

Data Rights di Era Surveillance Capitalism. Skandal Data Cambridge Analytica & Facebook dalam Pemilihan Presiden Amerika Serikat 2016

Maya Indah Bofa
Arfin Sudirman

Wawan Budi Darmawan

Mayabofa137@gmail.com

Program Magister Hubungan Internasional, Universitas Padjadjaran
Bandung, Indonesia

Abstract

In 2018, several major British media outlets published the result of a joint investigation which revealed that Cambridge Analytica, a political consulting and data analysis firm, collected about 87 million personal data of Facebook users which was then used without the knowledge of the data owner. This study aims to understand analyze the abuse of data rights involving Cambridge Analytica and Facebook in the 2016 US presidential election. The research method used in this study is descriptive qualitative method. This study found that Cambridge Analytica used personal data of Facebook users for Donald Trump's digital campaign in the 2016 US presidential election. The data include complete profiles such as name, gender, age, location, status updates, likes, friends, and even personal messages which are then translated into behavioral data. The data collected and analyzed by Cambridge Analytica then became the power in modifying behavior, especially voting behavior. Behavior modification by Cambridge Analytica was possible because the knowledge asymmetry in the use of data.

Keywords: *data rights, surveillance capitalism, behavioral modification, microtargeting*

Abstrak

Pada 2018, beberapa media besar Inggris mempublikasikan hasil investigasi bersama yang mengungkap bahwa Cambridge Analytica, sebuah perusahaan konsultan politik dan analisis data, mengoleksi sekitar 87 juta data pribadi pengguna Facebook yang kemudian digunakann tanpa sepengetahuan pemilik data. Penelitian ini bertujuan untuk memahami dan menganalisis penyalahgunaan *data rights* yang melibatkan Cambridge Analytica dan Facebook dalam pemilihan presiden Amerika Serikat 2016. Adapun metode yang digunakan dalam penelitian ini adalah kualitatif deskriptif. Penelitian ini menemukan bahwa Cambridge Analytica menggunakan data pribadi pengguna Facebook untuk kepentingan kampanye digital Donald Trump pada pemilihan presiden Amerika Serikat 2016. Data yang diambil meliputi profil lengkap seperti nama, jenis kelamin, usia, lokasi, pembaruan status, *likes*, teman, bahkan pesan pribadi yang kemudian diterjemahkan menjadi *behavioral data*. Data yang dikumpulkan dan dianalisis oleh Cambridge Analytica kemudian menjadi *power* dalam *behavioral modification*, khususnya *voting behavior*. Modifikasi tingkah laku oleh Cambridge Analytica dapat dilakukan sebab adanya *knowledge asymmetry* dalam penggunaan data.

Kata kunci: *data rights, surveillance capitalism, behavioral modification, microtargeting*

1. PENDAHULUAN

Pada konvensi partai Juli 2016, Demokrat dan Republikan secara resmi menominasikan kandidat presiden dari masing-masing partai yakni Hillary Clinton dan Donald Trump. Terdapat banyak kontroversi yang muncul dari sisi Donald Trump. Salah satunya adalah kampanye Trump yang menggambarkan imigran Meksiko sebagai pemerkosa dan penjahat. Pencalonannya sebagai presiden Amerika Serikat (AS) kerap memicu kegemparan (BBC, 2016). Namun pada 8 November 2016, Donald Trump terpilih

sebagai Presiden AS ke-45. Trump memenangkan *swing states* seperti Florida dan Ohio, bahkan Pennsylvania yang merupakan negara bagian yang sering dimenangkan oleh kandidat dari Demokrat. Trump juga memenangkan Wisconsin, negara bagian yang diprediksi dapat dimenangkan oleh Hillary Clinton (Hirschhorn, 2016). Dengan kampanyenya yang penuh kontroversi, kemenangan Trump merupakan hal yang tidak terduga.

Dua tahun kemudian, yakni 2018, beberapa media besar Inggris seperti *The Guardian* dan *Channel 4*, mempublikasikan hasil investigasi bersama. Melalui publikasi tersebut terkuak bahwa Cambridge Analytica (CA), sebuah perusahaan konsultan politik & analisis data yang berbasis di London, menjadi simbol global dari sisi gelap *big data* (Witt & Pasternack, 2019). Perusahaan tersebut terungkap mengoleksi sekitar 87 juta data pribadi pengguna Facebook yang kemudian disalahgunakan tanpa persetujuan pihak-pihak terkait (Goldhill, 2019). CA diketahui bekerja untuk kampanye Donald Trump dengan mengumpulkan data pengguna para pemilih AS, dan menggunakannya untuk membangun *software* untuk memprediksi dan mempengaruhi pilihan di kotak suara (Cadwalladr & Harrison, 2018). CA mengatakan bahwa mereka memiliki 5.000 *data points* pada setiap pemilih di AS. Dengan menggunakan analisis *psychographics* terhadap kumpulan data yang ada, CA mengklaim dapat menentukan tipe kepribadian tiap individu dan kemudian mengirim pesan atau iklan untuk mempengaruhi perilaku mereka (Westby, 2019). Dalam dokumen resmi CA, perusahaan tersebut mengklaim telah menyediakan keahlian dan intelijen yang membantu kampanye Trump (Cambridge Analytica, 2020).

Akses terhadap data dan pengaruh politik yang dimiliki oleh perusahaan teknologi menuai protes dan keluhan dari pengguna terkait pelanggaran privasi dan perlindungan data, serta keterlibatan dalam elektoral dan kegiatan politik lainnya (Atal, 2021). Diskusi mengenai CA berfokus pada dampaknya terhadap perlindungan privasi dan data pribadi. Setelah skandal data CA terkuak dan CA terbukti terlibat dalam pilpres AS, masyarakat internasional mendesak adanya tindakan terkait *data rights*. Selain itu, terdapat seruan terhadap perusahaan teknologi, terutama Facebook, untuk meregulasi penggunaan data pribadi pengguna (Humble, 2021).

Adapun alasan yang berkenaan dengan pemilihan pemilu AS 2016 sebagai masalah dalam penelitian ini yaitu melalui terungkapnya kasus ini, pelanggaran *data rights* yang dilakukan oleh CA menjadi isu global. Sebab setelah diselidiki, terungkap bahwa sebelum bekerja untuk kampanye Trump, CA melakukan eksperimen dengan terlibat dalam pemilu di berbagai negara seperti Trinidad & Tobago, Nigeria, hingga kampanye Brexit. Hal ini sebab pendiri CA adalah konglomerat AS yaitu Steve Bannon dan Robert Mercer yang memiliki tujuan untuk menjadikan Trump pemenang pada pemilihan presiden AS 2016. Oleh sebab itu, CA menjadikan pemilu di negara-negara lain sebagai *testing ground* sebelum akhirnya bekerja untuk proyek utama mereka yaitu kampanye Trump dalam pemilihan presiden AS 2016.

Terdapat beberapa studi terdahulu mengenai CA, *surveillance capitalism* dan *data rights* yang peneliti anggap relevan dalam penelitian ini. Adapun penelitian tentang CA yang menjadi isu politik global telah diteliti oleh Gordon (2019) dan Boldyreva et al., (2018). Kemudian penelitian mengenai *data rights* sebagai bagian dari *human rights* di era digital (Harris & Wyndham, 2015; Humble, 2021). Selanjutnya penelitian mengenai *surveillance capitalism* yang memungkinkan perusahaan-perusahaan teknologi untuk memiliki *political power* dan *power consolidation* (Atal, 2021; Langworthy, 2019; LeBaron et al., 2020).

Adapun perbedaan antara penelitian ini dengan beberapa penelitian di atas adalah fokus kajian dan teori. Dalam jurnal *Review of International Political Economy*, *surveillance capitalism* merupakan salah satu '*blind spot*' dalam Ekonomi Politik Internasional, oleh karena itu patut dikaji lebih lanjut. Melalui skandal data yang melibatkan CA dan Facebook dalam pemilihan presiden AS tahun 2016, penelitian ini berfokus pada *data rights* yang merupakan bagian dari *human rights* yang harus mendapat perhatian lebih di era digital seiring meningkatnya praktik *surveillance capitalism* yang menurut (Zuboff, 2019) merupakan '*economic logic in action*'.

Pengumpulan serta kemampuan utilisasi data yang dimiliki oleh perusahaan teknologi menimbulkan masalah terkait pelanggaran privasi dan perlindungan data, serta keterlibatan dalam elektoral dan kegiatan politik lainnya. Dengan demikian, berdasarkan latar belakang penelitian di atas, maka rumusan masalah dalam penelitian ini adalah: Bagaimana skandal data yang melibatkan CA dan Facebook dalam pemilihan presiden AS 2016 melanggar *data rights*?

2. KERANGKA ANALISIS

Meningkatnya kegunaan data juga memunculkan model bisnis baru yang disebut Zuboff (2019) *surveillance capitalism*. Karakteristik utama dari *surveillance capitalism* adalah data pribadi digunakan oleh perusahaan berbasis teknologi sebagai *main resource* tidak hanya untuk kepentingan ekonomi, namun juga politik. Tujuan penggunaan data adalah modifikasi tingkah laku (*behavioral modification*) tanpa sepengetahuan pemilik data sebab adanya *power* atau pengetahuan yang bersifat asimetris antara *surveillance capitalist* dan pengguna internet sebagai pemilik data. Dengan kata lain, *surveillance capitalist* dapat mengetahui segala sesuatu tentang pengguna internet sebagai pemilik data, sedangkan pengguna tidak mengetahui apapun mengenai *surveillance capitalist* dan apa yang mereka lakukan terhadap data pengguna. Dalam penelitian ini *surveillance capitalist* merujuk kepada kepada CA dan Facebook sebagai perusahaan teknologi yang mengeksploitasi data. *Surveillance capitalism* oleh Zuboff akan digunakan untuk melihat bagaimana CA dalam konteks pemilu AS 2016 mengreorientasi metode-metode yang ada di dalam *surveillance capitalism* di bidang politik.

Selanjutnya, kemampuan perusahaan teknologi dalam mengumpulkan dan mengeksploitasi data pribadi pengguna meningkatkan kemungkinan terjadinya pelanggaran *human rights*. Sebab data merepresentasikan '*a new system and a new right*' (Lang, 2019) maka *data rights* merupakan bagian dari *human rights* di era digital. Objek dari *data rights* adalah kumpulan data yang merupakan kombinasi, integrasi, dan agregasi data yang memiliki pola dan nilai tertentu (Lang, 20019). Dalam penelitian ini, data pengguna Facebook yang digunakan oleh CA merupakan objek dari *data rights*, sedangkan pengguna yang memiliki data tersebut adalah subjek dari *data rights*. Sebab data pribadi memiliki nilai ekonomi dan politik, maka *data rights* mencakup perlindungan yang diberikan terkait data. Dengan demikian, pemilik data sebagai subjek dari *data rights* memiliki hak untuk mengajukan klaim serta mengetahui aktivitas terkait data pribadi mereka (Lang, 2019). Konsep *data rights* akan digunakan untuk menjelaskan bagaimana CA dan Facebook melanggar *data rights* pada pemilu AS 2016. Serta mengkaji perkembangan terkait *data rights protection* setelah skandal data CA dan Facebook, terutama di tingkat global.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif dengan pendekatan deskriptif. Artinya peneliti menganalisis dan menjabarkan data terkait masalah yang diteliti yaitu penyalahgunaan *data rights* oleh CA dan Facebook pada pemilihan presiden AS 2016 secara deskriptif. Dalam penelitian ini, data didapat dari hasil wawancara dan studi literatur. Peneliti melakukan wawancara dengan David Carroll sebagai aktivis *data rights* dan Eduard Blasi yang merupakan *data protection lawyer*. Sedangkan literatur yang peneliti gunakan antara lain dokumen internal CA dan buku yang dirilis mantan data scientist CA yaitu Christopher Wylie. Selain itu, peneliti juga menggunakan sumber dari beberapa artikel jurnal serta situs web yang peneliti anggap kredibel. Adapun teknik analisis data terlebih dahulu dilakukan dengan mengoleksi data yang berkaitan dengan skandal data yang melibatkan CA dan Facebook dalam pemilu AS 2016. Kemudian peneliti melakukan reduksi data dengan memilih, merangkum serta memfokuskan hal-hal yang penting dan relevan. Selanjutnya data disajikan dengan teks naratif agar semakin

mudah dipahami. Setelah itu, peneliti menganalisa dan mengaplikasikan konsep *data rights* dan *surveillance capitalism* terhadap data yang ada. Terakhir, peneliti menarik kesimpulan dari data-data yang telah dianalisa.

4. HASIL DAN PEMBAHASAN

A. Keterlibatan *Cambridge Analytica* pada Pemilihan Presiden AS 2016

Cambridge Analytica adalah perusahaan konsultan politik yang berbasis di London dan merupakan anak perusahaan dari *Strategic Communication Laboratories (SCL) Group* yang telah berdiri sejak 1990. SCL merupakan perusahaan intelijen yang bergerak di bidang operasi militer melalui *psychological operations (psy-ops)* dan *influence* (Wylie, 2019). CA didirikan oleh Alexander Nix, Robert Mercer dan Steve Bannon pada 2013 (Hilder, 2019). Mercer yang memberikan investasi sebesar \$15 juta untuk mendirikan CA merupakan CEO dari perusahaan *hedge fund Renaissance* dan salah satu donor terbesar untuk Trump (Osborne, 2018). Sedangkan Bannon adalah salah satu pendiri *Breitbart News* yang diklaim sebagai platform untuk kelompok *alt-right* (Posner, 2016) yang kemudian menjadi juru kampanye Donald Trump pada Agustus 2016 (CLC, 2020). Selama masa pemilu 2016, Bannon masih merupakan salah satu pemegang saham di CA (CLC, 2020).

Dikutip dari dokumen internal perusahaan (CA, 2020) “*CA Political brings specialist data modeling, 25 years of experience at the forefront of behavioral change and cutting edge technological capabilities together in one innovative team.*” Dengan keahlian tersebut, CA menawarkan jasa *audience targeting* kepada partai politik yang ingin mengubah perilaku audiens (Osborne, 2018). Dalam operasinya, metode utama yang digunakan oleh CA yaitu *behavioral microtargeting*. Metodologi ini diklaim telah terbukti sebagai bagian penting dalam membantu tim kampanye untuk memahami *voters turn out* dan pilihan yang mereka buat pada hari pemilihan (Cambridge Analytica, 2020).

CA dikenal luas karena satu *influence campaign* yaitu membantu Donald Trump dalam pemilihan presiden AS 2016. Dalam dokumen internal perusahaan, CA menuliskan bahwa mereka menyediakan keahlian dan intelijen yang membantu Trump memenangkan Gedung Putih. Dengan mengidentifikasi audiens kunci dan menargetkan pemilih dengan pesan yang tepat di waktu yang tepat CA mengklaim dapat mengubah keyakinan dan perilaku pemilih untuk mendapatkan suara mereka (Cambridge Analytica, 2020). CA memanfaatkan *data science* dan keahlian analisis prediktifnya untuk membangun lebih dari 20 model khusus selama kampanye Trump. Model-model ini kemudian digunakan untuk mengidentifikasi isu-isu kebijakan, preferensi kandidat, kecenderungan pemilih dan kemungkinan pemilih untuk memilih lebih awal atau tidak menggunakan hak suaranya (Cambridge Analytica, 2020).

CA melakukan pemodelan data, penargetan dan penayangan iklan digital, pembuatan daftar dan polling untuk proyek kampanye seperti *Make America Number One* dan *Defeat Crooked Hillary* selama pemilihan presiden 2016 (Cambridge Analytica, 2020). Upaya utama dari operasi CA adalah untuk menghasilkan *Principal Audience (PA)*, yaitu kelompok pemilih yang dimodelkan paling mungkin dipersuasi oleh (Cambridge Analytica, 2020). Setelah menentukan PA, langkah selanjutnya adalah menentukan pesan atau iklan apa yang akan dikirim (Cambridge Analytica, 2020). Pada Maret 2018, *The Guardian*, *The New York Times*, dan *Channel 4 News* secara bersamaan menerbitkan hasil investigasi bersama untuk mengungkap kebenaran tentang apa yang terjadi di dalam CA dan Facebook (Wylie, 2019). Kemudian Juni 2018, Christopher Wylie bersaksi kepada Kongres AS tentang CA sebagai direktur riset perusahaan tersebut. Wylie membawa bukti terkait data Facebook yang dijadikan senjata oleh perusahaan tersebut. Perusahaan tersebut mengeksploitasi Facebook untuk mengakses lebih dari 87 juta akun pribadi dan menggunakan data tersebut salah satunya untuk menekan pemilih Afrika-Amerika (Wylie, 2019). Adapun kumpulan data tersebut meliputi profil lengkap dari puluhan ribu pengguna seperti nama, jenis kelamin, usia, lokasi, pembaruan status, *likes*, teman, bahkan pesan pribadi (Wylie, 2019).

Dari data yang dikumpulkan CA dapat mengidentifikasi orang-orang yang menunjukkan neurotisme dan mereka yang lebih rentan terhadap kemarahan impulsif atau konspirasi. CA kemudian menargetkan mereka, menyebarkan narasi melalui grup Facebook, iklan, atau artikel yang diketahui dari pengujian internal perusahaan cenderung memicu amarah dan membuat mereka terlibat (Wylie, 2019). CA dapat melakukan itu dengan fitur spesifik dari algoritma Facebook di mana algoritma situs akan mulai menyarankan cerita dan halaman serupa untuk meningkatkan *engagement*. Selanjutnya, CA mengembangkan halaman palsu di Facebook dan platform lain yang terlihat seperti forum sungguhan. CA melakukan ini di tingkat lokal dengan membuat halaman *alt-right* dengan nama palsu seperti *Smith Country Patriots* atau *I love My Country*. Dengan algoritma rekomendasi Facebook, halaman-halaman ini akan muncul di beranda orang-orang yang menyukai konten serupa.

Kemudian, setelah orang-orang bergabung dengan grup palsu tersebut, CA akan memposting video dan artikel yang memicu emosi dan amarah (Wylie, 2019). Selain grup palsu dan iklan digital, *trolling* dan *cyberbullying* juga menjadi alat utama untuk memanipulasi kelompok *alt-right*. Bannon mengubah CA menjadi alat untuk intimidasi otomatis dan kekerasan psikologis berskala besar salah satunya dengan menyebarkan konten tentang persaingan rasial di AS (Wylie, 2019). Gambar di bawah menggambarkan bagaimana ketika *behavioral psychology*, *big data* dan *targeted engagement* dikombinasikan untuk mengubah tingkah laku target.

Gambar 1. Cambridge Analytica's Sales Presentation



Sumber: (Netflix UK & Ireland, 2019)

Kampanye iklan digital *Defeat Crooked Hillary* diklaim CA sangat sukses dalam menjangkau dan membujuk pemilih yang masih ragu. Secara keseluruhan, iklan tersebut dilihat sebanyak 21.718.189 kali dan lebih dari 1.433.331 pengguna mengunjungi *defatcrookedhillary.com* dan *2016truths.com*. Iklan tersebut paling sukses di Facebook dan Google Search (Cambridge Analytica, 2020). Video berjudul '*Can't Run Her House*' juga diklaim sangat efektif dalam membujuk wanita di kelompok PA untuk tidak memilih Hillary Clinton. Setelah melakukan *Ad Recall* and *Impact Survey*, CA menemukan bahwa iklan tersebut efektif khususnya di negara bagian Florida dengan meningkatkan niat untuk memilih Donald Trump lebih dari 8 persen. (Cambridge Analytica, 2020) Video ini diperlihatkan kepada subset PA yang memandang keamanan nasional sebagai salah satu dari tiga isu terpenting bagi mereka (Cambridge Analytica, 2020). Selain menyebarkan iklan di media sosial, CA juga mendesain dan mengelola tiga situs web antara lain, *Defeat Crooked Hillary*, *2016 Truths*, dan *Save the Supreme Court* (Cambridge Analytica, 2020).

CA juga menjalankan dua kampanye dengan berbagai jenis subjek email. Subjek email dikembangkan secara khusus untuk orang-orang dengan skor neurotisme yang tinggi. Dengan kata lain, email dirancang untuk meyakinkan orang-orang yang biasanya memiliki kecenderungan untuk khawatir (Cambridge Analytica, 2020). Beberapa diantaranya dirancang untuk meyakinkan misalnya '*Calm the storm, stop Hillary*'. Adapula yang dirancang untuk memunculkan ketakutan seperti '*Electing Hillary destroys our nation*' (Cambridge Analytica, 2020). Menurut CA, subjek email yang berbasis ketakutan menunjukkan hasil

terbaik sebab 10% lebih banyak dibuka daripada email yang berisi pesan umum, dan tingkat *open rate* hampir 20% lebih besar daripada subjek email yang dirancang untuk meyakinkan (Cambridge Analytica, 2020).

Platform media sosial memiliki kapasitas untuk memantau dan memanipulasi apa yang dapat dan tidak dapat dilihat atau dialami secara online, dengan tujuan membuat pengguna tetap berada di situs mereka selama mungkin. Dengan membajak perhatian, mengumpulkan data pribadi, menjual akses ke data pengguna, perusahaan dapat menargetkan pengguna dengan iklan click-bait dan konten viral yang terkadang memiliki konsekuensi yang tidak diinginkan. Adapun konsekuensi tersebut seperti membuat pengguna rentan terhadap aktor yang menyebarkan disinformasi serta lingkungan online yang memicu kemarahan seperti yang dilakukan CA. Hal ini akan dibahas lebih lanjut pada sub-bab selanjutnya yaitu data yang menjadi *power* dalam *behavioral modification*, khususnya *voting behavior*.

B. Data sebagai *Power* dalam *Behavioral Modification*

Dominasi digital dan eksploitasi data pengguna oleh perusahaan merupakan kekuatan struktural hegemonik yang membentuk kapitalisme di era digital (Fuchs, 2019). Para *surveillance capitalist* tidak puas hanya dengan mengetahui perilaku pengguna, mereka juga ingin membentuknya. Seperti yang dituliskan Zuboff (2019) “*the purpose is not to simply “automate information flows about us” but to “automate us”*”. Kapasitas untuk membentuk perilaku pengguna untuk kepentingan perusahaan atau pihak lain memunculkan apa yang disebut Zuboff (2019) sebagai *instrumentarianism* atau *instrumentarian power*. Bentuk *power* ini muncul di perusahaan, bukan negara.

Zuboff (2019) menggambarkan *instrumentarian power* sebagai “*the whole digital surround that is now the instrumented medium that is producing the knowledge that creates the opportunity for the power to modify your behavior*”. Dengan kata lain, instrumentasi tersebut ada di sekitar kita termasuk perangkat-perangkat digital yang terkoneksi internet. Hal ini dirancang agar semua aktivitas individu dapat dipantau, diukur, dan dimodifikasi. *Instrumentarian power* memungkinkan *surveillance capitalist* untuk melakukan mobilisasi dalam skala besar. Dengan demikian, *social influence* relatif mudah untuk dilakukan di platform media sosial. Kemudian yang terjadi adalah para *data scientist* yang dilatih untuk menguasai “*digital nudge*” untuk kepentingan perusahaan (Whitehead, 2019). Hal tersebut menjadi dasar dalam *behavioral modification* dalam skala besar dan merupakan *power* untuk memanipulasi perilaku untuk kepentingan politik, sosial, dan ekonomi. Terlebih, eksperimen online oleh *surveillance capitalist* dapat dilakukan tanpa sepengetahuan atau persetujuan orang-orang yang diawasi (Whitehead, 2019).

Dalam bukunya Wylie (2019) menceritakan bagaimana CA mengetahui segala informasi pribadi tentang seorang perempuan di Nebraska, mulai dari foto, nomor telepon, anak, tempat kerja, alamat rumah, riwayat *voting*, bahkan mobil yang ia kendarai. Informasi tersebut juga diperbarui secara *real-time*. CA memiliki data tentang berapa gaji yang orang tersebut hasilkan, apakah ia memiliki senjata. CA juga memiliki foto satelit rumahnya yang diperoleh dengan mudah dari Google Earth. CA tidak hanya memiliki semua data Facebooknya tetapi juga menggabungkannya dengan semua data komersial yang mereka beli. *Instrumentarian power* yang dimiliki CA tercermin sebagaimana yang diakui Wylie (2019) “*we had re-created her life in our computer and she had no idea*”.

Data Facebook merupakan salah satu sumber pengayaan dan penggunaan data yang paling terkenal seperti analisis kluster dan *deep learning* untuk mengetahui pola pengguna sebagai sumber wawasan tentang perilaku dan preferensi pengguna (Benchman, 2019). Adapun perbedaan antara data yang diperoleh dari survei dan data media sosial seperti Facebook adalah pengguna membuat lebih banyak *data points* tentang diri mereka di media sosial (Benchmann, 2019). Hal tersebut sebab data Facebook berisi *data points* yang beragam seperti minat (*likes* dan *shares*), akun dan opini pribadi (pembaruan status, foto, tautan, dan komentar), serta *behavioral data* (kunjungan ke situs lain dengan *plugin*

Facebook). Oleh karena itu, data Facebook dapat diakses dan digunakan untuk berbagai tujuan seperti pengoptimalan layanan, pengawasan sistematis, hingga kampanye politik (Benchmann, 2019) seperti yang dilakukan CA yang telah dibahas pada sub-bab sebelumnya.

Data pribadi berperan sebagai infrastruktur informasi granular yang kuat dan dapat meningkatkan efektivitas pesan kampanye untuk menjangkau orang-orang atau kelompok orang yang tidak dapat dijangkau dengan metode kampanye konvensional (Laterza, 2021). Keunggulan data yang terdapat di media sosial adalah jejak informasi pribadi terperinci, dan tidak membutuhkan pengamatan yang cermat selama berbulan-bulan untuk dikumpulkan. Dengan banyaknya data, psikolog dapat mempercepat penilaian tentang disposisi tiap pengguna (Wylie, 2019). Hal ini kemudian mendorong penelitian mengenai *psychological profiling* yang dapat diotomatisasi dengan algoritma *machine learning*. Algoritma ini memungkinkan CA untuk memperluas jangkauan mereka melalui otomatisasi dengan ketepatan *targeted message* (Wylie, 2019).

Dengan data pribadi, CA dapat mengukur atau menyimpulkan ciri-ciri tertentu pada individu (Wylie, 2019). Seperti halnya *hacking* yang bertujuan untuk menemukan titik lemah dalam suatu sistem dan kemudian mengeksploitasi kerentanan itu, CA mencoba meretas pikiran dengan mengidentifikasi bias kognitif yang terdapat pada individu dan kemudian mengeksploitasinya (Wylie, 2019). Intinya adalah dengan data yang ada, CA dapat mencari tahu bagian mana dari informasi penting yang harus dikumpulkan untuk mempengaruhi perasaan seseorang, apa yang dia yakini, dan bagaimana dia berperilaku (Wylie, 2019).

Selanjutnya, terdapat keuntungan melalui komodifikasi data yaitu dengan menampilkan konten yang sesuai dengan preferensi pengguna (Benchman, 2019). Maka dari itu, salah satu strategi bisnis Facebook adalah menyajikan postingan kontroversial yang memicu banyak reaksi emoji sebab cenderung membuat pengguna lebih aktif. *Data scientist* yang bekerja di Facebook juga mengkonfirmasi bahwa postingan yang memicu emoji reaksi marah cenderung menyertakan informasi yang salah, toksisitas, dan berita berkualitas rendah (Merrill & Oremus, 2021). Ini artinya Facebook secara sistematis membiarkan dan menyebarkan postingan tersebut di platformnya demi meningkatkan *engagement*. Hal ini memunculkan kekhawatiran bahwa platform seperti Facebook mempengaruhi pemilihan dengan mengarahkan pengguna ke konten yang selaras dengan satu sudut pandang politik dan menekan sudut pandang yang lain (Eipstein & Robertson, 2015).

Terkait hal ini, setelah terpilihnya Donald Trump sebagai presiden AS pada tahun 2016, komentator media menuduh Facebook mempengaruhi pemilihan terhadap Trump dengan membiarkan penyebaran berita palsu, yang membuat tuduhan tidak berdasar terhadap Hillary Clinton dan tersebar luas di platform (York & Zuckerman, 2019). Pada tahun 2016, berita palsu yang sebagian besar pro-Trump tersebar di Facebook. Hal tersebut membuat Trump menghasilkan lebih banyak *engagement* Facebook daripada Clinton (Bakir & McStay, 2018). Meskipun berita palsu, baik untuk kepentingan ekonomi atau politik, telah ada sejak lama, namun ekologi media digital dengan model bisnis *surveillance capitalism* semakin mengintensifikan skala berita palsu. Algoritma Facebook menghasilkan *echo chamber* atau *filter bubble*, dan secara selektif mengukur informasi apa yang ingin dilihat pengguna berdasarkan data pribadi pengguna yang telah dikumpulkan dan dianalisis. Hal ini menyebabkan pengguna menjadi terpisah dari paparan informasi yang lebih luas atau yang berbeda dengan pandangan mereka. Dan hal tersebut mungkin terjadi tanpa orang-orang menyadari prosesnya. Oleh karena itu, Facebook menjadi platform yang sesuai bagi CA untuk menjalankan operasinya dan maraknya berita palsu saat pemilu AS 2016.

Jika dalam kapitalisme industri *power* diidentifikasi dengan kepemilikan *the means of production*, di bawah *surveillance capitalism*, *power* diidentifikasi dengan kepemilikan *the means of behavioral modification*. Dalam kasus ini dapat dilihat bahwa CA merupakan pihak yang memiliki kapasitas untuk melakukan *behavioral modification*. CA melakukan

segmentasi terhadap *target audience* berdasarkan atribut psikografis, menggunakan riset ilmiah yang canggih dan metodologi analisis sosial untuk memahami, mengukur, dan mempengaruhi perilaku pemilih (Cambridge Analytica, 2020). Dalam dokumen internalnya, CA mengklaim “*by identifying look-a-like voters, we can effectively target prospective supporters*”.

Pada hari ketiga debat antara Trump dan Clinton, CA menguji 175.000 variasi iklan yang berbeda untuk argumennya melalui Facebook untuk menemukan versi yang paling tepat. Pesan-pesan itu sebagian besar berbeda hanya dalam detail mikroskopis, untuk menargetkan penerima secara psikologis: judul yang berbeda, warna, keterangan, dengan foto atau video. Ketidakkonsistenan Trump yang mencolok dan banyak dikritik, serta rangkaian pesan yang kontradiktif, kemudian menjadi aset besarnya yaitu pesan yang berbeda untuk setiap pemilih (Graesseger & Krogerus, 2017). Hal itu sebab di balik kampanye Trump terdapat praktik *microtargeting* yang muncul di mana algoritma *machine learning* menyerap data pemilih dalam jumlah besar untuk membagi pemilih menjadi segmen-segmen sempit dan memprediksi individu mana yang merupakan target terbaik untuk dibujuk dalam pemilihan (Wylie, 2019). Tidak hanya itu, menurut Brittany Kaiser “*rather than engaging in blanket political advertising to persuade voters, “to get people to act, you created the conditions under which they would be more likely to do what you wanted them to do”* (Bakir, 2020). Hal ini menunjukkan upaya *behavioral modification* yang dilakukan oleh CA untuk kampanye digital Trump.

Fokus utama dari kampanye digital yang dilakukan CA adalah menargetkan sekitar 9 juta pemilih, khususnya di New Hampshire, Pennsylvania, Virginia, North Carolina, Florida, Ohio, Iowa, Colorado, Nevada, dan Michigan, yang merupakan *swing states* yaitu negara bagian di mana suara tidak dapat diprediksi akan dimenangkan oleh Republik atau Demokrat. Dokumen internal CA juga menunjukkan bahwa sebagian besar pemilih yang ditargetkan oleh kampanye digital CA termasuk pemilih Clinton yang dapat dibujuk untuk tidak memilih Clinton atau memilih Trump. Selain itu, pemilih Partai Republik juga menjadi sasaran dalam kampanye ‘*get out the vote*’ yang bertujuan untuk meningkatkan peluang mereka untuk berpartisipasi dalam pemilu (Cambridge Analytica, 2020)). Dengan sistem *electoral college*, CA hanya perlu mempengaruhi perilaku pemilih sebagian kecil masyarakat. Trump memenangkan pemilu berkat 80.000 pemilih di Michigan, Pennsylvania, Wisconsin, meskipun ia tertinggal di belakang Clinton dengan hampir 3 juta suara dalam penghitungan nasional (Laterza, 2021). Dua dari tiga negara bagian tersebut yaitu Michigan dan Pennsylvania merupakan target utama CA.

Wylie dalam Zuboff (2019) menyatakan “*we exploited Facebook to harvest millions of people’s profiles, and built models to exploit what we know about them and target their inner demons.*” Kasus CA memperlihatkan bahwa ilmu pengetahuan yang berorientasi pada pengembangan *behavioral technology* (lihat *daftar istilah*) yang dilakukan oleh perusahaan cenderung melihat manusia sebagai subjek yang dapat dimanipulasi daripada agen rasional (Shaw, 2018). Sebagaimana yang dituliskan Kosinski, Stillwell, Nave, dan Matz (2017) di dalam artikel mereka “*psychological mass persuasion could be abused to manipulate people to behave in ways that are neither in their best interest nor in the best interest of society*”.

Dari penjelasan di atas dapat dilihat bagaimana data menjadi *power* dalam *behavioral modification* khususnya *voting behavior* dalam pemilu AS 2016. Metode yang dilakukan CA untuk tujuan *behavioral modification* memperlakukan pengguna sebagai sarana untuk mencapai tujuan perusahaan. Dari segi ekonomi, pengumpulan data untuk kampanye Trump di Facebook sangat menguntungkan Facebook sebab ekonomi sosial media didasarkan oleh *engagement* pengguna di platform tersebut. Kemudian dari segi politik, reorientasi *instrumentarianism* dalam kampanye politik memungkinkan perusahaan teknologi seperti CA dan Facebook untuk mengontrol informasi apa saja yang bisa dilihat oleh pengguna, tanpa sepengetahuan pengguna.

C. *Knowledge Asymmetry* dalam Penggunaan Data

Perusahaan teknologi menghasilkan uang dari kemampuan mereka untuk memetakan dan mengatur informasi. Inti dari model bisnis ini adalah *knowledge asymmetry* di mana perusahaan tahu banyak tentang perilaku pengguna, tetapi pengguna hanya tahu sedikit tentang mereka (Wylie, 2019). *Behavioral modification* yang dilakukan CA dapat terjadi sebab adanya distribusi *power* atau pengetahuan yang asimetris. Asimetri ini dibentuk melalui monopoli *data science*, dominasi *machine intelligence*, pasar prediksi yang menguntungkan, kemampuan mereka untuk membentuk perilaku pengguna, serta kepemilikan dan kendali mereka atas saluran pengguna untuk partisipasi sosial (Naughton, 2019).

Knowledge asymmetry ini berpihak kepada *surveillance capitalist* yaitu CA dan Facebook sebagai aktor yang memiliki akses dan kemampuan untuk memaknai data (West, 2019). Di sisi lain, pengguna tidak memiliki kendali formal atas proses ini seperti akses atau kontrol atas data mereka yang telah diambil dan dimanfaatkan oleh perusahaan. Sebab data pengguna telah menjadi komoditas, maka artinya, terdapat insentif ekonomi untuk menciptakan informasi asimetris yang substansial antara perusahaan dan pengguna. Agar dapat mengubah perilaku pengguna menjadi keuntungan, perusahaan perlu mengetahui segalanya tentang perilaku penggunanya, sementara pengguna tidak mengetahui apapun tentang apa yang dilakukan orang-orang yang mengoperasikan platform. Oleh karena itu, CA menilai asimetri ini merupakan lingkungan yang sempurna untuk melakukan kampanye digital dalam pemilihan presiden AS 2016.

Knowledge asymmetry dalam penggunaan data memungkinkan CA untuk melakukan *profiling* tanpa sepengetahuan pemilik data. Sementara teknik kampanye pada umumnya bertujuan untuk membujuk pemilih dengan memberikan informasi, kampanye CA dilakukan dengan memanfaatkan *knowledge asymmetry* dalam penggunaan data. Kampanye digital CA membatasi informasi dan memuaskan target dengan konten yang sesuai dengan ideologi mereka. Publik tidak dapat melihat proses yang dilakukan CA untuk membuat profil dan memberi mereka informasi sesuai dengan profil psikologis yang telah dibuat CA (Ward, 2018). Dengan kata lain, konten kampanye digital CA yang berdasarkan *microtargeting* membatasi akses terhadap informasi terkait pemilu. Selain itu, pengguna bahkan tidak menyadari bahwa pesan kampanye yang mereka terima telah disetel secara psikologis dan memainkan prasangka ideologis mereka. Hasilnya, *behavioral microtargeting* menghambat kemampuan pengguna untuk mengetahui bagaimana mereka dimanipulasi dan dihadapkan pada konten yang dirancang dengan cara yang tidak dapat mereka pahami (Ward, 2018).

Kapasitas penyimpanan komputasi modern yang terus meningkat membuat tersedianya akumulasi data dalam jumlah besar berada di tangan beberapa perusahaan. Teknologi data yang semakin berkembang saat ini digunakan untuk membangun dan mempercepat pertumbuhan asimetri antara orang yang menggunakan teknologi dan mereka yang mengeskplotasinya. Penggunaan kecerdasan buatan dan informasi juga membuka kemungkinan asimetris yang luas untuk mengurangi potensi perlawanan dari target (Wylie, 2019). Setelah skandal Cambridge Analytica pada Maret 2018, Facebook mengumumkan bahwa pengguna dapat mengunduh data pribadi mereka. Namun data tersebut sebagian besar terdiri dari informasi yang disediakan oleh pengguna sendiri, termasuk informasi yang telah mereka hapus: teman, foto, video, iklan yang telah diklik, coleskan, posting, lokasi, dan sebagainya. Data tersebut tidak termasuk *behavioral surplus*, prediksi, dan informasi terkait data yang diperjual belikan atau digunakan untuk *behavioral modification*. Dengan kata lain, seperti yang dituliskan (Zuboff, 2019) “*When you download your personal information, you access the stage, not the backstage*”. Hal ini menunjukkan contoh lain dari *knowledge asymmetry* dalam skandal data ini.

CA dapat beroperasi dengan lancar selama bertahun-tahun sebab tidak ada yang mencegahnya (Wylie, 2019). Seperti yang dikatakan Lazerta (2021) ada dua hal yang

menjadikan AS sebagai tempat bermain yang ideal untuk operasi CA yaitu penetrasi internet dan media sosial yang sangat tinggi sehingga menghasilkan data pribadi dalam jumlah besar dan tidak adanya mekanisme regulasi yang melindungi pengambilan data pribadi oleh perusahaan swasta. Hal ini kemudian memungkinkan perusahaan seperti CA untuk melakukan apa yang mereka inginkan dengan tersedianya sejumlah besar data pribadi (Laterza, 2021).

Metode kampanye CA dilakukan dengan eksploitasi data tanpa sepengetahuan pengguna yang menjadi target. Mereka tidak mengetahui bahwa mereka telah dimanipulasi untuk tujuan pihak lain yaitu perusahaan dan politisi yang secara aktif mendukung infrastruktur *surveillance capitalism*. *Knowledge asymmetry* dalam penggunaan data juga menyebabkan ketidakseimbangan *power* dan kontrol antara perusahaan sebagai pihak yang mengumpulkan dan mengolah data dengan pengguna sebagai pemilik asli dari data. Sehingga, dalam kasus ini pihak yang paling diuntungkan adalah pihak yang memiliki kendali atas data pribadi. Terlebih, operasi yang dilakukan CA tidak hanya dalam pemilu AS, namun juga dalam pemilu di beberapa negara seperti yang telah dibahas pada bab sebelumnya. Jika praktik tersebut tidak diawasi, hal ini akan berdampak terhadap jalannya demokrasi di dunia. Oleh karena itu, perlu adanya sistem hukum untuk melindungi hak pengguna sebagai subjek data rights yang utama. Hal ini akan dibahas pada sub-bab selanjutnya.

D. Kerangka Kerja Internasional Terkait Perlindungan Data

Privasi data merupakan hak yang dijamin dalam *United Nations International Bill of Human Rights*, sebagaimana tercantum dalam *International Covenant on Civil and Political Rights* (ICCPR) (Lathrop, 2019). Dalam Pasal 17 GC No. 16-10 ICCPR dituliskan “*the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law*” (UN Human Rights Committee, 1988). Melalui ICCPR, badan HAM PBB menyimpulkan bahwa untuk menghormati hak atas privasi, pemerintah harus mengatur bagaimana perusahaan swasta memperlakukan data pribadi (Human Rights Watch, 2021). Meskipun perjanjian-perjanjian terkait HAM seperti ICCPR hanya berlaku bagi negara, namun terdapat *Guiding Principle on Business & Human Rights* yang berisi norma bahwa pelaku bisnis harus menghormati HAM (UNHCHR, 2011). UNHCHR juga secara khusus menyerukan perusahaan berbasis web untuk memperhatikan HAM dalam praktik bisnis mereka.

Dalam *The Right to Privacy in the Digital Age*, UNHCHR membahas tentang perlindungan hak atas privasi dalam konteks *surveillance* dan/atau penyadapan komunikasi digital serta pengumpulan data pribadi, termasuk dalam skala besar (Human Rights Council, 2014). Resolusi 68/167 terkait hak atas privasi di era digital memperhatikan bahwa lajunya perkembangan teknologi memungkinkan individu di seluruh dunia untuk menggunakan teknologi informasi dan komunikasi. Pada saat yang sama hal tersebut meningkatkan kapasitas pemerintah dan perusahaan untuk melakukan pengawasan, penyadapan, dan pengumpulan data, yang dapat melanggar atau menyalahgunakan hak asasi manusia, khususnya hak atas privasi (UN, 2014). Kemudian resolusi tersebut menekankan bahwa pengawasan dan/atau penyadapan komunikasi yang melanggar hukum atau sewenang-wenang, serta pengumpulan data pribadi yang melanggar hukum atau sewenang-wenang dianggap sebagai tindakan yang sangat mengganggu, melanggar hak atas privasi dan kebebasan berekspresi dan dapat bertentangan dengan prinsip masyarakat demokratis (UN, 2014).

Selanjutnya, resolusi 68/167 terkait hak atas privasi di era digital tersebut secara khusus meminta semua negara untuk mengambil langkah-langkah untuk mengakhiri pelanggaran hak-hak tersebut dan untuk menciptakan kondisi yang dapat mencegah pelanggaran tersebut. Hal ini termasuk dengan memastikan adanya undang-undang nasional yang relevan sesuai dengan kewajiban mereka di bawah hukum hak asasi manusia internasional (UN, 2014). Negara-negara juga diminta untuk meninjau prosedur, praktik dan

undang-undang mengenai pengawasan komunikasi, penyadapan dan pengumpulan data pribadi, termasuk pengawasan massal, dengan maksud untuk menegakkan hak atas privasi secara penuh dan efektif di bawah hukum hak asasi manusia internasional (UN, 2014).

Meningkatnya perhatian terhadap privasi di tingkat internasional tercermin dalam *UN Special Rapporteur on the Right to Privacy* pada tahun 2015. Pada bulan Maret 2016, Joe Cannataci, dalam posisinya sebagai pemegang mandat menyerukan peningkatan perhatian terhadap pengumpulan dan penggunaan data pribadi oleh perusahaan (Jorgensen, 2019:177). Dikutip dari OHCHR (2021), hal ini bertujuan antara lain untuk mempromosikan dan melindungi hak atas privasi dengan meninjau kebijakan dan undang-undang pemerintah terkait penyadapan komunikasi digital dan pengumpulan data pribadi. Mengidentifikasi tindakan yang mengganggu privasi tanpa justifikasi yang meyakinkan. Membantu pemerintah dalam untuk membawa pengawasan global di bawah supremasi hukum. Mengartikulasikan tanggung jawab sektor swasta untuk menghormati hak asasi manusia. Serta membantu memastikan prosedur dan hukum nasional konsisten dengan kewajiban hak asasi manusia internasional.

Seiring semakin banyaknya kegiatan sosial dan ekonomi yang dilakukan secara online, pentingnya privasi dan perlindungan data juga semakin diakui. Adapun yang menjadi perhatian yaitu pengumpulan, penggunaan, dan pembagian informasi pribadi kepada pihak ketiga tanpa pemberitahuan atau persetujuan individu yang memiliki data. Menurut laporan (UNCTAD, 2021) 128 dari 194 negara telah memberlakukan undang-undang untuk mengamankan perlindungan data dan privasi.

E. Analisis *Data Rights* dalam Skandal Data Cambridge Analytica dan Facebook

Michelle Bachelet (2019) *UN High Commissioner for Human Rights* (UNHCHR) dalam "*Human rights in the digital age*" menyatakan bahwa "*focusing on human rights in the digital age is key*". Seiring terus meningkatnya baik jumlah maupun kegunaan data, maka data pribadi rentan akan penyalahgunaan atau digunakan tanpa persetujuan pemilik data. Sisi gelap *big data* tidak hanya mengancam privasi dan keamanan, tetapi juga merusak pemilihan umum yang bebas dan adil, membahayakan kebebasan berekspresi, informasi, berpikir dan berkeyakinan, serta mengubur kebenaran dengan berita palsu. Sehingga hal ini bukan hanya sebagai masalah privasi, tetapi juga berkaitan dengan pengambilan dan penyalahgunaan data secara besar-besaran, dan manipulasi pemilih dalam pemilihan umum (Bachelet, 2019) seperti yang dilakukan CA pada pemilihan presiden AS 2016.

Semua yang dilakukan di dunia maya meninggalkan jejak digital yang dapat mengungkapkan secara detail keyakinan politik atau agama, gerakan, teman, kontak, dan aktivitas tiap pengguna. Oleh karena itu, di sosial media individu direpresentasikan melalui data mereka dan terhubung serta diproses melalui algoritma (Benchmann, 2019). Jadi, dari sudut pandang algoritmik atau *developer*, data tidak dapat diperlakukan sebagai sesuatu yang bukan manusia, sebab data memang merupakan bagian integral dari manusia (Benchmann, 2019). Dengan kata lain, penyalahgunaan data pribadi seperti yang dilakukan CA terhadap data pengguna Facebook termasuk pelanggaran terhadap *data rights* yang merupakan bagian hak asasi manusia di era digital.

Skandal data CA adalah contoh di mana data pengguna Facebook yang memiliki unsur kepribadian digunakan untuk melatih model guna menemukan perilaku dan atribut pengguna Facebook yang paling prediktif. Seperti yang telah dituliskan sebelumnya, data pengguna Facebook digunakan untuk membuat profil psikologis tertentu yang memungkinkan CA untuk menargetkan pemilih dengan konten yang disetel secara psikologis dan ideologis. Skandal data yang melibatkan CA dan Facebook menunjukkan bagaimana data pribadi digunakan tanpa persetujuan untuk kepentingan politik.

Hak atas data terdiri dari sejumlah hak yang berkaitan dengan data, seperti hak untuk memiliki, mengumpulkan, menyimpan dan memanfaatkan data, hak atas privasi data, dan

hak untuk mendapatkan informasi terkait data (Lang, 2019). Pada prakteknya, individu berperan sebagai produsen utama dan sumber data. Ketika data dikumpulkan, diproses, dan dianalisis oleh pihak lain, individu tidak lagi menjadi satu-satunya kontributor, pemroses, atau pengontrol data tersebut. Dengan kata lain, individu hanyalah penyedia data. Tanpa layanan jaringan dan dukungan teknis yang disediakan oleh pengumpul data, data tidak dapat dihasilkan dan tidak ada informasi penting yang terkandung dalam data (Lang, 2019). Skandal data yang melibatkan CA dan Facebook menunjukkan hambatan signifikan yang dihadapi pengguna dalam menuntut hak-hak atas data pribadi mereka. Korban hanya dapat mengajukan klaim jika mereka tahu hak-hak mereka telah dipertaruhkan. Pada skandal data ini, Facebook dilaporkan telah mengetahui situasi pada tahun 2015 dan mengklaim bahwa mereka mencari jaminan dari CA bahwa data penggunaannya telah dihapus. Namun, pengguna hanya diberi tahu setelah jurnalis investigasi mengungkapkan skandal data ini bertahun-tahun kemudian yaitu pada 2018 (LeCocq, 2018).

Terkait subjek *data rights*, Prof Carroll menjawab pertanyaan yang peneliti ajukan terkait hak-hak legal yang dimiliki oleh subjek *data rights* dengan mengatakan bahwa hal ini sangat bervariasi tergantung di mana data diproses dan disimpan dan/atau tempat tinggal subjek data. Saat individu tinggal di negara bagian atau negara dengan *data access rights*, seperti negara anggota Uni Eropa, atau negara bagian AS seperti California, institusi tertentu berkewajiban untuk menanggapi permintaan formal secara hukum. Hal ini juga berarti ketika data seseorang diproses dalam negara yang memberikan perlindungan data, maka subjek diberikan hak dari jarak jauh.

Prof Carroll selanjutnya memberi contoh dalam kasus CA, perusahaan induknya yakni SCL Elections Ltd adalah pengontrol data yang terdaftar untuk CA US, dan melakukan pemrosesan di Inggris untuk pemilihan presiden 2016. Oleh karena itu, mereka berkewajiban untuk menanggapi permintaan data Prof Carroll, dan regulator mereka, *Information Commissioners Office*, harus menanggapi keluhan Prof Carroll dan melakukan tuntutan sesuai dengan peraturan yang berlaku. Dengan demikian menurut Prof Carroll wajar jika penduduk Uni Eropa dan California lebih memiliki hak atas data daripada penduduk di tempat lain. Perusahaan yang berbasis di Eropa dan California juga memiliki lebih banyak kewajiban perlindungan data daripada yang lain. Hal ini diamini oleh Eduard Blasi yang mengatakan bahwa semua perusahaan yang berlokasi di Uni Eropa atau yang berada di luar Uni Eropa tetapi memproses data dari Eropa harus memberikan hak subjek data yang terdapat dalam GDPR meliputi hak atas akses, pembetulan, penghapusan (termasuk hak untuk dilupakan), oposisi serta pembatasan pemrosesan dan portabilitas data. Selanjutnya, terkait skandal data CA, Prof Carroll mengungkapkan:

"I was not impressed with the UK ICO's ability to fulfill a complete disclosure to enforce that basic right. In the end, it was a leaker to journalists (Channel 4 News) that revealed the true 2016 Trump database and not the ICO's seizure of the Cambridge Analytica servers under criminal warrant in the spring of 2018. Beyond that, there are so many other ways that the law is generally deferential to business and hostile to the individual or community. For example, CA/SCL was able to use insolvency/bankruptcy law to essentially "get away with it."

Ketika peneliti mengajukan pertanyaan terkait apakah terdapat perubahan tentang regulasi *data rights* setelah terungkapnya skandal CA, Prof Carroll memberikan tanggapan bahwa skandal CA mempercepat pengesahan undang-undang perlindungan data di berbagai tempat. Di AS, negara bagian California melalui undang-undang *California Privacy Rights Act* (CPRA) menekan industri agar menerima konsesi yang serius. Negara-negara lain juga telah meloloskan dan memperkuat undang-undang perlindungan data mereka setelahnya, termasuk Brasil, India, dan Cina. Berdasarkan kasus CA, menurut Prof Carroll *"...passing data protection laws is one thing, but enforcing them is another. Regulators do not really have the tools and authorities they need to enforce the laws on the books"*.

Kemudian ketika ditanya bagaimana seharusnya negara-negara membuat perusahaan besar seperti CA dan Facebook bertanggung jawab atas pelanggaran *data rights*, menurut Prof Carroll regulator membutuhkan lebih banyak alat, seperti penguraian algoritma, di mana mereka dapat memaksa perusahaan untuk tidak hanya menghapus data yang tidak sah, tetapi juga algoritma dan model data yang berasal dari data ilegal. Sedangkan menurut Eduard Blasi, *data protection lawyer* yang berbasis di Barcelona, otoritas Perlindungan Data menunjuk otoritas terkemuka di Uni Eropa yang bertanggung jawab untuk melaksanakan prosedur untuk perusahaan besar. Selain itu, sejak berlakunya GDPR denda telah meningkat pesat di Eropa dapat mencapai hingga 4% dari omset global suatu perusahaan.

Akibat keterlibatan dalam skandal data CA, Facebook dikenakan denda sebesar 5 miliar dolar AS. Dilansir dari situs resmi *US Federal State Commission* (2019) denda tersebut adalah denda terbesar yang pernah dikenakan pada perusahaan karena melanggar privasi konsumen dan hampir 20 kali lebih besar daripada hukuman privasi atau keamanan data yang pernah dikenakan di seluruh dunia. Terkait denda, Prof Carroll memiliki pandangan yang berbeda dengan Eduard Blasi. Denda mungkin ampuh untuk mencegah perusahaan namun sangat tidak memadai sebagai suatu hukuman. Sebab menurut Prof Carroll, *'a fine for data abuse is just the cost of doing business'*. Oleh sebab itu, penguraian algoritma harus menjadi alat utama dalam perangkat pengatur perlindungan data. Selain itu, perusahaan kecil, menengah, besar, dan monopolistik harus diberi konsekuensi misalnya data dan algoritma berharga mereka dapat disita dan dihancurkan jika ketahuan melakukan penyalahgunaan data secara massal, atau mengeksploitasi data dengan cara yang bertentangan dengan hak asasi manusia.

Dari paparan di atas dapat disimpulkan bahwa meskipun sebenarnya pengguna memiliki *data rights*, namun implementasi kebijakan perlindungan data dalam skandal data CA belum memadai. Regulasi yang ada pada saat itu belum cukup kuat untuk melindungi data pribadi dari praktik yang dilakukan perusahaan. Oleh sebab itu, hak-hak pengguna salah satunya hak untuk mendapatkan informasi terkait data tidak terpenuhi. Hingga saat ini, perusahaan teknologi sebagian besar masih bersifat *self-regulate*. Oleh karena itu, meskipun CA sudah tidak lagi beroperasi dan Facebook sempat dikenakan denda dan mengalami penurunan nilai saham, hampir tidak ada konsekuensi langsung baik bagi perusahaan-perusahaan maupun orang-orang yang terlibat dalam skandal ini. Hal ini menunjukkan belum adanya hukum atau regulasi yang secara efektif mengatur tentang *data rights*, perusahaan-perusahaan teknologi, *data scientist* dan arsitek yang bekerja di bidang tersebut.

5. KESIMPULAN

Akses terhadap data serta kemampuan utilisasi data yang dimiliki oleh perusahaan teknologi menimbulkan masalah terkait pelanggaran privasi dan perlindungan data, serta keterlibatan dalam elektoral dan kegiatan politik lainnya. Saat ini, praktik bisnis yang menjadikan data pengguna sebagai aset perusahaan teknologi yang kemudian dikomodifikasi untuk tujuan bisnis dan politik menimbulkan kemungkinan adanya pelanggaran terhadap *data rights*. Dalam kasus skandal data yang melibatkan CA dan Facebook, pengguna Facebook tidak mengetahui bahwa data mereka dikumpulkan untuk kepentingan kampanye Trump. CA mengeksploitasi data calon pemilih yang telah dikumpulkan untuk tujuan *behavioral modification*. Metode *microtargeting* yang dilakukan CA memungkinkan CA untuk memutuskan informasi apa yang dapat dilihat orang-orang, sehingga setiap calon pemilih menerima pesan kampanye yang berbeda sesuai dengan profil psikologis yang telah dibuat oleh CA. Hal tersebut tidak hanya membatasi informasi terkait pemilu, tetapi juga membuat pengguna rentan terhadap disinformasi dan konten yang menghasut kekerasan. Selanjutnya, pengguna Facebook sebagai subjek data dalam skandal data yang melibatkan CA dan Facebook menghadapi hambatan signifikan dalam menuntut

hak-hak atas data pribadi mereka. Salah satu contoh sulitnya subjek data untuk menuntut hak-hak atas data pribadinya adalah litigasi bertahun-tahun yang dilakukan oleh David Carrol untuk mengambil kembali data pribadinya dari CA tidak membuahkan hasil. Hal ini juga menunjukkan kurangnya ketegasan dalam implementasi terkait regulasi perlindungan data pribadi. Dalam negara demokratis seperti AS, dapat dilihat bahwa data pribadi belum sepenuhnya aman, bahkan rentan untuk disalahgunakan di era digital saat ini. Pemilu sebagai praktik demokrasi yang seharusnya transparan dan objektif, pada praktiknya masih terdapat banyak celah untuk dimanipulasi. Dengan demikian, penggunaan data pribadi tanpa izin seperti yang dilakukan CA pada pemilihan presiden AS 2016 tidak hanya berdampak pada *human rights*, khususnya *data rights*, namun juga terhadap jalannya demokrasi.

DAFTAR PUSTAKA

- Atal, M. R. (2021). The Janus faces of Silicon Valley. *Review of International Political Economy*, 28(2), 336-350. <https://doi.org/https://doi.org/10.1080/09692290.2020.1830830>
- Bachelet, M. (2019). *Human rights in the digital age*. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E>
- Bakir, V. (2020). Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting. *Frontiers in Communication*, 5(September), 1-16. <https://doi.org/10.3389/fcomm.2020.00067>
- Bakir, V., & McStay, A. (2018). Fake News and The Economy of Emotions: Problems, causes, solutions. *Digital Journalism*, 6(2), 154-175. <https://doi.org/10.1080/21670811.2017.1345645>
- BBC. (2016). *US Election 2016: All you need to know*. [Www.Bbc.Com](http://www.Bbc.Com). <https://www.bbc.com/news/world-us-canada-35356941>
- Benchman, A. (2019). Data as Humans: Representation, Accountability, and Equality in Big Data. In *Human Rights in the Age of Platforms* (pp. 75-94). The MIT Press.
- Boldyreva, E. L., Grishina, N. Y., & Duisembina, Y. (2018). Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. *The European Proceedings of Social & Behavioural Sciences*, 91-102. <https://doi.org/10.15405/epsbs.2018.12.02.10>
- Cadwalladr, C., & Harrison, E. G. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Cambridge Analytica. (2020). *An Overview of Cambridge Analytica's Political Division*. <https://archive.org/details/ca-docs-with-redactions-sept-23-2020-4pm/page/n12/mode/2up>
- CLC. (2020). *CLC supplemental complaint re: Cambridge Analytica and Make America Number 1* (Vol. 1, Issue 1). <https://campaignlegal.org/document/clc-supplemental-complaint-re-cambridge-analytica-and-make-america-number-1%0A>
- Federal Trade Commission. (2019). *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions%0A>
- Fuchs, C. (2019). Karl Marx in the Age of Big Data Capitalism. In *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data* (pp. 53-71). University of Westminster Press. <https://doi.org/10.16997/book29.d>
- Goldhill, O. (2019). *A "big data" firm sells Cambridge Analytica's methods to global politicians, documents show*. <https://qz.com/1666776/data-firm-idea-uses-cambridge-analytica-methods-to-target-voters/>
- Gordon, J. (2019). *When Data Crimes are Real Crimes: Voter Surveillance and the Cambridge Analytica Conflict* [Saskatchewan].

- https://dspace.library.uvic.ca/bitstream/handle/1828/11075/Gordon_Jesse_MA_2019.pdf?sequence=1&isAllowed=y
- H. Graesseger, M. K. (2017). *The Data that Turned the World Upside Down*. https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win
- Harris, T. L., & Wyndham, J. M. (2015). Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing. *Journal of Empirical Research on Human Research Ethics*, 10(3), 334-337. <https://doi.org/10.1177/1556264615591558>
- Hilder, P. (2019). *They were planning on stealing the election': Explosive new tapes reveal Cambridge Analytica CEO's boasts of voter suppression, manipulation, and bribery*. <https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/>
- Hirschhorn, D. (2016). *How Donald Trump Shocked The World*. Time.Com. <https://time.com/4563946/election-2016-donald-trump-victory-how/>
- Human Rights Council. (2014). *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
- Human Rights Watch. (2021). *Data Privacy is a Human Right*. <https://www.hrw.org/news/2018/04/19/data-privacy-human-right#:~:text=Human rights courts have also,proportionate to a legitimate goal>
- Humble, K. P. (2021). International law, surveillance and the protection of privacy. *International Journal of Human Rights*, 25(1), 1-25. <https://doi.org/10.1080/13642987.2020.1763315>
- J. B. Merrill, W. O. (2021). *Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation*. Washington Post. <https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/>
- Lang, P. (2019). *Data Rights Law 1.0: The Theoretical Basis* (L. Yuming (ed.)). Peter Lang Ltd, International Academic Publishers.
- Langworthy, S. (2019). *Power Dynamics in an Era of Big Data*. LSE Ideas. <https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Power-Dynamics-in-an-Era-of-Big-Data.pdf>
- Laterza, V. (2021). Could Cambridge Analytica Have Delivered Donald Trump's 2016 Presidential Victory? An Anthropologist's Look at Big Data and Political Campaigning. *Public Anthropologist*, 3(1), 119-147. <https://doi.org/10.1163/25891715-03010007>
- Lathrop, A. (2019). *Human Rights Horizon: Are data rights human rights?* <https://www.centeronhumanrightseducation.org/data-rights/>
- LeBaron, G., Mügge, D., Best, J., & Hay, C. (2020). Blind spots in IPE: marginalized perspectives and neglected trends in contemporary capitalism. *Review of International Political Economy*, 28(2), 283-294. <https://doi.org/10.1080/09692290.2020.1830835>
- LeCocq, S. (2018). *Cambridge Analytica is more than a data breach - it's human rights problem*. The Conversation. <https://theconversation.com/cambridge-analytica-is-more-than-a-data-breach-its-a-human-rights-problem-96601%0A>
- Naughton, J. (2019). *The goal is to automate us": Welcome to the age of surveillance capitalism*. The Guardian. <https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook>
- Netflix UK & Ireland. (2019). *The Insane Cambridge Analytica Interference Revelations in The Great Hack*. <https://www.youtube.com/watch?v=omc-5zj70M0>
- OHCHR. (2021). *Special Rapporteur on the right to privacy*. <https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx>

- Osborne, H. (2018). *What is Cambridge Analytica? The firm at the center of Facebook's data breach*. The Guardian. <https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach>
- Posner, S. (2016). *How Donald Trump's New Campaign Chief Created an Online Haven for White Nationalists*. <https://www.motherjones.com/politics/2016/08/stephen-bannon-donald-trump-alt-right-breitbart-news/>
- R. Eipstein, R. E. R. (2015). The Search Engine Manipulation Effect (SEME) and Its Possible Impact on the Outcomes of Elections. *Proceedings of the National Academy of Sciences of the United States of America*, E4512- E4521.
- S. C. Matz, M. Kosinski, G. Nave, D. J. S. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America*, 114(48), 12714-12719. <https://doi.org/https://doi.org/10.1073/pnas.1710966114>
- Shaw, T. (2018). *The New Military-Industrial Complex of Big data Psy-Ops*. <https://www.nybooks.com/daily/2018/03/21/the-digital-military-industrial-complex/>
- UN. (2014). *Resolution adopted by the General Assembly on 18 December 2013 68/167*.
- UN Human Rights Committee. (1988). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. <https://www.refworld.org/docid/453883f922.html>
- UNCTAD. (2021). *Data Protection & Privacy Legislation Worldwide*. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
- UNHCHR. (2011). *Guiding Principles on Business and Human Rights*. https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
- Ward, K. (2018). Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting. *Journal of Media Ethics*, 33(3), 133-148. <https://doi.org/https://doi.org/10.1080/23736992.2018.1477047>
- West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*, 58(1), 20-41. <https://doi.org/10.1177/0007650317718185>
- Westby, J. (2019). *'The Great Hack': Cambridge Analytica is just the tip of the iceberg*. <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>
- Whitehead, M. (2019). *Book Review Whitehead on Zuboff*. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf
- Witt, J., & Pasternack, A. (2019). *Before Trump, Cambridge Analytica's parents built weapons for war*. [Www.Fastcompany.Com. https://www.fastcompany.com/90235437/before-trump-cambridge-analytica-parent-built-weapons-for-war](https://www.fastcompany.com/90235437/before-trump-cambridge-analytica-parent-built-weapons-for-war)
- Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World*. Profile Books.
- York, J. C. & Zuckerman, E. (2019). Moderating the Public Sphere. In *Human Rights in the Age of Platform* (pp. 137-187). The MIT Press.
- Zuboff, S. (2019). *The Age of Surveillance capitalism: The Fight for a Human Future at The New Frontier of Power*. Public Affair.