



PELANGGARAN PRIVASI DAN ANCAMAN TERHADAP KEAMANAN MANUSIA DALAM KASUS CAMBRIDGE ANALYTICA

Faris Azhar Zaelany, Ika Riswanti Putranti

Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik

Universitas Diponegoro

Jalan Prof. H. Soedarto, SH, Tembalang, Kota Semarang.

Website : <http://www.fisip.undip.ac.id/> Email : fisip@undip.ac.id

ABSTRACT

Cambridge Analytica is a data-based political consulting firm that intervened in the US elections (2016) using the OCEAN method to attract voters. The problem here is the data obtained using illegal methods through quizzes and advertisements on Facebook. With the data obtained by Cambridge Analytica, they can use this data for the benefit of their companies and their clients, thereby endangering the targeted citizens. This research wants to explain how the violation cause by Cambridge Analytica become a threat. In answering this question, the concept of Human Security and cybersecurity is used. This study uses an descriptive method in answering the problem. The results of this study found that the threat posed by this case harmed not only citizens but the state and also the violations that occur can cause a collapse in security and social life.

Keywords: Cambridge Analytica, Privacy, Personal data, Security Threats

PENDAHULUAN

Kasus Cambridge Analytica (CA) adalah yang pertama disebarakan pada tahun 2018 oleh salah satu mantan pekerja Cambridge Analytica yaitu Christopher Wylie. Wylie menyampaikan rahasia pertama mereka kepada 'TheGuardian', sebuah media di Inggris. Wylie mengatakan bahwa Cambridge Analytica 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).

Cambridge Analytica sendiri merupakan perusahaan konsultasi politik yang berasal dari Inggris, sebagai perusahaan yang memanfaatkan perkembangan teknologi saat ini, yaitu menggunakan big data (Wylie, 2019). Cambridge Analytica dapat memengaruhi keputusan para pemilih, menggiring opini, menyebarkan berita disinformasi dan lainnya. Cambridge Analytica 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).

Cambridge Analytica 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 di awal akunnya, “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).

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 Analytica ini melanggar privasi pengguna dikarenakan eksploitasi yang dilakukan tersebut.

METODE DAN KERANGKA TEORI

Untuk menjawab pertanyaan pada penelitian ini, konsep keamanan manusia (*Human Security*) dan cyber security digunakan untuk mendeskripsikan bagaimana pelanggaran privasi dan ancaman terhadap keamanan manusia yang dilakukan oleh Cambridge Analytica. Kategori-kategori yang ada pada konsep keamanan Human Security yaitu keamanan personal, keamanan komunitas, dan keamanan politik digunakan sebagai indikator yang digunakan untuk menganalisis bagaimana pelanggaran privasi dan ancaman oleh Cambridge Analytica dapat dideskripsikan. Indikator ini juga berguna untuk melihat bagaimana ancaman ini mengancam keamanan manusia terutama pada masyarakat Amerika Serikat. Sementara konsep Cyber Security digunakan untuk menjelaskan istilah-istilah siber dan dunia maya yang dipakai dikarenakan kasus Cambridge Analytica terjadi di media sosial dan dunia maya.

Tulisan ini menggunakan metode kualitatif dengan sumber data dari hasil kajian literatur yang memanfaatkan sumber-sumber literatur terpercaya seperti dokumen-dokumen terkait, jurnal internasional, situs-situs berita terkait maupun laporan tentang kasus Cambridge Analytica.

PEMBAHASAN

Identitas dan Privasi

Data Pribadi merupakan identitas pribadi dari seseorang, Identitas pribadi yang terkepos membuat masyarakat menjadi terancam. Hal ini merupakan bagian inti dari permasalahan utama dari kasus ini. Identitas pribadi yang terekspos dapat disalahgunakan oleh berbagai pihak, Cambridge Analytica yang memakai data-data masyarakat ini adalah salah satunya. Menurut presentasi yang disampaikan oleh Nix dan di situs web perusahaan, Cambridge Analytica menggunakan data untuk memotivasi perilaku individual.

Karena jumlah berkas individu yang dimilikinya dikumpulkan, perusahaan dapat membuat profil seputar kombinasi kepribadian OCEAN dan titik data demografis/geografis/psikografis. Ini kemudian dapat diekstrapolasi ke populasi umum Amerika. Dengan demikian, akses ke sejumlah titik data terbatas tentang satu orang dapat menyarankan ke Cambridge untuk menganalisis ciri-ciri OCEAN individu tersebut dan, sebagai hasilnya, cara menyesuaikan

pesan persuasif untuk orang itu, yang dibuat dan disampaikan pada langkah terakhir metode ini. Dalam kasus ini, berarti pesan bertarget mikro perilaku ke audiens online yang ditargetkan secara ketat, membujuk mereka untuk memilih Trump atau, secara teoritis, untuk tidak memilih saingannya Hillary Clinton berdasarkan preferensi yang diturunkan secara psikologis. Penggunaan data Facebook yang tidak baik oleh Cambridge Analytica untuk tujuan politik menghadirkan dilema etika kontemporer yang masif sebagai pengguna Facebook tidak mengetahui untuk apa data mereka digunakan.

Pertama, perusahaan membangun analisis kepribadian untuk individu menggunakan kuis sukarela pada atau melalui media sosial untuk mengestimasi kepribadian individu dalam bentuk lima kepribadian: keterbukaan (*Openess*), atau kenikmatan baru pengalaman, Kesadaran (*Conciouness*), atau kecenderungan dalam kontrol impuls pikiran, Ekstraversi (*Extraversion*); cara berinteraksi dengan orang, *Agreeableness* merupakan keramahan atau preferensi untuk menempatkan kebutuhan orang; lain di atas kebutuhan sendiri, dan Neurotisme (*Neuroticism*), atau kecenderungan untuk khawatir.

Analisis kepribadian OCEAN gabungan ini mewakili komponen dari psikolog perilaku menyebut penanda kepribadian "lima besar", yang menurut penelitian adalah cukup untuk secara akurat mencirikan kepribadian individu. Pada Maret 2017, Nix mengatakan Cambridge Analytica telah menganalisis kepribadian "pemalu" beberapa juta orang," yang terdiri dari kumpulan data yang sangat besar (Cadwalladr, 2018). Dalam langkah kedua metodenya, perusahaan mencocokkan atribut OCEAN individu dengan massa titik data yang diketahui tentang orang itu. Informasi yang dikumpulkan mencakup informasi demografis dan geografis, termasuk ras, etnis, jenis kelamin, usia, tempat tinggal, tempat tinggal sebelumnya, pendapatan, dan sebagainya, tetapi juga data psikografis, yang berpotensi termasuk preferensi dan aktivitas politik dan ideologis, kebiasaan membeli, hobi, dan sebagainya (Cadwalladr, 2018).

Dalam kasus ini tidak memiliki akun Facebook pun tidak memberikan perlindungan data dan karena sumber data yang tersedia tidak terbatas dengan yang hanya ada di Facebook, dan analisisnya dapat dengan mudah diterapkan ke titik preferensi pribadi lainnya. Selain itu, setiap situs web dengan logo Facebook yang ditautkan ke Facebook, memungkinkan pelacakan non-anggota serta anggota yang mungkin tidak memilih untuk ikut serta dalam layanan (Laterza, 2018). Ada banyak sumber pelacakan online yang serupa misalnya, suar web yang sebagian besar dikaitkan dengan "cookie" yang dapat digunakan di seluruh situs web, dan akses dapat dijual kepada pembeli yang berminat (Lapaire, 2018). Dengan menggabungkan berita nyata dengan informasi yang salah atau konten Internet yang tidak dibatasi, pemilih target akan menemukan pesan yang menguatkan di banyak situs tanpa menyadari bahwa mereka adalah beberapa dari sedikit orang di dunia yang mendapatkan pesan-pesan itu, juga tidak diberi peringatan bahwa ini adalah pesan kampanye politik (Isaak & Hanna, 2018).

Facebook memiliki aturan privasi konsumen untuk melindungi data-data para penggunanya. Namun yang dilakukan Cambridge Analytica dengan mengeksploitasi dan menggunakan data tersebut untuk tujuan yang tidak sesuai dengan *Code of Conduct Facebook* (Facebook, 2021). Aturan facebook ini membahas sensitivitas dan kerahasiaan data pengguna Facebook dan pentingnya melindungi data pengguna. Mengenai aturan ini yang dilakukan oleh Cambridge Analytica terhadap data pengguna merupakan sebuah pelanggaran privasi dikarenakan aturan yang ditetapkan dilanggar demi kepentingan Cambridge Analytica.

Regulasi merupakan salah satu bentuk keamanan dalam *Cyber security*, maka melihat dari kasus ini kelemahan dalam regulasi yang ada di Facebook pada saat itu sebenarnya dapat

dimanfaatkan oleh berbagai pihak terutama dalam hal ini adalah Cambridge Analytica. Ketika keamanan data privasi ini bocor maka pihak-pihak yang mendapatkan data pengguna dapat dimanfaatkan dengan berbagai cara. Ketika data privasi pengguna bocor maka yang dapat terjadi bukan hanya masyarakat yang menggunakan Facebook saja yang terancam namun negara juga dikarenakan banyak pengguna Facebook itu bukan hanya kalangan umum namun juga petinggi negara.

Dan dalam kasus ini yang terjadi adalah dibuatnya manipulasi melalui iklan namun ini juga membuat kerusakan dengan memberikan influensi yang membuat masyarakat tergiring opininya dan membuat pilihan mereka seakan-akan diatur. Skandal Cambridge Analytica yang menggunakan data pribadi untuk kepentingan politik tanpa adanya persetujuan dari masyarakat membuat publik semakin takut untuk menggunakan media sosial karena merasa kebebasan berbicara semakin terbatas dan kepercayaan yang semakin menurun. Penyalahgunaan data pribadi membuat orang semakin gampang dalam menyampaikan pendapat maupun menyampaikan data pribadi untuk keperluan publik ataupun untuk keperluan pemerintah. Hal ini membuat kepercayaan publik terhadap sosial media semakin menurun maka dapat berdampak pada penurunan pemakaian internet. Namun, karena kasus ini berhubungan terhadap pemilihan umum maka kepercayaan terhadap pemerintah juga semakin menurun.

Berdasarkan salah satu komponen *Human security* yaitu Freedom from Fear. Masyarakat selayaknya harus dilindungi hak sipilnya serta kebebasannya dalam bertindak. Namun yang terjadi adalah ketakutan yang diakibatkan pengambilan data pribadi secara ilegal yang dapat merusak kehidupan bermasyarakat.

Keamanan terhadap data pribadi merupakan hak individu maka ketika hal ini terlanggar dan privasi terancam maka memungkinkan untuk terjadinya kekacauan yang lebih. Walaupun

kasus Cambridge Analytica pada saat ini tergolong sudah selesai namun efek dari kasus ini sangat besar dan mengubah pandangan dunia terhadap privasi dan data pribadi. Masyarakat dahulu menganggap bahwa apapun yang terjadi di sosial media dan internet tidak akan memiliki dampak yang konsekuensinya nyata.

Microtargeting dan Misinformasi Terhadap Masyarakat

Microtargeting merupakan teknik untuk mengumpulkan data online melalui jejak digital secara banyak dan dijadikan satu set data untuk menganalisa masyarakat yang kemudian data tersebut digunakan untuk membuat pesan atau iklan sesuai dengan kebiasaan individual dan personalitanya (Ward, 2018). Hal tersebut biasa digunakan untuk kepentingan komersial namun dalam kasus ini disalahgunakan.

Selama dan setelah kampanye, sumber, termasuk Cambridge Analytica sendiri, mengklaim perusahaan menggunakan data besar untuk memengaruhi perilaku pemilih dengan cara yang sebelumnya tidak terbayangkan oleh khalayak ramai. Secara khusus, diklaim bahwa perusahaan telah menyortir sekitar 220 juta orang Amerika ke dalam profil perilaku yang memakai data yang dikumpulkan dari sosial media seperti Facebook dan dibeli dari pialang data seperti Acxiom dan Nielson. Dengan menggunakan kumpulan data besar ini, perusahaan menyampaikan pesan yang mendukung kampanye Trump yang disesuaikan dengan psikologis ciri-ciri masing-masing individu penerima pesan dalam praktik yang disebut penelitian ini sebagai *behavioral microtargeting*.

Pesan semacam itu dimainkan untuk harapan, ketakutan, prasangka, dan khayalan yang mungkin tidak diterima oleh penerima pesan, sendiri, bahkan telah menyadarinya. Hasilnya, klaim Cambridge Analytica, telah mengumpulkan 1,4 miliar tayangan online dan menghasilkan keuntungan nyata bagi kampanye Trump yang mengungguli Clinton dalam penghitungan elektoral (NYtimes, 2017).

Microtargeting yang dilakukan dengan mengirim pesan-pesan untuk mendukung kampanye Trump dengan cara mengirim video-video ini terbukti berhasil untuk mengubah opini-opini masyarakat Amerika Serikat sehingga dapat memenangkan pemilu umum Amerika Serikat 2016. Dari hal ini dapat dijelaskan juga bahwa Microtargeting ini mengancam status dan kebebasan masyarakat. Microtargeting yang dilakukan oleh Cambridge Analytica, sebagaimana yang dijelaskan oleh Brittany Kaiser pada sebelumnya bahwa yang dilakukan sudah seperti taktik komunikasi tingkat senjata. Karena yang dilakukan sudah seperti propaganda yang mana informasi yang diberikan kepada target-target yang dituju itu mendiskreditkan lawan dengan bukti yang tidak cukup kuat atau pun hoax.

Gambar 1 Tahapan 50 Juta Catatan Facebook Dibajak



Sumber : *The Guardian*

Berdasarkan gambar diatas dapat disimpulkan bahwa data-data pribadi yang diambil melalui Facebook secara ilegal ini dibentuk melalui pola yang dirancang dengan menggabungkan perilaku-perilaku pengguna Facebook sehingga terbentuklah algoritma untuk memperkirakan bagaimana sikap dan perilaku pengguna Facebook, dalam kasus ini adalah bagaimana sikapnya terhadap pemilu umum Amerika Serikat. Maka ketika mereka sudah menemukan pengguna

yang cocok dengan seleksi yang telah dibuat melalui metode OCEAN, pengguna Facebook akan ditarget dengan iklan-iklan yang ditujukan untuk mengubah pandangan terhadap opini Trump seperti yang dijelaskan sebelumnya. *Behavioural Microtargeting* ini sudah sering digunakan untuk keperluan marketing pada barang/jasa. Contohnya, ketika membuka Facebook atau media sosial lainnya yaitu munculnya iklan-iklan yang mungkin pernah diucapkan atau website yang sebelumnya pernah dikunjungi sehingga sering muncul di laman iklan.

Menurut Konsep *Human security*, keamanan termasuk dalam individu dan komunitas. Pada kasus ini terlihat jelas bahwa ancaman yang terjadi akibat microtargeting yang dibuat oleh Cambridge Analytica dapat mengakibatkan permasalahan dalam kehidupan. Dengan mudahnya informasi-informasi yang diberikan pada target-target sesuai dengan kebutuhan perusahaan dan klien ini memberikan efek yang luas sehingga masyarakat dapat terkelabui. Ketika hal seperti ini tidak diregulasi maka tidak hanya masyarakat satu negara saja yang terancam namun masyarakat internasional juga.

Ancaman ini bukanlah ancaman tradisional sehingga cocok dengan konsep *human security* yang bertujuan untuk kemananan dan kesejahteraan manusia. Ancaman yang sering terjadi pada saat ini adalah ancaman yang berbentuk fisik dan nyata adanya sementara dalam kasus ini berbentuk data dan tidak ada fisiknya namun mempengaruhi masyarakat secara luas dan mengganggu kebebasan dalam bertindak serta politik serta efeknya yang tidak kecil membuat ancaman ini terasa secara nyata. Keamanan Pribadi merupakan hal yang paling relevan dalam konsep *Human security* pada kasus Cambridge Analytica ini. Melalui metode OCEAN yang sebelumnya disebutkan ini dipakai untuk memprediksi perilaku seseorang, maka ketika data-data identitas yang didapatkan oleh Cambridge Analytica ini bisa dimanfaatkan untuk menggiring opini dan pandangan masyarakat. Maka kasus Cambridge Analytica ini jelas

melanggar dan mengancam status, kebebasan, dan preferensi politik warga negara Amerika Serikat.

Preferensi Politik dan Kepercayaan Publik

Melihat dari kasus ini hal yang terjadi dapat mengancam kehidupan berpolitik dalam bermasyarakat. Melalui kasus ini dapat dilihat bahwa prediksi yang dibuat melalui metode OCEAN yang dipakai Cambridge Analytica dapat mengganggu preferensi politik masyarakat, dengan mengotak-ngotakkan orang berdasarkan data-data tersebut maka Cambridge Analytica dapat memanfaatkan data tersebut untuk memanipulasi orang-orang yang kemungkinan besar dapat dipengaruhi melalui iklan-iklan berdasarkan Microtargeting yang dibahas sebelumnya.

Menurut artikel ICCPR no.1 yang menyatakan bahwa “Semua orang memiliki hak untuk menentukan nasib sendiri (ICCPR, 1966). Berdasarkan hak itu mereka dengan bebas menentukan status politik mereka dan dengan bebas mengejar perkembangan ekonomi, sosial dan budaya mereka” (ICCPR, 1966). Ketika preferensi politik ini terganggu maka sistem demokrasi yang diterapkan negara juga seperti tidak terasa. Hal-hal yang dilakukan oleh Cambridge Analytica memang efektif dalam pemilihan umum dan bahkan bisa dibilang sukses untuk mengambil suara-suara masyarakat.

Namun cara yang dilakukan ini termasuk tidak ideal dan ilegal dikarenakan memanfaatkan data-data pribadi masyarakat tanpa diketahui sehingga dapat dimanipulasi sampai ke pola pikir masyarakat. Preferensi politik merupakan kecenderungan atau perilaku seorang individu dalam berpolitik baik itu memihak dan memilih. Kecenderungan ini dapat berubah tergantung dengan pemikiran tiap individu terhadap afiliasi politik baik *left-wing* maupun *right-wing*. Individu dalam suatu negara memiliki kekuatan untuk memenangkan pemilihan umum dengan suaranya.

Kasus Cambridge Analytica yang telah diuraikan di atas bisa lepas dari jeratan hukum, walaupun telah berdampak merugikan pengguna sosial media maupun warga masyarakat pada umumnya, yang selama ini mengekspresikan pandangan-pandangan mereka secara bebas di internet ataupun di dalam media sosial. Publik akan cenderung cemas ketika mereka akan mengungkapkan pandangan mereka di media sosial. Ketakutan ini pada dasarnya disebabkan mereka khawatir data-data yang dimilikinya akan digunakan oleh pihak-pihak lain untuk keuntungan pihak lain tersebut yang berarti artinya keuntungan sepihak.

Alhasil kepercayaan masyarakat terhadap pemerintah yang seharusnya melindungi menjadi berkurang dan membuat negara menjadi tidak stabil dikarenakan kemananan terhadap politik dan masyarakat menjadi tidak aman dan membuat hasil pemilihan tidak adil. Negara sebagai pelindung masyarakat harus menerapkan peraturan baru untuk perlindungan data agar tidak terjadi kejadian yang sama.

KESIMPULAN

Berdasarkan penelitian ini, Peneliti menemukan berbagai faktor yang menjelaskan bagaimana skandal Cambridge Analytica melanggar privasi dan mengancam keamanan manusia terutama di Amerika Serikat. Faktor pertamanya adalah kebocoran data privasi masyarakat yang melanggar privasi oleh Cambridge Analytica dan mengancam keamanan manusia. Dalam hal ini kebocoran data privasi yang dilakukan Cambridge Analytica terhadap Facebook yang melanggar aturannya mengakibatkan ketakutan pada masyarakat yang membuat kepercayaan terhadap pemerintah juga menurun. Ketika privasi masyarakat terlanggar maka kebebasan semakin terkekang dan akibat dari konsekuensi ini akan semakin memburuk dikemudian hari. '*Freedom from fear*' yang merupakan bagian komponen dari *Human security* dapat menjelaskan bagian ini karena kebebasan dari ketakutan merupakan keamanan terhadap individu yang paling penting agar kehidupan masyarakat dapat dijalani dengan aman, nyaman, dan tentram.

Kemudian faktor kedua adalah *Microtargeting* yang mempengaruhi pemikiran masyarakat. *Microtargeting* yang dilakukan oleh Cambridge Analytica dengan mengirimkan iklan-iklan yang didesain khusus untuk masyarakat yang ditarget agar pemikiran opini mereka

berubah terhadap Trump serta semakin mendiskreditkan lawan dengan opini *hoax* atau *black campaign* sehingga kebebasan berpolitik dan preferensi politik masyarakat terganggu. Namun jika melihat dari kasus ini maka terlihatlah bagaimana bentuk kampanye di masa depan, menurut peneliti model kampanye yang dibuat oleh Cambridge Analytica ini merupakan model yang sangat efektif namun dengan catatan bahwa data-data yang digunakan tersebut diambil secara ilegal. Jika data-data ini diambil secara sah dan iklan-iklan yang dibuat tidak memberikan informasi yang salah maka memungkinkan di masa depan nanti akan dipakai seperti ini. Faktor Ketiga analisis OCEAN yang dapat menganalisis perilaku masyarakat agar sesuai dengan pesan yang diinginkan oleh perusahaan agar dapat dimanfaatkan demi kepentingan klien. Dengan menggunakan metode OCEAN ini yang memiliki prediksi dengan keakuratan yang lumayan tinggi dapat mengganggu preferensi dan kebebasan berpolitik pada masyarakat. Ketika masyarakat dapat diprediksi perilakunya hanya melalui karena interaksi dan jejak digital membuat kebebasan di internet semakin terbatas dan terjadinya ketakutan terhadap sosial media.

Ancaman yang dibuat oleh kasus ini terhadap Amerika Serikat adalah nyata adanya. Pelanggaran privasi yang dilakukan oleh Cambridge Analytica dengan melanggar aturan privasi dan belum adanya regulasi yang ketat pada saat itu terhadap perlindungan data dapat dimanfaatkan oleh Cambridge Analytica dengan tujuan kepentingan politik.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Mbak Ika Riswanti Putranti, S.H., M.H., Ph.D. selaku dosen pembimbing Penulis yang telah membimbing Penulis sehingga penelitian ini bisa diselesaikan.

REFERENSI

- Cadwalladr, C. (2018). 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower. *The Guardian*, 1–15.
<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>
- Facebook. (2021). *Keep Building Better: The Facebook Code of Conduct*.
https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2021/06/FB-Code-of-Conduct.pdf#:~:text=Act lawfully%2C honestly%2C ethically and,Facebook users at all times.&text=Never retaliate against anyone who,who cooperates in an investigati
- Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>
- Lapaire, J.-R. (2018). Why content matters. Zuckerberg, Vox Media and the Cambridge Analytica data leak. *Antares: Letras e Humanidades*, 10(20), 88–110.

<https://doi.org/10.18226/19844921.v10.n20.06>

Laterza, V. (2018). Cambridge Analytica, independent research and the national interest. *Anthropology Today*, 34(3), 1–2. <https://doi.org/10.1111/1467-8322.12430>

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: Exploring Questions of Media Morality*, 33(3), 133–148. <https://doi.org/10.1080/23736992.2018.1477047>

Wylie, C. (2019). *Christopher Wylie - Mindfuck - Cambridge Analytica and the Plot to Break America (Mindfuck)-Penguin Random House LLC*. Penguin Random House LLC.

Zinolabedini, D., & Arora, N. (2013). The Ethical Implications of the 2018 Facebook-Cambridge Analytica Data Scandal. *Journal of Chemical Information and Modeling*, 53(9), 1689–1699.