BAB 2

PELANGGARAN PRIVASI DAN KEAMANAN SIBER PADA KASUS CAMBRIDGE ANALITYCA

2.1 Kasus Cambridge Analityca

Kasus Cambridge Analytica (CA) adalah yang pertama disebarkan pada tahun 2018 oleh salah satu mantan pekerja Cambridge Analityca yaitu Christopher Wylie. Wylie menyampaikan rahasia pertama mereka kepada 'TheGuardian', sebuah media di Inggris. Wylie mengatakan bahwa Cambridge Analityca menggunakan aplikasi '*thisisyourdigitallife*' di Facebook yang dikembangkan oleh Alexander Kogan, dan pengembang aplikasi juga disebut Dr.Spectre (The Guardian, 2018).

Cambridge Analytica adalah perusahaan yang menawarkan layanan kepada bisnis dan partai politik yang ingin "mengubah perilaku audiens" (The Guardian, 2018). mereka mengklaim dapat menganalisis data konsumen dalam jumlah besar dan menggabungkannya dengan ilmu perilaku untuk mengidentifikasi orang-orang yang dapat ditargetkan oleh organisasi dengan materi pemasaran. (The Guardian, 2018) Itu mengumpulkan data dari berbagai sumber, termasuk platform media sosial seperti Facebook, dan pollingnya sendiri (The Guardian, 2018).

Dengan kantor pusatnya di London, perusahaan ini didirikan pada tahun 2013 sebagai cabang dari perusahaan lain bernama SCL Group, yang menawarkan layanan serupa di seluruh dunia (The Guardian, 2018).

Perusahaan ini sebagian dimiliki oleh Robert Mercer, seorang miliarder teknologi dan pengelola investasi global (hedge fund) asal Amerika Serikat (Confessore, 2018). Mercer merupakan salah satu tokoh sayap kanan di Amerika

Serikat dan pendukung Donald Trump dalam kontestasi pemilu AS (Confessore, 2018).

Cambridge Analityca sendiri merupakan perusahaan konsultasi politik yang berasal dari Inggris, sebagai perusahaan yang memanfaatkan perkembangan teknologi saat ini, yaitu menggunakan big data (Wylie, 2019). Cambridge Analityca dapat memengaruhi keputusan para pemilih, menggiring opini, menyebarkan berita disinformasi dan lainnya. Cambridge Analityca adalah anak perusahaan dari Strategic Communication Laboratories (SCL) Group, yang telah berdiri dari tahun 1990 dan telah terlibat dalam perpolitikan di berbagai penjuru dunia (Wylie, 2019).

Kogan menawarkan aplikasi ini untuk Donald Trump sebagai strategi kampanye karena aplikasi asli Cambridge Analityca yang dibuat oleh Wylie dan teman-teman memiliki banyak bug dan tidak dikembangkan dengan benar, kata Ted Cruz, kepala kampanye Trump (The Guardian, 2018). Cambridge Analityca akhirnya setuju untuk memberikan kesempatan pada Kogan untuk mengembangkan aplikasi. Aplikasi ini dengan menganalisis psikologi pengguna Facebook dengan menghubungkan aplikasi dengan Facebook, lalu Cambridge Analityca bisa mendapatkan data pribadi pengguna facebook dan teman mereka. Setelah aplikasi ini digunakan untuk periode 3-5 bulan, Cambridge Analityca bisa mendapatkan sekitar lima juta data (The Guardian, 2018).

Studi yang dilakukan Kogan ini tidak biasa, baik dalam hal itu dilakukan oleh seorang akademisi universitas untuk perusahaan swasta yang dia operasikan, dan dalam hal data yang diteruskan ke pihak ketiga. Namun kesamaan di balik kontroversi ini, seperti peringatan studi bahwa orientasi seksual seseorang dapat ditentukan dari kehadiran online mereka (Wylie, 2019). Data digunakan dengan

cara yang jauh melampaui apa yang diharapkan atau dimaksudkan oleh pengguna. Data dirangkum yang ditentukan oleh algoritme maka titik data yang tidak berbahaya dapat mengungkapkan informasi yang mungkin diharapkan pengguna untuk tetap pribadi dan yang mungkin digunakan dengan cara yang tidak mereka sukai (Wylie, 2019).

Wylie, seorang pakar analisis data dari Kanada yang bekerja di Cambridge Analytica dengan Alexander Kogan untuk merancang dan mengimplementasikan skema tersebut, memberikan bukti tentang penyalahgunaan data kepada The Observer yang menimbulkan pertanyaan tentang kesaksian mereka (Cadwalladr, 2018). Dia telah menyerahkannya ke unit kejahatan dunia maya Badan Kejahatan Nasional dan Kantor Komisi Informasi. Ini termasuk email, faktur, berkas, dan nota yang mengungkapkan kemungkinan lebih dari 50 juta pengguna itu adalah milik pemilih pemilu Amerika Serikat yang diambil dari situs tersebut masuk dalam salah satu pelanggaran data Facebook terbesar yang pernah ada. Facebook mengatakan bahwa mereka juga menangguhkan Wylie dari mengakses platform saat melakukan penyelidikan, meskipun perannya sebagai pelapor. Wylie, pakar data Kanada yang bekerja dengan Cambridge Analytica dan Kogan untuk merancang dan mengimplementasikan skema tersebut, menunjukkan bukti tentang analisis data kepada The Observer yang memperkuat pertanyaan tentang membuktikan mereka(Cadwalladr, 2018). Dia telah menyerahkan data-datanya ke unit kejahatan siber Badan Kejahatan Nasional dan Kantor Komisi Informasi. Ini termasuk email, faktur, kontrak, dan bank transfer yang mengungkapkan lebih dari 50 juta profil dan sebagian besar milik pemilih yang tercatat AS, diambil dari situs tersebut dalam satu pelanggaran data Facebook terbesar yang pernah ada.

Cambridge Analityca berhasil menemukan cara untuk memanfaatkan data pribadi orang yang diungkapkan melalui aktivitas orang di Facebook sehubungan dengan data yang dibeli dari agen kredit, pialang data, dan sumber lainnya untuk membuat profil psikologis dengan cara yang akan mengungkapkan jenis pesan politik yang pengguna mungkin terima. “Facebook,” seperti yang Wylie katakan “bukan lagi sekadar perusahaan. Ini adalah pintu masuk ke benak orang-orang Amerika dan Mark Zuckerberg membiarkan pintu itu terbuka untuk Cambridge Analytica, Rusia, dan orang lainnya.”(Wylie, 2019).

Ide tentang "likes" dari Facebook yang dapat membuka jendela ke dalam jiwa orang tidak berasal dari Cambridge Analityca, tetapi dalam penelitian yang dilakukan di Universitas Cambridge. Wylie memahami bahwa pentingnya penelitian ini dan dia memiliki keterampilan pemrograman untuk membangun alat yang terukur untuk menyimpulkan dari ciri-ciri psikologis data pemilih yang kemudian dapat dieksploitasi untuk tujuan politik (Wylie, 2019).

Survei dan quiz yang mengumpulkan informasi dari teman-teman Facebook dari peserta dan mengakumulasi kumpulan data yang berjumlah kira-kira 50 juta (Wylie, 2019). Kebijakan dari Facebook hanya mengizinkan pengumpulan data teman untuk meningkatkan pengalaman pengguna di aplikasi dan tidak diperbolehkan untuk komersil (Lapaire, 2018). Penemuan yang belum pernah terjadi sebelumnya pengumpulan data, dan penggunaannya, menimbulkan pertanyaan baru yang mendesak tentang peran Facebook dalam menargetkan pemilih dalam pemilihan presiden AS. Informasi ini datang hanya beberapa minggu setelah dakwaan 13 orang Rusia oleh penasihat khusus Robert Mueller

yang menyatakan mereka telah menggunakan platform tersebut untuk melakukan "perang informasi" melawan AS (Heawood, 2018).

2.2 Pelanggaran Privasi Terhadap Masyarakat

Pelanggaran privasi merupakan sebuah pelanggaran yang mana melanggar jati diri manusia itu tersendiri karena bisa terjadi manipulasi terhadap orang tersebut sehingga hal seperti ini tidak hanya akan mengancam seseorang namun seluruh masyarakat di dunia. Pada era ini, masyarakat terancam privasinya dengan gaya hidup setiap hari. Dengan munculnya internet, *smartphone*, media sosial, dan lain-lain. Semua orang dapat mengetahui apa yang dilakukan setiap orang seperti momen ulang tahun, pernikahan, atau hanya sekedar bermain bersama teman. Aksesibilitas ini memang memudahkan setiap orang untuk berhubungan antar sesama namun juga membuat setiap orang rentan terhadap kriminalitas yang mungkin muncul akibat kemudahan ini.

Kondisi masyarakat pada era ini dikatakan sebagai masyarakat modern karena sekarang teknologi berbasis informasi. Dengan semakin cepat perkembangan teknologi internet dan informasi, semakin banyak juga informasi atau data pribadi yang bersifat sensitif terkumpul dan tersimpan (Landon-Murray, 2016). Fenomena seperti ini, dikenal dengan istilah era big data (Landon-Murray, 2016).

Privasi memiliki perkembangan yang panjang dalam sepanjang sejarah; umurnya sama dengan umur manusia. Namun, apa yang dianggap pribadi berbeda menurut zaman, masyarakat dan individu. Juga apa yang dianggap pribadi dan apa yang secara hukum dilindungi sebagai pribadi dapat berbeda. Maka dari itu kepentingan ini muncul dalam penciptaan gagasan privasi modern, yang pertama

kali muncul di studi bernama (*The Right to Privacy*) yang ditulis oleh Louis Brandeis dan Samuel Warren, makalah ini mendefinisikan bahwa hak privasi sebagai "hak untuk tidak dicampur tangani". Sejak itu, hak atas privasi telah dikenal dan diakui secara luas, mulai berkembang dan menjadi hak asasi manusia dalam masyarakat barat (Lukacs, 2017).

Privasi memastikan hak individu atas kebebasan berbicara dan berekspresi, yang dilindungi dari penganiayaan ras/agama/politik/seksual, disediakan hak atas kebebasan dan pilihan untuk berbagi atau menyembunyikan informasi pribadi dari orang lain. Privasi adalah keadaan tidak diawasi atau diganggu tanpa pengetahuan dan persetujuan orang lain. Hak privasi memastikan masyarakat bebas dari pengawasan negara, bebas untuk memiliki milik diri sendiri memiliki pemikiran dan pandangan unik, bebas dari sikap adil, bebas dari pembuatan profil dan pembuatan katalog pada berbagai karakter, bebas protes, bebas memilih, bebas berpikir, bebas dibiarkan sendiri dan lain sebagainya.

Dalam memahami Privasi, Solove mengurutkan konsepsi privasi menjadi empat kelompok besar yaitu: terutama selaras dengan pertanyaan yan berkaitan dengan privasi informasi: pengumpulan informasi, informasi pemrosesan, penyebaran informasi, dan invasi. Taksonominya mengalihkan fokus jauh dari tema isolasi yang mapan dan control terhadap privasi sebagai konstruk yang bergantung secara kontekstual (Solove, 2017). Melakukannya mengaburkan definisi privasi; itu membuatnya tidak perlu memperdebatkan apakah itu positif atau negatif secara universal konsep. Seperti cahaya dalam prisma, privasi dibagi menjadi serangkaian sinar, masing-masing berbeda tetapi serupa kualitas. Jadi, meskipun masalah privasi terkait dengan pengumpulan dan pemrosesan informasi, berbagi banyak

sifat, termasuk minat inti dalam data pribadi, Etika masing-masing dapat diidentifikasi tanpa membatasi karakteristik yang lain.

Pada saat yang sama, masing-masing dari empat kategori Solove dapat menjadi dibagi lebih lanjut. Pemrosesan informasi, misalnya, berisi isu-isu terpisah dari agregasi, identifikasi, ketidakamanan, penggunaan sekunder, dan pengecualian. Proyek ini secara terpusat berkaitan dengan agregasi dan penggunaan sekunder. Melalui taksonomi Solove, kemudian, ini dapat dieksplorasi sebagai privasi kekhawatiran yang terkait dengan tetapi berbeda dari identifikasi, ketidakamanan, dan pengecualian.

Konsepsi privasi ini, yang mengidentifikasi hak atas privasi sebagai hak untuk kontekstual aliran informasi yang tepat, menarik pendekatan kontekstual Solove secara jelas ke dalam ranah data digital, menyempurnakan lebih jauh perbedaan di antara berbagai jenis masalah privasi. Utilitas dalam mengeksplorasi dimensi etis pengumpulan dan penggunaan data membuatnya sangat cocok untuk studi ini dan, sebagai hasilnya, definisi Nissenbaum tentang privasi sebagai integritas kontekstual diadopsi dalam studi kasus setelah tinjauan literatur ini (Hansen & Nissenbaum, 2009)

Solove dan Nissenbaum berbeda dalam sejauh mana pendekatan yang bergantung pada konteks ini untuk perlindungan privasi. Meskipun Solove mengakui bahwa mekanisme pasar gagal melindungi pengguna web individu karena ketidakseimbangan kekuatan akibat massa informasi yang dimiliki oleh penyedia layanan, menurutnya tidak mungkin untuk mengendalikan pengumpulan(Solove,2017) . Determinisme sangat cocok dengan ideologi penyedia/pengumpul konten web, yang mengklaim bahwa keduan praktik

pengumpulan dan penggunaan mereka secara inheren progresif dan sebagian besar positif (Healey & Woods,2017).

Pada masa kini, keprihatinan terhadap hal ini telah diungkapkan karena kebijakan dan praktik yang mengeksploitasi kerentanan teknologi komunikasi digital terhadap pengawasan dan intersepsi elektronik di negara-negara di seluruh dunia telah terungkap (United Nations, 2014). Contoh pengawasan digital yang terbuka dan terselubung di yurisdiksi di seluruh dunia telah berkembang biak, dengan pengawasan massal pemerintah muncul sebagai kebiasaan yang berbahaya dan bukan tindakan yang luar biasa. Pemerintah dilaporkan mengancam akan melarang layanan perusahaan peralatan telekomunikasi dan nirkabel kecuali diberi akses langsung ke lalu lintas komunikasi, kabel serat optik yang disadap untuk tujuan pengawasan, dan mewajibkan perusahaan secara sistematis untuk mengungkapkan informasi massal tentang pelanggan dan karyawan (United Nations, 2014).

Perlindungan data sekarang lebih relevan dari sebelumnya sampai saat ini, Perlindungan data tampaknya menjadi topik khusus, dipertimbangkan hanya oleh sekelompok kecil ahli. Namun, selama setahun terakhir, dengan munculnya penerapan GDPR dan serangkaian skandal terkemuka terkait pengumpulan dan penggunaan data pribadi, khususnya yang berkaitan dengan penggunaan data pribadi pada kampanye pemilu membuat relevansi perlindungan data bagi masyarakat luas terlihat jelas fokus (Hallinan et al., 2019).

Kasus Cambridge Analityca, jika dibiarkan secara hukum, itu akan merugikan pengguna media sosial atau netizen dalam mengungkapkan pendapatnya secara bebas di internet atau di media sosial. Orang akan cenderung takut ketika

mereka ingin mengekspresikan opini di media sosial (Masruroh & Satria, 2018). Ketakutan ini tidak berdasar karena mereka takut data mereka akan digunakan oleh orang-orang tertentu pihak untuk kepentingan mereka. Berdasarkan kasus Cambridge Analityca, data hanya digunakan oleh pihak-pihak tertentu. Tetapi jika data mereka digunakan untuk pengembangan sebagai demi negara, maka itu baik karena tujuan politik dunia maya (Masruroh & Satria, 2018).

Namun, jika dilihat melalui pandangan hak asasi manusia hal ini justru melanggar karena privasi manusia merupakan bagian dari kebebasan itu tersendiri. Ketika masyarakat tidak mempunyai perlindungan privasi maka tidak hanya kehidupannya sendiri yang terancam namun kehidupan orang lain. Negara selaku pelindung masyarakatnya seharusnya menjaga privasi mayarakat dengan baik, karena hal ini akan mengeskpos masyarakatnya maka secara langsung negara pun terancam. Menurut laporan Office of the United Nations High Commissioner for Human Rights (OHCHR), perlindungan pada data pribadi diperlukan dan harus diterapkan, akibat efek dari kemajuan teknologi dan informasi maka perlindungan data pribadi juga berhubungan dengan perlindungan hak asasi manusia (Council, 2021).

Amerika Serikat memiliki aturan tentang privasi yang disebut dengan Undang-Undang Privasi tahun 1974. Undang-Undang Privasi tahun 1974 yang mengatur penanganan informasi pribadi di pemerintah federal. Diberlakukan setelah skandal Watergate dan Program Kontra Intelijen (COINTELPRO) yang melibatkan pengawasan ilegal terhadap partai politik oposisi dan individu yang dianggap "subvfsolersif", Undang-Undang Privasi berupaya memulihkan kepercayaan pada pemerintah dan menangani apa yang pada saat itu dipandang

sebagai ancaman eksistensial terhadap demokrasi Amerika (Winn, 2020). Namun Amerika Serikat belum mempunyai undang-undang tentang perlindungan data pada tingkat federal seperti halnya GDPR di Uni Eropa. Amerika masih dalam tahap proses untuk membuat peraturan perlindungan data. Rancangan undang-undang S.3300 yang merupakan Undang-Undang Perlindungan Data tahun 2020 ini menjelaskan tentang menetapkannya dalam cabang eksekutif sebuah Badan Perlindungan Data (DPA) yang independen untuk mengatur pemrosesan data pribadi (SENATE OF THE UNITED STATES, 2020).

Pada tahun 2021 diproposalkan juga rancangan undang-undang H.R.8152 - Undang-Undang Privasi dan Perlindungan Data Amerika. RUU ini menetapkan persyaratan tentang bagaimana perusahaan, termasuk organisasi nirlaba dan operator umum, menangani data pribadi, yang mencakup informasi yang mengidentifikasi atau secara wajar dapat ditautkan ke seseorang(SENATE OF THE UNITED STATES, 2022). Secara khusus, undang-undang tersebut mengharuskan sebagian besar perusahaan untuk membatasi pengumpulan, pemrosesan, dan transfer data pribadi yang secara wajar diperlukan untuk menyediakan produk atau layanan yang diminta dan untuk keadaan tertentu lainnya. Kedua undang-undang ini jika ditetapkan oleh pemerintah Amerika Serikat dapat membantu agar tidak terjadinya kejadian Cambridge Analityca terjadi lagi, namun kedua RUU ini tidak lanjut untuk diproses.

2.3 Keamanan Siber dan Ancamannya

Keamanan Siber atau *Cyber security* merupakan sebuah konsep yang muncul setelah perang dingin atas respon dari pencampuran inovasi teknologi dan perubahan kondisi geopolitik. ‘Keamanan siber’ pertama kali digunakan oleh

ilmuwan di awal 1990-an untuk menjelaskan serangkaian ancaman yang terkait dengan jaringan komputer yang bergerak melampaui konsep teknis keamanan komputer, pendukung konsep ini menganggap bahwa ancaman yang timbul dari teknologi digital dapat memiliki efek sosial yang menghancurkan (Hansen & Nissenbaum, 2009).

Keamanan siber merupakan komponen penting dalam era inovasi teknologi. Dengan semakin banyaknya orang yang menggunakan internet dan sistem informasi yang terhubung dengan jaringan, risiko keamanan siber semakin meningkat. Keamanan siber dapat didefinisikan sebagai tindakan untuk melindungi sistem jaringan, informasi, dan data yang disimpan di dalamnya dari serangan atau penyusupan yang tidak sah. Keamanan siber tidak hanya melibatkan teknologi, tetapi juga mencakup proses, standar, dan praktik yang dapat membantu menjamin bahwa sistem jaringan dan informasi tetap aman dari ancaman yang ada.

Komputer dan jaringan internet yang tidak terlindungi dengan baik dapat menjadi sasaran bagi para pelaku kejahatan siber seperti hacker dan penipu. Mereka dapat mencuri data pribadi, melakukan pencurian uang, atau bahkan mengganggu operasional suatu perusahaan. Kejahatan siber dapat mengakibatkan kerugian yang besar, serta merusak reputasi suatu organisasi. Oleh karena itu, penting bagi setiap pengguna internet untuk menjaga keamanan siber mereka sendiri. Dengan berbagai cara yang dapat dilakukan, seperti menggunakan password yang kuat, mengaktifkan fitur keamanan pada perangkat yang digunakan, dan selalu waspada terhadap aktivitas yang mencurigakan di internet.

Ada beberapa cara untuk menjaga keamanan siber, antara lain dengan menggunakan software keamanan yang terupdate, membuat sandi yang kuat, dan

melakukan backup data secara rutin. Selain itu, penting juga untuk selalu waspada terhadap tindakan yang tidak sah seperti phishing dan malware. Selain itu, pemerintah juga harus turut serta dalam menjaga keamanan siber. Hal ini dapat dilakukan dengan cara menerapkan peraturan yang ketat terkait dengan keamanan siber, serta memberikan edukasi kepada masyarakat tentang pentingnya keamanan siber. Secara umum, keamanan siber adalah bagian penting untuk menjamin keberlangsungan bisnis serta aktivitas individu dan organisasi di dunia maya. Dengan menjaga keamanan siber, masyarakat dapat terhindar dari ancaman. Maka keamanan siber harus menjadi prioritas utama bagi setiap individu dan organisasi. Keamanan siber merupakan salah satu hal yang sangat penting dalam dunia teknologi saat ini. Dengan semakin tingginya tingkat kebutuhan akan teknologi, maka tentunya keamanan siber juga menjadi hal yang sangat diperhatikan.

Pertama, keamanan siber sangat penting untuk menjaga privasi data pribadi. Dengan banyaknya akses ke internet, maka data-data pribadi masyarakat bisa mudah tersebar dan disalahgunakan. Keamanan siber diperlukan untuk menjaga privasi agar tidak dimanfaatkan untuk kejahatan. Kedua, keamanan siber juga sangat penting untuk menjaga stabilitas sistem teknologi. Dengan adanya serangan siber, maka sistem teknologi yang individu gunakan bisa saja terganggu dan menyebabkan kerusakan. Oleh karena itu, keamanan siber diperlukan untuk menjaga stabilitas sistem teknologi agar tidak terganggu oleh serangan siber. Ketiga, keamanan siber juga sangat penting untuk menjaga keamanan negara. Dengan semakin tingginya penggunaan teknologi, maka negara juga bisa saja menjadi sasaran serangan siber.

Oleh karena itu, keamanan siber diperlukan untuk menjaga keamanan negara agar tidak terganggu oleh serangan siber. Dengan demikian, keamanan siber merupakan hal yang penting dalam perkembangan teknologi. Oleh karena itu, masyarakat harus terus memperhatikan dan meningkatkan keamanan siber agar dapat menjaga privasi data pribadi, stabilitas sistem teknologi, serta keamanan negara. Kesadaran akan pentingnya keamanan siber harus ditanamkan sejak dini kepada semua pengguna internet, baik individu maupun organisasi. Dengan demikian, semua orang dapat terhindar dari ancaman kejahatan siber dan menggunakan internet secara aman dan nyaman.