BAB 1 PENDAHULUAN

1.1 Latar belakang Masalah

Data Pribadi adalah informasi apapun yang berkaitan dengan orang yang dapat diidentifikasi ('subjek data'); orang alami yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan merujuk pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengenal online atau satu atau lebih faktor spesifik untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau sosial dari orang itu alami (GDPR, 2016). Dengan penggunaan media sosial di mana-mana melalui internet, jumlah yang belum pernah terjadi sebelumnya data tersedia dan menarik bagi banyak bidang studi termasuk sosiologi, bisnis, psikologi, hiburan, politik, berita, dan aspek budaya masyarakat lainnya (Barbier, 2011).

Mengenai data pribadi untuk mendapatkan aksesnya diperlukan adanya persetujuan karena 'persetujuan' pemilik berarti bagian yang diberikan dengan bebas, spesifik, terinformasi, dan pasti tentang subjek melalui konfirmasi yang jelas, menandakan persetujuan untuk pemrosesan data pribadi (GDPR, 2016). Maka itu data pribadi sangat dibutuhkan ketika melakukan pendaftaran pada sosial media di internet agar dapat menujukkan bahwa orang yang medaftar adalah orang asli dan bukan palsu namun, ketika data pribadi terekspos pada publik ini dapat disalahgunakan oleh orang lain maupun perusahaan yang didaftarkan. Mengenai hal tersebut penulis menilik kasus yang sempat menggemparkan khalayak karena

menurut penulis hal ini mungkin dapat mengancam tidak hanya orang-orang namun negara, yaitu kasus Cambridge Analityca.

Cambridge Analytica dimulai pada 2014, ketika ilmuwan Aleksandr Kogan (alias Aleksandr Spectre) dan beberapa lainnya terhubung dengan berbagai cara dengan Cambridge University mendirikan perusahaan bernama Global Science Research untuk memasarkan aplikasi Facebook, "Thisisyourdigitallife," yang mengambil informasi pribadi dari peserta yang mengira mereka mengambil semacam tes kepribadian, dan memanfaatkan informasi itu untuk mendapatkan politis kecerdasan yang berguna pada sekitar 50 juta orang. (Booth, 2018)

Cambridge Analytica (CA) adalah perusahaan data yang berdiri pada tahun 2013 merupakan anak perusahaan Strategic Communication Laboratories (SCL). Perusahaan berfokus untuk bisnis dan politik yang menggabungkan data mining, data brokerage, dan analisis data dengan komunikasi strategis selama proses kampanye pemilihan (Raben, 2018). Dengan menggunakan data-data yang dikumpulkan Cambridge Analityca, klien-klien mereka dapat lebih efektif menentukan strategi penjualan ataupun kampanye politik yang ingin dilakukan (Raben, 2018). Data dilaporkan datang melalui sebuah aplikasi yang dibuat pada tahun 2013 oleh akademik psikolog Aleksandr Kogan. Pada waktu tersebut, Facebook mengizinkan pengembang aplikasi untuk mengumpulkan data tidak hanya tentang aplikasi pengguna tetapi juga teman-teman Facebook mereka, menurut Mark CEO Facebook Zuckerberg. Secara tertulis dari bukti kepada komite parlemen Inggris, Kogan menegaskan bahwa aplikasinya itu mengumpulkan data dari teman pengguna jika pengaturan privasi diizinkan akses ke informasi itu, termasuk nama, tanggal lahir, lokasi dan jenis kelamin (Tarran, 2018).

Bahkan perusahaan analisis data yang berbasis di AS, Cambridge Analytica mengklaim memiliki database dengan personal profil sekitar 220 juta warga AS, yang sesuai dengan sebagian besar populasi pemilih AS (Srivastava, 2008). Cambridge Analytica menyadari bahwa mereka dapat mengintegrasikan informasi ini dengan berbagai data dari platform media sosial, browser, pembelian online, hasil pemungutan suara, dan lebih banyak lagi untuk membangun "5.000 titik data pada 230 juta orang dewasa AS." Dengan menambahkan analisis OCEAN ke swasta lainnya dan data publik diperoleh, Cambridge Analytica mengembangkan kemampuan untuk "Microtargeting" konsumen atau pemilih perorangan dengan pesan yang paling mungkin mempengaruhi perilaku mereka (Ward, 2018).

Dengan sejumlah besar data yang mungkin untuk dilakukan yang dapat memengaruhi peristiwa politik yang signifikan seperti misal pemilihan presiden atau acara sosial utama, demonstrasi anti-homofobia misalnya (Srivastava, 2008).

Seperti dijelaskan oleh CEO Cambridge Analytica, kuncinya adalah mengidentifikasi orang-orang yang mungkin tertarik untuk memilih klien mereka atau berkecil hati untuk memilih lawan mereka. Setiap suara ditambahkan atau diganggu (dengan cara yang dimaksudkan) memberi tip pada hasil pemilihan (Isaak & Hanna, 2018).

Dan ketika kasus di UK terjadi pada Brexit. Brittany Kaiser mantan data analyst SCL perusahaan di bawah naungan Cambridge Analytica, dia mentestimonikan di House of Common bahwa taktik komunikasi media sosial Cambridge Analytica sebagai teknik komunikasi "senjata" yang digunakan melawan Inggris. (Heawood, 2018)

Kutipan lengkap Kaiser, sebagaimana dicatat oleh House of Commons, mengatakan bahwa: ”Saya pernah memiliki keprihatinan karena ketika saya bergabung dengan perusahaan. Saya tidak ingat ini, tetapi setelah mengingat kembali, Saya menemukan dokumen dari Nigel Oakes yang merupakan pendiri SCL Group, yang bertanggung jawab atas divisi pertahanan kami, yang menyatakan bahwa metodologi analisis audiens target ini dikendalikan oleh Pemerintah Inggris. Berarti metodologi tersebut dianggap sebagai taktik komunikasi tingkat senjata yang berarti bahwa kami harus memberi tahu Pemerintah Inggris jika itu akan dikerahkan di negara lain di luar Inggris”.

Maka ketika data yang ada dimanipulasi untuk melakukan micro targeting maka privasi seseorang juga dalam hal ini telah dilanggar karena orang-orang terekspos bagaimana kehidupan dan sosialnya sehingga dapat dimanfaatkan untuk kepentingan Cambridge Analityca. Dalam hal ini Cambridge Analityca memanipulasi data dengan metode microtargeting berdasarkan prediksi perilaku untuk menggeser opini sehingga orang-orang yang terkena media-media yang dikhususkan pada mereka oleh Cambridge Analityca menjadi semakin mendukung.

Dalam penanganan data pengguna Facebook, Facebook hanya melakukan sedikit tindakan penanganan data sementara Cambridge Analytica berulang kali merusak pedoman data Facebook (Zinolabedini & Arora, 2013). Kebocoran data Facebook yang diakibatkan oleh Cambridge Analityca ini melanggar privasi pengguna dikarenakan eksploitasi yang dilakukan tersebut.

Melalui latar belakang masalah tersebut, penulis tertarik untuk mengetahui bagaimana pelanggaran privasi dan ancaman dari kasus Cambridge Analityca terhadap keamanan manusia.

1.2 Rumusan masalah

Berdasarkan penyusunan pada latar belakang dapat dirumuskan sebuah rumusan masalah yaitu bagaimana pelanggaran privasi dan ancaman oleh Cambridge Analityca dapat menjadi ancaman bagi keamanan manusia?

1.3 Tujuan Penelitian

Adapun tujuan penulisan yang diajukan terhadap penelitian ini adalah:

1. Menjelaskan dan menganalisa secara mendalam mengenai pelanggaran privasi dan ancamannya terhadap keamanan manusia.

1.4 Manfaat Penelitian

Adapun manfaat yang didapatkan dari penelitian ini dapat dibedakan menjadi dua bagian yakni manfaat akademis serta manfaat praktis.

1.4.1 Manfaat Akademis

Untuk dapat memperkaya kajian di bidang hubungan internasional, khususnya mengenai *cyber security* dan keamanan manusia.

1.4.2 Manfaat Praktis

1. Memberikan pemahaman terhadap masyarakat luas mengenai pelanggaran privasi yang dilakukan oleh Cambridge Analytica
2. Sebagai bahan acuan rekomendasi pemerintah dan rezim internasional dalam menyusun dan menjalankan kebijakan yang berhubungan dengan *cyber security*, sehingga penelitian ini dapat menjadi pertimbangan maupun pembelajaran bagi pemerintah dan rezim internasional dalam menangani pelanggaran privasi terutama dalam menanganinya.

1.5 Kerangka Teori

Untuk menganalisa rumusan masalah dalam penelitian ini, peneliti menggunakan konsep *Human security* dan *Cyber Security*, untuk menganalisa pelanggaran privasi dan ancaman terhadap keamanan dalam kasus Cambridge Analytica.

i. *Human security*

Human security merupakan satu dari isu-isu global kontemporer yang menjadi salah satu isu yang sangat serius untuk dibahas, baik di kalangan akademisi, maupun di kalangan para pengambil kebijakan(Hossain, 2018). Pasca Perang Dingin, isu *human security* baru mulai mendapat perhatian dari masyarakat luas di seluruh dunia setelah sebelumnya mengalami kegagalan di akhir Perang Dunia II(Cartwright, 2010).

Human security juga ikut mengalami pergeseran sejalan dengan kemunculannya di dunia internasional. Konsep keamanan dari *human security* mengalami perubahan dari isu-isu militer dan politik menjadi fokus terhadap permasalahan dan kondisi yang terjadi dalam individu dan masyarakat dan pergeseran dari national security pada masa Perang Dunia I dan II, serta Perang Dingin menjadi *human security*(Hossain, 2018).

United Nations Development Program (UNDP) dalam Human Development Report 1994 merupakan badan Perserikatan Bangsa-Bamgsa (PBB) pertama yang memperkenalkan konsep *Human security* (UNDP, 1994). Badan PBB berpendapat bahwa konflik yang terjadi saat ini lebih banyak terjadi di dalam negara dibandingan dengan konflik antarnegara (UNDP,

1994). Berbeda halnya ketika kita kembali pada masa Perang Dunia I, Perang Dunia II, dan Perang Dingin yang diliputi oleh konflik antarnegara, sehingga masih terpusat pada keamanan nasional (UNDP, 1994).

Konsep *human security* lebih bersifat universal. Artinya, konsep keamanan ini tidak hanya terbatas pada sebuah negara saja, namun berlaku untuk umum (UNDP, 1994). Bagi seluruh umat manusia di dunia. Mengingat bahwa ancaman bisa datang kepada siapa saja, tanpa memandang negara mana manusia tersebut berada (UNDP, 1994). Sebuah peristiwa pun dapat dikategorikan sebagai *human security* apabila telah sampai mengancam keamanan nasional suatu negara (UNDP, 1994). Karena dari ancaman keamanan nasional, bukan tidak mungkin akan meluas hingga mencapai lingkup global. Untuk itulah mengapa *human security* sangat mendapatkan perhatian di era sekarang ini, bahkan menjadi prioritas utama PBB untuk memberantas segala bentuk ancaman *human security* yang ada (UNDP, 1994).

Ada tujuh komponen keamanan manusia (*human security*) menurut UNDP (2004) yang pemenuhannya wajib menjadi tanggung jawab pemerintah setiap negara. Ketujuh komponen tersebut adalah keamanan ekonomi (*economic security*), keamanan makanan (*food security*), keamanan kesehatan (*health security*), keamanan lingkungan (*environment security*), keamanan personal (*personal security*), keamanan komunitas (*community security*), dan keamanan politik (*political security*) (Elpeni Fitrah, 2005).

Beberapa kriteria yang terkait dengan keamanan ekonomi termasuk pendapatan dasar dan pekerjaan yang diasuransikan, dan akses ke jaring pengaman sosial tersebut. Keamanan makanan pada dasarnya hanya akses ke

nutrisi dasar dan pasokan makanan. Sementara keamanan Kesehatan memiliki masalah lebih kompleks karena mencakup banyak isu berbeda seperti akses ke air bersih, hidup di lingkungan yang aman, akses ke layanan kesehatan, akses ke keluarga berencana yang aman dan terjangkau dan dukungan dasar selama kehamilan dan persalinan, pencegahan HIV/AIDS dan penyakit lain. Keamanan lingkungan bersifat langsung dan mencakup isu-isu seperti pencegahan pencemaran air, pencegahan pencemaran udara, pencegahan penggundulan hutan, konservasi lahan irigasi, pencegahan bencana alam seperti kekeringan, banjir, angin topan, gempa bumi, dll. Keamanan komunitas di sisi lain mencakup konservasi tradisional dan budaya, bahasa dan nilai-nilai yang dianut secara umum. Hal ini juga mencakup penghapusan diskriminasi etnis, pencegahan konflik etnis, dan perlindungan masyarakat adat. Keamanan politik berkaitan dengan perlindungan hak asasi manusia dan kesejahteraan semua orang. Ini juga mencakup perlindungan terhadap orang-orang dari represi negara seperti kebebasan pers, kebebasan berbicara, dan kebebasan memilih. Penghapusan penahanan politik, pemenjaraan, perlakuan buruk sistematis, dan penghilangan juga tercakup dalam keamanan politik (Elpeni Fitrah, 2005). Tujuh komponen di atas bisa disimplifikasi menjadi dua komponen utama, yaitu *freedom from fear* (bebas dari rasa takut) dan *freedom from want* (bebas dari ketidakmampuan untuk memiliki) (Elpeni Fitrah, 2005).

ii. Cyber security

Cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. *Computer security* atau

keamanan komputer bertujuan membantu *user* agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi (Security et al., n.d.). *Cyber security* juga berarti teknologi, proses dan praktik yang dirancang untuk melindungi jaringan, komputer, program dan data dari serangan, kerusakan atau akses yang tidak sah. *Cyber security* juga disebut sebagai upaya untuk melindungi informasi dari adanya *cyber attack*. *Cyber attack* dalam operasi informasi adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi (Wilson & Kiy, 2014).

1. Ancaman yang ditimbulkan oleh penggunaan komputer jaringan sebagai media atau panggung untuk antisosial, organisasi yang mengganggu, atau berbahaya dan komunikasi. Ini termasuk, misalnya, situs web dari berbagai kelompok kebencian rasial dan etnis, situs yang mengoordinasikan perencanaan dan tindakan kejahatan (terutama penipuan), situs web dan mekanisme lain yang memberikan pornografi anak, dan mungkin yang paling mendesak pada saat itu penulisan makalah ini - penggunaan Internet untuk mendorong aksi teroris dan untuk operasional perencanaan serangan teroris (Cybersecurity, 2018).
2. Ancaman serangan terhadap infrastruktur sosial yang kritis, termasuk utilitas, perbankan, pemerintah administrasi, pendidikan, kesehatan, manufaktur dan media komunikasi. Di sini, itu Argumennya adalah karena sistem kritis semakin tergantung pada sistem informasi jaringan, mereka rentan terhadap serangan jaringan.' (Wilson & Kiy, 2014)

3. Ancaman terhadap sistem informasi jaringan sendiri mulai dari kecacatan berbagai macam dan derajat ke - dalam kasus terburuk – selesai kelemahan. Klaim utama dari artikel ini adalah bahwa dua konsep keamanan tampaknya mendorong upaya di komputer (dan jaringan) keamanan dan perbedaannya signifikan untuk regulasi dan desain. Sebuah perbedaan yang paling jelas terlihat adalah ruang lingkup: cybersecurity tumpang tindih dengan keamanan teknis tetapi mencakup lebih banyak. (Wilson & Kiy, 2014)

1.6 Argumen Penelitian

Argumen dari penelitian ini adalah Cambridge Analityca selaku konsultan strategi politik untuk partai republik Amerika Serikat melanggar privasi dengan mengambil data-data secara ilegal serta memanfaatkannya untuk mengubah pandangan masyarakat. Dalam hal ini, hal tersebut dapat mengancam kehidupan bermasyarakat serta negara.

1.7 Definisi Konseptual

1.7.1 Data Pribadi

Data pribadi adalah data kepemilikan atau identitas diri. Definisi lainnya data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebernaran serta dilindungi kerahasiaannya. Data pribadi dapat teridentifikasi melalui system elektronik maupun nonelektronik.

1.7.2 Pelanggaran Privasi

Pelanggaran Privasi merupakan bentuk penyalahgunaan akses data pribadi orang lain yang melawan hukum yang mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seizin yang bersangkutan.

1.8 Definisi Operasional

1.8.1 Data Pribadi

Data Pribadi yang dimaksud di penelitian ini adalah pengumpulan data secara tidak sadar atau ilegal yang dilakukan oleh Cambridge Analityca dan digunakan sebagai sarana untuk mengubah opini publik yang dapat mengancam keamanan negara.

1.8.2 Pelanggaran Privasi

Pelanggaran Privasi yang dimaksud pada penelitian ini ada pelanggaran yang dilakukan oleh Cambridge Analityca terhadap data-data yang diambil secara illegal.

1.9 Metodologi Penelitian

1.9.1 Tipe Penelitian

Tipe penelitian ini merupakan penelitian deskriptif dimana tipe penelitian deskriptif berguna untuk menggambarkan bagaiamana suatu fenomena terjadi. Tujuan dari penelitian ini adalah untuk menguji variabel-variabel yang akan diteliti sehingga gambaran yang akan diperoleh dari penelitian ini adalah gambaran dari hasil hubungan sebab-akibat.

1.9.2 Situs Penelitian

Penelitian dilakukan di perpustakaan kampus dan lingkungan sekitar peneliti.

1.9.3 Subjek Penelitian

Subjek penelitian merupakan individu dan organisasi terkait dalam penelitian yang dilakukan sebagai sumber informasi untuk pengumpulan data.

1.9.4 Jenis Data

Jenis data penelitian kualitatif yang diambil adalah data yang berupa: teks, kata-kata tertulis, frasa-frasa dan simbol-simbol, yang merepresentasikan atau menggambarkan individu-individu, tindakan-tindakan dan fenomena dalam kehidupan sosial.

1.9.5 Sumber Data

Sumber-sumber yang diambil merupakan data sekunder. Sumber data yang diambil merupakan repositori jurnal yang telah dicek kredibilitasnya seperti JSTOR, Science Direct, Scopus, dll. Sumber data lain yang dipakai diperoleh melalui internet seperti situs resmi pemerintah dan instansi, portal berita dengan publikasi resmi.

1.9.6 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini di antaranya melalui data sekunder. Data sekunder dalam penelitian ini di antaranya didapatkan melalui studi literatur dengan memanfaatkan berbagai buku maupun jurnal ilmiah yang akan menjelaskan fenomena yang ada serta mendukung data dalam penelitian ini. Selain itu juga peneliti akan melalui observasi terhadap media masa yang berhubungan dengan tema ini seperti pemberitaan di televisi, radio, internet dan beberapa media-media masa lainnya. Kajian Pustaka yang diambil untuk

data sekunder juga meliputi dokumen-dokumen yang terkait dan gambar yang diambil dari laman resmi terkait dengan tema pelanggaran privasi dan Cambridge Analityca

1.9.7 Teknik Analisis Data

Teknik analisa data dalam penelitian ini adalah menggunakan metode kualitatif. Metode kualitatif dalam penelitian akan menghasilkan data berupa kata- kata yang ditulis maupun lisan dari setiap aktor, selain itu penelitian kualitatif juga dapat berisi penjelasan mengenai perilaku yang dilakukan oleh setiap aktor (Moleong, 2007). Tujuan dari penelitian kualitatif sendiri adalah untuk menjelaskan hubungan kausalitas dengan menggambarkan dan menjelaskan (*to describe and explain*) (Moleong, 2007). Adapun dalam buku Metode Penelitian Kualitatif (Moleong, 2007) dijelaskan mengenai tahapan-tahapan analisa data menggunakan metode kualitatif, di antaranya diawali dengan menandai kata kunci yang ada di dalam data, kemudian mempelajari dan menemukan kata kunci yang ada dalam data, menuliskan model-model yang telah ditemukan dan yang terakhir adalah dengan melakukan koding data. Dalam penelitian ini variabel yang dipakai adalah a dan b, variabel a adalah pelanggaran privasi terhadap masyarakat dan variabel b ancaman terhadap masyarakat.

1.9.8 Kualitas Data

Pengesahan data peneltian kualitatif beraada pada halaman yang masuk akal berdasarkan kepercayaan atau kredibilitas terhadap suatu fenomena yang

terjadi. Kualitas penelitian ini akan dilihat dari kepercayaan hasil yang terkait (Moleong, 2007: 324).

a. Kredibilitas

Kredibilitas adalah bagaimana bahan dan hasil penelitian dapat dipercaya. Dilihat dari pengecekan metode dari informasi, sumber dan referensi untuk mengecek kebenaran. Untuk memenuhi standar kredibilitas data-data yang dimiliki telah dicek melalui sumber resmi yang terpercaya.

b. Keteralihan

Data-data yang didapatkan merupakan data yang dapat dialihkan secara konteks dan merupakan data yang setara dari dengan validasi yang resmi

c. Reliabilitas (kebergantungan)

Reliabilitas merupakan suatu penelitian yang apabila orang lain dapat mengulangi atau mereplikasi proses penelitian tersebut. Dalam penelitian ini uji reliabilitas dilakukan dengan cara melakukan audit terhadap keseluruhan proses penelitian. Caranya dilakukan oleh pembimbing untuk mengaudit keseluruhan aktivitas peneliti dalam melakukan penelitian.

1.9.9 Sistematika Penulisan

- Bab I berisi garis besar penelitian meliputi latar belakang masalah, rumusan masalah, tujuan penelitian, kerangka pemikiran, serta metodologi penelitian.
- Bab II membahas secara mendalam mengenai pelanggaran privasi serta keamanan siber pada kasus Cambridge Analityca.

- Bab III menganalisa pelanggaran privasi dapat menjadi ancaman bagi keamanan manusia
- Bab IV merupakan bagian kesimpulan yang berisi jawaban terhadap rumusan masalah.