Padjadjaran Journal of International Relations (PADJIR)
e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

ASEAN *Personal Data Protection* (PDP): Mewujudkan Keamanan Data Personal Digital pada Asia Tenggara

Trisa Monika Tampubolon
Program Studi Hubungan Internasional, Universitas Padjadjaran, Indonesia;
email:trisamonika@gmail.com
Rizki Ananda Ramadhan
Departemen Studi Hubungan Internasional, Universitas Padjadjaran, Indonesia;
email: rizkiar@gmail.com

Dikirim:	Direvisi:	Diterima:	Dipublikasikan:
1 Juli 2019	30 November 2019	28 Januari 2020	31 Januari 2020

Keywords
ASEAN, ASEAN PDP, cybersecurity, personal data protection, role theory

ABSTRACT
The purpose of this article is to explain the role of ASEAN in realizing the security of personal digital data through ASEAN Personal Data Protection (PDP) in the context of ASEAN digitalization. Researchers used the Role Theory proposed by Lisbeth Aggestam. In analyzing the role of ASEAN PDP, researchers used the role theory to analyze what roles the ASEAN PDP performed and how it contributed to the process of digitally securing personal data. In this study, researchers used qualitative methods with discourse analysis techniques used to analyze roles. It's found that ASEAN PDP has a crucial role in the process of realizing the security of digital personal data with an increase in cyber security programs and policies. Supported by other additional documents, such as ASEAN ICT Masterplan 2020 and Work Plan on ASEAN Cyber, ASEAN PDP has proven to be one of the 'tools' in assisting the ASEAN digitalization process which continues to this day.

Kata Kunci
ASEAN, ASEAN PDP, keamanan data personal, keamanan siber, teori peran

ABSTRAK
Tujuan dari artikel ini adalah menjelaskan bagaimana peran ASEAN dalam mewujudkan keamanan data personal digital melalui ASEAN *Personal Data Protection* (PDP) dalam rangka digitalisasi ASEAN. Peneliti menggunakan teori Peran (*Role Theory)* yang dikemukakan oleh Lisbeth Aggestam. Dalam menganalisis peran dari ASEAN PDP, peneliti menggunakan teori peran tersebut untuk menganalisis apa saja peran yang dilakukan ASEAN PDP dan bagaimana ia berkontribusi dalam proses pengamanan data personal secara digital. Dalam artikel ini, penulis menggunakan metode kualitatif dengan teknik analisis diskursus yang digunakan untuk menganalisis peran. Artikel ini menemukan bahwa ASEAN PDP memiliki peran yang krusial dalam proses mewujudkan keamanan data personal digital dengan adanya peningkatan program dan kebijakan keamanan siber. Didukung oleh dokumen tambahan lainnya, seperti ASEAN ICT *Masterplan* 2020 dan *Work Plan on* ASEAN *Cyber*, ASEAN PDP terbukti sebagai salah satu 'alat' dalam membantu proses digitalisasi ASEAN yang masih berlanjut sampai saat ini.

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

PENDAHULUAN

Data personal berkembang secara dinamis seiring kemajuan teknologi, terutama pada bidang perekonomian. Menurut UNCTAD, perkembangan ICT terbaru dapat dibagi menjadi tiga: *cloud computing; IoT;* dan *Big Data analytics* (UNCTAD, 2016).

'Ruang siber' yang tidak terbatas tersebut berpengaruh terhadap minimnya pengawasan negara untuk mengendalikan kegiatan pada 'ruang' bagian mereka. Di samping itu, minimnya pengetahuan serta kurangnya kemampuan untuk bersaing dengan model sistem yang lebih canggih dan *up-to-date*. Akibatnya, ancaman yang ditimbulkan dapat tidak terdeteksi sampai data pribadi terekspos tanpa pemberitahuan apapun.

Sebagai inti dari pergerakan aktivitas digital, data personal menjadi aset yang harus dilindungi untuk mencegah penyalahgunaan dari data tersebut. Oleh karena itu, isu ini tidak luput dari campur tangan penstudi Hubungan Internasional dimana keamanan data personal memerlukan regulasi ketat (UNCTAD, 2016).

Jika dikaitkan dengan kondisi ASEAN, tantangan yang dihadapi negara-negara anggota ASEAN masih seputar kesepakatan dengan pemerintahan yang belum mencakup seluruh negara anggota sehingga terjadi ketimpangan pengetahuan dimana keamanan siber masih berpusat pada negara Singapura, Malaysia, Thailand, dan Vietnam. Upaya konkrit dari pengembangan keamanan siber tersebut diupayakan melalui agenda kebijakan regional dengan pembentukan *Rapid Action Cybersecurity Framework*.

ASEAN sendiri merupakan hasil dari regionalisasi yang membentuk sebuah kesatuan yang terdiri atas negara-negara di Asia Tenggara (Mansfield & Solingen, 2010). ASEAN menjadi asosiasi yang didirikan pada tanggal 8 Agustus 1967 di Bangkok yang diprakarsai oleh Indonesia, Filipina, Malaysia, Singapura, dan Thailand. Anggota ASEAN kemudian berkembang menjadi 10 negara di Asia Tenggara yaitu Filipina, Indonesia, Malaysia, Singapura, Thailand, Brunei Darussalam, Vietnam, Laos, Mynmar, dan Kamboja (The ASEAN Charter, 2008, p. 1).

Berkaitan dengan AEC, integrasi tersebut juga menjadi wadah untuk meningkatkan kegiatan ekonomi antarnegara beserta regulasinya , salah satunya dalam masalah keamanan data pribadi. Maka dari itu, negara-negara anggota ASEAN berkomitmen untuk meningkatkan kerjasamanya, terutama pada isu non-tradisional. Agenda ASEAN terkait respon terhadap ancaman maupun serangan dibahas dalam beberapa badan sektor ASEAN, seperti AMMTC, ADMM-Plus, ARF, dan TELMIN.

Keamanan data personal menjadi agenda penting bagi negara anggota ASEAN akibat adanya indikasi bahwa ASEAN menjadi target utama akan aktivitas kejahatan siber. Hal ini terjadi karena beberapa alasan. *Pertama*, beberapa negara anggota dijadikan 'pusat' aktivitas internet yang berbahaya. Terdapat beberapa kasus sehubungan dengan penerobosan data pada negara-negara ASEAN yang terjadi dari tahun 2016 hingga sekarang.

Kedua, rendahnya kemampuan keamanan siber atau regulasi pada kawasan tersebut. *Ketiga*, kurangnya kemampuan serta industri yang berfokus pada keamanan siber. *Keempat*, adanya anggapan dari pemegang perusahaan bahwa keamanan siber tidak termasuk dalam prioritas bisnis yang menimbulkan kekosongan pendekatan nyata terhadap ketahanan siber (Sunkpho, Ramjan, & Ottamakorn, 2018). Keamanan yang tidak ketat memperluas kemungkinan terjadinya dampak negatif pada pasar melalui pengurangan kepercayaan konsumen hingga terlalu membatasi bisnis yang mengakibatkan kerugian (UNCTAD, 2016).

Urgensi akan peran ASEAN terhadap keamanan data personal selanjutnya berkaitan dengan potensi ASEAN dalam perekonomian digital pada tahun 2025 yang diprediksi mencapai pertambahan 1 triliun dolar terhadap APBN yang berlanjut hingga perkembangan layanan digital seperti sektor keuangan dan komersil (A.T. Kearney, 2018). Bahkan,

ASEAN memiliki potensi dalam ekonomi digital untuk menambahkan dana GDP hingga 10 tahun. Namun, resiko yang muncul tidak dapat ditanggung 'bersama' jika hanya beberapa negara anggota yang dapat mencapai target tersebut. Padahal, sebagai suatu organisasi regional, ASEAN dapat menjadi media penghubung dalam upaya peningkatan pengetahuan dan kemampuan negara yang masih 'tertinggal'.

Berdasarkan latar belakang yang telah dikemukakan, penulis merumuskan sebuah rumusan masalah, yaitu "Bagaimanakah peran ASEAN dalam mewujudkan keamanan data personal digital melalui ASEAN *Personal Data Protection*?"

KERANGKA KONSEPTUAL

Role Theory

Lisbeth Aggestam membagi peran organisasi internasional ke dalam beberapa fokus konsep, baik dari pemahaman subjektif atau penampilan sebenarnya, yang terdiri dari *role expectation, role conception, role performance,* dan *role-set*.

Role expectation memberikan ekspektasi bahwa aktor lain mengharapkan adanya *role-beholder* seperti yang diperlihatkan oleh institusionalisasi identitas yang menghasilkan harapan yang luas sehingga cenderung membatasi lingkup peran yang diperlihatkan oleh pembuat kebijakan. (Aggestam, 2006).

Role conception merupakan seperangkat norma yang menggambarkan orientasi tindakan dan sikap kebijakan luar negeri atau juga dikatakan sebagai peta bagi pembuat kebijakan untuk menyederhanakan dan memfasilitasi pemahaman terhadap realitas politik. Barnett (1993) berpendapat bahwa institusi mendapatkan kestabilannya ketika aktor mengadopsi konsepsi peran tertentu dan memodifikasi sikap mereka berdasarkan peran, sikap, dan harapan masing-masing secara konsisten (Aggestam, 2006).

Konsepsi peran mencakup perpaduan nilai dan deskripsi realitas yang mungkin sebagian atau umum dan kurang lebih nyata. Ia dapat memperlihatkan maksud dan tujuan dari aktor kebijakan luar negeri. Adapun konsepsi ini membantu pilihan strategi yang sesuai meskipun tidak langsung menentukan hasil akhirnya (Aggestam, 2006).

Di sini terdapat ekspektasi normatif dimana *role beholder* menyatakan ego-nya sendiri yang berkenaan dengan dimensi subjektif dari kebijakan luar negeri, yakni kewajiban dan tanggung jawab, untuk menyingkap maksud dari tindakan tersebut. Penting untuk diingat bahwa aktor internasional cenderung memiliki peran ganda yang disesuaikan dengan konteks situasi dan institusional. Peran yang dimainkan akan semakin stabil seiring semakin jauh sosialisasi pembuat kebijakan dalam konsepsi peran tersebut (Aggestam, 2006).

Pendekatan interaksional, dimana kapasitas aktor menentukan perannya, menjadi dasar dari *role-playing* dimana merupakan proses aktor. *Role-play* atau *role enacment* merupakan perilaku sesungguhnya yang dilakukan negara ketika suatu peran sudah ditentukan. *Role-play* serta *role conception* membentuk suatu proses relasi dimana entitas (ego) memposisikan dirinya dengan *Other* (alter). Berikut ini adalah gambaran pola umum dari perubahan peran.

Role performance menggambarkan perilaku kebijakan luar negeri mengenai pola karakter dari keputusan dan tindakan pada konteks situasional. Jika Holsti mengatakan bahwa perilaku tersebut dijelaskan oleh konsepsi peran, Aggestam melihat bahwa hubungan kedua konsep tersebut hanya dapat diterapkan secara umum dikarenakan peran aktor yang cenderung banyak. Dengan kata lain, konsepsi peran tidak langsung menentukan hasil tapi mendefinisikan lingkup opsi dan strategi potensial hingga akhirnya diterapkan.

METODE RISET

Artikel ini merupakan luaran riset skripsi yang disusun dengan menggunakan metode kualitatif. Objek kaji artikel ini adalah *Framework of* ASEAN PDP. Penulis memandang bahwa ASEAN PDP memiliki peran krusial dalam mewujudkan keamanan

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

data personal terutama pada kawasan Asia Tenggara. Penulis mengumpulkan bahan artikel, baik primer maupun sekunder, dengan cara studi literatur, wawancara, dan observasi.

PERAN ASEAN PDP DALAM KEAMANAN DATA PERSONAL

Kondisi Keamanan Siber

Sebagai kawasan yang dianggap memiliki potensi besar dalam perkembangan digital, ASEAN masih menghadapi ancaman *cyberattack*. Terdapat beberapa alasan yang mendasari pernyataan ini, antara lain kebijakan yang masih baru, kurangnya perlindungan terhadap ekonomi digital dan ahli keamanan siber, tidak ada pendekatan holistik terhadap ketahanan siber, hingga kompleksitas operasional yang memperlambat deteksi dan respon terhadap serangan siber. Selain itu, dibandingkan dengan besar PDB yang dihabiskan untuk pembangunan digital, negara anggota ASEAN hanya memakai 0,06 persen untuk keamanan siber dimana jumlah tersebut jauh dari rata-rata dunia, yakni lima kali PDB mereka.

Peningkatan keamanan siber secara signifikan tercermin dari Singapura dengan melakukan pembaharuan *National Cyber Security Master Plan*, *Cyber Watch Centre*, dan *Threat Assessment Centre*. Singapura membentuk Agensi Keamanan Siber (CSA) pada semua sektor sebagai mitra privat dan publik. Ancaman yang muncul diidentifikasi melalui adanya prakarsa yang dibentuk untuk mengatasi kelemahan dan 'gap' pada infrastruktur. Hukum yang terkait dengan keamanan siber meliputi *Computer Misuse and Cybersecurity Act*, *Electronic Transactions Act*, dan PDPA.

Isu ancaman siber juga menjadi topik hangat di Filipina seiring bertambahnya interaksi online seperti *cybersquatting*, pornografi anak, *cybersex*, pencurian data, serta pencemaran nama baik. Beberapa hukum yang terkait yakni *Cybercrime Prevention Act* tahun 2012, *Electronic Commerce Act* 2000, *Data Privacy Act* 2012. Sesuai dengan keputusan Pengadilan Tertinggi (SC), terdapat beberapa bidang yang diaggap sebagai bagian dari undang-undang, termasuk yang telah disebutkan di atas.

Negara anggota selanjutnya masuk sebagai 25 target tertinggi dari serangan *malware* yakni Thailand. Regulasi yang dibentuk seperti (amandemen) *Crime Bill*, *Personal Data Protection*, dan *Cybersecurity Bill*.

Dengan kondisi ASEAN tersebut, terdapat kekuatan dan kelemahan dalam mencapai keamanan siber regional. Wilayah yang luas menyumbang potensi yang besar dalam pertumbuhan ekonomi digital serta menjadikan kawasan ASEAN sebagai pusat kerjasama dengan negara-negara lain seperti Jepang, Amerika Serikat, Cina, bahkan Eropa. Akan tetapi, kebijakan dan pendekatan yang beragam berdampak pada ketidakseimbangan pengetahuan tentang ruang siber. Ketimpangan antarnegara meliputi keterpaduan regional, perbedaan jumlah ahli dan inovator, standardisasi, dan perekonomian maupun budaya.

Pertumbuhan pasar IoT yang pesat meningkatkan peluncuran program baru yang cenderung sederhana dan mudah diserang. Hal ini dapat dilihat dari Laporan NTT *Security* 2017 dimana 60 persen serangan IoT berpusat pada Asia. Secara umum, negara anggota ASEAN menyusun strategi tertentu dalam meningkatkan keamanannya. Contohnya, Singapura dan Malaysia mengembangkan ahli keamanan siber. Filipina telah menyusun *National Cybersecurity Plan* 2022. Kerjasama juga ditawarkan kepada Jepang dari Thailand untuk membentuk program pelatihan keamanan siber untuk ASEAN. Pelatihan dan usaha *capacity building* membutuhkan waktu yang lama sehingga jika ingin mengejar rata-rata dunia, masih banyak persiapan dan praktik yang perlu dilakukan oleh negara anggota ASEAN, terutama bagi negara yang bahkan belum memiliki regulasi di bidang keamanan siber (A.T. Kearney, 2018).

Kerjasama yang dilakukan negara anggota ASEAN di antaranya: (1) ASEAN

Cybersecurity Cooperation Strategy yang melibatkan peta koordinat pada daerah insiden serangan siber; (2) pembentukan ARF yang memimpin diskusi perihal isu keamanan siber; (3) perayaan *Cyber* SEA *Games* yang ditujukan bagi mereka yang memiliki keahlian di bidang siber (Access Partnership, Ltd, 2017).

Bentuk kerjasama tersebut menjadikan keamanan siber sebagai fokus kebijakan ASEAN. Selain AMMTC dan TELMIN, ASEAN juga mengupayakan pelatihan keamanan siber dan pengembangan kapasitas melalui ASEAN *Ministerial Conference on Cybersecurity* (ACMC), ARF, *Intter-Sessional Meeting* pada Keamanan ICT, ADMM Plus, hingga diskusi dengan pihak eksternal (contohnya Jepang). Menteri ASEAN akan membuat kemajuan pada: (1) diskusi ASEAN ICT dan Kementerian Keamanan Siber pada AMCC, TELMIN, serta badan lainnya seperti AMMTC, untuk mengidentifikasi norma praktis dari perilakun egara dalam ruang siber yang dapat diadopsi dan diterapkan; (2) memfasilitasi kerjasama lintas-batas dalam menangani kerentanan infrastruktur, serta (3) meningkatkan pengembangan kapasitas dan ukuran kerjasama untuk membahas penggunaan menyimpang dari *cyberspace* sesuai dengan rekomendasi pada 2015 *Report of the United Nations Group* atau UNGGE.

Dalam meningkatkan keamanan siber, ASEAN memiliki beberapa langkah-langkah kebijakan. *Pertama*, mempromosikan strategi untuk mendeteksi ancaman sesuai dengan hukum internasional dan prinsip-prinsipnya. *Kedua*, mempromosikan dialog terkait tindakan pengurangan resiko dengan membagikan perspektif setiap negara anggota dalam menggunakan ICT pada konflik. *Ketiga*, mendorong kerjasama antarnegara. *Keempat*, mengembangkan rencana keamanan dalam penggunaan ICT secara teoritis dan praktik. *Terakhir*, mempertimbangkan perluasan istilah-istilah dan definisi yang berhubungan dengan penggunaan ICT. ASEAN mulai meningkatkan hubungan negara di kawasan dengan membangun sektor ICT, salah satunya melalui pembentukan *Computer Emergency Response Team* (CERT).

Profil ASEAN PDP

ASEAN PDP merupakan kerangka kesepakatan yang dibentuk negara anggota ASEAN untuk memperkuat perlindungan data personal pada ASEAN dan memfasilitasi kerjasama antarnegara sambil berkontribusi mempromosikan dan mengembangkan perdagangan hingga arus informasi secara regional dan global. ASEAN PDP dibentuk sesuai dengan *blueprint* ASEAN *Economic Community* (AEC) 2025 yang diadopsi pada ASEAN Summit ke-27 tahun 2015 silam yang menekankan perlunya perkembangan kerangka kebijakan perihal perlindungan data personal secara komprehensif.

ASEAN TELMIN sendiri mulai dilakukan sejak Juli 2001 di Malaysia. TELMIN mengambil aspek teknologi dari program kerja e-ASEAN. Ada empat objektif dari Kerangka e-ASEAN yang dibawa *Telecommunications and Information Technology Senior Officials Meeting* (TELSOM), yakni untuk mengembangkan, memperkuat, dan meningkatkan daya saing sektor ICT, mengurangi pembagian digital di dalam dan antara negara ASEAN, mempromosikan kerjasama antara aktor publik dan privat, serta mengembangkan infrastruktur informasi ASEAN. Kolaborasi antarnegara dilanjutkan melalui ASEAN ICT *Masterplan* 2015 yang mengandung kegiatan dan proyek dengan target tertentu untuk menghasilkan empat poin penting: (a) UCT sebagai mesin penggerak pertumbuhan negara anggota ASEAN; (b) ASEAN dianggap sebagai penghubung ICT; (c) meningkatkan kualitas kehidupan masyarakat ASEAN; dan (d) kontribusi akan integrasi ASEAN.

Kerangka ASEAN PDP berupaya untuk membantu perkembangan kerjasama dan integrasi regional dalam mendorong ASEAN mencapai perekonomian yang aman dan berkelanjutan dan berbasis digital. Agar tujuan tersebut tercapai, ASEAN harus menguatkan keamanan data personal yang akan

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

berkontribusi terhadap promosi serta pertumbuhan perdagangan maupun arus informasi antar negara ASEAN dalam ekonomi digital. Kerangka ini diperlukan pemerintah negara Asia dimana ia sebagai satu dari dua kerangka perlindungan data dan privasi multilateral di wilayah tersebut untuk mengakomodasi tingkat-tingkat regulasi keamanan data dan privasi yang berbeda-beda secara fleksibel (GSMA, 2018).

Kesepakatan dalam kerangka ASEAN PDP lebih bersifat *voluntary* sesuai dengan bentuknya sebagai "*framework*", bukan "*agreement.*" *Framework* lebih bersifat *unbinding* dimana tidak memiliki target penerapan hukum perlindungan data di semua negara ASEAN. Maka dari itu, ASEAN PDP lebih merupakan *roadmap*, bukan kesepakatan. Aktivitas pada ASEAN PDP sejauh ini lebih berkisar pada *sharing experience* dalam penyusunan dan penerapan PDP *law* pada tingkat nasional. Terkait hal itu, sebenarnya sudah ada upaya untuk meningkatkan *political awareness* tentang pentingnya kesepakatan ini. Di antaranya dengan membawa isu tersebut pada ASEAN *Interparliamentary Assembly* tahun 2018 yang salah satu rekomendasinya adalah mendorong negara-negara anggota ASEAN untuk memperbanyak tukar pikiran tentang legislasi PDP.

Melalui ASEAN PDP, setiap negara anggota mengusahakan bentuk kerjasama hingga implementasi prinsip-prinsip kerangka ASEAN PDP tersebut pada regulasi dan hukum domestik serta menyediakan kebebasan arus informasi. Pada tingkat domestik, ada kemungkinan perubahan adopsi sesuai dengan situasi lokal dimana ASEAN PDP tidak mengikat pada ranah domestik atau internasional. Beberapa prinsip yang terdapat pada kerangka ASEAN PDP meliputi keamanan, akses dan koreksi, transfer (data), penyimpanan, dan akuntabilitas (GSMA, 2018, hal. 58).

Data Breaching

Dalam membahas isu siber secara lintas-sektor, Singapura membentuk mekanisme non formal sebagai bentuk forum untuk ASEAN, yakni ASEAN Ministerial Coordinating Meeting on Cyber (AMCC). Meskipun masih berbentuk kerangka, beberapa program yang dicanangkan atas dasar ASEAN PDP sudah mulai diberlakukan. Secara global sendiri, pembahasan siber di ranah PBB ada di pertemuan UN *Group on Governmental Expert on Cyber* pada tahun 2015. ASEAN PDP secara resmi dibunyikan di level tertinggi (*leaders*) di ASEAN Summit tahun lalu di Singapura. Berdasarkan APEC *Privacy Framework* tahun 2005, ASEAN Economic Community (AEC) mengadopsi Kerangka pada Perlindungan Data untuk mempromosikan kerjasama antara negara anggota AEC dalam implementasi Prinsip Perlindungan Data Personal yang sama pada hukum dan regulasi yang sama.

Pelanggaran data dapat terjadi akibat berbagai faktor yang dikategorikan menjadi tiga, yakni serangan siber (kriminal), sistem *glitch*, dan *human error*. Serangan siber menjadi ancaman utama dibandingkan kategori lainnya dimana setiap negara mengalami kerugian terbesar akibat serangan siber. Perusahaan dan organisasi di Amerika mengalami kerugian yang paling besar dibandingkan negara atau kawasan lainnya sedangkan Brazil mencetak biaya terendah. Di sisi lain, biaya kerugian tidak selamanya berbanding lurus dengan persentase setiap kategori. Misalnya, kerugian akibat kerusakan sistem bisa menghabiskan biaya yang lebih sedikit dibandingkan biaya untuk memperbaiki kerusakan akibat serangan siber walaupun persentase serangan siber lebih sedikit daripada persentase kerusakan sistem. Hal ini dapat dipengaruhi oleh faktor internal, seperti nilai dari informasi pribadi yang lebih tinggi daripada nilai infrastruktur itu sendiri.

Sebagai respon terhadap fenomena tersebut, melalui ASEAN TELMIN, ASEAN membentuk *Work Plan on* ASEAN *Cyber*

sampai tahun 2020. Hal ini mengacu kepada bentuk kerjasama atau pendekatan ekonomis dimana negara-negara anggota saling terkoneksi secara digital untuk kepentingan negara. Ketika ada satu negara anggota belum mampu mengembangkan sistem mereka, maka negara anggota ASEAN lainnya perlu membantu. ASEAN PDP sendiri lebih condong kepada upaya untuk menjaga agar data-data para *user* di negara anggota ASEAN tidak disalahgunakan oleh pihak ketiga. Sub bab selanjutnya akan mengelaborasikan poin-poin peran ASEAN melalui ASEAN PDP untuk menjaga keamanan siber bagi masing-masing negara anggota maupun hubungannya terhadap negara lain.

Institutional and International Role Expectation

Konsep peran, sesuai pernyataan Elgström dan Smith, mengacu pada "pola perilaku yang sesuai dan diharapkan". Aggestam mengajukan tiga perspektif perihal bagaimana peran dikonstruksi, dikembangkan, dan diubah yakni secara institusional, interaksional, dan intensional. Pandangan institusional menunjukkan bahwa bukan aktor yang menentukan peran, melainkan institusi. Institusi di sini diartikan sebagai pola umum atau kategorisasi kegiatan dan susunan tertentu yang dikonstruksi manusia, diorganisir baik secara formal maupun informal (Wang, 2012). Meskipun pendekatan ini dapat menjelaskan bagaimana struktur (sistem internasional) dapat mempengaruhi suatu instansi (kinerja peran), di sisi lain terdapat sedikit ruang untuk adanya interpretasi dan inovasi terhadap institusi itu.

Sebaliknya, perspektif interaksional menekankan pada konstruksi dan perubahan peran pada proses interaktif sehingga kapasitas aktor menjadi penentu suatu peran. Perspektif terakhir yakni intensional berfokus pada bagaimana aktor terlibat dalam mendefinisikan peran alias memiliki kebebasan untuk memilih (peran). Dengan begitu, peran yang dilakukan suatu aktor dan dampaknya terhadap *role performance* tergantung pada pertimbangan aktor akan posisi, tempat dan perilakunya dengan pihak lain dalam suatu lingkungan sosial dan pada reaksi maupun ekspektasi dari aktor lain (Elgström, 2006). Walaupun begitu, peran-peran yang ditentukan dalam konteks tersebut masih dapat dipilih oleh aktor untuk menentukan peran apa dan bagaimana yang akan dilakukannya dalam konteks institusional dan sosial (Elgström & Smith, 2006).

Sebagai organisasi regional, ASEAN memiliki fondasi sebagai dasar untuk menyusun kegiatan atau agenda setiap negara anggota. Berbeda dengan pendekatan interaksional, peran institusi menjadi fokus dalam menentukan kinerja peran dimana aktor diharapkan dapat melakukan perannya dalam tatanan sosial. Hal ini dapat dilihat dari Piagam ASEAN sebagai perjanjian legal yang bersifat mengikat kesepuluh negara anggota ASEAN. Piagam ASEAN ada sebagai "dasar dari Komunitas ASEAN dengan menyediakan status legal kepada, dan kerangka institusional untuk, ASEAN dimana piagam ini juga menyusun nilai dan peraturan hingga menetapkan target bagi ASEAN sehingga mempresentasikan akuntabilitas dan pemenuhan" (Dai & Gomez).

Meskipun Piagam ASEAN berusaha tampil sebagai bentuk perjanjian yang mengikat, ASEAN nyatanya lebih mengutamakan asas 'musyawarah' dan 'mufakat'. Prinsip non-intervensi yang dianut anggota ASEAN juga merupakan salah satu tantangan terbesar dalam proses pembuatan keputusan. Pembuatan keputusan yang didasarkan oleh konsensus membuat anggota ASEAN setuju akan adanya ekspektasi kolektif terhadap ruang siber dan identitas bersama di dalam domain siber. Dengan adanya konsensus tersebut, terdapat potensi bagi negara anggota untuk mengikuti peraturan yang ditentukan. Di sisi lain, ketaatan tersebut dapat mengurangi pemahaman akan nilai-nilai yang disetujui. Hal ini dapat terjadi akibat kurangnya mekanisme atau koordinasi untuk mencapai tujuan dari keputusan yang dibuat sehingga keputusan yang dibuat pada tingkat regional

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

tetap disesuaikan dengan regulasi tingkat nasional (Dai & Gomez).

Agenda yang disusun oleh negara anggota ASEAN cenderung bersifat *framework* atau kesepakatan sehingga tidak harus dilakukan setiap negara anggota. Ini sejalan dengan konsep 'ASEAN Way' yang dianggap paling sesuai dengan norma dan kepercayaan masing-masing negara anggota. ASEAN Way, menurut pemahaman Gillian Goh, dipandang "memiliki dampak melembagakan budaya politik yang sangat pribadi dan informal hingga adanya etiket sosial yang didasarkan pada ketidaklangsungan dan harmoni sosial." Dengan ini, ASEAN Way memiliki beberapa karakteristik seperti pembentukan konsensus, informalitas, pragmatisme, condong kepada persetujuan dan harmoni, kesopanan, sensitivitas, diplomasi privat v. *public shaming*, dan *non-legalistic* (Goh, 2003).

Selain itu, ada juga ASEAN Minus X yang muncul sejak tahun 1980an dimana anggota ASEAN dapat maju ke suatu area spesifik yang akan diikuti oleh negara lain ketika mereka siap ASEAN07. Dengan begitu, partisipasi negara bersifat fleksibel sesuai dengan kesiapan mereka untuk berkomitmen pada suatu proyek. Meskipun mekanisme ini memperkecil kemungkinan kesepakatan penuh, negara anggota yang mau berkomitmen dalam proses pembuatan peraturan siber dapat melakukan hal tersebut sambil membantu negara lain yang masih berada pada tahap persiapan. Berbagai bentuk kerja sama yang dilakukan dengan negara mitra dan badan penelitian non-pemerintah juga cukup berdampak pada infrastruktur kritis dan rencana ekonomi digital Asia Tenggara sehingga berpotensi pada stabilitas politik dan kepercayaan publik. Walaupun begitu, hasil dari usaha tersebut sangat bermanfaat pada posisi internasional negara anggota. Ini juga terlihat dalam konsesus yang mengarah pada pernyataan ASEAN yang pertama dalam PBB sekaligus keputusan bersama untuk menyetujui 11 norma global dari laporan 2015 UN *Group of Governmental Experts* (Heinl, 2019).

Kesepuluh negara anggota ASEAN memiliki perbedaan kapasitas yang cukup signifikan, terutama negara-negara yang masih mementingkan ranah fisik mereka. Maka, ASEAN mengajukan beberapa cara untuk mempersempit jarak kapabilitas antarnegara, seperti melakukan kerjasama dalam sektor IT dan pendidikan, yakni dengan meningkatkan ketersediaan *broadband internet connectivity* di instansi pendidikan, menambah kapasitas tenaga pengajar dalam penggunaan IT, hingga memasukkan ICT ke dalam kurikulum pendidikan. Kemudian, adanya kerjasama dengan *stakeholders* yang mampu menambah pengetahuan perihal ICT yang diiringi dengan peningkatan akses akan teknologi digital.

Melalui perspektif ini, ASEAN memegang peran untuk menentukan hingga mendesak hak dan tanggung jawab dari peran kepemimpinan sesuai dengan konteks tersebut. ASEAN PDP ditargetkan menjadi alat bagi pebisnis di ASEAN dalam mengembangkan program perlindungan data digital yang kuat, baik dari segi regulasi hingga implementasi. Peningkatan perlindungan tersebut dipercaya dapat meningkatkan kepercayaan konsumen dalam implementasi ekonomi digital sehingga menciptakan lingkungan yang kondusif bagi kegiatan bisnis pada era digital seiring peningkatan *startups* dalam kawasan Asia Tenggara.

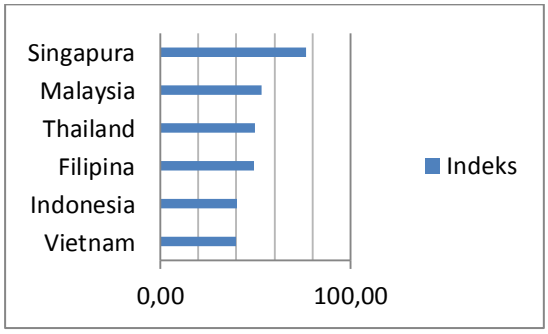
International role expectation sendiri memberikan ekspektasi bahwa aktor lain mengharapkan adanya *role-beholder* seperti yang diperlihatkan oleh institusionalisasi identitas dimana menghasilkan harapan yang luas sehingga cenderung membatasi lingkup peran yang diperlihatkan oleh pembuat kebijakan. Maka dari itu, ekspektasi peran internasional dilihat sebagai hal normatif yang dihasilkan berbagai institusi (Aggestam, 2006).

Pengaruh ASEAN dapat dilihat dari kekuatan dan kelemahannya sebagai suatu organisasi kawasan pada aspek keamanan siber. Proses digitalisasi secara nasional dapat dilihat dari beberapa aspek, seperti

pembangunan infrastruktur jaringan serta *Networked Readiness Index* (NRI) di negara-negara ASEAN. Berdasarkan laporan PCMag, Asia Tenggara akan memiliki tingkat pertumbuhan pengguna internet tertinggi di dunia pada tahun 2020 mendatang dengan Indonesia sebagai penyumbang utama atas kenaikan penggunaan internet (Yap, 2016). Tidak hanya itu, analisis A.T. Kearney mencatat Indonesia sebagai negara berpotensi terbesar sebagai lahan investasi ekonomi digital dengan perkiraan 24 miliar dolar secara kumulatif dalam pengembangan keamanan siber ATKEARNEY.

Meskipun begitu, berdasarkan grafik yang tertera berikut ini, negara anggota ASEAN belum memiliki infrastruktur yang mampu mendukung pertumbuhan penggunaan internet.

Gambar 1. Indeks Infrastruktur Jaringan di ASEAN



(Sumber: *We are Social)*

Dari riset yang dilakukan perusahaan media Inggris, *We are Social*, pada enam negara di kawasan Asia Tenggara, Singapura memiliki indeks tertinggi sebesar 76,43. Posisi kedua dengan indeks 53,11 dipegang oleh Malaysia dan diikuti oleh Thailand dan Filipina dengan perbedaan besar indeks yang tipis, masing-masing sebesar 49,66 dan 49,22. Indonesia sendiri masih tertinggal dengan perolehan indeks 40,41 sebelum Vietnam sebagai posisi terakhir dengan indeks sebesar 39,72. Hal ini menggambarkan kesenjangan yang cukup jauh antara Singapura dengan negara anggota lainnya. Bahkan, empat negara anggota lainnya masih belum tercatat dalam riset yang ada (katadata, 2017).

Di samping itu, untuk mempermudah pengawasan terhadap pertumbuhan revolusi ICT secara global, *World Economic Forum*, bekerjasama dengan INSEAD dan Universitas Cornell, mempublikasikan *The Global Information Technology Report* dengan menggunakan *Networked Readiness Index* (NRI). NRI adalah sebagai alat penilaian kesiapan negara dalam memanfaatkan perkembangan teknologi pada era transformasi digital. Sejak tahun 2001, NRI digunakan untuk mengukur kesiapan suatu negara dalam penggunaan ICT berdasarkan 53 indikator yang terbagi dalam empat kategori meliputi lingkungan penggunaan teknologi, kesiapan jaringan pada infrastruktur, pemakaian teknologi oleh kelompok *stakeholder*, serta dampak sosial dari teknologi tersebut.

Tabel 1. *Networked Readiness Index*

Negara	*Networked Readiness Index* (NRI) *Indicators*				Peringkat NRI Dunia	Nilai
	Environment Sub-index Rank	*Readiness Sub-index Rank*	*Usage Sub-index Rank*	*Impact Sub-index Rank*		
Singapura	1	16	1	1	**1**	6,0
Malaysia	21	73	30	30	**31**	4,9
Thailand	54	62	63	65	**62**	4,2
Indonesia	62	81	78	78	**73**	4,0
Filipina	89	92	66	62	**77**	4,0
Vietnam	86	82	81	76	**79**	3,9
Laos	93	107	117	104	**104**	3,4
Kamboja	119	100	110	117	**109**	3,4
Myanmar	133	118	137	135	**133**	2,7

(Sumber: WEF)

Selanjutnya, tabel di atas mengandung aspek-aspek yang ada pada setiap negara anggota ASEAN sesuai dengan urutan NRI secara global. Singapura berhasil menempati urutan pertama sebagai negara dengan NRI tertinggi yang diikuti oleh Malaysia sebagai pemimpin perekonomian Asia pada tahun 2016 dengan naik ke urutan 31 sebagai dampak dari dukungan pemerintah terhadap pertumbuhan agenda digital. Negara anggota lain mulai mengejar ketertinggalan mereka dengan mengikuti jejak kedua negara tersebut untuk mengembangkan proses digitalisasi. Vietnam, misalnya, menguatkan kebijakan dan infrastruktur negara untuk mencapai *cashless economy* (Baller, Dutta, & Lanvin, 2016). Meskipun begitu, negara anggota lain masih berada di bawah peringkat 40, bahkan Brunei Darussalam belum terdaftar dalam daftar

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

tersebut. Hal ini semakin menguatkan perlunya kerjasama yang signifikan antarnegara anggota dalam penggunaan ICT.

Sebagai bagian dari ASEAN *Cyber Capacity Program* Singapura terkait perlindungan data personal, ASEAN juga mendorong kemajuan pengetahuan keamanan siber melalui program yang dijalankan dari pemerintah Singapura yakni *Singapore International Cyber Week* (SICW) sebagai bentuk partisipasi dalam dikusi kebijakan, legislasi, hingga ketahanan siber secara regional maupun global. SICW pertama yang diselenggarakan pada tahun 2016 menghadirkan ASEAN *Cybercrime Prosecutors' Roundtable Meeting* dimana *prosecutor* kejahatan siber dan pihak penegak hukum dari semua negara anggota membentuk kapasitas legal untuk ASEAN. Di samping itu, SICW juga bekerja sama dengan *GovernmentWare* (GovWare) dengan mengadakan Rapat Tahunan Global Forum on Cyber Expertise (GFCE) pada tahun 2018 lalu. Ini juga diaplikasikan melalui *platform* ASEAN lainnya seperti ASEAN CERT *Incident Drill* (ACID), ASEAN *Network Security Action Council* (ANSAC), ARF, dan *workshop* lainnya (Cyber Security Agency of Singapore, 2016).

Dengan adanya forum, perjanjian, dan sentrum aktif dalam isu keamanan siber, dalam jangka panjang, ASEAN dapat berkembang menjadi organisasi yang menjanjikan di antara negara mitra dengan adanya kebijakan regional dan kerja sama teknis, bahkan menyatukan perbedaan nilai-nilai politik dan budaya dalam membentuk keamanan dan ancaman siber. Lebih lanjut lagi, ASEAN dapat berkontribusi dalam stabilitas internasional melalui kerja sama dengan NATO atau kebijakan khusus Eropa perihal pelatihan dan pendidikan siber. Tidak hanya itu, ASEAN dapat melanjutkan praktiknya dengan badan regional lain di Amerika dan Eropa (Heinl, 2019).

Gabungan dari kekuatan negara anggota ASEAN menyajikan suatu IT *hub* yang berada pada posisi utama antara Amerika, Eropa, Jepang, dan Tiongkok dimana memudahkan perkembangan jaringan kawasan. Di sisi lain, beberapa kelemahan negara anggota cenderung terkait pada minimnya ahli di tiap negara, kurangnya pendekatan dan perpaduan strategi, standar yang masih rendah, maupun kesenjangan budaya dan ekonomi (Nguyen & Ionannidis, 2016). Namun, secara internasional, peran ASEAN dapat dikatakan cukup berpengaruh dengan adanya berbagai kerjasama antara anggota ASEAN dan organisasi internasional lainnya dimana menunjukkan posisi ASEAN yang lebih ajeg pada masyarakat internasional sehingga meningkatkan efektivitas perannya dalam isu regional hingga global.

Implementasi Peran ASEAN PDP

Konsepsi peran menyarankan adanya perpaduan norma dan nilai budaya dalam perilaku kebijakan luar negeri yang diharapkan dan orientasi tindakan dimana konsepsi peran memfasilitasi pembuat kebijakan sebagai petunjuk arah. Sebagai kategori yang luas, konsepsi peran memungkinkan adanya interpretasi dimana telah resmi dilembagakan beserta sejumlah tindakan spesifik, begitu pun dengan sentralitasnya yang bergantung pada konteks dan waktu tertentu. Dalam beberapa kasus, konsepsi peran dapat mengalami perubahan, contohnya jika ada konflik peran atau sentralitas yang kurang kuat. Hal ini disebabkan oleh 'celah' dari konsep peran. *Pertama*, konsepsi peran yang bersifat 'mengambang' cenderung gagal menyediakan konsistensi yang dibutuhkan pembuat kebijakan sebagai aktor intensional pada kebijakan luar negeri. *Kedua*, hubungan dialektik antara konsepsi peran kebijakan luar negeri dan identitas nasional dimana konsepsi yang pokok dikelilingi oleh institusi yang membuatnya sebagai bagian dari budaya politik bangsa. Meskipun begitu, adanya ketahanan konsep yang melekat membuatnya sulit diubah (Aggestam, 2005, hal. 81-98).

Berbeda dengan organisasi internasional lainnya, seperti Uni Eropa, ASEAN berpegang pada konsep 'ASEAN Way' yang dianggap paling sesuai dengan norma dan kepercayaan masing-masing negara anggota. Gillian Goh (2003) memandang ASEAN Way "memiliki dampak melembagakan budaya politik yang sangat pribadi dan informal hingga adanya etiket sosial yang didasarkan pada ketidaklangsungan dan harmoni sosial." Maka dari itu, ASEAN Way memiliki beberapa karakteristik seperti pembentukan konsensus, informalitas, pragmatisme, condong kepada persetujuan dan harmoni, kesopanan, sensitivitas, diplomasi privat v. *public shaming*, dan *non-legalistic* (Goh, 2003). Prinsip ini didasarkan pada Pasal 2 dari Piagam ASEAN serta *The Treaty of Amity and Cooperation in Southeast Asia* (TAC) 1976 meliputi:

1) Menghormati kemerdekaan, kedaulatan, integritas wilayah, dan identitas nasional antarnegara anggota;
2) Masing-masing negara anggota berhak menjaga eksistensi nasionalnya sehingga bebas dari adanya campur tangan eksternal, subversi, maupun pemaksaan;
3) Mengusung prinsip 'non-intervensi' terkait urusan internal antarnegara anggota;
4) Menyelesaikan bentuk perselisihan dan perbedaan secara damai;
5) Menolak segala bentuk ancaman atau penggunaan kekuatan; dan
6) Mengusung kerjasama dengan sesama negara anggota.

Peran yang dijalankan ASEAN dalam hal ini direfleksikan melalui prinsip-prinsip kerangka ASEAN PDP yang terdiri atas konsen, akurat, melindungi, akses dan perbaikan, (aturan) transfer ke luar negara atau wilayah, penyimpanan, dan akuntabilitas. Ranah siber sendiri terbagi ke dalam beberapa bagian. Pada sisi keamanan, masalah siber terpecah menjadi beberapa bagian, dari sisi pertahanan dan keamanan, kedaulatan, hingga proteksi infrastruktur nasional, seperti jaringan internet di kementerian, presiden, militer, atau polisi yang melihat kerjasama penanganan kriminalitas dengan media internet, misalnya pelacakan transfer uang dari satu negara ke negara lain. Di sisi ekonomi, ASEAN PDP ditujukan sebagai peluang bagi pebisnis dalam menjaga kerahasiaan asset hingga meningkatkan pelayanan publik, terutama pelayanan online-satu-pintu.

ASEAN PDP juga mengambil contoh model keamanan data dari organisasi kawasan lainnya, seperti *General Data Protection Regime* (GDPR) milik Uni Eropa dan *Cross-Border Privacy Rules* (CBPR) dari APEC. Jika mengacu pada konsep ASEAN Way, ASEAN akan menyesuaikan prinsipnya dengan model yang ada sehingga mengarah pada CBPR. Di sisi lain, model GDPR mengatur segala regulasi perihal perlindungan data regional dalam satu payung dimana sangat bertentangan dengan kepercayaan ASEAN. Berdasarkan pengamatan A.T. Kearney, ada empat agenda yang diperlukan untuk mencapai keamanan data personal digital yakni: meningkatkan keamanan siber pada kebijakan regional; menyiapkan komitmen penuh; memperkuat ekosistem; dan membangun gelombang kapabilitas keamanan siber. Langkah pertama dan kedua dapat dikatakan vital untuk mendorong perubahan sudut pandang pada masalah keamanan siber yang belum sepenuhnya dianggap penting.

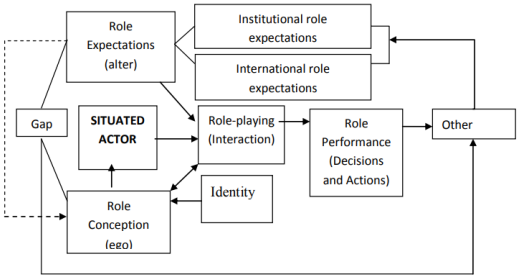
Untuk mendorong kesadaran akan pentingnya keamanan siber, ASEAN PDP dapat membantu penambahan *platform* khusus terkait koordinasi operasional secara regional yang mencakup kerjasama, aktivitas perkembangan pasar, serta harmonisasi standar keamanan siber. Adanya *platform* tersebut dapat membantu peningkatan kapabilitas keamanan siber masing-masing negara anggota sesuai rancangan program yang didasarkan pada prinsip ASEAN PDP. Agar peningkatan standar keamanan dapat terlaksana, \penyamarataan standar keamanan

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

siber dapat dijadikan salah satu agenda utama pada *platform* ini. Dengan begitu, kapabilitas setiap negara akan berkembang secara signifikan dan merata dalam batas waktu yang ditentukan.

Pendekatan interaksional, dimana kapasitas aktor menentukan perannya, menjadi dasar dari *role-playing* sebagai proses pembentukan (peran) aktor. *Role-play*, atau *role enacment*, merupakan perilaku sesungguhnya yang dilakukan negara ketika suatu peran sudah ditentukan. *Role-play* serta *role conception* membentuk suatu proses relasi dimana entitas (ego) memposisikan dirinya dengan *Other* (alter) (Wang, 2012). Berikut adalah pola umum dari perubahan peran.

Gambar 2. Pola umum perubahan peran



Dari pola tersebut, proses interaksi *role-playing* suatu aktor dapat digambarkan. Aktor menggunakan peran tertentu dengan adanya konsepsi peran yang sudah ada sebelumnya. Konsepsi peran tersebut, ditentukan dari kapasitas dan identitas aktor, dibentuk ulang melalui konfrontasi dengan ekspektasi eksternal (Aggestam, 2005).

Elgström menyatakan bahwa formasi peran sendiri dapat dikatakan sebagai suatu "hubungan yang kompleks dan dinamis antara *self-images* dan otonomi aktor pada satu sisi, dan (adanya) ekspetasi peran yang terkendali secara struktural" (Elgström O. , 2006). Berdasarkan pola tersebut, *role performance* sangat dipengaruhi oleh interaksi dari konsep dan ekspektasi peran dimana 'eksekusi' yang dilakukan akan berpengaruh pada ekspektasi aktor lain. Di samping itu, adanya 'celah' yang muncul akibat perbedaan ekspektasi aktor lain dengan konsep peran aktor utama juga dapat menimbulkan perubahan peran aktor (Wang, 2012).

Peran yang dilakukan ASEAN PDP dapat ditelusuri dari tujuan awal pembentukannya. ASEAN *Personal Data Protection* muncul untuk mendukung peningkatan keamanan data personal dalam ranah siber. Hal ini memicu pergeseran fokus kawasan ASEAN menuju keamanan non-fisik di samping keamanan tradisional. Sejak ASEAN mengadopsi Deklarasi ASEAN terhadap Hak Manusia pada tahun 2012 silam, data privasi menjadi salah satu aspek penting dalam keamanan siber. Kerangka ASEAN PDP berfungsi membawa ASEAN untuk mencapai kondisi ekonomi yang aman, berkelanjutan, dan digital sehingga diperlukan kontribusi dari perlindungan data sebagai bentuk promosi dan perkembangan perdagangan hingga arus informasi digital. Maka, partisipan dari kerangka tersebut dituntut bekerjasama menerapkan prinsip-prinsip ASEAN PDP berdasarkan hukum domestik masing-masing.

Ada 7 (tujuh) prinsip utama yang ditekankan dalam kerangka ASEAN PDP. Pertama, konsen dan tujuan dari penggunaan data personal dimana setiap individu perlu mengetahui tujuan perusahaan untuk mengumpulkan data mereka berdasarkan ketentuan regulasi setempat. Kedua, data personal yang akurat dengan individu untuk kepentingan yang diperlukan. Ketiga, data tersebut harus dilindungi dari kehilangan atau akses pihak ketiga untuk mengurangi resiko penyalahgunaan data. Keempat, setiap individu berhak mengakses data mereka dalam waktu yang ditentukan serta memperbaikinya jika terdapat kesalahan, apabila diperbolehkan. Kelima, data personal tidak boleh ditransfer ke negara lain tanpa izin dari individu yang bersangkutan atau jaminan keamanan data. Keenam, dokumen yang mengandung data personal tidak boleh ditahan oleh organisasi tertentu kecuali penyimpanan tersebut tidak dibutuhkan untuk tujuan bisnis atau hukum.

Terakhir, suatu organisasi harus mampu memenuhi prinsip-prinsip ini yang disertai dengan kebijakan perlindungan data dan kontak organisasi (GSM Association, 2018).

Sebagai bentuk inisiatif dari leaders ASEAN, program *capacity building* menjadi poin utama dalam meningkatkan kapabilitas keamanan siber yang diusung oleh Singapura sesuai dengan kemampuan *cyber resilience*-nya yang paling bagus di antara negara-negara anggota ASEAN. Namun demikian, untuk memaksimalkan potensi ini, negara-negara ASEAN lain juga menginginkan agar *capacity building program* tidak hanya diberikan hanya oleh satu negara, tetapi benar-benar terencana dengan menggunakan sumber daya bersama negara-negara ASEAN. Tidak hanya sampai di situ, *capacity building program* juga dilakukan melalui kerjasama dengan negara-negara di luar ASEAN, misalnya dengan adanya pendirian ASEAN-Japan *Cybersecurity Capacity Building Center* di Bangkok. Pada pertemuan ASEAN tahun 2018, ASEAN juga menjalin kerja sama dengan Rusia. Selain itu, ASEAN menerima bantuan *capacity building program* dari Amerika Serikat melalui *International Visitors Leadership Program* (IVLP) mengenai keamanan siber yang diikuti oleh perwakilan pemerintah hingga sektor swasta dari negara-negara ASEAN.

Salah satu respon baik terhadap usaha peningkatan keamanan siber datang dari negara Filipina. Bekerja sama dengan Komisi Perlindungan Data Singapura, Komisi Privasi Nasional milik Filipina turut serta dalam pembentukan ASEAN *Framework on Digital Data Governance* yang diterima oleh Raymund Enriquez Liboro selaku Komisioner pada saat 2nd *Working Group Meeting on ASEAN Digital Data Governance Framework*. Filipina sendiri dipilih sebagai *co-leader* dari ASEAN *Data Protection and Privacy Forum* (*initiative*) sebagai bagian dari *framework* yang diajukan pada Desember 2018. Adapun tujuannya yakni mencapai kesepakatan terhadap regulasi data dan kerangka pemerintahan di kawasan serta mendorong inovasi dalam ekonomi digital (Umail, 2019).

Dari dampak yang ditimbulkan ASEAN PDP, kesepakatan ini dapat menggambarkan bagaimana kesadaran akan keamanan siber diterapkan secara efisien dalam pengembangan kapasitas keamanan siber ASEAN yang diajukan Singapura. Meskipun isu tersebut belum menjadi prioritas bagi negara tertentu, pengetahuan dan kesempatan yang telah didapat akan sangat berguna sebagai referensi di masa depan, terutama pada era komunikasi dan informasi sekarang ini. Terlepas dari penyebab tantangan tersendiri bagi negara-negara berkembang, isu siber yang diangkat menjadi isu regional membuka peluang besar bagi sesama negara anggota ASEAN untuk meningkatkan pengaruhnya dalam aspek sosial maupun ekonomi.

Role performance menggambarkan perilaku kepemimpinan mengenai pola karakter dari keputusan dan tindakan pada konteks situasional. Aggestam melihat bahwa hubungan kedua konsep tersebut hanya dapat diterapkan secara umum dikarenakan peran aktor yang cenderung banyak. Berdasarkan pola perubahan peran di atas, sebagian besar kinerja peran dikarakterisasi oleh interaksi dari konsepsi dan ekspektasi peran dimana kinerja peran mempengaruhi harapan aktor lain terhadap peran (yang ditentukan). Selain itu, jarak antara ekspektasi peran dengan konsepsi peran atau kinerja peran aktor tersebut juga berpengaruh terhadap persepsi maupun ekspektasi peran aktor yang mana juga dapat mengubah peran aktor itu.

Tindakan yang dilakukan negara anggota ASEAN dipengaruhi oleh beragam alasan berdasarkan kepentingan setiap negara anggota seperti adanya kesenjangan perhatian terhadap isu keamanan siber. Malaysia dan Singapura termasuk dalam kelompok negara yang paling siap menghadapi serangan siber. Sementara itu, negara seperti Indonesia dan Thailand belum terlalu lama memusatkan perhatiannya untuk menangani isu siber sedangkan negara-negara seperti Cambodia dan Laos masih pada tahap awal. Dengan demikian, prioritas negara-negara ASEAN berbeda satu sama lain. Perbedaan ini disebabkan oleh tiga faktor.

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

Pertama, negara-negara anggota ASEAN memiliki perbedaan persepsi dan kepentingan dalam menghadapi ancaman keamanan. Negara Myanmar dan Filipina menganggap ancaman utama keamanan mereka bukan terletak pada ancaman serangan siber tetapi pada ancaman internal. Akibatnya. ranah siber tidak menjadi prioritas pada agenda atau peraturan mereka.

Kedua, ranah siber merupakan area yang membutuhkan penguasaan IPTEK yang tinggi dimana tidak semua negara anggota ASEAN memiliki kapasitas yang memadai untuk meningkatkan kemampuan siber, baik dari segi literasi maupun kapabilitas teknologi. Maka, daripada menginvestasikan biaya dan energi untuk keamanan siber, beberapa negara anggota ASEAN lebih memilih untuk memperkuat diri pada aspek keamanan yang konvensional, misalnya seperti pembelian senjata. *Ketiga*, negara-negara anggota ASEAN memiliki perbedaan siginifikan mengenai kontribusi teknologi IT pada perekonomian. Singapura, misalnya, adalah pusat informasi dan teknologi di Asia Tenggara dan hampir semua sektor di Singapura terintegrasi dengan IT. Akibatnya, jika terjadi serangan siber, banyak infrastruktur kritis di Singapura yang akan terpengaruh. Hal ini berbeda dengan negara anggota lain, seperti Indonesia, dengan tingkat penetrasi penggunaan IT yang tidak terlalu besar. Dengan berbagai variasi tersebut, sulit mendefinisikan perhatian utama keamanan siber di ASEAN. Tapi, ada dua hal yang menjadi *common interests* bagi negara-negara ASEAN, yaitu (1) *capacity building* dan (2) pembangunan *voluntary norms* untuk mencegah perang siber.

Dari pembentukan ASEAN ICT Masterplan 2015, terdapat beberapa inisiatif yang mengarah pada keamanan siber, di antaranya *initiative* 2.4 dan 4.2. Inisiatif pertama terdiri dari adanya kepercayaan untuk mempromosikan transaksi yang aman dalam ASEAN serta kesadaran akan keamanan siber sedangkan yang kedua mengacu kepada integritas jaringan, keamanan informasi, perlindungan data, dan kerjasama CERT. Untuk mencapai ekspektasi dari ASEAN PDP, ASEAN menyusun beberapa program yang berfokus pada *capacity building* dan kerjasama teknis, meliputi: a) Pengembangan prinsip data proteksi regional sebagai panduan bagi negara anggota ASEAN dalam melaksanakan kerjasama proteksi data pribadi; b) Pengembangan keamanan jaringan regional melalui pembentukan wadah digital yang berfungsi sebagai tempat pertukaran informasi secara aman (misalnya, *cloud computing*); c) Penguatan kerjasama *cyber incident emergency response* dengan melakukan studi dalam pengembangan ASEAN CERT, kerangka *public private partnership* (PPP), serta menyusun kerangka pelaporan insiden siber; dan d) Adanya kerjasama dalam bentuk pertukaran informasi, *joint research*, maupun seminar.

Seiring waktu, ASEAN ICT kembali disusun dengan menambah detail-detail pada aspek *initiative*, termasuk perihal keamanan informasi di ASEAN yang tercantum pada poin *initiative* 8.1 dan 8.2 dari ASEAN ICT Masterplan 2020. *Initiative* pertama terdiri dari tiga poin yakni: a) mengembangkan prinsip perlindungan data regional; b) mengembangkan praktik keamanan jaringan regional dan; c) mengembangkan praktik ketahanan infrastruktur informasi regional. Poin pertama menjadi landasan utama untuk mempromosikan perlindungan data di ASEAN melalui pembentukan pedoman regional. Adapun target kegiatan dari proyek tersebut masih berputar pada *masterplan* 2015. Penambahan subpoin lainnya lebih cenderung kepada pengembangan keamanan jaringan ICT dan infrastruktur informasi sebagai bentuk pertahanan dari serangan siber yang akan datang. Adapun target kegiatannya juga mirip dengan sebelumnya.

Selanjutnya, *initiative* 8.2 menyajikan rencana awal dalam pembentukan kesiapan keamanan informasi di ASEAN yang berfokus pada efektivitas *Cyber Incident Emergency*

Response Collaboration dimana mendorong adanya kerjasama untuk menciptakan jaringan CERT secara *real-time* terhadap pelanggaran keamanan *online*. Target kegiatan yang akan dilakukan mencakup pembentukan ASEAN CERT dengan kepemilikan melalui pemerintahan AMS atau *Public-Private Partnership* (PPP), pembentukan *Incident Reporting Framework* dan ASEAN *Network Security Council* (*multi-stakeholders*), serta promosi kolaborasi dan dialog antar *stakeholder* mengenai keamanan siber melalui kampanye hingga pertukaran materi. Hal ini dilakukan untuk mencapai visi AIM 2020 yakni ASEAN sebagai 'komunitas' yang serba digital, aman, dan berkelanjutan (TRPC Pte Ltd, 2015).

Pertemuan yang digelar ASEAN untuk menyelesaikan isu keamanan siber meliputi AMMTC, ADMM-Plus, dan ARF. ASEAN *Senior Officials Meeting on Transnational Crime Working Group on Cybercrime* (SOMTC WG on CC) digelar dalam forum AMMTC yang menghasilkan kerja sama untuk memberantas kejahatan siber melalui pertukaran informasi, pengembangan kapasitas, penelitian, hingga pelatihan seminar atau lokakarya. Selanjutnya, pada tanggal 17 Juli 2017 silam, ASEAN melakukan pertemuan ADMM-Plus *Experts' Working Group on Cyber Security* di Manila yang membahas kebijakan nasional negara di ranah siber dan upaya mengatasi kejahatan siber.

Sebagai bagian dari ASEAN PDP, pembentukan CERT pada setiap negara anggota menjadi salah satu pilar dari Singapore-ASEAN *Cybersecurity Centre of Excellence* (ASCCE) yang baru saja diluncurkan tahun 2019 ini. Sentrum tersebut diprediksi dapat mencakup kebijakan, strategi, legislasi, dan operasi melalui tiga pilar utama yakni memperkuat perkembangan strategi antarnegara anggota ASEAN dengan pelatihan dan riset, meningkatkan ketahanan Asia Tenggara melalui CERT, dan mempromosikan pembagian informasi yang bersifat terbuka. ASCCE bertujuan menjamin sentralitas ASEAN, mendukung kolaborasi internal negara anggota, dan bekerjasama dengan negara mitra secara efektif. Prinsip seperti inklusivitas dan pramagtisme kerja semakin terlihat pada beberapa bulan terakhir pada tingkat PBB (Heinl C. , 2019).

Dalam jangka panjang, ASCCE diprediksi mampu mempromosikan pemahaman bersama hingga luar ASEAN. Adapun kerjasama lainnya diperkirakan akan terjalin dengan entitas penelitian serupa yang sedang dikembangkan kawasan lain. Kolaborasi ini dapat menjadi perpanjangan program dari kesepakatan yang dibentuk sejak awal, terutama ASEAN PDP. Meskipun program yang dijalankan tidak hanya berpusat pada data privasi, perlindungan data personal tetap menjadi salah satu aspek utama dalam peningkatan keamanan siber.

KESIMPULAN

Isu keamanan siber masih belum menjadi prioritas bagi sebagian negara anggota ASEAN. Padahal, dampak yang diakibatkan pelanggaran data secara *online* mengakibatkan kerugian yang besar, baik secara finansial maupun struktural. ASEAN sebagai wadah berkembang bagi negara anggota sangat berperan dalam mewujudkan keamanan siber. Pada bab sebelumnya, periset telah memaparkan peran-peran ASEAN secara spesifik berdasarkan kategori peran Aggestam yang terdiri dari *role conception, role playing,* dan *role performance*. Dari konsep 'ASEAN Way', ASEAN secara bertahap membentuk ASEAN PDP hingga bekerjasama dengan organisasi kawasan untuk menentukan kebijakan kawasan. Komitmen tersebut semakin diperkuat dengan pembentukan CERT pada negara anggota.

Meskipun begitu, belum ada dokumen ASEAN yang memberikan aturan kepada perusahaan maupun negara jika melanggar kesepakatan mengenai pelanggaran akses data personal disebabkan ASEAN condong kepada pemberian 'imbauan' jika ada kepentingan atau masalah. Lebih lanjut lagi, negara anggota ASEAN sendiri masih punya *gap* antarnegara sehingga perlakuannya berbeda dan diberikan

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (270-286) doi: 10.24198/padjir.v1i3.26197

kepada negara masing-masing. Konsep tersebut sesuai dengan prinsip ASEAN sendiri tapi, kenyataannya, kepercayaan tersebut cenderung mempersulit kemajuan satu kawasan yang dinamis.

Oleh karena itu, peran ASEAN sendiri dapat dikatakan belum maksimal dimana pihak yang terlibat cenderung negara anggota yang sudah maju. Di sisi lain, ASEAN mempermudah adanya kerjasama antar *dialogue partnership* seperti Jepang, Tiongkok, dan Amerika. Jika berbicara sudah sejauh apa peran ASEAN pada isu ini, karena ASEAN lebih condong kepada 'kesepakatan', ASEAN perlu meninjau ulang komponen-komponen yang dibutuhkan untuk mendorong kesuksesan ASEAN PDP. Di samping itu, isu siber sendiri juga masih menjadi perjuangan bagi ASEAN karena termasuk isu baru sehingga masih diperlukan usaha ekstra untuk menarik minat negara anggota.

Berdasarkan riset yang dilakukan, peneliti menemukan bahwa teori keamanan non tradisional seperti ruang siber masih memiliki banyak celah yang belum ditelusuri. Adapun unsur yang ditekankan ialah perihal masalah sosial sehingga secara teknis masih meraba-raba mengenai definisi dari fenomena pelanggaran data tersebut. Maka itu, pemaparan terkait dampak *data breaching* dan kasus siber yang serupa perlu diperdalam untuk mencapai solusi yang efektif dan efisien.

ASEAN perlu merangkul negara yang masih pasif agar keamanan siber dapat meningkat secara menyeluruh. Jika diperlukan, ASEAN dapat mempertimbangkan pembuatan mekanisme tertentu dalam pelaporan dan peninjauan pelanggaran data yang terjadi pada masing-masing negara anggota, contohnya dengan melakukan investigasi forensik terhadap kejahatan siber. Menyusul kebutuhan akan pengamanan siber, negara anggota yang sudah paham di bidang ini dikabarkan akan membentuk ASEAN *CyberSecurity Operational Network* sebagai himpunan CERT negara ASEAN. Untuk itu, negara yang belum memiliki kebijakan mengenai ruang siber juga perlu ditelusuri lebih lanjut agar program yang diadakan tidak sia-sia. Jika memungkinkan, ASEAN dapat membuat kesepakatan tertentu perihal pendanaan dan inisiatif program yang ditanggung secara kolektif agar bermanfaat secara efektif alih-alih hanya untuk kepentingan negara semata.

DAFTAR PUSTAKA

A.T. Kearney. (2018). *Cybersecurity in ASEAN: An Urgent Call To Action.* A.T. Kearney Inc.

Access Partnership, Ltd. (2017). Norms for Cybersecurity in Southeast Asia: Policy Options for Collaborative Security in the Southeast Asian Region. *Access Partnership, Ltd* , 3-17.

Aggestam, L. (2005). Role identity and the Europeanisation of foreign policy: a political–cultural approach. Dalam B. Tonra, & T. Christiansen, *Rethinking European Union Foreign Policy* (hal. 81-98). Manchester University Press.

Aggestam, L. (2006). Role theory and European foreign policy: a framework of analysis. Dalam O. Elgström, & M. Smith (Penyunt.), *The European Union's Roles in International Politics: Concepts and analysis* (hal. 11-29). New York: Routledge.

(2008). *ASEAN Economic Community Blueprint*. Jakarta: ASEAN Secretariat.

Baller, S., Dutta, S., & Lanvin, B. (2016). *The Global Information Technology Report 2016: Innovating in the Digital Economy*. World Economic Forum.

Cyber Security Agency of Singapore. (2016). *Singapore's Cybersecurity Strategy.* Singapore: CSA Singapore.

Dai, C. T., & Gomez, M. A. (t.thn.). *Challenges and Opportunities for Cyber Norms in ASEAN*. Dipetik March 2019

Elgström, O. (2006). *Leader or Foot-dragger? Perceptions of the European Union in Multilevel International Negotiations.* SE: Swedish Institute for European Policy Studies.

Elgström, O., & Smith, M. (2006). *The European Union's Roles in International Politics.* London: Routledge.

Goh, G. (2003). The ASEAN Way: Non-Intervention and ASEAN's Role in

Conflict Management. *Stanford Journal of East Asian Affairs* .

GSM Association. (2018). *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation.* London: GSMA.

GSMA. (2018). *Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Inovation.* London.

Heinl, C. (2019, February). *An ASEAN Way of Cybersecurity*. Dipetik June 2019, dari Policy Forum: www.policyforum.net

Heinl, C. (2019, January). *An ASEAN way of cybersecurity: Unpacking the proposed ASEAN-Singapore Cybersecurity Centre of Excellence*. Dipetik May 2019, dari Asia & The Pacific Policy Society: https://www.policyforum.net/an-asean-way-of-cybersecurity/

Krisman, K. (2013). A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies* , 41-53.

Lago, C. (2018, August 21). *Looking back on the biggest data breaches to impact ASEAN*. Dipetik November 26, 2018, dari Channel Asia Singapore: https://sg.channelasia.tech/article/645512/looking-back-biggest-data-breaches-impact-asean/

Lee, J., & Perone, M. (2016, January). *The Influx of Cybercrime Across Southeast Asia and the Cyber Security and Data Protection Measures That Are Being Placed to Bolster Security Within the Region*. Dipetik January 2019

Mansfield, E. D., & Solingen, E. (2010, Februari 16). *Waseda University*.

Nguyen, A., & Ionannidis, S. (2016). *Toward EU-ASEAN Cooperation in Cyber Security.* Hanoi: CONNECT2SEA.

Nguyen, A., & Ionannidis, S. (2016, May 11). Towards closer EU-ASEAN collaboration in cybersecurity. Hanoi, Vietnam: Connect2SEA.

Ponemon Institute. (2018). *2018 Cost of a Data Breach Study: Global Overview.* Michigan: Ponemon Institute LLC.

Reksoprodjo, Y. (2016). Challenges and Opportunities for Better Communication, Cooperation, and Collaboration in International Cybersecurity in Asia. (C. Heinl, & E. Tan, Penyunt.) *RSiS* , 33-38.

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018). Cybersecurity Policy in ASEAN Countries. *17th Annual Security Conference* (hal. 1-7). Las Vegas: ResearchGate.

Symantec. (2017). *Internet Security Threat Report.* California: Symantec Corporation.

(2008). *The ASEAN Charter.* Jakarta: The ASEAN Secretariat.

TRPC Pte Ltd. (2015). *The ASEAN ICT Masterplan 2020.* ASEAN Secretariat.

Umail, T. (2019, May). *Philippines and Singapore to co-lead the ASEAN Data Protection and Privacy Forum*. Dipetik June 20, 2019, dari OPENGOV : https://www.opengovasia.com/philippines-and-singapore-to-co-lead-the-asean-data-protection-and-privacy-forum/

UNCTAD. (2016, April). Data protection regulations and international data flows: Implications for trade and development. New York, USA: United Nations.

Wang, D. (2012). Role in Changing: An Empirical Analysis of the European Union's Leadership Role in International Climate Change Negotiations under UNFCCC. Lund, Swedish: Lund University.

Yap, V. (2016, Juli 18). *Google: Southeast Asia Expected to Become a US$200 Billion Digital Economy by 2025*. Dipetik May 2019, dari PNCEws.

BIOGRAFI

Trisa Monika Tampubolon merupakan mahasiswa Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran. Tertarik mengkaji tentang keamanan siber secara regional, terutama terkait dengan data personal.

Rizki Ananda Ramadhan adalah pengajar pada Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran yang mendalami kajian mengenai Keamanan Siber dalam hubungan internasional.