# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Kondisi Uni Eropa pada masa pasca perang dingin banyak mengalami perubahan dengan adanya kemajuan teknologi yang sangat pesat melalui revolusi industri. Revolusi industri adalah revolusi dalam sistem yang mengelilingi kehidupan manusia, adanya langkah-langkah perubahan dalam interaksi yang kompleks antara manusia dan teknologi, dan adanya transformasi yang menghasilkan cara-cara baru (Philbeck dan Davis, 2019). Revolusi industri kini telah memasuki era 4.0 yang menegaskan bahwa perubahan teknologi adalah pendorong transformasi yang relevan bagi seluruh kegiatan industri dan bagian dari masyarakat (Philbeck dan Davis, 2019). Era yang sering disebut sebagai era *the Internet of Things* (IoT) ini telah memunculkan berbagai macam produk dan layanan digital yang memanfaatkan *Information Technology* (IT). Adanya kemajuan yang sangat pesat dalam bidang teknologi ini kemudian menjadi bagian yang sangat penting dan tidak terpisahkan bagi kehidupan masyarakat Uni Eropa. Dengan adanya kemajuan teknologi ini berbagai aspek penting dalam kehidupan menjadi saling terinterkoneksi, sehingga diharapkan dapat membawa efektifitas dan efisiensi yang menguntungkan.

Revolusi industri 4.0. telah membawa perubahan dalam industri yang kini identik dengan digitalisasi *(digitalization)* dan otomatisasi pintar *(smart automation)* (Chou, 2019). Kemajuan yang membawa kemudahan transfer data dan otomatisasi ini menjadi peluang yang terus dikembangkan oleh Uni Eropa

dalam menciptakan *European Union Digital Single Market*. Uni Eropa kini dapat memanfaatkan kemudahan otomatisasi dan transfer data untuk meningkatkan pertumbuhan ekonomi melalui pembentukan *Digital Single Market*. Melalui pembentukan *Digital Single Market*, *European Commission* bertujuan untuk menciptakan *European Union Single Market* yang cocok di era digitalisasi. Upaya ini dilakukan oleh *European Commission* dengan mengintegrasikan 28 *digital market* nasional dari masing-masing Negara Anggota menjadi suatu *Digital Single Market* yang terintegrasi di tingkat Uni Eropa (European Commission, 2020) .

*Digital Single Market* yang mulai diberlakukan pada 6 Mei 2015 ini merupakan satu dari sepuluh prioritas politik utama *European Commission* (European Commission, 2020). Menurut *European Commission* terdapat tiga pilar kebijakan utama dalam *Digital Single Market*. Pilar yang pertama yaitu "*improving access to digital goods and services"*, melalui *Digital Single Market* barang dan jasa dapat tersedia di pasar yang berbasis *online* di area lintas batas Eropa sehingga dapat memperluas akses konsumen dan *e-commerce* tanpa adanya hambatan. Pilar yang kedua yaitu *"an environment where digital networks and services can prosper"*, *Digital Single Market* memiliki tujuan untuk menciptakan suatu lingkungan yang tepat untuk jaringan dan layanan digital dengan menyediakan infrastruktur dan layanan yang berkecepatan tinggi, aman dan dapat dipercaya, dan didukung oleh regulasi yang tepat yang mengutamakan keamanan siber, perlindungan data/*e-privacy*, dan keadilan dan transparansi pada media online. Pilar yang ketiga yaitu *"digital as a driver for growth", Digital Single Market* memiliki tujuan untuk memaksimalkan

potensi pertumbuhan ekonomi digital Eropa sehingga dapat memberikan manfaat yang maksimal kepada masyarakat Uni Eropa.

Melalui *Digital Single Market*, Uni Eropa menciptakan suatu pasar dimana pergerakan sumber daya manusia, berbagai layanan, dan arus modal dapat terjadi secara bebas dan terjamin, dalam hal ini individu dan pebisnis dapat mengakses dan terlibat secara lebih mudah melalui aktivitas yang berbasis *online* (European Commission, 2020). Dengan demikian, diharapakan dapat tercipta peningkatan kompetensi, peningkatan spesifikasi produk, serta skala ekonomi yang lebih luas, sehingga dapat mengalirkan barang-barang dan faktor produksi ke area yang lebih menghargainya (European Commission, 2015). Hal ini dapat meningkatkan efisiensi alokasi sumber daya di Uni Eropa. Namun, disaat yang bersamaan adanya *Internet of Things (IoT)* juga rentan menciptakan celah untuk bertindak kejahatan melalui ruang siber. Berbagai macam serangan siber berpotensi menyerang berbagai pemangku kepentingan dalam *Digital Single Market* melalui penyerangan jaringan, komputer, maupun perangkat lainnya yang terlibat. Hal ini turut mengancam keamanan Uni Eropa secara komprehensif yang banyak bergantung pada Teknologi Informasi (TI).

Adanya kemudahan otomatisasi dan transfer data di ruang siber dimanfaatkan oleh seluruh pemangku kepentingan untuk meningkatkan efektifitas dan efisiensi dalam berbisnis di dalam *Digital Single Market*. Aktivitas yang terjadi di ruang siber ini menghasilkan aliran data yang sangat besar yang terpapar secara bebas di ruang siber yang bersifat lintas batas dan tidak terdapat otoritas diatasnya sehingga tidak kebal dari berbagai ancaman yang berpotensi menyerang. Isu keamanan siber utama yang berpotensi mengancam keamanan berbagai aktor yang terlibat dalam *Digital*

*Single Market* adalah isu *Big Data*. Hal ini dapat membahayakan pelaku bisnis sebagai penyedia produk, layanan, dan proses digital melalui berbagai serangan siber seperti infeksi *malware, spyware, ransomware, cross-site scripting, SQL injection attack,* hingga *DDoS attack* (Smith, 2019). Adapun kejahatan siber yang paling mengancam *Digital Single Market* adalah pencurian data *(data theft)* terhadap berbagai data yang berisi informasi sensitif baik berupa data-data pribadi konsumen hingga data-data rahasia perusahaan yang terkumpul sebagai *Big Data*. Dengan demikian, disamping membawa keuntungan yang sangat besar, penggunaan Teknologi Informasi dan Komunikasi (TIK) dalam *Digital Single Market* juga menciptakan isu keamanan di ruang siber yang sangat mengancam seluruh pemangku kepentingan yang terlibat dalam pasar digital.

Menangapi hal tersebut, Uni Eropa sebagai lembaga supranasional di kawasan Eropa menjadi aktor yang berperan penting dalam menjaga kemanan Uni Eropa dari berbagai ancaman yang telah berkembang menggunakan kemajuan teknologi di ruang siber. Dalam menghadapi ancaman siber pada *Digital Single Market,* Uni Eropa telah menetapkan regulasi *The Cybersecurity Act* yang mulai diberlakukan pada 27 Juni 2019 (European Commission, 2019). *The Cybersecurity Act* merupakan rezim internasional yang telah dibentuk, disetujui, dan diberlakukan di seluruh Negara Anggota yang terlibat dalam *European Union Digital Single Market*. Dalam *The Cybersecurity Act*, Badan ENISA diberikan peran kunci untuk membangun keamanan siber *Digital Single Market* melalui pembentukan *The EU Cybersecurity Certification Scheme*.

Penelitian terkait pengaruh *The Cybersecurity Act* terhadap *European Union Digital Single Market* masih sedikit dilakukan karena kebijakan *The Cybersecurity Act* baru ditetapkan pada tahun 2019. Yosif Korcev dalam

artikelnya menjelaskan terkait *European Union Single Market* yang berpotensi terancam oleh berbagai serangan siber, sehingga memerlukan tindakan legislatif oleh *European Commission* dengan dibentuknya *Directive on Network and Information Security* (Kovchev, 2017). Dalam penelitian ini penulis memiliki fokus yang berbeda, yaitu analisa pengaruh *The Cybersecurity Act* terhadap *European Union Digital Single Market* yang perkembangannya belum banyak diteliti sebelumnya. Dengan demikian, melalui penelitian ini penulis berusaha untuk melengkapi penelitian-penelitian terdahulu dengan meneliti secara lebih mendalam keamanan siber *Digital Single Market* Uni Eropa dengan menganalisis pengaruh penetapan rezim internasional *The Cybersecurity Act*.

## 1.2. Rumusan Masalah

Dari latar belakang yang telah dijabarkan di atas, penulis menarik sebuah rumusan masalah yang akan di teliti secara lebih lanjut, yaitu :

> "Bagaimana Pengaruh *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa?".

## 1.3. Tujuan Penelitian

Tujuan dari penelitian ini secara umum adalah untuk memberikan pengetahuan mengenai adanya peran rezim internasional dalam menyelesaikan permasalahan/isu internasional. Dalam penelitian ini, permasalahan yang diangkat oleh penulis adalah isu keamanan siber *Digital Single Market* Uni Eropa. Upaya Uni Eropa dalam menghadapi permasalahan ini adalah dengan membentuk suatu rezim internasional yaitu *"The Cybersecurity Act"* yang

mengatur tentang pembentukan sertifikat keamanan siber yang berlaku di seluruh Uni Eropa yaitu *The EU Cybersecurity Certification Scheme*. Melalui skema sertifikasi tersebut, tatanan *Digital Single Market* dapat diamankan melalui jaminan sertifikasi produk, layanan, dan proses yang melibatkan penggunaan teknologi digital pada tingkat keamanan tertentu.

### 1.4. Manfaat Penelitian

Adapun berbagai manfaat yang akan diberikan melalui penelitian ini, antara lain :

a. **Manfaat Teoritis :** Penelitian ini berupaya menambah wawasan dan rujukan dalam ilmu pengetahuan mengenai teori liberlisme institusionalis atau neoliberalisme institusional.
b. **Manfaat Akademis** : Penelitian ini berupaya memberikan kontribusi ilmiah berupa pemahaman terkait adanya peran rezim internasional dalam menjaga keamanan internasional dengan berfokus menkaji rezim *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa.
c. **Manfaat Praktis** : Penelitian ini berupaya memberikan kontribusi wawasan kepada masyarakat umum tentang perkembangan kejahatan siber dan salah satu upaya penanganannya melalui pembentukan rezim internasional.

## 1.5. Kerangka Pemikiran

### 1.5.1. Teori Liberalisme Institusional / Neoliberalisme Institusional

Dalam penelitian ini, penulis menggunakan teori liberalisme institusionalis atau neoliberalisme institusional yang merupakan salah satu aliran dalam teori neoliberalisme. Teori neoliberalisme sendiri merupakan kepanjangan dari teori liberalisme klasik dalam klasifikasi filosofi politik libertarianisme. Liberalisme adalah suatu ideologi, pandangan filsafat, dan tradisi politik yang didasarkan pada pemahaman bahwa kebebasan dan persamaan hak adalah nilai politik yang utama (Suardi, 2015). Secara umum, pandangan liberalisme menolak segala bentuk pembatasan terutama berbagai pembatasan yang dilakukan oleh pemerintah dan agama. Cita-cita dari pandangan liberalisme adalah menciptakan suatu tatanan masyarakat yang bebas. Hal ini dicirikan dengan adanya kebebasan dalam berpikir bagi tiap-tiap individu.

Liberalisme berlandaskan pada argumentasi moral yang menjamin hak-hak tiap-tiap individu yang meliputi kehidupan *(life)*, kebebasan *(liberty)*, dan hak milik *(property)* sebagai tujuan tertinggi dari pemerintah (Meiser, 2018). Dalam pandangan liberalisme, kesejahteraan individu merupakan suatu hal yang mendasar yang harus diwujudkan dalam sistem politik. Dengan demikian, dalam pandangan liberalisme pembentukan institusi bertujuan untuk melindungi kebebasan individu. Sehingga, institusi yang melindungi kebebasan individu adalah suatu kekuatan politik yang terus dibatasi dan diperiksa oleh tiap-tiap individu tersebut.

Meskipun teori liberalisme banyak membahas permasalahan politik dalam negeri, dalam perkembangannya ranah hubungan internasional juga berperan penting bagi pandangan liberalisme, hal ini dikarenakan aktivitas negara di luar negeri memiliki pengaruh yang kuat terhadap kebebasan di dalam negeri (Meiser, 2018). Pandangan liberalisme sangat menentang adanya kebijakan luar negeri yang cenderung militeristik. Dengan adanya kebijakan yang bersifat militeristik, maka negara akan cenderung membangun kekuatan militer yang juga dapat digunakan untuk menindas warga negaranya sendiri. Adapun kontribusi terkuat yang diberikan oleh liberalisme terhadap teori hubungan internasional adalah teori perdamaian demokratis (Meiser, 2018). Teori ini menegaskan bahwa negara yang demokratis tidak akan berperang terhadap satu sama lain. Hal ini dikarenakan negara yang demokratis akan cenderung mengedepankan kebebasan tiap-tiap individu yang mana hal ini akan mengekang kekuasaan suatu negara. Selain itu, negara demokrasi akan cenderung melihat satu sama lain dalam sudut pandang yang positif sebagai suatu entitas yang sah dan tidak berpotensi mengancam. Dengan demikian, akan menghasilkan suatu kondisi dimana adanya kapasitas yang lebih tinggi untuk membangun kerja sama yang saling menguntungkan.

Sebagai kepanjangan dari teori liberalisme, muncullah teori neoliberalisme sebagai penyempurna yang telah disesuaikan dengan tatanan hubungan internasional yang semakin kompleks. Teori neoliberalisme didasarkan pada konsep-konsep seperti rasionalitas dan kontrak serta berfokus pada adanya peranan institusi dan organisasi dalam

tatanan politik internasional (Martin, 2007). Teori ini berfokus pada politik, ekonomi, dan *human security* dan menekankan adanya pengaruh aktor-aktor non-negara *(non-state actors)* dalam mencapai perdamaian dan kerjasama internasional dengan meminimalisir terjadinya konflik antar kepentingan. Dalam pandangan teori ini, seluruh aktor menginginkan tercapainya *absolute gains* yang diperoleh melalui kerjasama internasional. Hal ini sebagaimana dipaparkan oleh Burchill (2005), bahwa negara akan terus memaksimalkan adanya kerjasama internasional untuk mencapai keamanan dan kemakmuran. Dengan demikian, selain diperlukan pembentukan institusi sebagai wadah yang menampung seluruh kepentingan aktor, juga diperlukan peranan aktor-aktor non-negara *(non-state actors).*

Dalam penelitian ini, penulis akan lebih spesifik menggunakan teori liberalisme institusionalis atau neoliberalisme institusional yang merupakan salah satu aliran dalam teori neoliberalisme untuk mengkaji fenomena yang diangkat. Teori neoliberalisme institusional merupakan hasil pemikiran dari Robert O Keohane sebagai kritik terhadap pemikiran realisme dan neorealisme. Neoliberalisme institusional berasumsi bahwa aktor memiliki sifat utilitarian dan rasionalistik yang beroperasi di dalam sistem politik internasional yang anarkis. Pemikiran teori liberalisme institusionalis ini sejalan dengan pemikiran utama teori liberalisme yang mengandung tujuh konsep politik yang saling timbal balik yaitu; kebebasan, rasionalitas, individualitas, progress, mudah bergaul, kepentingan umum, dan kekuatan yang terbatas dan bertanggung jawab (Freeden, 2015).

Dalam teori neoliberalisme institusionalis, Robert O Keohane lebih menekankan adanya pembentukan institusi dalam kerjasama internasional. Secara umum, institusi merupakan seperangkat aturan dan praktik-praktik yang dapat menentukan peran, pemaksaan akan suatu tindakan, dan dapat membentuk suatu harapan (Keohane, 1989). Sehingga, menurut Robert O Keohane neoliberalisme institusional memandang bahwa dalam kerjasama internasional perlu adanya pembentukan institusi sebagai suatu aturan yang dapat diterapkan oleh aktor-aktor dalam hubungan internasional. Selain itu, institusi yang dibentuk juga dapat menentukan perilaku aktor yang terlibat. Dengan demikian, kerjasama dapat lebih jelas dan lancar. Adapun bentuk-bentuk institusi menurut Keohane antara lain; organisasi, seperangkat peraturan, dan konvensi (Keohane, 1989).

Disamping itu, sebagai kritik terhadap teori neorealisme, kaum neoliberalisme institusional tidak menyangkal asumsi dasar kaum neorealis bahwa kondisi sistem internasional adalah anarki. Menurut Lechner (2017), terdapat tiga pengertian yang berbeda dalam konsep anarki sendiri, yaitu anarki dapat diartikan sebagai suatu kondisi dimana tidak adanya superior umum dalam domain interaksi, anarki juga dapat diartikan sebagai suatu kondisi yang kacau atau terdapat gangguan, dan anarki juga dapat diartikan sebagai suatu hubungan yang horizontal antar entitas yang setara secara nominal sebagai suatu negara berdaulat. Dalam pandangan realisme, manusia merupakan suatu makhluk yang penuh dengan anarki. Neorealisme sebagai pandangan pembaruan dari paradigma realisme memiliki pandangan yang sedikit berbeda.

Neorealisme setuju dengan pandangan realisme bahwa sistem internasional merupakan suatu sistem yang anarki (Baldwin, 1993). Namun, dalam pandangan neorealisme kondisi anarki dapat menjadi alat bagi negara untuk menyelesaikan suatu peramasalahan. Neorealis menyetujui bahwa kerjasama di tingkat internasional dapat dilaksanakan, tetapi teori ini tetap mempertahankan asumsi bahwa kerjasama tersebut akan sangat sulit untuk dicapai dan dijaga (Baldwin, 1993).

Teori neoliberalisme institusional cenderung lebih optimis dalam memandang kondisi sistem internasional. Sekalipun sistem internasional dalam kondisi yang anarki, kerjasama tetap dapat dilakukan dengan baik dan lancar. Menurut kaum institusionalis, dalam kondisi sistem internasional yang anarki kerjasama dapat terjalin melalui pembentukan rezim internasional sebagai pembuat aturan main yang berupa "seperangkat prinsip, aturan, norma, dan prosedur pembuatan keputusan dimana harapan-harapan aktor disandarkan" (Keohane, 1984). Dengan diadopsinya gagasan neorealis bahwa sistem internasional merupakan suatu sistem yang anarki, maka negara berdaulat memiliki kebebasan secara mutlak untuk tunduk atau tidak tunduk pada aturan suatu rezim internasional. Dengan demikian, penelitian ini akan berfokus mengkaji permasalahan melalui konsep rezim internasional dalam teori neoliberal-institusionalisme.

Sebagai mana dipaparkan oleh Chayes dan Chayes (1993), faktor-faktor seperti efisiensi, kepentingan, serta norma tidak dapat dipisahkan dari kepatuhan dan efektivitas suatu rezim internasional. Kebijakan suatu rezim internasional akan menimbulkan konsekuensi

ekonomi bagi negara anggotanya, penerapan kebijakan tersebut kedalam kebijakan suatu negara memerlukan biaya yang cukup besar. Dengan demikian, keikutsertaan suatu negara dalam suatu rezim internasional akan sangat mempertimbangkan faktor efisiensi dari rezim internasional tersebut. Selain itu, kebijakan-kebijakan suatu negara baik kebijakan luar negeri maupun kebijakan domestik akan selalu berorientasi kepada negara, suatu negara tidak akan memutuskan untuk beraliansi dalam suatu perjanjian apabila tidak sesuai dengan kepentingannya (Chayes dan Chayes, 1993). Kemudian, menurut Chayes dan Chayes (1993) peraturan dan perjanjian ada untuk dipatuhi. Hal ini dikarenakan telah terjadinya internalisasi pemikiran yang fundamental melalui proses sosialisasi sejak dini bahwa norma dan hukum merupakan suatu hal yang wajib untuk dipatuhi bagi masyarakat. Menurut Young (2011) efektivitas suatu rezim internasional dapat diukur dari seberapa besar tujuan dari suatu kerjasama dapat dicapai.

Penelitian ini berfokus pada pengaruh *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa. *The Cybersecurity Act* dibentuk, disetujui, dan diberlakukan di seluruh Negara Anggota Uni Eropa sebagai upaya untuk mencapai tujuan dan cita-cita bersama yaitu menciptakan suatu tatanan pasar yang luas dengan persaingan yang sehat serta memiliki sistem jaringan yang aman secara siber. Hal ini sejalan dengan asumsi dasar teori liberalisme institusionalis atau neoliberalisme institusional bahwa dalam kondisi sistem internasional yang anarki kerjasama dapat terjalin melalui pembentukan rezim internasional (dalam penelitian ini *The Cybersecurity Act)*, sebagai pembuat aturan main yang

berupa “seperangkat prinsip, aturan, norma, dan prosedur pembuatan keputusan dimana harapan-harapan aktor disandarkan” (Keohane, 1984).

## 1.6. Hipotesis

Dalam penelitian ini hipotesis penulis adalah pembentukan rezim internasional yaitu *The Cybersecurity Act* berpengaruh terhadap *Digital Single Market* Uni Eropa karena dapat mengamankan *Digital Single Market* Uni Eropa melalui pembentukan *The EU Cybersecurity Certification Scheme* yang berguna untuk mengevaluasi dan menjamin keamanan siber produk, layanan, dan proses digital yang terdapat pada *Digital Single Market* pada tingkat keamanan tertentu dan berlaku di seluruh Uni Eropa.

## 1.7. Metode Penelitian

### 1.7.1. Definisi Konseptual

#### 1.7.1.1. Ruang Siber *(Cyberspace)*

Ruang siber *(Cyberspace)* merupakan suatu lingkungan nosional dimana terjadi komunikasi melalui jaringan komputer (LEXICO, 2020). Menurut Brussell (2013), ruang siber tidaklah berbentuk, ruang ini bersifat “virtual” yang terbentuk dari tautan antara komputer, perangkat yang mendukung internet, server, router, dan komponen lainnya dari infrastruktur internet. Ruang ini berada dalam ruang lingkup internet, sehingga berbagai aktivitas

seperti mengirim email, pengelolaan situs website, bermain game, dll terjadi di dalam ruang siber. Karena sifat dari ruang ini adalah nosional dan virtual, maka ruang siber terlepas dari otoritas negara-bangsa tertentu.

#### 1.7.1.2. Kejahatan Siber *(Cybercrime)*

Kejahatan siber *(Cybercrime)* adalah kejahatan terhadap komputer dan sistem informasi, tindak kejahatan ini bertujuan untuk mendapatkan akses tidak sah kedalam suatu perangkat atau menolak akses dari pengguna yang sah (INTERPOL, 2020). Kejahatan siber saat ini telah menjadi semakin penting karena komputer telah menjadi pusat perdagangan, hiburan, dan pemerintahan (Dennis, 1998). Tindak kejahatan ini dilakukan tidak dengan melakukan serangan fisik terhadap korban. Melainkan, kejahatan terhadap komputer ini dilakukan dengan menyerang jaringan komputer pribadi atau organisasi yang menjadi target penyerangan yang memuat sekumpulan atribut informasi penting terkait pribadi atau organisasi tersebut.

#### 1.7.1.3. Serangan Siber *(Cyberattack)*

Serangan siber *(Cyberattack)* merupakan segala bentuk manuver yang bersifat ofensif yang menyerang sistem informasi komputer, infrastruktur, jaringan komputer, atau perangkat komputer pribadi sebagai target sasarannya. Serangan siber dapat terjadi dalam berbagai bentuk dengan disertai berbagai konsekuensi, serangan ini mencakup baik yang berskala kecil seperti penolakan sementara layanan terhadap situs web hingga

yang berskala besar seperti penghancuran fasilitas senjata nuklir (Lin, 2016). Serangan ini dilakukan dengan serangan *malware, spyware, ransomware, cross-site scripting, SQL injection attack,* hingga *DDoS attack* (Smith, 2019).

#### 1.7.1.4. Keamanan Siber *(Cybersecurity)*

Keamanan siber *(Cybersecurity)* merupakan suatu upaya mengamankan berbagai sistem, jaringan, dan program yang berpotensi menjadi sasaran serangan digital. Keamanan siber merupakan suatu hal yang penting karena negara, militer, perusahaan, organisasi finansial, dan organisasi medis mengumpulkan, memproses, dan menyimpan data dalam jumlah yang sangat besar dalam komputer dan perangkat lainnya (Groot, 2020). Data-data tersebut pada umumnya mencakup berbagai informasi sensitif yang akan terus disalurkan dalam jaringan berbagai perangkat digital yang digunakan oleh suatu organisasi, sehingga perlu adanya kemanan siber untuk melindungi informasi dan sistem yang digunakan dalam proses tersebut.

#### 1.7.1.5. Rezim Internasional *(International Regime)*

Rezim Internasional merupakan suatu aturan main yang berupa "seperangkat prinsip, aturan, norma, dan prosedur pembuatan keputusan dimana harapan-harapan aktor disandarkan" (Keohane, 1984). Melalui rezim internasional diharapkan dapat menciptakan stabilitas dan perdamaian dalam tatanan internasional yang sesuai dengan peraturan yang telah dilegitimasi oleh berbagai aktor yang terlibat. Dengan demikian, meskipun tatanan

internasional merupakan suatu sistem yang anarki, kerjasama tetap dapat dilakukan melalui pembentukan rezim internasional.

### 1.7.2. Definisi Operasional

#### 1.7.2.1. Ruang Siber *(Cyberspace)*

Ruang siber *(Cyberspace)* merupakan ruang yang bersifat "virtual" yang terbentuk dari tautan antara komputer, perangkat yang mendukung internet, server, router, dan komponen lainnya dari infrastruktur internet. Dalam penelitian ini, ruang siber memfasilitasi adanya otomatisasi dan kemudahan transfer data yang dimanfaatkan oleh Uni Eropa dalam pembentukan *Digital Single Market*. Ruang yang bersifat *cross-border* ini membuka peluang baru bagi perekonomian Eropa yang sebelumnya hanya berbentuk pasar terbuka secara *offline* dengan semakin memudahkan akses terhadap beberapa barang dan jasa yang kini tersedia secara *online*. Dengan demikian, tercipta suatu pasar yang lebih menguntungkan bagi konsumen dan pebisnis dengan memanfaatkan transformasi digital.

#### 1.7.2.2. Kejahatan Siber *(Cybercrime)*

Kejahatan siber *(Cybercrime)* adalah kejahatan terhadap komputer dan sistem informasi, tindak kejahatan ini bertujuan untuk mendapatkan akses tidak sah kedalam suatu perangkat atau menolak akses dari pengguna yang sah (INTERPOL, 2020). Dalam penelitian ini, penulis akan berfokus pada kejahatan siber *(cybercrime)* yang menyerang sistem jaringan komputer pribadi

dan organisasi yang terlibat dalam *European Union Digital Single Market*.

#### 1.7.2.3. Serangan Siber *(Cyberattack)*

Serangan siber *(Cyberattack)* merupakan suatu tindak kejahatan yang dilakukan oleh seorang individu, kelompok, maupun negara dengan melakukan suatu tindak penyerangan terhadap sistem jaringan komputer pihak yang dituju. Dalam penelitian ini, penulis akan berfokus membahas serangan siber berupa pencurian data *(data theft)* berbagai data-data yang berisi informasi sensitif baik berupa data-data pribadi konsumen hingga data-data rahasia perusahaan-perusahaan yang terkumpul sebagai *Big Data*. Serangan siber berupa pencurian data *(data theft)* ini sangat potensial terjadi pada *Digital Single Market* Uni Eropa sebagai pusat aset data-data penting berbagai aktor dalam sektor perekonomian Uni Eropa.

#### 1.7.2.4. Keamanan Siber *(Cybersecurity)*

Keamanan siber *(Cybersecurity)* merupakan suatu upaya mengamankan berbagai sistem, jaringan, dan program yang berpotensi menjadi sasaran serangan digital. Dalam penelitian ini, keamanan siber *Digital Single Market* Uni Eropa menjadi suatu hal yang sangat penting karena rentan terhadap berbagai serangan. Keaman siber *Digital Single Market* Uni Eropa menjadi suatu aspek yang penting karena turut mempengaruhi keamanan Uni Eropa secara komprehensif. Dengan demikian, berbagai upaya pengamanan sistem, jaringan, dan program yang terlibat dalam

*Digital Single Market* Uni Eropa terus dikembangkan oleh Uni Eropa. Penelitian ini berfokus pada upaya Uni Eropa dalam menjamin keamanan siber *Digital Single Market* Uni Eropa melalui regulasi *The Cybersecurity Act*.

#### 1.7.2.5. Rezim Internasional *(International Regime)*

Rezim Internasional merupakan suatu peraturan yang berisi harapan aktor-aktor yang terlibat. Dalam penelitian ini, rezim internasional yang dimaksud adalah *The Cybersecurity Act* yang. Seperangkat peraturan ini berisi berbagai aturan dalam mencapai keamanan siber *Digital Single Market* Uni Eropa yang telah dibentuk, disetujui, dan diratifikasi oleh seluruh Negara Anggota.

### 1.7.3. Tipe Penelitian

Tipe penelitian yang digunakan oleh penulis untuk mengkaji permasalahan adalah tipe penelitian kualitatif. Penulis menggunakan tipe penelitian ini untuk menjelaskan pengaruh regulasi *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa. Dengan demikian, penelitian ini bersifat deskriptif yang akan menjelaskan pengaruh regulasi *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa melalui analisis teori liberalisme institusionalis atau neoliberalisme institusional.

### 1.7.4. Jangkauan Penelitian

Jangkauan penelitian ini adalah sejak dijalankannya strategi *Digital Single Market* Uni Eropa pada 6 Mei 2015 yang belum memiliki

sistem ketahanan siber yang baik hingga setelah diberlakukannya *The Cybersecurity Act* pada 27 Juni 2019.

### 1.7.5. Metode Pengumpulan Data

Teknik pengumpulan data yang digunakan oleh penulis merupakan teknik studi pustaka atau studi literatur. Melalui teknik ini, pengumpulan data-data yang diperlukan oleh penulis bersumber dari buku-buku yang terkait dengan penelitian penulis, serta bersumber dari situs-situs internet terpercaya yang menyediakan layanan untuk dapat mengakses jurnal-jurnal internasional yang berkonsentrasi sesuai dengan penelitian penulis. Selain itu, penulis akan terus berupaya untuk mendapatkan informasi dari sumber utama baik dari pihak Uni Eropa, pihak penyedia produk dan layanan digital yang terlibat dalam *Digital Single Market* Uni Eropa, maupun masyarakat Uni Eropa sebagai pihak konsumen dalam *Digital Single Market* Uni Eropa.

### 1.7.6. Metode Analisis Data

Teknik analisis data yang digunakan oleh penulis merupakan analisis data kualitatif. Teknik ini digunakan dengan menganalisis data melalui studi mendalam terkait suatu kasus. Melalui teknik ini, diharapkan data-data dalam penelitian penulis dapat dianalisis dengan menggunakan teori yang telah ditentukan untuk menjawab rumusan masalah yang telah dikemukakan.

### 1.7.7. Sistematika Penulisan

- **BAB I :** Bagian pendahuluan yang memberikan gambaran secara umum terkait penelitian yang dilakukan dengan memaparkan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, kerangka teori, hipotesis, metodologi penelitian, dan sistematika penulisan.
- **BAB II :** Bagian pembahasan terkait *Digital Single Market* Uni Eropa, isu keamanan siber yang menyertainya, dan upaya Uni Eropa untuk mengatasinya melalui pembentukan *The Cybersecurity Act*.
- **BAB III :** Bagian pembahasan yang lebih mendalam terkait pengaruh *The Cybersecurity Act* terhadap *Digital Single Market* Uni Eropa.
- **BAB IV :** Bagian terakhir yang berisi kesimpulan dan saran, melalui bab ini penulis berupaya memaparkan inti permasalahan dari keseluruhan penelitian serta menambahkan saran berbagai penelitian yang dapat dilakukan di masa mendatang guna melengkapi penelitian ini.