BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang begitu pesat memaksa dunia untuk menghadapi era teknologi informasi. Era teknologi informasi yang memiliki peranan penting bagi semua aspek kehidupan baik individu, organisasi, ataupun suatu Negara. Informasi pun menjadi komponen yang sangat krusial dalam menghadapi segala permasalahan yang terjadi saat ini. Di era teknologi informasi berbagai bentuk informasi cenderung disampaikan melalui bentuk digital. Digitalisasi terjadi di berbagai bidang membawa perubahan yang signifikan dalam kehidupan manusia.

Kehadiran internet menjadi salah satu kunci penting dalam era teknologi informasi. Berbagai bentuk aktivitas yang terjadi secara digital berjalan di dalam jaringan internet. Segala sesuatu telah berhubungan dengan internet disebut sebagai *Internet of Things* (IoT). Dengan adanya *Internet* of Things ini, maka manusia serta manusia lain atau benda benda di sekitarnya dapat terkoneksi satu sama lain melalui jaringan internet (Morgan, 2014). Situasi ini memunculkan dunia baru yang disebut sebagai *cyber space. Cyber space* inilah yang menjadi ruang dimana interaksi dan komunikasi terjadi. Kehadiran *cyber space* menyebabkan masyarakat modern ini sulit terlepas arus komunikasi dan informasi. Kemudahan yang diberikan oleh internet memberikan berbagai dampak positif bagi kehidupan manusia. Efisiensi ruang dan waktu dapat diwujudkan dengan lebih maksimal di dalam *cyber space*. Namun, bagai pisau bermata ganda, internet juga memberikan dampak negatif bagi kehidupan manusia. Ancaman dalam *cyberspace* tersebut dapat bersumber dari pemerintah, organisasi, individu, atau pengusaha, baik secara disengaja maupun tidak demi mendapatkan keuntungan secara finansial, militer, politik, maupun tujuan lainnya (Smith, Research Handbook on International Law, 2015).

Cyber Space sendiri telah menjadi ranah baru yang dikaji dalam Ilmu Hubungan Internasional. Sebuah artikel dalam theeconomist.com menyebutkan *"After land, sea, air and space, warfare has entered the fifth domain: cyberspace"* (economist.com, 2010). Pernyataan ini didasari fakta bawa ranah siber telah mempengaruhi berbagai aspek

kehidupan terutama aspek politik dan ekonomi. Berbagai pengambilan kebijakan pada masa kini pun dipengaruhi oleh keterkaitannya dengan *cyber space.* Kekuatan siber suatu negara saat ini dapat menjadi *power* untuk negara mempengaruhi negara lainnya. Belakangan, akademisi HI pun menjadikan isu siber sebagai bagian dari studi keamanan dan juga studi strategis yang berfokus pada implikasi teknologi dengan keamanan serta isu strategis nasional dan Internasional. Pembahasan ini tidak terlepas dari berbagai konsep dasar dalam HI seperti, *power,* kedaulatan *global governance,* dan sekuritisasi.

Karena lingkup siber memiliki begitu banyak pengaruh, *cyber security* saat ini menjadi suatu bagian yang sangat melekat dengan keamanan nasional maupun internasional. Berbagai negara bahkan institusi regional di dunia menerapkan berbagai regulasi untuk menjaga stabilitas dalam lingkup siber. Upaya untuk membentuk suatu rezim siber di dunia terus berlanjut hingga saat ini. Hal ini tidak terlepas dari perlunya keamanan siber dalam menangani isu-isu yang bersifat *high-politics* dalam sistem pemerintahan. Beberapa institusi internasional seperti Uni Eropa dan NATO telah menunjukkan kepedulian mereka terhadap keamanan siber dengan membentuk badan-badan penanggulangan serta pengembangan siber. Tindakan ini dilakukan mengingat bahwa kerugian akibat serangan siber dapat berdampak sangat besar baik dari segi materi maupun non-materi.

Di Kawasan Asia Tenggara, ASEAN menjadi institusi yang mengupayakan penanganan berbagai masalah dalam lingkup regional, salah satunya terkait isu *cyber*. ASEAN sendiri merupakan hasil dari regionalisasi yang membentuk sebuah kesatuan yang terdiri atas negara-negara di Asia Tenggara (Mansfield & Solingen, 2010). ASEAN merupakan asosiasi yang didirikan pada tanggal 8 Agustus 1967 di Bangkok, Thailand. Pada awalnya ASEAN diprakarsai oleh Indonesia, Filipina, Malaysia, Singapura, dan Thailand. Hingga saat ini, anggota ASEAN berkembang menjadi 10 negara di Asia Tenggara yaitu Filipina, Indonesia, Malaysia, Singapura, Thailand, Brunei Darussalam, Vietnam, Laos, Mynmar, dan Kamboja (ASEAN, ASEAN Charter, 2008).

Integrasi yang dilakukan oleh ASEAN ditujukan dalam berbagai aspek seperti ekonomi, politik, keamanan, social, dan kebudayaan. Dalam bidang keamanan, dan ekonomi

ASEAN menyoroti isu-isu tradisional maupun non-tradisional. Isu *cyber security* menjadi salah satu bahasan non-tradisional yang penting dalam beberapa tahun terakhir. Hal ini dikarenakan adanya urgensi untuk menghadapi globalisasi serta perkembangan teknologi informasi yang begitu pesat saat ini. Hal ini diwujudkan dalam berbagai pembahasan terkait dengan *cyber security* dalam berbagai forum yang diadakan oleh ASEAN. Beberapa forum yang membahas *cyber security* adalah *Association of South East Asian Nation Regional Forum (ARF),* (ASEAN *Ministerial Meeting on Transnational Crime*) AMMTC, (*ASEAN Defence Minister's Meeting)* ADMM-Plus, dan (*ASEAN Telecommunications and IT Ministers Meeting*) TELMIN.

Pembahasan mengenai *cyber security* juga menjadi urgensi yang penting melihat data bahwa ASEAN merupakan salah satu Kawasan dengan pertumbuhan penduduk tercepat di dunia dengan total 634 juta penduduk. Ditambah lagi, ASEAN juga merupakan pasar dengan populasi terbesar nomor tiga di dunia dengan total GDP dikombinasikan mencapai lebih dari $2.55 triliun (ASEANStats, 2019). Hal ini menunjukkan bahwa ASEAN merupakan kawasan yang sangat potensial dalam pasar digital. Selain itu, kedaulatan siber juga merupakan salah satu bahasan dan tujuan dalam ASEAN *Blueprint* 2025. Untuk menyokong potensi tersebut, tentunya regulasi serta keamanan siber di Kawasan ASEAN haruslah bersifat jelas dan tegas. Dalam ASEAN Blueprint 2025 pun dijelaskan bahwa ASEAN berupaya membangun ekosistem digital yang melalui Kerjasama siber. Dalam ASEAN Blueprint 2025 disebutkan bahwa salah satu misi ASEAN adalah membangun kepercayaan ekosistem digital termasuk melalui penguatan Kerjasama dalam keamanan siber dan pengembangan takaran dalam perlindungan data pribadi (ASEAN, ASEAN Blueprint 2025, 2015).

Dengan perkembangan siber yang begitu pesat serta potensi ekonomi yang begitu besar, Perlindungan data pribad dalam dunia digital menjadi sebuah bahasan krusial dalam *cyber security*. Data pribadi menjadi sebuah objek vital yang dapat memberikan dampak dalam berbagai aspek. Data pribadi yang disebarluaskan secara daring tanpa adanya *consent* maupun pertanggungjawaban yang tepat dikhawatirkan dapat mengancam hak privasi warga negara bahkan lebih parahnya dapat mengancam kedaulatan informasi pada suatu negara.

Dibutuhkan regulasi yang tepat untuk menghindari kebocoran data yang berpotensi mengancam keamanan dan stabilitas Kawasan. Berdasarkan tiga tujuan spesifik kebijakan siber yang telah disebutkan sebelumnya, diungkapkan pula dalam poin ketiga bahwa Pemerintah negara-negara di ASEAN dituntut untuk memastikan bahwa privasi warganya dengan cara memastikan bahwa data pribadi mereka di dunia maya terlindungi secara aman dan tidak disalahgunakan untuk hal yang merugikan mereka. Hal ini sangat diperlukan mengingat informasi ini akan memberikan dampak yang sangat signifikan terhadap perekonomian serta keamanan

Perlindungan data pribadi dianggap sebagai bahasan yang penting dikarenakan data-data pribadi masyarakat ASEAN sangat berdampak dan berpengaruhi terhadap perekonomian digital di ASEAN. CSO Online menyebutka bahwa biaya rata-rata yang dihabiskan oleh gangguan peretasan data yang terorganisir di ASEAN memakan biaya sebesar 2.62 juta Dollar Amerika Serikat dengan rata-rata kerugian yang ditimbulkan oleh tiap peretasan adalah 22.500 Dollar Amerika Serikat. Salah satu kasus kebocoran data pribadi yang cukup terkenal adalah kebocoran data salah satu *E-commerce* besar asal Indonesia Tokopedia pada Mei 2020 lalu. 91 juta data pengguna Tokopedia diperjualbelikan secara bebas di sebuah forum terbuka di Internet Raidsforum seharga 5000 USD. Data ini diperjualbelikan dan berpotensi disalahgunakan untuk hal-hal tidak bertanggungjawab seperti *Scamming, Carding,* dan sebagainya. (CNN, 2020).

Selain di Indonesia, negara ASEAN lainnya seperti Singapura, Malaysia, Vietnam, Thailand juga kerap kali mendapatkan serangan siber terkait dengan perlindungan data. Pada Desember 2019, sebanyak 2400 data personil dari Kementerian pertahanan Singapura diketahui bocor. Informasi seperti nomor kependudukan, nama lengkap, alamat, dan email diperjualbelikan oleh pihak tidak bertanggungjawab. Hal ini menyebabkan kerugian begitu besar pada sektor logistic dan militer Singapura. Sebelumnya pula, pada bulan Januari 2019 Kementerian Kesehatan Singapura mengalami pencurian data pribadi yang menyebabkan bocornya data-data pribadi seperti nama, nomor telepon, alamat, serta kontak masyarakat Singapura. Hal yang sama juga pernah menimpa salah satu badan Kementerian Kesehatan

Singapura, SingHealth pada tahun 2018 lalu (Lago, 2020). Peretasan-peretasan yang terjadi ini menimbulkan kerugian berupa penyalahgunaan data pengguna untuk hal-hal seperti penipuan, *online scamming, carding,* dan kejahatan lainya.

Hingga saat ini ASEAN masih tidak memiliki badan khusus yang menangani masalah perlindungan data pribadi maupun badan yang menangani secara khusus terkait dengan *cyber security*. Penanganan terkait dengan *cyber security* masih bersifat domestik dan lebih difokuskan kepada masing-masing negara anggota. Hal ini juga didasari oleh prinsip *non-interference* yang menjadi bagian dari ASEAN *Ways*. Namun, ASEAN terus mengupayakan berbagai bentuk integrasi dalam penanganan peningkatan *cyber security* salah satunya dalam masalah perlindungan data pribadi. Dalam hal ini, ASEAN terus menerus mengupayakan fungsinya sebagai institusi regional dalam mewujudkan keamanan serta kestabilan di Kawasan.

European Union (EU/Uni Eropa) adalah salah satu contoh institusi regional yang telah menerapkan regulasi terkait dengan PDP. Peraturan tersebut disebut sebagai GDPR (*General Data Protection Regulation*). Peraturan ini diberlakukan dan diterapkan oleh seluruh negara anggota Uni Eropa dalam penanganan isu terkait perlindungan data pribadi. Berkaca pada region tetangga serta melihat adanya urgensi terkait dengan isu ini, pada November 2016 lalu, *ASEAN Telecommunications And Information Technology Ministers Meeting* (TELMIN) membentuk sebuah kerangka kerja terkait dengan perlindungan data pribadi (*Framework On Personal Data Protection*). Kerangka kerja tersebut disetujui oleh seluruh negara anggota ASEAN pada 25 November 2016 di Bandar Seri Begawan, Brunei Darussalam. Keberadaan dari kerangka kerja ini memiliki tujuan untuk memperkuat keamanan data privasi di ASEAN serta memfasilitasi Kerjasama antar negara yang berpartisipasi. Berdasarkan 2017 *Cost of Data Breach Study* dari Institusi Ponemon, penerobosan data pribadi rata-rata memakan biaya sekitar 2,36 juta dolar di kawasan ASEAN pada tahun 2017 lalu.

ASEAN *Framework On Personal Data Protection* menyatakan tujuh prinsip dasar ASEAN dalam perlindungan data pribadi, yaitu (1) Persetujuan, pemberitahuan dan persetujuan tujuan, pemberitahuan dan tujuan; (2) Akurasi data pribadi; (3) Perlindungan keamanan; (4) Akses dan koreksi; (5) Transfer data ke negara atau wilayah lain; (6) Retensi; dan (7) akuntabilitas (TELMIN, 2016). Keenam prinsip ini menjadi dasar bagi ASEAN untuk memperkuat perlindungan data pribadi di negara-negara anggotanya. Dalam penerapannya, setiap negara diberikan waktu untuk menyesuaikan dan menerapkan regulasi yang dianggap tepat dengan situasi dan kondisi dalam negeri masing-masing negara anggota. Beberapa bentuk Kerjasama dan kolaborasi yang diharapkan dari adanya kerangka kerja ini adalah pertukaran dan berbagi informasi, workshop, seminar atau aktivitas *capacity building* lainnya, serta Kerjasama penelitian di bidang terkait.

Walaupun memiliki beberapa poin penekanan, keberadaan dari ASEAN *Framework on Personal Data Protection* terlihat masih belum mampu menciptakan standar operasional dalam penerapan hukum dan peraturan terkait perlindungan data pribadi di Kawasan Asia Tenggara. Belum terlihat adanya koordinasi dalam pembuatan regulasi di negara-negara anggota ASEAN ini. Prinsip non-intervensi yang dianut oleh ASEAN membatasi campur tangan ASEAN sebagai organisasi regional dalam penanganan isu ini. Penanganan isu ini pun kembali difokuskan ke ranah domestic masing-masing negara anggota. Bahkan, di dalam kerangka kerja itu sendiri disebutkan bahwa penerapan regulasi waktu terhadap perlindungan data pribadi disesuaikan dengan situasi dan kondisi dari masing-masing negara. Sehingga tidak memberikan tekanan dan dorongan yang cukup. Penerapan dari hasil rumusan kerangka kerja yang telah dibuat pun bersifat *voluntary* dari negara anggota ASEAN tanpa adanya peraturan yang mengikat. Selain itu, ketimpangan yang terjadi pada negara-negara ASEAN juga menyebabkan ketidakmerataannya perwujudan PDP di negara-negara ASEAN.

Hingga saat ini, empat dari sepuluh negara ASEAN telah menerapkan undang-undang terkait dengan perlindungan data pribadi. Negara-negara yang telah menerapkan peraturan tersebut antara lain adalah Malaysia, Singapura, Thailand, Filipina. Sebagian besar negara mengeluarkan regulasi terkait dengan perlindungan data pribadi yang dinaungi oleh

peraturan terkait dengan *cyber security*. Namun, ada pula beberapa negara seperti Indonesia yang belum memiliki undang-undang khusus yang mengatur mengenai perlindungan data pribadi, tetapi memiliki peraturan terkait dengan perlindungan pribadi yang tersisipi di dalam perundang-undangan lain, yaitu dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik.

Dalam penelitian ini, peneliti ingin mencoba menjelaskan ASEAN sebagai sebuah organisasi internasional tingkat Kawasan dalam menerapkan ASEAN *Framework on Personal Data Protection* kepada negara-negara anggotanya Hal ini ditinjau dari berbagai Langkah dan upaya yang diambil ASEAN dalam menjalankan tiga poin implementasi dari kerangka kerja tersebut. Tiga poin implementasi tersebut antara lain adalah (1) Berbagi dan bertukar informasi; (2) *Workshop*, Seminar, kegiatan pembangunan karakter lainnya; (3) Penelitian gabungan di bidang terkait. Berdasarkan poin tersebut ASEAN telah mengambil beberapa Langkah dalam mewujudkan poin-poin tersebut. Selain itu, akan dibahas pula beberapa negara ASEAN yang telah terlebih dahulu memiliki peraturan dan kebijakan terkait dengan perlindungan data pribadi. Kemunculan peraturan serta kebijakan tersebut disebakan karena sama-sama adanya kesadaran untuk melindungi informasi yang bersifat sensitif seperti data perdagangan, data professional, finansial, serta data-data yang bersifat rahasia di lingkup pemerintahan dan swasta. Perlindungan terhadap data-data tersebut akan berpengaruh besar bagi iklim investasi serta perekonomian di suatu negara.

1.2 Rumusan Masalah

Perkembangan dalam dunia siber menunjukkan akan pentingnya perlindungan data pribadi di dunia digital. ASEAN sebagai sebuah organisasi regional pun mengambil peranan untuk menciptakan integrasi dalam meningkatkan *cyber security* salah satunya dalam bidang Perlindungan data pribadi. Hal ini diwujudkan dengan dibentuknya ASEAN *Framework on Personal Data Protection*.

Sejak tahun 2016 saat ditandantanganinya kerangka kerja tersebut, hingga tahun 2020, penerapan ASEAN *Framework on Personal Data Protection* melakukan berbagai kegiatan

dan agenda sebagai upaya mewujudkan perlindungan data pribadi di Kawasan Asia Tenggara melalui tiga poin implementasi dari kerangka kerja tersebut. Hal ini menimbulkan pertanyaan:

"Bagaimana bentuk upaya ASEAN dalam mengimplementasikan kerangka kerja perlindungan data pribadi di Asia Tenggara dari tahun 2016-2020?"

1.3 Tujuan Penelitian

Berdasarkan Latar Belakang dan Rumusan Masalah yang telah dijelaskan diatas, dapat disimpulkan bahwa tujuan penelitian ini adalah agar dapat mengetahui bentuk implementasi dari ASEAN *Framework on Personal Data Protection* di negara-negara anggota ASEAN.

1.4 Manfaat Penelitian

Diharapkan penelitian ini dapat memberikan manfaat seperti:

1.4.1 Manfaat Akademis

Penelitian ini diharapkan dapat memberikan kontribusi literatur terkait *cyber security* di ASEAN terutama dalam isu perlindungan data pribadi. Diharapkan pula penelitian ini memberikan kontribusi ilmu pengetahuan bagi civitas universitas, khususnya kepada mahasiswa Hubungan Internasional Universitas Pembangunan Nasional Veteran Jakarta (UPNVJ) dan juga penstudi HI lainnya.

1.4.2 Manfaat Praktis

Hasil dari penelitian ini diharapkan memberikan kontribusi dalam pembentukan saran dan informasi dalam meningkatkan pengetahuan terhadap perkembangan *cyber security* dan *personal data protection* di Kawasan ASEAN baik bagi pemerintah, akademisi, maupun masyarakat luas.

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini penulis akan menjabarkan mengenai latar belakang dari pentingnya perlindungan data pribadi pada era digital saat ini. Penulis mencoba menjelaskan mengenai perlindungan data pribadi di kawasan Asia Tenggara serta peranan ASEAN dalam mengintegrasikan Negara anggotanya dalam membentuk peraturan dan kebijakan terkait perlindungan data pribadi.

BAB II TINJAUAN PUSTAKA

Pada bab ini penulis akan menjelaskan dan menjabarkan karya tulis ilmiah terdahulu yang memiliki pembahasan yang berkaitan dan memiliki hubungan terkait dengan topik yang diambil dalam penulisan ini. Karya tulis ilmiah yang penulis gunakan sebagai bahan tinjauan pustaka adalah skripsi, dan jurnal ilmiah. Selain itu untuk mempermudah dalam melakukan penulisan, penulis mencantumkan kerangka pemikiran dan alur pemikiran. Terakhir, penulis juga mencantumkan asumsi yang merupakan landasan penulisan yang dilakukan.

BAB III METODE PENELITIAN

Pada bab ini penulis akan menjelaskan metode yang digunakan dalam melakukan penelitian yang dilakukan oleh peneliti. Metode penelitian digunakan untuk mempermudah penulis dalam memperoleh data dan menyelesaikan penelitian. Metode penelitian sendiri terdiri atas jenis penelitian, jenis data, teknik pengumpulan data, teknik analisis data, dan jadwal penelitian.

BAB IV PERLINDUNGAN DATA PRIBADI DAN PERKEMBANGANNYA

Bab ini membahas tentang perlindungan data pribadi secara umum. Pada bab ini dijelaskan mengenai hakikat dan pentingnya perlindungan data pribadi. Selain itu, bab ini juga menjelaskan mengenai perkembangan perlindungan data pribadi di Asia Tenggara serta perkembangan kebijakan dan peraturannya di Negara anggota ASEAN.

BAB V ANALISIS ASEAN FRAMEWORK ON PERSONAL DATA PROTECTION

Bab ini menjelaskan mengenai analisis serta implementasi dari ASEAN Framework on Personal Data Protection menggunakan teori dan konsep yang telah dijelaskan

BAB VI PENUTUP

Bab ini berisikan kesimpulan dan saran yang diharapkan berguna bagi penelitian-penelitian selanjutnya.