BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan dunia teknologi dengan hadirnya internet juga membawa manfaat yang luar biasa bagi perkembangan peradaban manusia, dimana seseorang dapat dengan mudah mengakses informasi dari penjuru dunia hanya dengan memakai perangkat internet yang sudah terhubung ke seluruh dunia.Hal ini menyebabkan kebutuhan untuk menjaga keamanan nasional perlu untuk dipertimbangkan kembali, mengingat masifnya perkembangan internet (Zulfikar, 2023). Era Globalisasi telah mengalami banyak mengalami macam perubahan yang sebelumnya kita hanya terpaku kepada 5 faktor pada saat produksi seperti *Man, Machine, Material,Money, and Method.* Maka di Era Industri 4.0 saat ini ada banyak hal yang dapat merubah peranan faktor produksi yang sebagian besar tenaga diambil alih oleh mesin. Salah satunya *Internet of things* (IoT) dan Industri 4.0 yang merupakan sebuah tindakan yang digunakan untuk memperluas konektivitas internet antara benda-benda di sekitar kita dengan berbaga aktivitas/pekerjaan yang secara otomatis melalui pertukaran data.

Seluruh sistem tersebut terhubung dalam jaringan siber dan fisik dengan memanfaatkan komputasi awan (Doddy, 2021). Perkembangan teknologi informasi kian begitu pesat memudahkan masyarakat dalam keperluan sehari-hari. Namun adanya perkembangan teknologi bukan hanya berdampak positif hal ini juga bisa berdampak negatif apabila kita salah memahami atau bahkan menjadikan ini ladang untuk berbuat kejahatan. Perkembangan Pengguna Internet di Indonesia terus

bertambah dari tahun. dan terdapat 77 persen penduduk Indonesia menggunakan Internet.

Hal itu di sampaikan langsung oleh Ketua Umum Asosiasi Penyelenggara Jasa Internet di Indonesia yang biasa di singkat APJII. Pertumbuhannya cukup sangat fantastis dikarenakan sebelum adanya pandemi angkanya hanya menyampai 175 juta. Sedangkan data terbaru APJII di tahun 2022 pengguna internet di Indonesia mencapai sekitar 210 juta yang berarti terdapat 35 juta pengguna Internet yang ada di Indonesia. Efek dari pandemi ini dikarenakan di sepanjang pandemi banyak masyarakat yang menggunaka video conference, e-learning, video streaming e-commerce dan lain-lain (Rakhmayanti, 2022).

Kebocoran data yang terus terjadi di Indonesia juga bisa berpengaruh terhadap ketidakpercayaan Dunia Internasional kepada Indonesia akan terus meningkat. Maka dari itu Rancangan Undang-Undang Perlindungan data Pribadi (RUU PDP) yang sudah di sahkan oleh Joko Widodo. Namun, hal ini belum bisa dianggap angin segar bagi mahasiswa karena masih belum ada sanksi yang memberatkan pelaku Sehingga hal ini masih lemah untuk menjadi celah hukum yang membuat pelaku akasi pencurian dan membocorkan data belum bisa di hukum dengan hukuman yang maksimal.

Indonesia memiliki jumlah penduduk kurang lebih mencapai 250 juta jiwa dan pengguna smartphone di Indonesia juga tumbuh dengan pesat. Hal ini diperkuat oleh lembaga riset digital marketing Emarketer memperktakan pada 2018 jumlah pengguna aktif smartphone di Indonesia lebh dari 100 juta orang. Apabila kita melihat dari jumlah tersebut, Indonesia memiliki celah untuk menjadi negara

dengan pengguna aktif smartphone terbesar keempat di dunia setelah China, India, dan Amerika. Indonesia memiliki banyak peluang untuk tumbuh dengan cepat. Namun dukungan dari pemerintah mash dianggap kurang untuk memperkuat industri digital Indonesia dengan cara memperbarui ketertinggalan oleh negara lain. Salah satunya yaitu dengan memperbaiki sistem internet dengan cepat. Bukan hanya di daerah jawa namun juga di daerah lain di indonesia (Indah, 2015).

Sayangnya sistem keamanan siber di Indonesia bukannya kian membaik namun malah sebaliknya. Masalah kebocoran data yang sering terjadi bahkan telah menjadi penyakit yang kunjung sembuh di Indonesia. Salah satunya kebobrokan sistem keamanan siber yang ada di Indonesia yang baru saja terjadi yaitu kebocoran data dari Bank Rakyat Indonesia atau yang biasa kita kenal dengan Bank BRI. Bukan hanya itu *cyber-attacks* ini juga menargetkan aplikasi pemerintah seperti Kotak Pemilihan Umum (KPU) dan juga data pribadi pasien covid-19 pada tahun 2020. Badan Penyelenggara Jaminan Sosial (BPJS) juga menjadi salah satu aplikasi yang mengalami hal serupa dengan aplikasi lainnya (Abdurrohim et al, 2022).

Perkembangan Teknologi khususnya Internet memiliki banyak dampak untuk Indonesia. Adapun beberapa gejala perubahan dan pengaruhnya erhadap demokrasi Indonesia yaitu Bagaimana Perubahan ini menjadi ancaman untuk demokrasi Indonesia. Hal ini akan terlihat dari naiknya pertumbuhan pasar ekonomi yang ada di Indonesia dan masalah sosial serta politik di dalamnya (Paterson, 2019). Salah satunya terkait dibutuhkannya perlindungan keamanan siber terkait kebocoran data tersebut diperlukan dalam perspektif hak asasi manusia dimana

Internet telah menjadi sarana yang sangat diperlukan mewujudkan pembangunan dan kemajuan manusia.

Perlindungan HAM dan internet telah menjadi salah satu pembahasan penting di PBB. Pada tahun 2012, PBB mengeluarkan Resolusi tentang Pemajuan, Perlindungan dan Penikmatan HAM atas Internet, yang salah satu nya mengakui bahwa ekspresi yang disampaikan secara online mendapat perlindungan yang sama dalam berbagai aktivitas ekpresi secara online. Indonesia sendiri masalah pengaturan internet dan HAM masih menjadi salah satu tantangan, karena internet telah menjadi salah satu aspek penting dalam kehidupan masyarakat Indonesia.

Pada tahun 2012, Indonesia menduduki posisi 8 di dunia dan posisi 4 di 51.096.860. Namun perlindungan HAM di Indonesia masi belum memadai dan Indonesia masih menghadapi beberapa masalah terkait kesenjangan aksesm penyaringan dan pemblokiran sensor yang belum terumuskan secara pribadi dan kebebasan dalam menggunakan internet dan sebagainya dan data pribadi, kebebasaan dalam menggunakan internet dan sebagainya (Arum Prastyanti, n.d.)

Kasus kebocoran data tersebut merupakan salah satu hal yang memperkuat bahwa keamanan sber di Indonesia memang lemah bahkan menurut data *Cyber security Index* dari NCSI. Indonesia berada di posisi 83 dari 160 negara perihal keamanan siber. Sehingga indonesia mendapatkan skor 38,96 pada indeks keamanan siber dan skor 46,84 pada tingkat pengembangan digital.

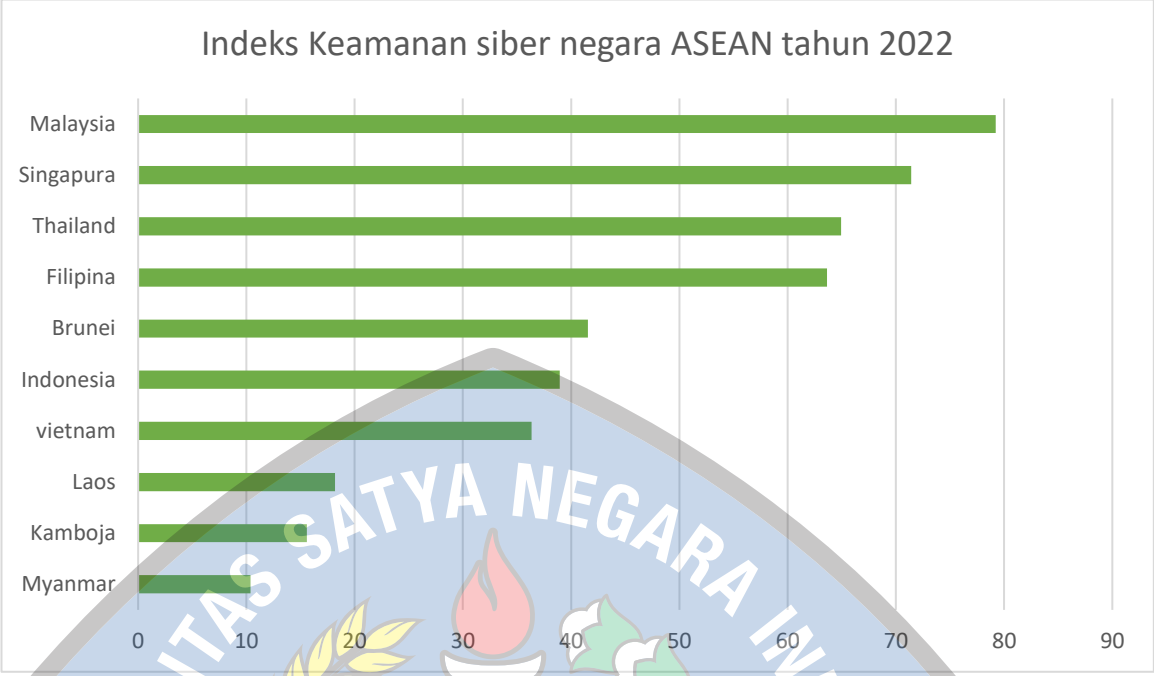
Ind

Peringkat	Negara	Indeks Keamanan Siber	Tingkat Pengembangan Digital	Selisih
46.	India	59,74	40,02	19,72
83.	Indonesia	38,96	46,84	-7,88

Gambar 1. 1 Indeks Keamanan siber global tahun 2022

Sumber (NCSI, 2022)

Indeks keamanan siber negara ASEAN di tahun 2022. Indonesia berada di peringkat 6 dari 10 dalam indeks keamanan siber. Negara tetangga yaitu malaysia berada di posisi pertama dengan skor 79,22. Negara lainnya seperti Singapura yang berada di posisi kedua dengan skor 71,43. Berikut merupakan data diagram dari Indeks keamanan siber negara ASEAN.



Gambar 1. 2 Indeks kemanan siber negara asean

Sumber : Diolah kembali oleh peneliti berdasarkan data dari (NCSI, 2022)

Hal diatas menandakan bahwa Indonesia masih menjadi negara yang paling rentan dan beresiko dalam hal keamanan siber. Oleh Karena itu, pemerintah Indonesia dibawah naungan Presiden Joko Widodo pada tanggal 19 mei 2017 telah menandatangani peraturan presiden (Perpes) Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara atau biasa di singkat dengan BSSN. BSSN sendiri merupakan Lembaga pemerintah Non kementerian yang berada di bawah tanggung jawab Presiden melalui kementrian yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelenggaraan pemerintah di bidang politik, hukum, dan keamanan (Sudarmadi et al., 2019). BSSN tidak tinggal diam dalam menghadapi ancaman siber di Indonesia serta memiliki strategi dimana dalam proses strategi dari keamanan tentu akan terdapat actor utama yang melakukan

proses tersebut. Aktor dari strategi keamanan tersebut memiliki penelitian yang berkaitan dengan Lembaga-lembaga suatu institusi negara.

Seperti kementrian pertahanan, Kementrian Komunikasi dan Informatika. Salah satu kerja sama yang dilakukan Indonesia melalui BSSN yaitu Kerjasama dengan negara tetangga yaitu Australia dimana Indonesia telah bekerjasama dengan Australia terkait *Cyber issues* pada tahun 2017. Sebelum Kerjasama tersebut terlaksana Australia pernah membantu Amerika Serikat yang pada saat itu menargetkan Indonesia menjadi sasaran penyadapan oleh AS. Penyadapan tersebut dilakukan oleh *National Security Agency* NSA Amerika yang bekerja sama dengan Direktorat Sandi Pertahanan (DSD) Australia. Salah satu contoh yang dilakukan yaitu NSA-AS meminta bantuan pada DSD-Australia untuk memata-matai Indonesia pada waktu Konferensi perubahan Iklim PBB yang diadakan di Bali tanggal 3-14 Desember 2007. Penyadapan itu dilakukan Amerika dan Australia untuk memnatau struktur jaringan komunikasi keamanan Indonesia (Sudarmadi et al., 2019)

Tahun 2017 merupakan awal Presiden Indonesia yaitu Joko Widodo meresmikan Badan Siber dan Sandi Negara untuk memperbaiki sistem siber yang ada di Indonesia dan awal dimana kerja sama antar negara Indonesia – Australia di tetapkan terkait *Cyber-issues* yang terjadi di Indonesia. Pertemuan pertama antara Indonesia – Australia di laksanakan pada 4 Mei 2017 di Australia dan Kerjasama ini bertujuan untuk mempererat kerja sama siber dan kemitraan diantara kedua negara untuk berbagi informasi, praktik terbaik Keamana siber dan pengembangan

kapasitas serta pengembangan ekonomi digital serta penangan kejahatan siber (BSSN, 2020).

Teknologi dan keamanan siber adalah dua sektor dimana kerja sama antara Australia dan Indonesia mempunyai banyak potensi. Nota kesepahaman mengenai kerja sama siber antara kedua negara ditandatangani pada tahun 2018, dan sejak itu sering terjadi diskusi mengenai kebijakan siber yang memungkinkan perwakilan berbagai lembaga untuk bertukar praktik terbaik. Pejabat dari kedua belah pihak menandatangani sebuah dokumen pada bulan September tahun lalu yang mengikat mereka untuk bekerja sama dalam berbagi informasi tentang strategi siber nasional dan mengoordinasikan tanggapan terhadap insiden siber **(Gatra, 2022)**.

Dalam pertemuan ini dijelaskan bahwa kerja sama yang terjalin antara Indonesia – Australia diatas *"Memorandum Of Understanding" on Cyber Cooperation* selama dua tahun dianggap membuahkan hasil bagi kedua negara. Kerja sama di antara kedua negara terus berlanjut dengan adanya perpanjangan kerja sama diatas MoU pada tahun 2018 dengan masa kerja sama 2020 – 2024 dalam kerja sama *plan of action for Indonesia – Australia (2020 – 2024)* , Namun belum sampai tahun 2024 kerja sama antara dua negara ini selesai. Terdapat kejadian yang tidak menguntungkan bagi masyarakat sipil di Indonesia yang mengalami kebocoran data pengguna pada tahun 2021 sampai dengan akhir tahun 2022 yang mengakibatkan kebocoran data instansi pemerintah merugikan masyarakat sipil Indonesia yang mengguanakan aplikasi tersebut.

Dengan demikian kerja sama ini hanya menguntungkan pemerintah yang menjadi perantara didalamnya namun merugikan masyarakat sipil dan bagaimana implementasi kerja sama siber antara Indonesia – Australia ini berlangsung terhadap penanganan kejahatan transnasional di Indonesia.

1.2 Pertanyaan Penelitian

Berlandas dari Latar Belakang yang penulis bahas diatas, pertanyaan penelitian yang menumbuhkan ketertarikan dalam mengkaji lebih dalam terkait **"Bagaimana Implementasi Kerjasama Indonesia-Australia Dalam Menangani Kejahatan Siber Transnasional di Indonesia?"**

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang terdapat di bagian sebelumnya tentu penulis memiliki tujuan untuk menjawab permasalahan yang ada. Yaitu dengen menjelaskan implementasi kerja sama yang terjalin antara Indonesia – Australia dalam menangani kejahatan siber Transnasional di Indonesia. Sehingga apakah kerja sama tersebut tidak hanya menguntungkan bagi Indonesia dan Australia. Namun juga masyarakat sipil yang menjadi pengguna data internet itu sendiri.

1.4 Manfaat Penelitian

Manfaat dari penelitian yang penulis buat yaitu penulis berharap mampu berbagi manfaat baik informasi serta ilmu yang dapat penulis sampaikan pada penelitian ini. Penulis membagi manfaat penelitian ini menjadi dua, yaitu manfaat teoritis juga manfaat praktis yang dapat penulis uraikan sebagai berikut:

1.4.1 Manfaat Teoritis

Manfaat teoritis pada penelitian ini penulis berharap antara lain;

1. Membantu berbagi mengenai pemikiran serta pengetahuan baru, khususnya pada bidang studi Ilmu Hubungan Internasional.

2. Membantu menjawab penanganan kejahatan siber transnasional yang memiliki dampak negatif terhadap masyarakat sipil di Indonesia.

3. Menjadi sumber referensi untuk penulis berikutnya yang mengangkat permasalahan yang sama khususnya terkait keamanan data siber, dan implementasi kerja sama yang dilakukan Indonesia – Australia dalam memperbaiki keamanan siber di Indonesia.

1.4.2 Manfaat Praktis

Manfaat praktis pada penelitian ini penulis berharap antara lain:

1. Menambah materi bagi para peneliti serta mahasiswa yang sedang mengerjakan penelitian sehingga dapat melihat sudut pandang yang berbeda.

2. Memberikan ilmu pengetahuan serta edukasi terkait keamanan data siber sangat penting bukan hanya untuk masyarakat sipil namun juga negara. Serta memberikan beberapa gambaran bagaimana kejahatan siber bisa menjadi salah satu pemicu fenomena lain muncul seperti kejahatan transnasional.

3. Menjadikan penelitian ini bahan rekomendasi bagi para pemangku jabatan yang memiliki kepentingan terkait permasalahan Keamanan data siber yang menjadi kejahatan transnasional di Indonesia.

1.5 Sistematika Penulisan

Penulis membagi beberapa bagian sistematika penulisan yang mana terbagi menjadi 5, yaitu;

BAB I: PENDAHULUAN

Di dalam bab pendahuluan ini terdapat latar belakang yang penulis angkat sebagai isu utama dari penelitian ini, lalu disambung oleh pertanyaan penelitian dimana pada masalah atau kasus yang akan penulis kaji, penulis juga memasukan tujuan serta manfaat yang ingin di dapatkan oleh penulis dan tidak lupa pula dicantumkannya sistematika penulisan untuk memperjelas setiap bab yang penulis telah buat dalam penelitian ini.

BAB II: TINJAUAN PUSTAKA

Di dalam tinjauan pustaka terdapat penelitian yang sudah dilakukan sebelumnya dan memiliki kesamaan dan relevansi dengan tema yang penulis angkat. Pada bagian landasan teori dan konsep yang juga merupakan hal pokok yang membahas mengenai keamanan data dan informasi serta keamanan siber. Pada akhir dari Tinjauan pustaka terdapat pula alur pemikiran yang mana penulis juga berikan

arahan bagaimana penelitian ini dapat bekerja yang dikaitkan oleh teori, konsep, serta permasalahannya supaya dapat dipahami oleh penulis serta orang lain.

BAB III: METODOLOGI PENELITIAN

Pada metodologi penelitian di bab ini akan menjelaskan mengenai bagaimana cara penelitian yang penulis gunakan, sudut pandang penulis dalam meneliti, pendekatan yang penulis ambil, jenis penelitian, unit analisis, Teknik pengumppulan data, dan juga bagaimana Teknik dari keabsahan data dimana semua data penelitian yang penulis kumpulkan akan saling terhubung satu sama lain sehingga dapat menjadi sebuah metode penelitian yang dapat menjawab permasalahan penelitian yang penulis ajukan.

BAB IV : PEMBAHASAN

Bab ini berisi mengenai pembahasan dari bagaimana kerja sama antara Indonesia dan Australia berjalan dalam menangani Kejahatan Siber Transnasional di Indonesia yang mengganggu beberapa aplikasi di sektor ekonomi di Negara Indonesia.

BAB V : PENUTUP

Bab ini merupakan penutup, yang terdiri dari kesimpulan