# BAB II

# *EUROPEAN UNION DIGITAL SINGLE MARKET* DALAM DIGITALISASI EKONOMI UNI EROPA

Digitalisasi telah menjadi aspek yang sangat penting bagi Uni Eropa. Perkembangan ekonomi global yang semakin didukung dengan adanya perkembangan teknologi menjadi faktor pendorong bagi Uni Eropa untuk terus mengembangkan strategi digitalisasi terutama pada bidang ekonomi untuk mempertahankan posisinya sebagai salah satu kekuatan ekonomi terbesar dunia. Namun, terbentuknya ekonomi digital melalui *Digital Single Market* juga menciptakan tantangan baru bagi Uni Eropa. Dalam bab ini, penulis akan memaparkan secara mendalam mengenai *Digital Single Market* di Uni Eropa, ancaman yang menyertainya, dan peran Uni Eropa dalam menghadapinya.

## 2.1. Digitalisasi Ekonomi Uni Eropa melalui Pembentukan *Digital Single Market*

Teknologi telah menjadi aspek yang sangat diandalkan oleh manusia dalam menjalankan aktivitas sehari-hari. Hal ini dapat dilihat dalam tatanan masyarakat digital di Uni Eropa yang sangat ditunjang dengan adanya efektifitas dan efisiensi melalui penggunaan teknologi. Pada tahun 2019, sekitar 77% populasi di EU-27 dilaporkan telah menggunakan internet setiap hari selama tiga bulan sebelum survei; angka ini 3% lebih tinggi dibandingkan tahun 2018 dan

31% lebih tinggi dibandingkan satu dekade sebelumnya (46% pada tahun 2009) (European Commission, 2020). Dalam perkembangannya, kemajuan teknologi di Uni Eropa dan seluruh dunia bermula dari adanya 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 mulanya ditujukan untuk meningkatkan proses produksi dalam industri di Eropa tepatnya di Inggris melalui penemuan berbagai teknologi mutakhir. Hal ini menunjukan bahwa perkembangan teknologi sangat erat kaitannya dengan sektor perdagangan dan ekonomi guna memberikan keuntungan yang lebih signifikan bagi kehidupan masyarakat. Pada saat ini, revolusi industri telah memasuki era 4.0 yang menciptakan digitalisasi di Uni Eropa melalui konektivitas terhadap internet secara menyeluruh *(omnipresent connectivity)*.

Dalam ekonomi digital, penggunaan teknologi canggih tidak hanya mempengaruhi kinerja dari suatu bisnis tertentu, namun juga mempengaruhi fungsi ekonomi secara keseluruhan. Hal ini dibuktikan dengan temuan di berbagai negara yang mengkonfirmasi adanya pengaruh positif penggunaan teknologi informasi dan komunikasi pada pertumbuhan ekonomi. Sebagai contoh, peningkatan 10% dalam penetrasi *broadband* dikaitkan dengan peningkatan 1,4% dalam pertumbuhan PDB di pasar negara berkembang (Kvochko, 2013). Selain itu, banyak penelitian dari berbagai perusahaan terkemuka seperti BCG, IMF, dan *World Economic Forum* yang menunjukan bahwa setiap kali perusahaan mengurangi investasi teknologi yang bertujuan

untuk menopang keuntungan, hasilnya adalah sebaliknya, karena keuntungan turun secara signifikan, dan, sebagai efek samping, PDB juga turun secara drastis, kemudian mengakibatkan jatuhnya produktivitas tenaga kerja setelah beberapa tahun kemudian (Cavallo, 2016). Oleh sebab itu, pemerintahan di seluruh dunia terus berinvestasi secara besar-besaran dalam mengembangkan ekonomi digital untuk meningkatkan nilai-nilai dan kemakmuran (IMD, 2020). Hal ini menjadi latar belakang penciptaan *Digital Single Market* sebagai salah satu prioritas utama *European Commission* (European Commission, 2015).

*Digital Single Market* merupakan suatu pasar tunggal dimana terdapat pergerakan bebas dari barang, orang, layanan, dan modal serta terdapat kemudahan bagi individu dan bisnis untuk mengakses internet dengan perlindungan yang tinggi terhadap data, terlepas dari kebangsaan atau tempat tinggal mereka (European Commission, 2015). Melalui pembentukan *Digital Single Market*, *Eropean Commission* bertujuan untuk menciptakan *European Union Single Market* yang cocok di era digital. Upaya ini dilakukan oleh *European Commission* dengan mengintegrasikan 28 pasar digital nasional (sebelum peristiwa Brexit) masing-masing Negara Anggota menjadi suatu *Digital Single Market* yang terintegrasi di tingkat Uni Eropa. Dengan demikian, akan tercipta suatu bentuk pasar digital yang paling luas dan paling berharga di dunia untuk berbagai bisnis yang berbasis online. Dengan dicanangkannya strategi *Digital Single Market* ini akan mempertahankan posisi Uni Eropa sebagai pemimpin dunia dalam ekonomi digital. Adanya *Digital Single Market* yang berfungsi secara penuh akan memberikan kontribusi sebesar 415 miliar

euro pertahun terhadap perekonomian dan menciptakan ratusan ribu pekerjaan baru (European Commission, 2017).

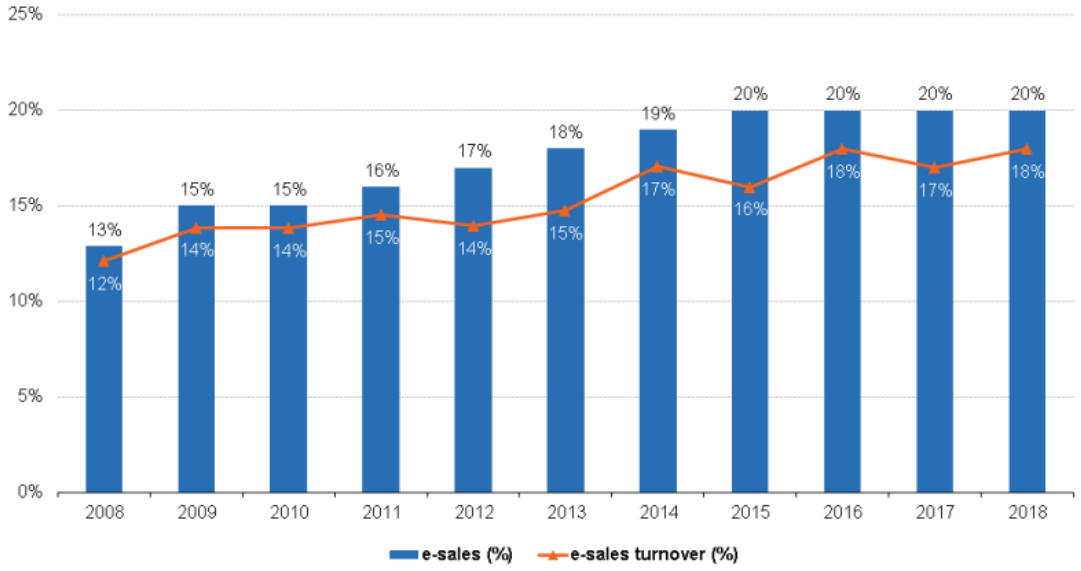
*Digital Single Market* di Uni Eropa dibangun berdasarkan tiga pilar kebijakan utama. Pilar yang pertama yaitu *"improving access to digital goods and services"*, Uni Eropa berupaya untuk membentuk pasar yang berbasis online di area lintas batas Eropa sehingga dapat memperluas akses konsumen dan *e-commerce* tanpa adanya hambatan *(geo-blocking)*. Pilar yang kedua yaitu *"an environment where digital networks and services can prosper",* Uni Eropa berupaya mencipkan suatu lingkungan pasar yang tepat untuk jaringan dan layanan digital dengan infrastuktur dan layanan yang berkecepatan tinggi, aman dan dapat dipercaya, serta didukung dengan regulasi yang tepat (meliputi regulasi keamanan siber, perlindungan data, serta keadilan dan transparansi media online). Pilar yang ketiga yaitu *"digital as a driver for growth"*, Uni Eropa berupaya memaksimalkan pertumbuhan ekonomi melalui pembentukan pasar yang sesuai di era digital.

Berbagai organisasi di seluruh dunia kini telah berlomba-lomba untuk mencanangkan strategi transformasi digital *(digital transformation)* untuk meningkatkan kinerjanya. Transformasi digital, pada dasarnya, berarti penerapan dan penggunaan teknologi modern dalam proses bisnis organisasi untuk mencapai tunjuannya dan meningkatkan efisiensi (I.V & A.I, 2020). Dalam tatanan *Digital Single Market*, berbagai pelaku bisnis baik perusahaan besar *(large enterprises)* maupun perusahaan kecil dan menengah *(small and medium enterprises)* kini terus memaksimalkan penggunaan teknologi canggih dalam berbagai kegiatan bisnisnya. Dalam kegiatan perdagangan, perusahaan kini

mulai beralih menggunakan strategi marketing *e-commerce* yang merujuk pada kegiatan perdagangan barang atau jasa melalui jaringan komputer seperti internet dengan metode yang di desain secara spesifik untuk menerima atau melakukan pemesanan (Eurostat, 2020). Hal ini bertujuan untuk menjangkau *customer* yang lebih banyak bagi pelaku bisnis dan memberikan pilihan yang lebih beragam bagi konsumen. Menurut data yang diperoleh dari *E-commerce Statistics* (Lihat Grafik 2.1.1.), jika diakumulasikan di seluruh Negara Anggota Uni Eropa (EU-28) telah terdapat peningkatan *e-sales* sebesar 7% disertai dengan peningkatan pendapatan sebesar 6% yang berasal dari kegiatan *e-sales* pada periode 2008-2018.

**Grafik 2.1.1.**

**Tingkat *E-sales* dan Hasil Pendapatan E-sales, EU-28, 2008-2018**



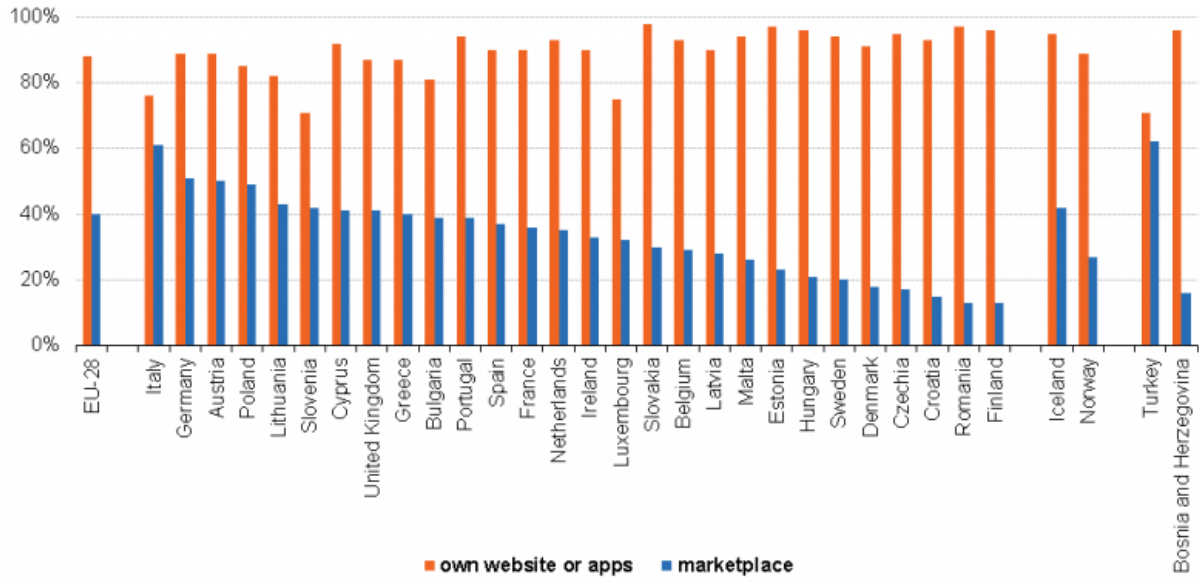

Sumber : (Eurostat, 2020)

Di dalam *Digital Single Market*, media yang banyak digunakan *e-commerce* adalah situs web atau aplikasi baik yang dikembangkan oleh masing-

masing perusahaan atau melalui *e-commerce marketplace*. Sebagaimana ditunjukan dalam Grafik 2.1.2., berbagai perusahaan di Negara Anggota Uni Eropa lebih memilih mengembangkan situs web atau aplikasi milik perusahaan sendiri daripada menggunakan situ web atau aplikasi *e-commerce marketplace*. Tingkat penggunaan tertinggi dari situs web atau aplikasi milik perusahaan sendiri terdapat di Slovakia (98%), Estonia dan Romania (masing masing 97%). Namun, di beberapa negara Eropa Barat penggunaan situs web *e-commerce marketplace* juga cukup tinggi yaitu sebesar 61% di Italia, 51% di Jerman, dan 50% di Austria.

**Grafik 2.1.2.**

**Tingkat Penggunaan Situs Web dan Aplikasi di Uni Eropa**



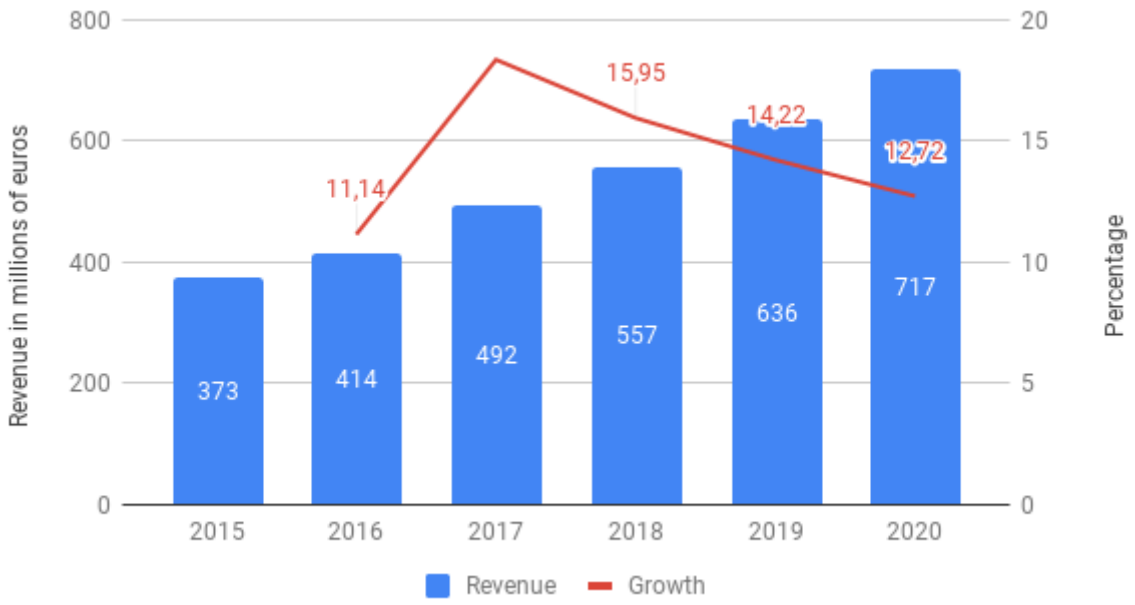

Sumber : (Eurostat, 2020)

Dalam perkembangannya, hasil perdagangan melalui *e-commerce* terus meningkat hingga mencapai 621 miliar euro pada tahun 2019 dan mencapai 717 miliar euro pada tahun 2020 (E-commerce News, 2020). Hal ini

menunjukan adanya peningkatan pendapatan sebesar 12.7% pada tahun 2020 jika dibandingkan dengan tahun sebelumnya (Lihat Grafik 2.1.3.). Adapun berbagai toko online terbesar di Uni Eropa yang saat ini terus aktif melakukan kegiatan *e-sales* antara lain; Otto (Jerman), Groupe Casino (Perancis), dan Zalando (Jerman).

**Grafik 2.1.3.**

**Tingkat penghasilan *E-sales* melalui *E-commerce* Tahun 2015 - 2020**




Sumber : (E-commerce News, 2020).

Dalam tatanan perekonomian digital, selain penggunaan *e-commerce* dalam strategi penjualan, pelaku bisnis juga melibatkan teknologi canggih lainnya untuk mengelola bisnis agar lebih efektif dan efisien. Melalui *Digital Economy and Society Index Report* 2020, *European Commission* telah memaparkan bahwa perusahaan di Uni Eropa kini telah semakin terdigitalisasi. Dimana 38,5% perusahaan besar sangat bergantung pada penggunaan teknologi

canggih seperti layanan awan *(cloud services)* dan 32.7% perusahaan besar telah menggunakan analitik *big data* (European Commission, 2021).

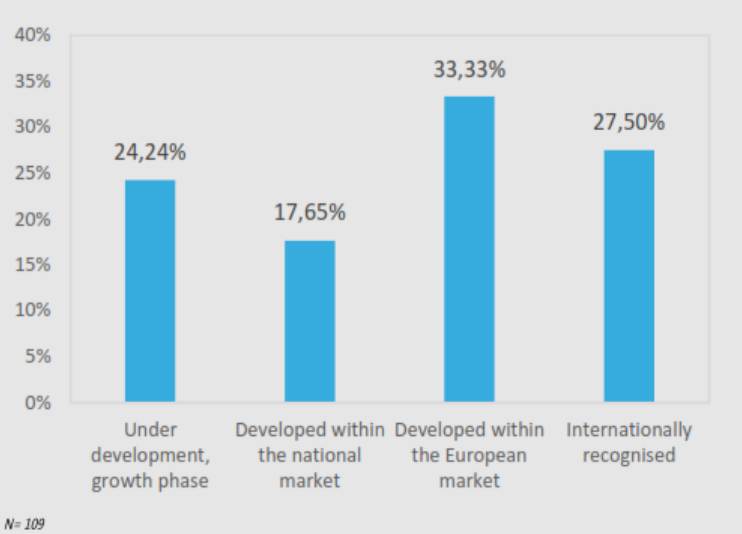
Berbagai perusahaan di Uni Eropa kini telah menggunakan teknologi *cloud* secara signifikan. Komputasi awan sangat penting untuk pasar tunggal yang murni dan kompetitif untuk berbagai data dan layanan (European Commission, 2020). Hal ini dikarenakan pelaku bisnis yang mengadopsi teknologi tersebut mengatakan bahwa mereka bertujuan untuk lebih melibatkan klien (88%), meningkatkan strategi pemasaran dan periklanan (71%), meningkatkan penjualan (67%), dan meningkatkan daya saing (50%) (European Commission, 2018). Melalui teknologi komputasi awan maka perusahaan dapat memanfaatkan teknologi komputer yang terkoneksi dalam suatu jaringan internet sehingga dapat menjalankan program atau aplikasi melalui suatu jaringan yang terpusat. Penggunaan teknologi *cloud* dapat berdampak positif pada *customer relationship management* (CRM), pemasaran operasional perusahaan, jaminan kualitas, dan manajemen proyek perusahaan.

Selain teknologi layanan awan *(cloud services)* yang digunkan dalam perusahaan, penggunaan teknologi akan menghasilkan aliran data yang sangat besar dan bervariasi *(big data)* di ruang siber. Data-data tersebut dapat berupa data yang dibuat oleh manusia atau yang dihasilkan oleh mesin seperti sensor, citra satelit, gambar dan video digital, catatan transaksi pembelian, sinyal GPS, dan lain lain yang sangat berharga untuk keberlangsungan suatu perusahaan terutama yang terlibat dalam tatanan pasar digital. Dengan demikian, data kini telah menjadi aset baru yang sangat vital untuk pertumbuhan ekonomi. Oleh karena itu, diperlukan kemampuan analitik data pada perusahaan yang terlibat dalam *Digital Single Market* untuk mengambil keputusan bisnis yang tepat

melalui ekstraksi *big data* yang dimiliki. *Big data* kini telah mulai digunakan oleh berbagai bisnis yang dikembangkan di pasar Eropa (sebesar 33%) dan pada bisnis yang telah diakui secara internasional (27,5%) (Lihat Grafik 2.1.3.). Adapun nilai dari ekonomi berbasis data di Uni Eropa mencapai 272 miliar euro pada tahun 2015, angka ini mendekati 1,9% dari PDB (European Commission, 2017).

**Grafik 2.1.3.**

**Tingkat Adopsi *Big Data* dan Analitik Data di Pasar Eropa**




Sumber : (European Commission, 2018)

Melalui pemanfaatan *big data*, perusahaan dapat meningkatkan daya saing, penjualan, dan menganalisis informasi terkait produk, layanan, dan karyawan. Sebesar 86% perusahaan yang menggunakan analisis *big data* telah menyatakan bahwa mengadopsi teknologi ini memiliki dampak yang positif (European Commission, 2018). Menurut sebuah studi Accenture, 79% eksekutif perusahaan mengatakan bahwa perusahaan yang tidak mengadopsi *big data* akan tertinggal dalam persaingan (Boichenko, 2020). Hal ini dikarenakan kemampuan

analisis *big data* dapat memungkinan perusahaan untuk meningkatkan tiga fungsi bisnis yang utama yaitu *operational marketing*, *customer relationship management* (CRM), *project management*, dan *quality assurance.* Dengan demikian, berbagai perusahaan dapat berkembang dengan pesat dengan memanfaatkan analisis *big data* yang dihasilkan dari kegiatan bisnis secara digital.

Penggunaan teknologi canggih dalam *Digital Single Market* membawa banyak keuntungan dan kemudahan baik bagi pelaku bisnis maupun *customer*. Hal ini dibuktikan dengan terus meningkatnya *e-commerce* dalam tatanan *Digital Single Market* Uni Eropa dan disertai dengan peningkatan penghasilan *(turnover)* yang dihasilkan melalui *e-sales* terhadap GDP Uni Eropa. Serta adanya berbagai manfaat dengan mengadopsi teknologi canggih lainnya seperti *big data* dan *layanan awan* yang dapat dimanfaatkan pelaku bisnis dalam mengelola perusahaan dalam tatanan ekonomi digital yang semakin kompetitif. Dengan demikian, dapat disimpulkan bahwa strategi *Digital Single Market* yang dicanangkan oleh Uni Eropa telah mampu meingkatkan pertumbuhan ekonomi melalui efektifitas dan efisiensi dalam perdagangan lintas batas di Uni Eropa, memperluas pasar dan memperketat persaingan, serta memberikan kemudahan bagi *customer* di seluruh Uni Eropa untuk mengakses produk dan layanan yang dibutuhkan.

## 2.2. Ancaman Kejahatan Siber terhadap *Digital Single Market* di Uni Eropa

Adanya kemajuan teknologi telah membawa banyak peluang bagi perekonomian di Uni Eropa. Namun disaat yang bersamaan penggunaan teknologi canggih juga turut membawa ancaman yang sangat besar terhadap

keamanan *Digital Single Market* yang melibatkan ruang siber dalam operasi perdagangan lintas batas. Baik bisnis berskala kecil maupun berskala besar yang menggunakan teknologi informasi dan telekomunikasi sangat berpotensi menjadi target ancaman siber. Hal ini dibuktikan melalui survei *The UK Government Information Security Breaches* yang mengindikasikan bahwa diantara seluruh peserta survei 90% organisasi besar telah mengalami pelanggaran keamanan serta 74% terjadi pada organisasi berskala kecil pada tahun 2015 (ENISA, 2015).

Penggunaan sistem informasi dan jaringan tentu disertai risiko keamanan dan privasi informasi yang dimiliki oleh perusahaan. Oleh sebab itu, adanya adopsi teknologi canggih seperti layanan *cloud* dan *big data* dalam perusahaan juga turut membawa ancaman yang tidak kalah besar terhadap berbagai aktor yang terlibat dalam pasar digital yang bersifat lintas batas. Adapun ancaman kejahatan siber yang paling mengancam tatanan perekonomian digital saat ini adalah pencurian data *(data theft)*. Pencurian data *(data theft)* atau biasa disebut pelanggaran data *(data breach)* merupakan suatu bentuk pelanggaran keamanan terhadap informasi yang dimiliki oleh seorang individu, suatu entitas, atau organisasi tertentu. Secara umum, pelanggaran data merupakan suatu peristiwa terilisnya *Personally Identifiable Information* (PII) milik individu tanpa persetujuan atau sepengetahuan dari individu tersebut (Goodman, 2008). Adapun tindak pelanggaran keamanan ini biasanya dilakukan dengan menyalahgunakan informasi pribadi seseorang seperti nama, nomor jaminan sosial, alamat email, kata sandi, kartu debit/kredit, informasi akun keuangan, catatan medis, SIM, dan lain lain baik dalam bentuk kertas maupun elektronik untuk tujuan penipuan.

Ancaman kejahatan siber berupa pencurian data kini sangat masif terjadi di seluruh industri baik keuangan, manufaktur, retail, telekomunikasi, perhotelah, dan berbagai layanan lainnya termasuk fasilitas kesehatan, pemerintahan, pendidikan, dll. *The Privacy Rights Clearinghouse metodology* telah mengklasifikasikan jenis pelanggaran data ke dalam beberapa kategori (Holtfreter & Harrington, 2015). Kategori yang pertama yaitu pengungkapan data yang tidak disengaja yang dilakukan dengan menyalahgunakan informasi sensitif yang diposting secara publik di sebuah situs *website* kemudian dikirimkan ke pihak yang salah melalui email, faks, atau surat.

Kategori yang kedua yaitu *Hacking/Malware* dimana seorang penjahat siber masuk melalui perangkat elektronik dan melakukan pelanggaran data. Kategori yang ketiga yaitu penipuan kartu pembayaran yang melibatkan kartu debit dan kredit yang tidak dilakukan melalui peretasan melainkan melalui penggeledahan perangkat di terminal titik layanan. Kategori yang keempat yaitu melalui orang dalam yang mendapat akses secara sah namun dengan sengaja melakukan pelanggaran terhadap informasi, hal ini biasa dilakukan oleh karyawan atau kontraktor.

Kategori yang kelima yaitu kehilangan secar fisik berbagai dokumen berbentuk non-elektronik yang hilang, dibuang, atau dicuri. Hal ini dapat terjadi dengan hilangnya dokumen berbentuk kertas atau dokumen yang terdapat pada perangkat portabel seperti laptop, PDA, *smartphone,* perangkat memori portabel, CD, *hard drive*, pita data, dan lain lain yang hilang, dibuang, atau dicuri. Kategori yang keenam yaitu melalui perangkat stasioner yang hilang, dibuang, atau dicuri seperti komputer atau server. Dan kategori yang keenam tidak diketahui. Ancaman keamanan ini dapat berakibat fatal terhadap perusahaan

karena dapat mengganggu kelangsungan bisnis, reputasi moneter perusahaan hingga menimbulkan berbagai kerugian lainnya. Dengan demikian, diperlukan suatu strategi keamanan lintas batas guna menanggulangi ancaman yang sangat besar terhadap arus data yang masif dalam tatanan *Digital Single Market* Uni Eropa yang mencakup aktivitas perdagangan online secara lintas batas di seluruh wilayah Uni Eropa.

Pada nyatanya, ancaman keaman siber berupa pencurian data tersebut pernah terjadi dalam krisis keamanan siber yang menyerang *Digital Single Market* Uni Eropa pada tahun 2017 melalui serangan "*WannaCry" Ransomware Epidemics* terhadap berbagai *high profiles* di Uni Eropa seperti *Britain's National Health Service,* perusahaan telekomunikasi Spanyol yaitu Telefonica, dan perusahaan mobil multinasional Renault. Serangan ini dilakukan dengan pengiriman email yang dirancang untuk mengelabuhi penerima agar mengklik lampiran atau mengunjungi situs web tertentu. Kemudian setelah dilakukan eksekusi, *ransomware WannaCry* akan mereplikasi dirinya dan menyebar secara cepat di dalam jaringan komputer dan menginfeksi mesin yang rentan lainnya. Setelah menginfeksi mesin, *ransomware* akan mengenkripsi file dan data yang ditargetkan pada sistem. Kemudian *hacker* akan meminta pembayaran tebusan *(ransom)* dalam bentuk *bitcoin* (mata uang kripto) untuk mengembalikan file dan data yang sudah di enkripsi.

*Ransomware epidemics* ini merupakan serangan terakhir dan terbesar dari serangkaian serangan pada krisis keamanan siber yang melanda Uni Eropa pada tahun 2016-2017. Lebih dari 4.000 serangan *ransomware* telah terjadi hampir setiap hari sejak awal tahun 2016, hal ini menunjukan peningkatan yang sangat drastis yaitu sebesar 300% jika dibandingkan dengan tahun 2015

(European Commission, 2017). Menurut penelitian PwC pada tahun 2016, jumlah insiden keamanan siber di seluruh industri meningkat sebesar 38% pada tahun 2015, ini menunjukan peningkatan terbesar selama 12 tahun terakhir, dimana setidaknya 80% perusahaan di Eropa pernah mengalami satu kali insiden keamanan siber (European Commission, 2017).

Insiden siber tentunya membawa dampak negatif bagi bisnis di Eropa, dimana tingkat kepercayaan pemangku kepentingan seperti masyarakat dan pebisnis terhadap tatanan ekonomi digital menjadi menurun. Dalam sebuah studi yang diadakan pada tahun 2014, telah diestimasikan bahwa dampak dari kejahatan siber di Uni Eropa mencapai 0.41% dari EU GDP (atau sekitar 55 miliar EUR); dimana Jerman menjadi negara yang paling terdampak diantara Negara Anggota lainnya (kerugian mencapai 1.6% dari total GDP) (European Commission, 2017). Adapun layanan yang paling terdampak adalah berbagai layanan utama seperti layanan finansial, energi, teknologi, industri, dll.

Dalam serangan *ransomware epidemic* pada tahun 2017, telah menimbulkan dampak yang sangat merugikan bagi Uni Eropa. Serangan *ransomware* ini telah mengakibatkan 19.000 perjanjian dibatalkan di *Britain's National Health Service*, dengan biaya £ 20 juta antara 12 Mei hingga 19 Mei dan £ 72 juta untuk pembersihan dan peningkatan sistem teknologi informasi (Field, 2018). Kerugian juga dialami oleh perusahaan telekomunikasi Spanyol yaitu Telefonica. Serangan ditujukan pada ratusan komputer milik Telefonica, mengenkripsi file dan meminta tebusan sejumlah $300 dalam bentuk bitcoin untuk mendekripsi file yang disandera (Dellinger, 2017). Selain itu, kerugian juga dirasakan oleh perusahaan *automobile* multinasional Renault, dimana perusahaannya terpaksa harus menutup pabrik di seluruh Eropa (Kostov, 2017).

Jika diestimasikan, serangan "*WannaCry" ransomware epidemics* telah membawa kerugian yang sangat besar bagi perekonomian global yang mencapai 120 miliar dolar (£92 miliar), jumlah ini setara dengan kerugian pada bencana alam yang sangat dahsyat seperti Badai Katrina dan Badai Sandy (European Commission, 2017).

### 1.3. Penetapan *The Cybersecurity Act* dan Pembentukan *The EU Cybersecurity Certification Scheme*

Dalam menghadapi ancaman di ruang siber terhadap *Digital Single Market*, *European Commission* membentuk suatu upaya legislatif untuk meningkatkan keamanan siber dengan menetapkan *The Cybersecurity Act* pada tahun 2019 melalui *Regulation (EU) 2019/881*. *The Cybersecurity Act* merupakan suatu regulasi yang dibentuk untuk meningkatkan keamanan siber Uni Eropa dengan memberikan mandat permanen pada Badan ENISA. Selain itu, *The Cybersecurity Act* juga menetapkan pembentukan kerangka sertifikasi keamanan siber pertama yang di sepakati pada tingkat Eropa untuk mengevaluasi dan menjamin keamanan produk, layanan, dan proses digital dalam *Digital Single Market* pada tingkat tertentu yang berlaku di seluruh Negara Anggota Uni Eropa.

Melalui penetapan *The Cybersecurity Act*, sebagaimana telah diatur dalam *Regulation* (EU) 2019/881 *(The Cybersecurity Act)* pasal 8, Badan *European Union Agency for Network and Information Security* (ENISA) diberikan peran untuk membentuk *The EU Cybersecurity Certification Framework*. Secara khusus, Badan ENISA akan memiliki peran kunci dalam

menyiapkan dan memelihara *The European Union Cybersecurity Certification Framework* dengan mempersiapkan landasan teknis untuk skema sertifikasi dan menginformasikan kepada publik tentang skema sertifikasi dan sertifikat yang dihasilkan melalui suatu situs web khusus (European Commission, 2021). Sertifikasi ini berperan penting dalam meningkatkan kepercayaan dan keamanan pada produk dan layanan dalam *Digital Single Market* (European Commission, 2020). Pembentukan sertifikat ini merupakan suatu upaya untuk mengamankan pasar internal Uni Eropa yang telah terdigitalisasi. Sehingga dapat berfungsi secara aman dan terhindar dari berbagai ancaman siber. Selain itu, melalui pembentukan sertifikasi ini dapat mengatasi permaslaahan fragmentasi dan hambatan pada *Digital Single Market* Uni Eropa dikarenakan telah terdapat banyak skema sertifikasi keamanan siber yang berbeda-beda di berbagai Negara Anggota.

Pembentukan *European Cybersecurity Certification Framework* ini telah diatur dalam *Regulation (EU) 2019/881* pada pasal 46 yaitu:

> *"The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes."*

Kerangka kerja sertifikasi ini menyediakan skema sertifikasi di seluruh Uni Eropa sebagai seperangkat aturan, persyaratan teknis, standar dan prosedur yang komprehensif (European Commission, 2020). Adapun

seperangkat aturan, persyaratan teknis, serta standar dan prosedur yang komprehensif tersebut ditujukan untuk mengatur produk, layanan, dan proses digital yang terdapat pada tatanan pasar digital. Menurut pasal 2 *The Cybersecurity Act*, produk TIK *(ICT product)* berarti elemen atau sekelompok elemen dari jaringan atau sistem informasi. Layanan TIK *(ICT service)* berarti layanan yang terdiri sepenuhnya atau terutama dalam transmisi, penyimpanan, pengambilan atau pemrosesan informasi melalui jaringan dan sistem informasi. Sedangkan proses TIK *(ICT proces)* berarti serangkaian kegiatan yang dilakukan untuk merancang, mengembangkan, menyampaikan atau memelihara produk TIK atau layanan TIK. Dengan demikian, area aplikasi tematik yang akan terpengaruh oleh ketentuan sertifikasi keamanan siber dalam *The Cybersecurity Act* mencakup produk teknologi informasi dan komunikasi (misalnya semikonduktor), layanan (misalnya layanan awan), dan proses (misalnya metode terkait keamanan informasi) (ENISA, 2019). Adapun aplikasi yang lebih nyata dari berbagai produk, layanan, dan proses digital yang akan di sertifikasi antara lain :

1) Produk-produk digital seperti berbagai aplikasi dan software, sebagai contoh: e-book, video games, konten digital seperti lagu dan film, dll.
2) Layanan-layanan digital seperti penggunaan layanan awan (*cloud service*) dan analitik *big data*.
3) Proses digital seperti proses jual-beli digital melalui *e-commerce* milik perusahaan tersebut atau *e-commerce market place*.