BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Kemajuan teknologi dan informasi berperan penting bagi semua orang, baik individu maupun organisasi. Berbagai alat yang digunakan untuk mempermudah kehidupan manusia pada saat ini merupakan bentuk dari kemajuan teknologi. Jika bicara mengenai informasi, sudah banyak perkembangan yang terjadi. Informasi yang dulu hanya disebarkan melalui media cetak, pada zaman sekarang penyebaran informasi dilakukan secara digital. Hampir seluruh akses sudah di-digitalisasi. Contohnya transportasi online, perbankan melalui m-banking, komunikasi melalui sosial media yang mana semua aplikasi tersebut sangat dekat dengan manusia dalam menjalani aktivitas sehari-hari. Kemajuan tersebut tidak terlepas dari internet yang membuat akses-akses dalam ruang digital dapat terkoneksi dengan baik.

Beberapa konsep yang berkaitan dengan internet diantaranya adalah telematika, multimedia, dan *cyber space*. *Cyber space* merupakan ruang virtual yang terbentuk dari jaringan komputer tanpa ada batasan geografis dan spasial. *Cyber space* adalah yurisdiksi baru yang sampai sekarang belum dicapai konsensus secara internasional mengenai negara manakah yang berhak untuk memutuskan atau melaksanakan yurisidiksi di *cyber space*, hal ini muncul karena sulitnya untuk menetapkan di wilayah mana *cyber space* dapat dikenai yurisdiksi sehingga hal tersebut menyebabkan adanya

ketidakpastian hukum.[1] Istilah telematika sendiri dikenal sebagai *the new hybrid of technology* yang muncul karena perkembangan teknologi digital yang membuat perkembangan teknologi telekomunikasi dan informatika semakin terpadu atau yang biasa disebut dengan konvergensi. Akhirnya kemajuan dalam teknologi telekomunikasi, media, dan informatika mendorong pengembangan sistem elektronik berbasis digital, yang kemudian dikenal sebagai *the net*. Salah satu gejala yang paling menonjol dalam teknologi informasi dan komunikasi (TIK) adalah konvergensi, yang muncul bersamaan dengan pesatnya kemajuan teknologi elektronik di akhir abad ke-20.[2] Salah satu kawasan regional yang paling maju dalam hal teknologi dan pengelolaan *cyber* di dunia adalah Uni Eropa.

Uni Eropa adalah organisasi politik dan ekonomi yang terdiri dari 27 negara anggota di Eropa. Didirikan untuk mendorong integrasi ekonomi dan politik, Uni Eropa bertujuan menciptakan stabilitas, kemakmuran, dan kerja sama antarnegara anggotanya. Pada awalnya pembentukan kerja sama ekonomi negara-negara Eropa, hanya 6 negara Eropa yang ikut berpartisipasi di dalamnya. Keenam negara tersebut di antaranya adalah Belgia, Jerman, Perancis, Italia, Luxemburg, dan Belanda yang kemudian keenam negara tersebut dianggap sebagai negara-negara pendiri Uni Eropa. Sejak bergabungnya Krosia pada tanggal 1 Juli 2013, Uni Eropa memiliki 28 negara anggota sebelum akhirnya Inggris keluar dari Uni Eropa. Uni Eropa merupakan badan otonom antara negara federal dan organisasi internasional

[1] Ayu Putriyanti, 2009, *Yurisdiksi Di Internet / Cyberspace*, Media Hukum, Vol. 9, No. 2, 2009, hlm.7

[2] Gunawan Hendro Cahyono, 2016, *Internet of Things (Sejarah teknologi dan Penerapannya)*, Swara Patra, Vol.6, No.3, 2016

yang mana negara-negara anggotanya tetap menjadi negara-negara yang berdaulat dan independen, tetapi mereka menggabungkan kedaulatan mereka. Hal ini disebut sifat supranasional yang berarti negara-negara anggotanya menyerahkan Sebagian kewenangannya dalam hal pengambilan keputusan kepada badan-badan uni eropa yang telah dibentuk sehingga keputusan untuk masalah-masalah tertentu yang melibatkan kepentingan bersama dapat diambil secara demokratis di tingkat Eropa.[3] Masalah tersebut termasuk kejahatan yang terjadi pada *cyber space* yang disebut *cyber crime*.

Cyber crime sudah banyak terjadi pada saat ini. Menurut Gregory, *cyber crime* adalah suatu bentuk kejahatan didalam ruang virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang juga terhubung dengan internet.[4] Salah satu bentuk dari *cyber crime* adalah kasus pelanggaran data pribadi oleh *Meta* (sebelumnya dikenal sebagai *Facebook*) yang melakukan pengumpulan data tanpa izin, kebocoran data-data pengguna, hingga penggunaan data untuk kepentingan yang tidak sesuai.

Kasus tersebut diawali dengan warga Austria yang bernama Maximilian Schrems, yang menggugat *Facebook* dan Komisi Perlindungan Data Pribadi Irlandia ke Mahkamah Eropa. *Facebook* sebelumnya melakukan transfer data dengan kesepakatan *Privacy Shield* yang memungkinkan perusahaan melakukan pemindahan data antar server. *Privacy Shield* adalah perjanjian yang menjembatani perbedaan standar hukum atas perlindungan

[3] Natalia Yeti Puspita, 2019, *HUKUM REGIONAL: ASEAN DAN UNI EROPA*, Universitas Katolik Indonesia Atma Jaya, hlm. 75

[4] Dista Amalia Arifah, 2011, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), Vol. 18, No. 2, 2011, Hlm. 185

data pribadi antara AS dan UE. Gugatan Maximilian menyatakan standar perlindungan data pribadi di Amerika Serikat lebih lemah dibandingkan dengan Uni Eropa karena aturan di AS memunkinkan data pengguna diakses oleh intelejen tanpa adanya pengawasan. Apabila menyaksikan *Instagram live* selebriti Eropa, data pribadi pengguna akan dikumpulkan dan akan ditempatkan di dalam server oleh *Instagram* kemudian data tersebut akan diolah untuk keuntungan atau dimonetisasi, salah satunya dengan memunculkan profil pribadi pengguna untuk keperluan iklan.[5] Disini dapat dikatakan bahwa *facebook* sebagai pihak ketiga, melakukan penyalahgunaan data untuk tujuan yang tidak atau tanpa izin dengan cara mengumpulkan data pengguna *facebook* dan mengeksploitasi data tersebut untuk keperluan diluar *consent* atau persetujuan dari pemilik data.

Kasus penyalahgunaan data oleh pihak ketiga juga terjadi pada tahun 2018 oleh *Google*. Kasus ini dimulai dari pengaduan oleh dua organisasi privasi digital, *None of Your Business* (NOYB) dan *La Quadrature du Net*, pada Mei 2018. Mereka mengajukan keluhan atas nama ribuan pengguna karena *Google* dianggap melanggar hak privasi mereka dalam penanganan data untuk tujuan komersial. *Google* mengumpulkan, memproses, dan menggunakan data pribadi pengguna untuk tujuan iklan dan tidak disampaikan dengan transparan kepada pemilik data. *Google* dikenakan denda sebesar 50 juta *poundsterling* oleh Komisi perlindungan data Prancis

[5] Rizky Banyu, *Belajar dari Gugatan terhadap Facebook di Eropa*, Berita, https://law.ui.ac.id/belajar-dari-gugatan-terhadap-facebook-di-eropa-oleh-rizky-banyu-s-h-ll-m/ , diakses pada 25 Maret 2024 Pukul 23.50 WIB

sesuai dengan ketentuan *General Data Protection Regulation* (GDPR).[6] Pasal 12 GDPR tentang "*Transparent information, communication and modalities for the exercise of the rights of the data subject"* mengharuskan perusahaan memberikan penjelasan yang sederhana dan mudah dimengerti tentang bagaimana data diproses dan *Google* dinilai gagal memenuhi standar ini.

Mendapatkan perlindungan atas data pribadinya merupakan hak dasar semua orang di dunia. Hal ini sudah sejak lama diatur didalam *Universal Declaration of Human Rights* (UDHR) yang menyatakan bahwa salah satu hak dasar manusia adalah mendapatkan kebebasan dan keamanan terhadap urusan pribadinya. Pasal 12 UDHR tentang *Right to privacy* menyatakan:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[7]

Ranah pribadi seseorang termasuk urusan pribadinya tidak dapat di intervensi atau diserang oleh pihak manapun dan harus mendapatkan perlindungan oleh hukum. Kemudian terkait dengan pencegahan untuk memindahkan data keluar dari yurisdiksi Uni Eropa diatur didalam Ketentuan Umum, pasal 3 tetang ruang lingkup teritorial, yakninya pada poin 3, *General Data Protection Regulation* (GDPR) yang berbunyi:

> *"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*."[8]

---

[6] Olivia Tambou, 2019, *Lessons from the First Post-GDPR Fines of the CNIL against Google LLC, EDPL, Rev. 80,* https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl5&div=15&id=&page=, diakses pada 29 November 2024 Pukul 2.25 WIB

[7] *Article 12 Universal Declaration of Human Rights (UDHR*)

[8] Ketentuan Umum, Pasal 3 tentang Ruang Lingkup Teritorial, angka 3, *General Data Protection Regulation.*

Pasal ini menegaskan bahwa pemrosesan data pribadi oleh suatu lembaga yang tidak didirikan di Uni Eropa, namun di tempat di mana hukum Negara Anggota berlaku berdasarkan hukum publik internasional. Adanya kasus-kasus pelanggaran data pribadi yang telah terjadi menunjukan betapa pentingnya menjaga keamanan ruang siber dengan dibentuknya suatu konsep keamanan ruang siber atau *cyber security*.

Cyber security mencakup semua alat, kebijakan, gagasan keamanan, perlindungan keamanan, pedoman, strategi manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi *cyber space* (ruang siber) dan organisasi dan aset pengguna. *Cyber security* juga mencakup perangkat lunak, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan semua informasi yang dikirimkan ke internet. *Cyber security* merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan siber. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.[9]

Cyber security sudah lama menjadi isu internasional. Pada tahun 2001 Dewan Eropa telah menyepakati perjanjian *Budapest Convention on Cybercrime* untuk mengatasi kejahatan komputer, termasuk akses ilegal, penghancuran atau modifikasi data, serta distribusi perangkat lunak yang dirancang untuk melakukan kejahatan siber. Konvensi Budapest telah

[9] Handrini Ardiyanti, 2016, *Cyber security dan Tantangan Pengembangannya di Indonesia*, https://vs-dprexternal3.dpr.go.id/index.php/politica/article/view/336/270 , hlm. 95, diakses pada 14 November 2023 Pukul 23.45 WIB

diratifikasi oleh 67 negara, yaitu sebagian besar Negara Eropa dan termasuk berbagai Negara diluar Eropa. Tahun 2019 Uni Eropa mengeluarkan sebuah regulasi yang mengatur keamanan siber regional Uni Eropa yang disebut *EU Cybersecurity Act* (EU 881/2019). *EU Cybersecurity Act* selanjutnya disebut dengan EUCA adalah peraturan yang diberlakukan oleh Uni Eropa untuk meningkatkan keamanan siber di Uni Eropa (UE) dan Wilayah Ekonomi Eropa. EUCA merupakan pengaturan atau kerangka kerja yang dinamis dan terus berkembang yang membahas berbagai aspek *cyber security*, termasuk ketahanan, penanganan, dan pencegahan terhadap serangan siber. Perjanjian ini berfokus pada penguatan kemampuan keamanan siber Uni Eropa, meningkatkan kerja sama di antara negara-negara anggota, mempromosikan inovasi keamanan siber, dan menjaga pasar tunggal digital. Strategi ini dapat mencakup langkah-langkah seperti meningkatkan respon insiden, meningkatkan perlindungan infrastruktur penting, mempromosikan penelitian dan inovasi keamanan siber, dan mendorong kerja sama internasional.[10]

Aspek *cyber security* yang yang menjadi cakupan dari EUCA diantaranya, memperkuat mandat *European Union Agency for Cybersecurity* (ENISA), memperkenalkan kerangka kerja sertifikasi keamanan siber di seluruh Uni Eropa untuk produk, layanan, dan proses Teknologi Informasi dan Komunikasi (TIK) yang memungkinkan perusahaan untuk mengesahkan tiga hal tersebut secara sekaligus dan diakui di seluruh Uni Eropa. EUCA juga mengusulkan amandemen yang memungkinkan adopsi skema sertifikasi Eropa untuk layanan keamanan terkelola, seperti respons insiden, audit

[10] A. Khurshid, *et al*., 2022, *EU Cyber Security Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme*, IEEE Access, Vol.10, No.129932-129948, 2022

keamanan, dan konsultasi. ENISA diberi mandat untuk meningkatkan kerja sama operasional di tingkat Uni Eropa dengan cara membantu Negara anggota Uni Eropa dalam menangani insiden keamanan siber jika terjadi serangan siber lintas batas berskala besar. Tugas ENISA diatur dalam pasal 8 angka 1 yang berbunyi:

> *"1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by:*
>
> *(a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available;*
>
> *(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services and ICT processes in accordance with Article 49;(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);*
>
> *(d) participating in peer reviews pursuant to Article 59(4);*
>
> *(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5)."*[11]

Dalam pasal 8 ini dijelaskan tugas ENISA yang yakninya mengembangkan dan mendorong kebijakan kebijakan mengenai sertifikasi *cyber security* produk dan layanan TIK, serta memberikan fasilitas terhadap penetapan dan penerapan standar Eropa dan Internasional untuk manajemen risiko dan keamanan produk, layanan, dan proses TIK. EUCA mengatur produk TIK untuk memastikan kualitas dan keandalan tingkat tinggi, melindungi Pasar Tunggal Digital Uni Eropa dan warganya serta menyelaraskan peraturan keamanan siber di seluruh Uni Eropa dan Wilayah

[11] Article 8 (1) EU *Cybersecurity Act* 2019

Ekonomi Uni Eropa. EUCA mempromosikan kerja sama dan berbagi informasi di antara Negara anggota Uni Eropa dan Komisi Eropa untuk meningkatkan keamanan siber. Hukuman dan Sanksi yang diatur didalam EUCA mencakup ketentuan terhadap ketidakpatuhan terhadap peraturan, memastikan bahwa perusahaan dan organisasi mematuhi kerangka kerja keamanan siber.[12]

Pengaturan tentang *cyber security* masih terbuka pada tinjauan dan pembaruan rutin untuk memastikan efektivitasnya dalam mengatasi ancaman keamanan siber yang terus berkembang atau tidak menutup kemungkinan bahwa akan terjadi pembaruan-pembaruan didalam regulasi yang mengatur tentang *cyber security* pada masa yang akan datang. Regulasi *cyber security* yang ada sampai saat ini belum mengatur secara khusus tentang perlindungan data pribadi. Disisi lain, aspek perlindungan data pribadi sangat amat penting dijaga dalam keamanan siber mengingat data pribadi merupakan indikator yang selalu diperlukan dalam akses di ruang siber. Tanpa mendaftarkan data pribadi, pengguna suatu *website* ataupun aplikasi tidak diperbolehkan mengakses *website* atau aplikasi tersebut. Oleh karena itu, sebuah regulasi yang mengatur tentang *cyber security* dalam seharusnya mengatur secara khusus tentang perlindungan data pribadi agar dapat dijadikan sebagai dasar hukum apabila terjadinya pelanggaran data pribadi di ruang siber. Sehubungan dengan latar belakang yang telah dipaparkan diatas, maka penulis mengangkat hal ini untuk diteliti lebih lanjut yang dituangkan dalam

[12] Eurosmart, 2019, *The European Cybersecurity Act*, https://www.eurosmart.com/wp-content/uploads/2019/07/CyberAct_analysis.pdf diakses pada 26 Maret 2023 Pukul 20.30 WIB

tulisan ini dengan judul "**ANALISIS CYBER SECURITY TERHADAP PELANGGARAN DATA PRIBADI DALAM HUKUM UNI EROPA**".

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana pengaturan *cyber security* dalam Hukum Uni Eropa?
2. Bagaimana *cyber security* mengatasi kasus pelanggaran data pribadi di Uni Eropa?

C. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, dapat ditetapkan bahwa tujuan dari penelitian ini adalah:

1. Untuk mengetahui bagaimana pengaturan *cyber security* dalam hukum Uni Eropa.
2. Untuk mengetahui bagaimana *cyber security* mengatasi kasus pelanggaran data pribadi di Uni Eropa.

D. Manfaat Penelitian

Berdasarkan tujuan yang telah dipaparkan di atas, maka penelitian ini diharapkan mempunyai manfaat sebagai berikut:

1. Manfaat Teoritis
    a. Penelitian ini diharapkan dapat menambah wawasan bagi mahasiswa dan akademisi di bidang hukum internasional, mengenai pengaturan hukum *cyber security* dalam hukum Uni Eropa.

b. Penelitian ini diharapkan dapat mempunyai kegunaan untuk pengembangan ilmu pengetahuan pada bidang hukum khususnya Hukum Internasional.

c. Hasil penelitian mengenai bagaimana pengaturan *cyber security* dalam hukum Uni Eropa ini dapat memperbanyak referensi kepustakaan di bidang Ilmu Hukum Internasional.

2. Manfaat Praktis

a. Penelitian ini diharapkan menambah pengalaman penulis dalam melakukan penelitian, memberikan sumbangan pemikiran ataupun masukan bagi peneliti lain.

b. Penelitian ini diharapkan dapat meningkatkan pengetahuan masyarakat untuk dapat memahami Pengaturan Hukum Regional tentang *cyber security*.

c. Bagi Masyarakat, sebagai media edukasi untuk mengetahui bagaimana analisis *cyber security* terhadap pelanggaran data pribadi dalam Hukum Uni Eropa.

E. Metode Penelitian

Dalam rangka untuk mempermudah dalam proses penelitian serta pengumpulan data yang akurat dan relevan guna menjawab permasalahan yang ada dalam tulisan ini, maka penulis menggunakan metode penelitian sebagai berikut:

1. Tipe Penelitian

Mengacu pada judul dan perumusan masalah, maka penulis menggunakan metode penelitian yuridis normatif dalam tulisan ini, yaitu

penelitian hukum yang dilakukan dengan meneliti bahan pustaka yang ada.[13] Tahapan pertama dari penelitian hukum normatif adalah penelitian yang ditujukan untuk mendapatkan norma dengan meneliti data sekunder belaka. Ditinjau dari jenisnya, penulisan ini merupakan penulisan *Library Research* (Penelitian Pustaka) yaitu suatu penulisan yang dilakukan dengan membaca buku-buku, literatur dan berbagai macam teori atau pendapat yang mempunyai hubungan dengan permasalahan yang diteliti.[14]

2. Pendekatan Penelitian

   Pendekatan yang digunakan penelitian ini adalah pendekatan perundang-undangan. Dalam penelitian ini, penulis melakukan pendekatan dengan menggunakan legislasi dan regulasi mengacu pada fokus sekaligus tema utama dalam penelitian ini.[15]

3. Sifat Penelitian

   Dalam menyelesaikan skripsi ini sifat penelitian yang digunakan adalah deskriptif analisis, yaitu penelitian dalam menyelesaikan suatu masalah dengan cara mendeskripsikan masalah melalui pengumpulan data berupa peraturan perundang-undangan dan dianalisis dengan konsep ilmu hukum terkait dengan isu hukum yang diangkat dalam penelitian, kemudian dijelaskan dan diberi kesimpulan.

[13] Soerjono Soekanto dan Sri Mamudji, 2010, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Raja Grafindo Persada, Jakarta, hlm. 13-14.

[14] Ranny Kautur, 2000, *Metode Penulisan untuk Penulisan Skripsi dan Tesis, Taruna Grafika*, Bandung, hlm. 38.

[15] Soerjono Soekanto, 2014, *Pengantar Penelitian Hukum*, Universitas Indonesia Press, Jakarta, hlm. 18

4. Sumber Data

a. Bahan hukum primer

Yaitu bahan-bahan hukum terdiri atas perundang-undangan, peraturan pemerintah, konvensi-konvensi internasional, dan perjanjian internasional. Bahan hukum primer ini antara lain:

1) *Budapest Convention on Cybercrime 2001*
2) *General Data Protection Regulation* (GDPR, 2016)
3) *NIS Directive 2016*
4) *EU Cybersecurity Act* (EUCA, 2019)

b. Bahan hukum sekunder

Bahan hukum yang memberikan penjelasan terhadap bahan hukum primer antara lain, hasil karya pakar hukum, hasil penelitian, pendapat para ahli, bahan pustaka atau literatur yang berkaitan dengan masalah yang diteliti.[16]

c. Bahan hukum tersier

Merupakan bahan hukum tambahan yang memberikan petunjuk ataupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder. Diantaranya yaitu Kamus Besar Bahasa Indonesia, jurnal hukum, ensiklopedia, internet dan sebagainya.

5. Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi dokumen atau studi pustaka. Studi dokumen dilakukan mengumpulkan data sekunder dengan cara menelaah dokumen atau bahan

[16] Zainuddin, 2009, *Metode Penelitian Hukum*, Sinar Grafika, Jakarta, hlm. 23

penelitian yang pada umumnya berbentuk tulisan berupa peraturan perundang-undangan, buku-buku dan literatur hukum yang berkaitan dengan masalah dalam penelitian ini. Penulis juga menggukanan metode *web sourcing* untuk mengumpulkan dan menelaah dokumen dan sumber-sumber yang berasal dari internet.

6. Analisis Data

Menurut F. Sugeng Istanto analisis data adalah suatu cara pengolahan data yang diperoleh untuk memperoleh kebenaran yang dicari dalam penelitian yang bersangkutan. Analisis data dalam penelitian hukum ini adalah kualitatif dengan menggunakan metode yang bersifat deskriptif analitis, dengan metode ini penulis menganalisis data yang diteliti dengan memaparkan data-data tersebut kemudian diperoleh kesimpulan.[17] Adapun penulis dalam penelitian ini menggunakan metode berpikir deduktif yaitu menganalisis dari pengetahuan yang bersifat umum untuk mendapatkan kesimpulan khusus.

F. Sistematika Penulisan

Sistematika penulisan berisi bagian bab dan sub bab yang akan memberikan gambaran jelas terkait permasalahan yang akan diteliti. Sistematika penulisan pada penelitian ini terdiri dari:

[17] Mardalis, 2004, *Metode Penelitian Suatu Pendekatan Proposal*, Bumi Askara, Jakarta, hlm. 2

BAB I : PENDAHULUAN

Pada bagian pendahuluan akan dipaparkan mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bagian ini menjelaskan mengenai tinjauan umum *cyber security*, data pribadi, hukum Uni Eropa, dan *EU Cybersecurity Act*.

BAB III : HASIL PENELITIAN DAN PEMBAHASAN

Bagian ini akan menyajikan hasil analisis mengenai pokok-pokok permasalahan yang telah diarahkan dengan rumusan masalah. Adapun hasil penelitian akan menjelaskan seputar pengaturan hukum *cyber security* dalam hukum Uni Eropa jika ditinjau dari *EU Cybersecurity Act* dan *EU Cybersecurity Act* dalam mengatasi kasus pelanggaran data pribadi.

BAB IV : PENUTUP

Bagian ini akan berisi kesimpulan terhadap penelitian yang telah dilakukan dan ditindaklanjuti dengan pemberian saran terhadap permasalahan.