yang terlibat dalam tata kelola keamanan siber di Indonesia yaitu pemerintah, sektor swasta dan masyarakat sipil, seperti dituangkan dalam tabel di bawah ini.

| Pemerintah | Sektor Swasta | Masyarakat Sipil |
|---|---|---|
| • Kemkominfo<br>• Kemenkopolhukam<br>• TNI<br>• POLRI<br>• BIN<br>• BSSN | • Telkom<br>• Google<br>• APJII<br>• IDEA | • Akademisi<br>• LSM<br>• Komunitas Teknologi |

**Gambar 1. Aktor yang terlibat dalam tata kelola keamanan siber di Indonesia**

Sumber: Diolah oleh penulis

**Pemerintahan**

Pendekatan lembaga pemerintah terhadap keamanan siber kebanyakan berfokus pada ancaman nasional dan perlindungan infrastruktur vital nasional. Saat ini, terdapat dua kementerian yang bertanggung jawab mengelola keamanan siber di Indonesia yaitu Kementerian Komunikasi dan Informatika dan Kementerian Koordinator Politik Hukum dan

[31] Rachma Fitriarti, Op.cit

Keamanan. Selain kedua kementerian ini, TNI, Polri, BIN dan BSSN juga berkontribusi dalam penanganan keamanan siber.

Kementerian Komunikasi dan Informatika membentuk ID-SIRTII pada tahun 2007 sebagai respon untuk perlunya strategi keamanan internet. Pada tahun 2010, Menkominfo mendirikan Direktorat Keamanan Informasi untuk membantu kementerian dalam merumuskan dan menerapkan kebijakan yang terkait dengan *cyber security*, bersama dengan penetapan norma, standar, prosedur dan kriteria di bidang informasi keamanan. Direktorat Keamanan Informasi dimasukkan di dalam struktur kemeterian, sementara ID-SIRTII bertindak sebagai badan negara yang independen.[32] Kementerian Koordinator Politik, Hukum, dan Keamanan juga memiliki desk keamanan siber, yang bertujuan untuk menangani dan mengelola ancaman keamanan siber nasional. Namun, semenjak BSSN dibentuk tahun 2017, tugas desk keamanan siber Kemenko Polhukam diambil alih oleh BSSN.[33] Hadirnya BSSN ditujukan untuk melaksanakan seluruh tugas dan fungsi di bidang persandian termasuk seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan termasuk infrastruktur telekomunikasi.

### Sektor Swasta

Dalam hal perkembangan teknologi, sektor swasta hampir selalu lebih maju dibandingkan pemerintah dan masyarakat sipil, hal ini juga berlaku dalam tata kelola keamanan siber. Di Indonesia, sektor bisnis berbasis teknologi kian meningkat, begitu pula dengan manajemen sibernya. Pendekatan sektor bisnis terhadap keamanan siber didasarkan pada perlindungan infrastruktur dan pengembangan bisnis. Sektor

---

[32] Meeting the cyber security challenge in Indonesia. DAKA Advisary Reports. British Embassy Jakarta. 2013.

[33] Pengantar Strategi Keamanan Siber Indonesia. https://bssn.go.id/strategi-keamanan-siber-nasional/

swasta atau bisnis memiliki pemahaman keamanan siber yang cukup baik karena mereka memiliki sumber daya untuk mengembangkan sistem dan peralatan yang diperlukan untuk perlindungan ruang siber. Dalam hal pembangunan kapabilitas, partisipasi sektor swasta akan menguntungkan bagi pengelolaan keamanan siber di Indonesia.

### Masyarakat Sipil

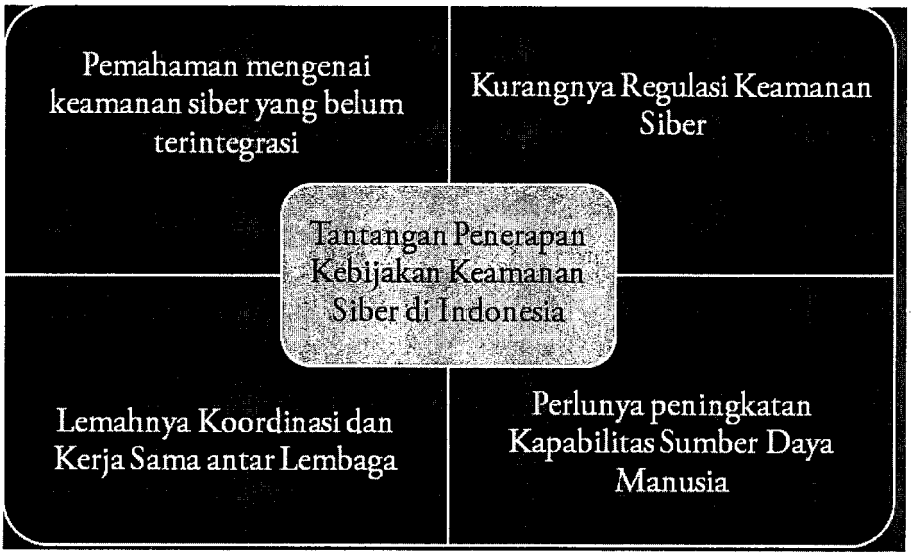
Menurut pendiri ID-CERT, Budi Raharjo, masyarakat sipil dan akademisi dapat memberikan kontribusi pada keamanan siber dengan meningkatkan kesadaran akan pentingnya membangun budaya penggunaan internet secara aman dan bertanggung jawab dalam segala bentuk aktivitas siber.[34] Seperti halnya pemerintah, komunitas masyarakat sipil juga memiliki pendekatan dan sudut pandang masing-masing terhadap keamanan siber. Misalnya, LSM yang menggunakan sudut pandang kebebasan menyuarakan pendapat, kelompok penggiat teknologi yang menyuarakan inovasi, atau kelompok akademisi yang menggunakan pendekatan keamanan nasional. Ragam prinsip-prinsip dasar ini pada akhirnya akan mengarah pada pendistribusian prioritas yang saling melengkapi satu sama lain.

## D. Problematika Kebijakan Siber di Indonesia

Berdasarkan tinjauan diatas mengenai implementasi kebijakan keamanan siber di Indonesia, terdapat empat permasalahan utama yang menjadi tantangan dalam pelaksanaan kebijakan keamanan siber nasional mulai dari regulasi, prosedur dan teknis, serta aktor-aktor yang terlibat, sebagaimana dituangkan pada diagram di bawah ini.

---

[34] Indonesia Computer Emergency Response Team https://www.cert.or.id/tentang-kami/id/




**Gambar 2. Tantangan Penerapan Kebijakan Keamanan Siber di Indonesia**

**Pemahaman mengenai keamanan siber yang belum terintegrasi**

Salah satu tantangan mendasar dalam penerapan sebuah kebijakan di Indonesia adalah mengenai penyelarasan pemahaman tentang objek kebijakan itu sendiri. Cara keamanan siber didefinisikan mencerminkan perspektif dan pendekatan yang berbeda dalam penentuan kebijakan. Tata kelola keamanan siber harus dapat merangkul beragam perspektif dan memungkinkan semua pemangku kepentingan untuk ambil bagian. Pendekatan keamanan yang bersifat partisipatif oleh berbagai lembaga mencerminkan bahwa nilai-nilai pemahaman bersama belum terealisasikan.

**Kurangnya regulasi keamanan siber**

Tidak dapat dipungkiri bahwa regulasi terkait keamanan siber perlu diselaraskan dengan peraturan-peraturan lainnya yang terkait, seperti Undang-Undang Telekomunikasi, Undang-Undang Anti-Terorisme, Undang-undang tentang Intelijen Negara, dan sejumlah peraturan

lainnya. Saat ini, peraturan yang paling relevan terkait dengan kasus siber adalah Undang-undang Telekomunikasi dan Undang-Undang Informasi dan Transaksi Elektronik (ITE). Namun, peraturan-peraturan ini dipandang ambigu dalam memberikan perlindungan bagi kebebasan berekspresi dalam batas-batas etika dan toleransi. Bahkan, jumlah kasus yang ditindak dalam UU UTE sebagian besar terkait dengan pencemaran nama baik. Hal ini mencerminkan perlunya meninjau peraturan yang ada, serta menyediakan seperangkat peraturan dan mekanisme yang lebih komprehensif dalam penanganan keamanan siber.

**Lemahnya Koordinasi dan Kerjasama antar-Lembaga**

Implementasi tata kelola keamanan siber di Indonesia pada saat ini belum terkoordinasi secara nasional serta masih bersifat sektoral berdasarkan kepentingan dan kemampuan masing-masing, khususnya pada sektor pemerintahan. Dengan adanya beberapa lembaga dan kementerian yang sama-sama menangani isu keamanan siber, menggambarkan adanya tumpang-tindih dalam penanganan keamanan siber itu sendiri. Walaupun terdapat pembedaan pendekatan di antara lembaga-lembaga tersebut, para aktor pemerintah ini masih memiliki mekanisme sendiri untuk menghadapi serangan siber. Lembaga yang berkaitan dengan penegakan hukum biasanya lebih fokus pada masalah kriminal siber, sementara yang terkait dengan kekuatan militer biasanya fokus pada spionase siber dan terorisme siber. Saat ini seluruh lembaga pemerintah terkait penanganan keamanan siber masing-masih berada langsung di bawah presiden. Belum adanya suatu badan koordinasi merupakan salah satu alasan mengapa implementasi kebijakan keamanan siber nasional Indonesia belum terintegrasi.

**Perlunya peningkatan kapabilitas sumber daya manusia**

Kesenjangan kapabilitas sumber daya manusia dalam bidang teknologi penting untuk diatasi. Menurut APJII (Asosiasi Penyedia Internet

Indonesia), sumber daya manusia dalam konteks siber didominasi oleh pekerja asing karena keahlian lokal masih dikategorikan rendah. Walaupun saat ini Indonesia memiliki sekitar lima ratus sektor profesional bersertifikat internasional dalam program keamanan siber seperti ISO270001, CEH, CISA, CISM dan CISSP, namun belum cukup untuk Indonesia sebagai salah satu negara pengguna internet terbesar di dunia dengan kerentanan serangan siber yang juga tinggi.[35] Penggunaan teknologi informasi akan mudah disadap atau diretas oleh para *hacker* maupun *cracker* dari negara asing, sehingga akan menciptakan kerawanan khususnya informasi intelijen yang menggunakan dunia maya sebagai sarana transmisi.

## E. Rekomendasi Implementasi Kebijakan Siber Nasional di Indonesia

Permasalahan keamanan ruang siber yang semakin marak terjadi di berbagai belahan dunia sebagai konsekuensi dari perkembangan teknologi informasi, merupakan permasalahan yang dihadapi seluruh negara di dunia. Dalam merespon hal ini, negara perlu menciptakan kondisi aman di ruang siber untuk memastikan warga negaranya mendapatkan perlindungan terbaik. Tujuan inilah yang menjadi referensi utama dalam merumuskan kebijakan siber yang sistematis, terkoordinasi dan terintegrasi. Hingga saat ini, implementasi kebijakan keamanan siber di Indonesia belum menjadi inisiatif nasional yang terkoordinasi. Langkah-langkah pelaksanaannya masih bersifat sektoral, dan sangat bergantung pada kepentingan dan kemampuan masing-masing sektor. Berdasarkan perbandingan dengan kebijakan keamanan siber yang diimplementasikan di berbagai negara terdapat beberapa rekomendasi yang dapat diterapkan di Indonesia sebagai berikut:

---

[35] Leonardus K. Nugraha And Dinita A. Putri. Op cit.

### 1. Menetapkan strategi keamanan siber melalui pendekatan menyeluruh

Penerapan kebijakan keamanan siber di berbagai negara didasarkan pada penetapan strategi yang tidak hanya mewakili kepentingan nasional masing-masing negara, tetapi juga melibatkan keseluruhan pemangku kepentingan di berbagai sektor secara menyeluruh. Pendekatan menyeluruh ini pula yang perlu diterapkan oleh Pemerintah Indonesia, yang melibatkan pemerintah, bisnis, akademisi dan oraganisasi masyarakat sipil untuk bersama-sama mengidentifikasi prioritas utama masing-masing. Pendekatan tata kelola keamanan siber harus dapat memfasilitasi seluruh sektor untuk fokus pada penanggulangan masalah keamanan siber. Sektor swasta bisa berfokus pada tata kelola infrastruktur, akademisi pada dimensi multidisipliner seperti sosial, ekonomi dan keamanan, dan komunitas teknologi pada isu keamanan jaringan, dengan saling berkoordinasi satu sama lain. Penetapan strategi keamanan siber secara menyeluruh membutuhkan komitmen jangka panjang, demi tercapainnya tujuan keamanan ruang siber nasional.

### 2. Penetapan regulasi kebijakan integratif

Implementasi kebijakan dan regulasi keamanan siber di Indonesia masih bersifat sektoral dan belum terintegrasi dan terkoordinasi dengan baik dan belum komprehensif sebagai satu kesatuan. Kementerian dan Lembaga Pemerintah yang terlibat dalam penanganan keamanan siber masih bekerja sendiri-sendiri, maka dari itu dibutuhkan suatu badan koordinasi untuk membangun sistem keamanan siber universal yang melibatkan keseluruhan sektor untuk melindungi negara dari ancaman siber. Selain koordinasi, ketersediaan payung hukum juga diperlukan sebagai bahan rujukan dalam menjalankan keseluruhan implementasi kebijakan keamanan siber nasional. Pengembangan dan penguatan kebijakan keamanan siber di Indonesia harus diintegrasikan dengan strategi nasional untuk membangun keamanan siber nasional, yang telah disiapkan oleh pemerintah. Strategi nasional mencakup upaya hukum

dan upaya teknis, seperti standar operasional penataan organisasi, manajemen keamanan siber, pengembangan kapasitas sumber daya manusia dan upaya untuk meningkatkan kerjasama internasional.

### 3. Kerjasama Internasional

Peningkatan kerjasama internasional juga penting dilakukan oleh Indonesia dalam menangani permasalahan keamanan siber. Salah satu aliansi strategis Indonesia dalam kebijakan keamanan dunia maya adalah dengan bekerja sama dengan Asosiasi Negara-negara Asia Tenggara (ASEAN) untuk menangani keamanan dunia maya. Indonesia juga telah secara konsisten bermitra dengan ASEAN di sektor keamanan siber, karena keunggulan pengembangan keamanan siber Singapura telah menyiapkan kebijakan, institusi, infrastruktur, dan program keamanan siber, dan upaya telah dibahas dalam forum kerjasama internasional. Singapura juga unggul dalam sumber daya manusianya, memiliki jumlah ahli keamanan informasi tertinggi di ASEAN. Selain di lingkup ASEAN, Indonesia juga perlu meningkatkan kerjasama di bidang keamanan siber dengan negara-negara yang memiliki *best practice* dalam kebijakan kemanan siber seperti Amerika Serikat, India dan Australia.

Ketiga rekomendasi di atas dapat diimplementasikan dalam implementasi kebijakan keamanan siber nasional Indonesia. Tidak dapat dipungkiri, rekomendasi di atas membutuhkan kerjasama dan koordinasi antar-aktor dan pemangku kepentingan yang terlibat. Misalnya, sektor swasta bisa menyediakan pelatihan bagi sektor pemerintah untuk meningkatkan pengetahuan terkait keamanan siber, komunitas pegiat teknologi dapat memfasilitasi diskusi perkembangan teknologi terkini, dan organisasi sipil dapat membantu pemerintah dalam merumuskan kebijakan dan mensosialisasikan informasi terkait keamanan siber kepada masyarakat.

## F. Penutup

Semakin pesatnya perkembangan teknologi informasi berdampak pada resiko ancaman di ruang siber yang mendorong negara untuk menata ulang kebijakan keamanan dalam merespon ancaman siber yang semakin nyata. Pencapaian kekuatan siber bergantung pada strategi dan kebijakan suatu negara dalam mengembangkan keamanan siber. Indonesia belum memiliki kebijakan khusus untuk mengelola dan menangani keamanan siber secara terintegrasi. Terdapat empat permasalahan utama dalam implementasi kebijakan keamanan siber di Indonesia. Pertama, Pemahaman mengenai keamanan siber yang belum terintegrasi. Kedua, Kurangnya Regulasi Keamanan Siber. Ketiga, Lemahnya Koordinasi dan Kerjasama antar-Lembaga. Keempat, Perlunya peningkatan Kapabilitas Sumber Daya Manusia.

Berdasarkan komparasi penerapan kebijakan keamanan siber di berbagai negara, terdapat tiga rekomendasi yang ditawarkan untuk diterapkan di Indonesia. Pertama, menetapkan strategi keamanan siber melalui pendekatan menyeluruh. Kedua, penetapan regulasi kebijakan integratif. Ketiga, peningkatan kerjasama internasional. Strategi keamanan siber yang kuat perlu diimbangi dengan dukungan hukum yang komprehensif dalam menghadapi ancaman keamanan siber. Penetapan regulasi yang tepat dan kerjasama dengan semua pihak baik pemerintah, sektor swasta dan masyarakat sipil, dapat menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.

## DAFTAR PUSTAKA

**Buku**

Clarke, R. A., & Knake, R. *Cyber War: The Next Threat to National Security and What to Do About It* (1st Edition ed.). New York: Harper Collins Publishers. 2010

Dorman, Andrew, et.al. *The Changing Face of Military Power*, Palgarave, 2002.

Ghernaouti-Hélie, S. *Cybersecurity Guide for Developing Countries* (Enlarged Edition ed.). Geneva: International Telecommunication Union. 2009

Gertz, Bill. iWar: War and Peace in the Information Age. 2017

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace.* Penguin Press. New York. 2017

Sterling, B. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books. 1992.

Thornton, Rod. *Asymmetric Warfare: Threat and Response in the 21st Century.* Cambridge: Polity Press.2006

**Jurnal**

Brenner, Susan W. Cyber-threats and the Limits of Bureaucratic Control, 14 Minn. J.L. Sci. & Tech. 137.2013

Fitriarti, Rachma. Membangun Model Kebijakan Nasional Keamanan Siber dalam Sistem Pertahanan Negara. 2014. Jakarta. Universits Pertahanan Indonesia.

Gazula, Mohan B. Cyber Warfare Conflict Analysis and Case Studies. Massachusetts Institute of Technology. 2017

Nugraha, Leonardus K. And Dinita A. Putri. Mapping the Cyber Policy Landscape:

Indonesia. Global Partners Digital. 2016

Rahmawati, Ineu. Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. Jurnal Pertahanan & Bela Negara. 2017. Vol 2.

Rizal, Muhammad & Yanyan M. Yani. Cybersecurity Policy and Its Implementation in Indonesia. Journal of ASEAN Studies, Vol. 4, No. 1.2016

Dokumen

Australia's Cyber Security Strategy. Commonwealth of Australia 2016.

Buku Putih Pertahanan Indonesia. Kementerian Pertahanan Indonesia.2015.

The Departement of Defense Cyber Strategy. United State's Departement of Defense. 2015.

National Cyber Security Policy. Ministry of Electronics & Information Technology. Government of India. 2013

Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2017 Tentang Perubahan Keempat Atas Peraturan Menteri Komunikasi Dan Informatika Nomor 26/Per/M.Kominfo/5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet

Singapore's Cybersecurity Strategy. Cyber Security Agency of Singapore, 2016.

Website

BIN: Australia menyadap Indonesia sejak 2007. https://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia

Cyber warfare: A different way to attack Iran's reactors. https://edition.cnn.com/2011/11/08/tech/iran-stuxnet/index.html

Indonesia Pertama Kali Bongkar Kasus "Cyber-Terrorism" https://www.antaranews.com/berita/42142/indonesia-pertama-kali-bongkar-kasus-cyber-terrorism

Mengenal DDoS, Teknik Peretasan yang Melumpuhkan Situs KPU https://tirto.id/mengenal-ddos-teknik-peretasan-yang-melumpuhkan-situs-kpu-cNn7

Secret US military computers 'cyber attacked' in 2008 https://www.bbc.com/news/world-us-canada-11088658

Serangan WannaCry di Indonesia Terbesar Kedua di Dunia. https://inet.detik.com/security/d-4007294/serangan-wannacry-di-indonesia-terbesar-kedua-di-dunia

United Nations Office on Drugs and Crime. Crimes Related to Computer Networks - Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Retrieved from United Nations Office on Drugs and Crime: https://www.unodc.org/document s/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.1 87.10_Crimes_Related_to_Comput er_Networks.pdf

Pengantar Strategi Keamanan Siber Indonesia. https://bssn.go.id/strategi-keamanan-siber-nasional/

Indonesia Computer Emergency Response Team https://www.cert.or.id/tentang-kami/id/

# Epilog

Tantangan politik siber yang erat bagi penguatan integrasi bangsa harus dijawab dengan komitmen melahirkan regulasi siber di tingkat peraturan perundang-undangan yang sejalan dengan iklim globalisasi. Pada titik inilah, ketentuan yang tertuang dalam regulasi siber diharapkan benar-benar dapat diandalkan dalam rangka menjaga kedaulatan negara dan sekaligus menjaga hak privasi individu sebagai bagian dari demokrasi.

Pemerintah di tengah membanjirnya informasi, termasuk informasi sampah atau muatan terorisme atau sekedar radikalisme, jangan sampai berfikir untuk menutup siber. Langkah yang tepat adalah dilakukan pengaturan secara tegas dalam pengelolaan siber agar media digital digunakan sebagai bentuk kemajuan bangsa dalam pengelolaan kedaulatan negara secara kondusif melalui kehadiran pemerintahan yang baik (*good governance*).

Pada hakikatnya tata kelola keamanan siber ditujukan untuk membangun keamanan sistem informasi baik di tingkat daerah, maupun saat berintegrasi dengan sistem di tingkat nasinal. Keamanan Sistem Informasi Internal bertujuan untuk menjaga, *pertama* **Kerahasiaan.** Untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumber daya manusia, dan sistem pengolahan transaksi, adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi. *Kedua,* **Ketersediaan.** Supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya. *Ketiga* **Integritas.** Seluruh sistem informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakili.

Kunci untuk mengembangkan *cyber security* oleh Pemda adalah 'menuntaskan infrastruktur *online* dan mempersiapkan SDM nya', setelah itu dituntaskan, barulah Pemda akan mampu menata diri bagi pengembangan *cyber security.* Pemda harus memacu diri untuk menerapankan sistem pemerintahan berbasis *online.* Hanya dengan kemajuan dalam dunia maya lah maka perang *cyber* dapat ditangani oleh Pemda. Serangan-serangan dari pihak-pihak yang tidak bertanggung jawab dalam dunia *cyber* yang mengedepankan sistem memecah-belah persatuan dan kesatuan masyarakat, harus diimbangi dengan kemampuan Pemda dalam menguasai teknologi *online,* terutama *cyber security.* Tanpa itu, tentu Pemda akan menjadi "bulan-bulanan" dari para kriminal *cyber* yang demi kepentingan pribadi atau golongannya semata, bisa menghancurkan kerukunan antar-warga.

Semakin pesatnya perkembangan teknologi informasi berdampak pada resiko ancaman di ruang siber yang mendorong negara untuk menata ulang kebijakan keamanan dalam merespon ancaman siber yang semakin nyata. Pencapaian kekuatan siber bergantung pada strategi dan kebijakan suatu negara dalam mengembangkan keamanan siber. Indonesia belum memiliki kebijakan khusus untuk mengelola dan menangani keamanan siber secara terintegrasi.

Terdapat empat permasalahan utama dalam implementasi kebijakan keamanan siber di Indonesia. Pertama, pemahaman mengenai keamanan siber yang belum terintegrasi. Kedua, kurangnya regulasi keamanan siber. Ketiga, lemahnya koordinasi dan kerjasama antar-lembaga. Keempat, perlunya peningkatan kapabilitas sumber daya manusia. Penetapan regulasi yang tepat dan kerjasama dengan semua pihak baik pemerintah, sektor swasta dan masyarakat sipil, dapat menjadi kunci dalam menghadapi tantangan dunia siber yang semakin kompleks.

Penyuting

# Indeks

# Profil Penulis

**Ahmad Budiman,** Lahir di Jakarta, 22 April 1969. Memperoleh gelar sarjana bidang komunikasi dari Institut Ilmu Sosial Ilmu Politik (IISIP) Jakarta tahun 1993 dan Magister Penelitian dan Evaluasi Pendidikan dari Universitas Muhammadiyah Prof. DR. HAMKA (2004). Jabatan saat ini adalah Peneliti Madya IV/b untuk bidang kepakaran komunikasi politik. Menjadi tim asistensi untuk pembahasan RUU tentang Keterbukaan Informasi Publik, RUU Rahasia Negara, RUU Intelijen Negara, RUU Penyiaran, RUU Hukum Disiplin Militer dan RUU Radio Televisi Republik Indonesia. Tulisan yang telah dibukukan di antaranya berjudul: "Bunga Rampai Keterbukaan Informasi Publik", dan "Aspirasi Masyarakat dan Respons DPR RI". Tulisan dalam bagian dari buku di antaranya "Peningkatan Citra Bangsa melalui Kemandirian Industri Pertahanan", "Optimalisasi Pengelolaan Keterbukaan Informasi Publik di DPR RI", "Kesiapan Lembaga Penyiaran Melaksanakan Digitalisasi Penyiaran", "Tata Kelola Keterbukaan Informasi di Era Pemerintahan Elektronik", dan "Urgensi Sistem Keamanan Telekomunikasi Bagi Peningkatan Kualitas Komunikasi Organisasi Pemerintah Daerah". Juga tulisan dalam jurnal ilmiah di ataranya berjudul "Pola Komunikasi Pembangunan Pada Daerah Pemekaran" dan "Mekanisme Pengaduan Masyarakat ke DPR RI". Email: a.budiman69@gmail.com

---

**Aryojati Ardipandanto,** menyelesaikan pendidikan sarjana Ilmu Pemerintahan dari Universitas Langlangbuana (Yayasan Bhrata Bhakti Polri) Bandung pada tahun 2003. Penelitian-penelitan yang dilakukannya terkait dengan masalah-masalah pemerintahan, politik, dan industri pertahanan. Ia pernah menjadi Tim Asistensi Penyusunan Rancangan Undang-Undang tentang Industri Pertahanan, yang sudah

disahkan menjadi UU No. 16 Tahun 2012 tentang Industri Pertahanan. Selain itu, penulis adalah anggota tim Pidato Sekretariat Jenderal DPR RI sejak tahun 2011 hingga sekarang. Ia terlibat pula sebagai anggota Tim Buku Kinerja Tahunan DPR RI.

Email: aryojati.ardipandanto@gmail.com

---

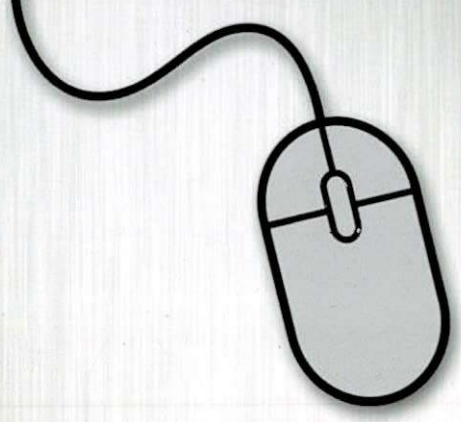
**Prayudi,** bekerja di Sekretariat Jenderal DPR RI sejak tahun 1990. Peneliti Bidang Politik Pemerintahan Indonesia di Pusat Pengkajian, Pengolahan Data dan Informasi Sekretariat Jenderal (P3DI Setjen DPR RI). Aktif melakukan beberapa penelitian lapangan dan riset kepustakaan terkait masalah-masalah sosial politik. Anggota Dewan Redaksi Jurnal *Kajian* P3DI Setjen DPR RI. Beberapa kegiatan lainnya, antara lain pernah ikut sebagai anggota Tim Asistensi pembahasan Rancangan Undang-Undang (RUU) tentang Penyelenggaran Pemilu (2007), RUU tentang Bahan Kimia dan Larangan Penggunaan Bahan Kimia Sebagai Senjata Kimia (2008), RUU tentang Rencana Pembangunan Jangka Panjang Nasional tahun 2005-2025 (2006), RUU tentang MPR, DPR, DPD, DPRD (2008-2009), RUU tentang Intelijen (2011) RUU tentang Desa (2013), dan RUU tentang Pemda (2013-2014).

Email: prayudi_pr@yahoo.com

---

**Aulia Fitri,** lahir di Bandung, 19 Mei 1988. Menyelesaikan Pendidikan S1 Hubungan Internasional di Universitas Katolik Parahyangan pada tahun 2010 dan Pendidikan S2 Manajemen Pertahanan di Universitas Pertahanan pada tahun 2015. Saat ini menjabat sebagai Calon Peneliti Bidang Politik Dalam Negeri untuk kepakaran Studi Pertahanan di Pusat Penelitian Badan Keahlian DPR RI. Kajian-kajian yang telah dilakukan penulis adalah mengenai Industri Pertahanan, Reformasi Sektor Keamanan, Terorisme dan Kerjasama Pertahanan.

Email. auliarosadi@gmail.com



Era Industri 4.0 yang didukung perkembangan teknologi komunikasi dan informasi amat cepat, telah merubah tatanan sosial dan bisnis serta perilaku masyarakat. Pada tahun 2018, pengguna internet di bumi sudah mencapai 3,6 miliar manusia. Karena itu, sangat diperlukan suatu antisipasi lembaga negara bukan hanya dalam bentuk formalitas yuridis melalui UU ITE, tetapi lebih pada penataan dalam mengelola arus komunikasi dan informasi yang berkembang di masyarakat dengan adanya keamanan ciber (cyber scurity).

Secara apik, buku ini mengulas hal-ikhwal cyber scurity dalam rangka mewujudkan keberadaan lembaga formal yang serius, profesional dan berkelanjutan sehingga melahirkan karaker bangsa dan nasionalisme yang kuat.
Selamat membaca



INTELIGENSIA
INTRANS PUBLISHING

ISBN: 978-602-603
9 786026 036728