10.18800/themis.202101.006

# EL EXTRACTIVISMO DE GRANDES DATOS (PERSONALES) Y LAS TENSIONES JURÍDICO-POLÍTICAS Y TECNOLÓGICAS VINCULADAS AL VOTO SECRETO

## *(PERSONAL) BIG DATA EXTRACTIVISM AND THE POLITICAL-LEGAL AND TECHNOLOGICAL TENSIONS RELATED TO THE SECRET VOTE*

**Ariel Hernán Vercelli***
**Consejo Nacional de Investigaciones Científicas y Técnicas**

*The power, scope and technological capacity of certain States and their corporations bring new and complex challenges for democracies in the 21st century. The extraction of personal big data, the creation of citizens psychographic profiles and the sending of microsegmented political propaganda can affect the secret ballot and weaken democracy.*

*This article reviews the case of Facebook Inc. – Cambridge Analytica in order to analyze how the extraction of personal big data, the violation of privacy and the use of psychography can favor the manipulation of people, groups, communities and populations. The article is part of a larger investigation that seeks to rethink internet regulations and strengthen democracies in the digital age.*

*Keywords: Extractivism; personal data; secret ballot; Facebook Inc.; Cambridge Analytica; psycography.*

*El poder, alcance y capacidad tecnológica de ciertos Estados y sus corporaciones plantea nuevos y complejos desafíos para las democracias del siglo XXI. El extractivismo de grandes datos personales, la creación de perfiles psicográficos de los ciudadanos y el envío de propaganda política microsegmentada pueden afectar el voto secreto y debilitar la democracia.*

*En este artículo se retoma el caso Facebook Inc. – Cambridge Analytica con el objeto de analizar como el extractivismo de grandes datos personales, la violación de la privacidad y el uso de psicografía pueden favorecer la manipulación de personas, grupos, comunidades y poblaciones. El artículo forma parte de una investigación mayor que busca repensar las regulaciones de internet y fortalecer las democracias en la era digital.*

*Palabras clave: Extractivismo; datos personales; voto secreto; Facebook Inc.; Cambridge Analytica; psicografía.*

* Doctor en Ciencias Sociales y Humanas. Consejo Nacional de Investigaciones Científicas y Técnicas de Argentina (CONICET) (Buenos Aires, Argentina). Contacto: arielvercelli@arielvercelli.org

El artículo se desarrolló gracias al apoyo del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), la Universidad Nacional de Mar del Plata (UNMdP) y Bienes Comunes A. C. La investigación se desarrolla dentro del Instituto de Humanidades y Ciencias Sociales (INHUS/CONICET - UNMdP) y el Grupo de Investigación 'Ciencia, Tecnología, Universidad y Sociedad' (CITEUS), OCA 347/05, Facultad de Humanidades, UNMdP.

Nota del editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 10 de enero de 2021, y aceptado por el mismo el 30 de mayo de 2021.

## I. INTRODUCCIÓN: LOS PROBLEMAS DEL EXTRACTIVISMO DE GRANDES DATOS (PERSONALES)

El uso masivo de las tecnologías digitales, las redes electrónicas distribuidas y las redes móviles ha generado (y está generando) profundos cambios en las sociedades contemporáneas. Muchos de estos cambios representan beneficios claros, ostensibles y masivos. Otros, sin embargo –más allá de las atractivas tecno-utopías–, profundizan injusticias socioeconómicas, generan asimetrías jurídico-políticas y contribuyen al deterioro de institutos clave para la vida democrática. Las crecientes y, muchas veces, compulsivas capacidades de extracción (recolección, procesamiento, archivo y explotación) de grandes datos alcanzadas por algunos Estados y sus corporaciones tecnológicas están planteando nuevos y complejos desafíos para los derechos humanos y las democracias representativas en el siglo XXI.

En la era digital, al igual que las piezas de un rompecabezas que aún no logran mostrar una figura completa, es posible advertir que el derecho humano a la privacidad (de personas, comunidades o poblaciones) se convirtió en un elemento central de la vida democrática. Al igual que otros sistemas complejos, los sistemas jurídico-políticos se caracterizan por conformar redes de relaciones: no hay forma de afectar (positiva o negativamente) alguno sin que otros derechos también resulten reconfigurados. Hace décadas se advierte que el exponencial aumento en las capacidades de extracción u explotación de grandes datos (personales, comunitarios y poblacionales) iba a afectar directamente el derecho a la privacidad y la protección de datos personales. Ahora bien, ¿la violación masiva y sistemática de estos derechos, su reconfiguración, o bien, su desaparición, podrían también acarrear consecuencias imprevistas?

Al respecto, es posible observar que los profundos cambios sobre el derecho humano a la privacidad comienzan a afectar también, de forma negativa e imprevista, la interpretación y el ejercicio de otros derechos y garantías constitucionales. ¿Es posible identificar casos recientes que evidencien estas tensiones jurídicos-políticas y tecnologías? Una de las hipótesis que atraviesa el artículo (y la investigación mayor en la que este se inserta) es que ciertos modelos tecnológicos corporativos están afectando negativamente las democracias representativas. Puntualmente, la violación masiva y sistemática del derecho humano a la privacidad –producto de la extracción y gestión tecnológica que llevan adelante algunos Estados y sus corporaciones tecnológicas– afecta la garantía constitucional del voto secreto y, con ello, se debilitan las democracias.

Es por ello por lo que, a los problemas ya suscitados por las modernas máquinas de votar y el voto electrónico[1], ahora es posible agregar nuevos problemas vinculados al extractivismo de grandes datos personales, la violación masiva y sistemática de la privacidad y ciertos diseños tecnológicos que degradan las libertades políticas y el sufragio universal. En el artículo se retoma el caso Facebook Inc. – Cambridge Analytica/Strategic Communications Laboratories (vinculado a las elecciones presidenciales de los Estados Unidos y el referéndum del Reino Unido en 2016) con el objetivo de analizar como el extractivismo de grandes datos personales y el uso de psicografía[2] pueden favorecer la manipulación de personas, comunidades y poblaciones y afectar negativamente las libertades políticas y las democracias en el siglo XXI.

## II. LA RELEVANCIA DE LA PRIVACIDAD Y DE LA PROTECCIÓN DE LOS DATOS PERSONALES

El derecho humano a la privacidad es reconocido y garantizado ampliamente en las Constituciones Nacionales y en numerosos instrumentos internacionales (por ejemplo, el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948)[3]. La privacidad es reconocida a cada ser humano individualmente, a grupos y comunidades específicas y, por cierto, también a las poblaciones. Se trata de un derecho que puede (y debe) interpretarse de forma amplia y respetando la di-

[1] Los numerosos intentos 'modernizadores' de los votos electrónicos (y de sus recuentos provisorios y definitivos) parecen no estar orientados a colaborar y fortalecer las democracias: el voto electrónico, telefónico, *online*, por computadora, por celular, entre otros, representan casos de retrocesos y vulnerabilidad para los sistemas y formas de votar. A través de estos sistemas, el voto podría dejar de ser secreto y/o se los podría identificar con facilidad (Hao & Ryan, 2017).

[2] La psicografía combina datos demográficos y psicológicos de las poblaciones (Nix, 2016). Se desarrolló como una herramienta del marketing (Samuel, 2016): releva si a los consumidores les gusta (o no) un producto o acuerdan (o desacuerdan) con alguna situación. Así se construyen perfiles de los ciudadanos (estilos de vida, rutinas y preferencias de consumo). Ver apartados IV y V en este artículo.

[3] El artículo 12 de la Declaración Universal de Derechos Humanos expresa que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (1948).

versidad de cada cultura (Francis & Francis, 2017). Tiene la particularidad de articularse con una red densa de otros derechos fundamentales: entre ellos, derechos políticos, libertades intelectuales (conciencia, creencias, pensamiento), libertad de expresión, protección del cuerpo, intimidad, confidencialidad, bienes materiales, autonomía, autodeterminación, domicilio y correspondencia.

A pesar de ser un derecho multiforme y de reciente reconocimiento mundial, el derecho a la privacidad reconoce a las personas la posibilidad de gozar de espacios de reserva, que, según diversidad de formas y alcances, pueda garantizar la intimidad, anonimidad o no intromisión por parte de los Estados, corporaciones u otras personas (sean estas físicas o jurídicas). Esta esfera de reserva, por fuera de las autoridades estatales y/o corporativas, ha recibido numerosos nombres y definiciones a lo largo de la historia. Entre otras, y con diferencias conceptuales y de alcances, se pueden mencionar conceptos tales como privacidad, vida privada, intimidad, confidencialidad, secreto, secretismo (Riofrío, 2015), olvido, reserva, no registro, anonimato y protección de datos sensibles.

A su vez, los cambios tecnológicos han ido afectando la codificación, configuración e interpretación del derecho a la privacidad a través de los años. Entre otras adecuaciones pueden citarse las tensiones generadas por las fotografías, las videocámaras, la telefonía fija o, más recientemente, el uso masivo de dispositivos móviles. El aumento exponencial de las capacidades tecnológicas de registro y archivo han resultado en la proliferación de todo tipo de información sobre las personas, grupos o poblaciones. En particular, formando parte del derecho a la privacidad, pero también de otros derechos fundamentales (intimidad, honor, identidad, integridad, libertades políticas), la era digital se caracteriza por haber regulado, a partir de la década del setenta y con mayor intensidad en los noventa, los principales aspectos del tratamiento de la información personal y de la protección de los datos personales.

Se han creado, con algo más de precisión, nuevos derechos orientados a resguardar la información personal (sensible), contenida en cualquier soporte (archivos, registros, bancos de datos u otros medios), frente a la gestión (más o menos automática) por parte de terceras personas (Estados, corporaciones comerciales, personas jurídicas sin fines de lucro)[4]. Aunque se trata de un derecho 'nuevo', de reciente construcción, todavía no existe a nivel mundial un estándar o posiciones uniformes sobre protección de datos personales. No obstante, más allá de las especificidades nacionales o regionales, por ejemplo, las de la Unión Europea (Hijmans, 2016; Reglamento 2016/679, 2016)[5], es posible identificar en las regulaciones algunos de los que podrían definirse como sus elementos comunes. A continuación, se describen los tres más relevantes para el presente análisis:

a) **Dato personal** es toda información sobre una persona (identificada o identificable) relacionada con, entre otros aspectos, nombres, documentos, origen étnico/racial, biometría, consumos, emociones, vida familiar/afectiva, domicilios, teléfonos, patrimonio, ideología, posiciones políticas, creencias (religiosas, morales), educación, salud, sexualidad;

b) Salvo excepciones legales, para la colecta de cualquier información o dato personal siempre se debe contar con el **consentimiento expreso** de la persona directamente afectada/involucrada (es decir, con su autorización expresa) obtenida a través de un medio que sea, entre otros requisitos exigibles, accesible, gratuito, comprensible, claro en sus términos y condiciones legales;

c) Estas **autorizaciones nunca podrán interpretarse de forma amplia, extensa o genérica**: es decir, los datos personales solo podrán usarse para los fines expresa y previamente autorizados. Las regulaciones nacionales e internacionales prohíben otros usos (sean por parte de quienes los colectaron o por parte de terceras personas).

[4] Se reconocen nuevos derechos a la ciudadanía para gestionar sus datos, saber dónde se almacenan, quiénes pueden acceder a ellos, con qué fines pueden usarlos o por cuánto tiempo se conservarán. En algunos países (como Argentina y Uruguay) los ciudadanos disponen de una acción específica (judicial) de *habeas data* orientada a poder conocer (rectificar, eliminar) los datos que constan en una base de datos del Estado o de personas privadas (con o sin fines de lucro).

[5] La Unión Europea (en adelante, UE) busca regular qué hacen algunas corporaciones extranjeras (Facebook Inc., Google Inc. Uber Inc., entre otras) con los datos de los ciudadanos europeos. El Reglamento General de Protección de Datos de la UE (Reglamento 2016/679, en vigor desde el 25 mayo de 2016 y aplicable desde el 25 de mayo de 2018), plantea reforzar el derecho a la privacidad, restringir la gestión automática de datos personales sin consentimientos expresos y ofrecer, entre otros puntos, mayor capacidad a las agencias europeas de inspeccionar, limitar y sancionar a las corporaciones que no cumplan con sus estándares: por ejemplo, las nuevas 28 autoridades de protección de datos podrán imponer multas de hasta 20 millones de EUROS o del 4 % del volumen de negocios. A partir de la aplicación del nuevo reglamento en la Unión Europea es posible advertir una creciente complejidad en el tratamiento de datos personales (Troncoso Reigada, 2021).

## III. LA VIOLACIÓN MASIVA Y SISTEMÁTICA DEL DERECHO HUMANO A LA PRIVACIDAD

Más allá de lo expresado en las diferentes leyes de protección de datos personales y, sobre todo, de sus interpretaciones legales y tecnológicas, es importante resaltar que la extracción de todo tipo de datos personales se ha transformado en una de las formas más rentables y lucrativas de explotar la experiencia e interacción humana en la era digital. De allí que la privacidad y la protección de datos personales se hayan convertido en una zona álgida, de conflictos y tensiones, sobre qué se puede o no se puede hacer con la información de los ciudadanos. La problemática fue denunciada a través de numerosos informes y documentos internacionales (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2014). Alemania y Brasil impulsaron la Resolución 68/167 (aprobada el 18 de diciembre de 2013 por Asamblea General de Naciones Unidas) sobre el derecho a la privacidad en la era digital.

A nivel internacional existen fuertes presiones de Estados y sus corporaciones tecnológicas para reconfigurar la regulación hacia sus propios intereses. Las corporaciones que se dedican a extraer y explotar datos personales de los usuarios pasaron a producir sus propias interpretaciones jurídico-tecnológicas sobre qué es y cómo se ejercen estos derechos. Esto ha tenido resultados negativos: muchas de las condiciones de uso de servicios, plataformas y redes sociales se han transformado en imposiciones abusivas e ilegales (o paralegales) sobre el tratamiento estos datos. Muchas de estas corporaciones tecnológicas, incluso, rechazan el sentido protectivo de estas regulaciones. De allí que la protección de datos personales, lejos de convertirse en un ejercicio ciudadano directo y efectivo, se haya convertido en algo dudoso, confuso, atrasado, costoso, técnico, solo para expertos.

Estas situaciones han favorecido que, a escala global, se produzca un tipo de violación masiva y sistemática de la privacidad (en general) y de los datos personales de los usuarios (en particular). Estas tensiones entre las regulaciones de los datos personales de los usuarios y las tecnologías digitales que se usan para extraerlos y explotarlos es posible identificarlas a partir de, al menos, dos fuertes tendencias a nivel mundial. Por un lado, la vigilancia masiva y el ciberespionaje: de público conocimiento a través de las filtraciones de Chelsea Manning[6] y Edward Snowden[7] (Assange, 2013; Poitras, 2014; Greenwald, 2014; Lefébure, 2014). Por el otro, los modelos de negocios y la comercialización de la publicidad/propaganda que llevan adelante las corporaciones tecnológicas más poderosas a nivel mundial (Reischl, 2008; Vaidhyanathan, 2011; Assange, 2014; Bartlett, 2018).

Los entornos digitales están siendo diseñados para extraer valor de todo tipo de experiencias humanas. Dentro de estos diseños tecnológicos y arquitecturas los seres humanos pasan a ser considerados recursos naturales, una fuente más para extraer valor. Las imágenes de la vigilancia y del panóptico devienen penetrantes. Similar a como Michel Foucault (1991) describía el panóptico de Jeremías Bentham, las redes electrónicas (internet, la red de redes) se convirtió en un (ciber)espacio donde se distribuyen asimétricamente las capacidades de ver y ser visto. Algunos pueden verlo todo, un gran panóptico electrónico distribuido, otros –disociados, atomizados, sujetos a máquinas digitales de extracción, producción y control–, no pueden siquiera verse a sí mismos como personas, comunidades o poblaciones.

Este panóptico, ahora electrónico, captura e intenta extraer valor de la totalidad de la vida humana. Se caracteriza por recombinarse con arquitecturas, disciplinas, tecnologías, regulaciones, algoritmos, ciencia de datos, inteligencias artificiales, análisis predictivos. Estos dispositivos, en suma, siguen funcionando como una especie de laboratorio de poder. Permiten observar un tipo de extractivismo que utiliza la experiencia humana como material crudo, lo traduce en 'datos conductuales' (en conductas) y lo ofrece como dispositivos de predicción (sobre lo que puede ocurrir ahora, pronto o después). Aquello que Zuboff (2019) define como un mercado de conductas futuras. Se trata de un tipo

[6] Chelsea Elizabeth Manning (llamada al nacer Bradley Edward Manning) es una soldado de inteligencia del ejército de los Estados Unidos de Norteamérica (fuera de servicio). Fue quién filtró al sitio WikiLeaks.com cables diplomáticos (sobre embajadas) y documentos de la inteligencia de EE. UU sobre las guerras de Afganistán e Irak. Entre otros, el video filtrado más reconocido fue Collateral Murder (Asesinato Colateral) (Assange, 2013). Desde 2014 cumple condena a 35 años de prisión en los EE. UU.

[7] Edward Snowden es un experto en tecnologías de información norteamericano, actualmente asilado en Rusia, que trabajó para la CIA (Agencia Central de Inteligencia), la DIA (Agencia de Inteligencia en Defensa), la empresa Dell y la firma Booz Allen Hamilton (trabajando para la National Security Agency, en Hawaii), que filtró en 2013 miles de documentos clasificados sobre los sistemas de vigilancia masiva de la Agencia Nacional de Seguridad de EE.UU (NSA) a los medios de comunicación y, específicamente, al periódico inglés The Guardian (a través de los periodistas Glenn Greenwald y Laura Poitras). Al respecto se puede ver el documental Citizenfour (Poitras, 2014).

de extractivismo compulsivo, invasivo, violatorio de derechos, oculto y antidemocrático.

## IV. FACEBOOK INC. – CAMBRIDGE ANALYTICA: A LA CAZA DE LOS DATOS (PERSONALES)

A mediados de marzo del año 2018, Channel 4[8], The New York Times[9] y The Observer (The Guardian)[10] comenzaron a publicar material de investigación sobre como algunas corporaciones favorecían el uso masivo de los datos personales de la ciudadanía con fines electorales. Las investigaciones periodísticas –que incluyeron cámaras ocultas, entrevistas a exempleados y documentos oficiales– dejaron entrever una trama oscura entre la red social norteamericana Facebook Inc.[11] y, entre otras, la empresa británica Cambridge Analytica (en adelante, CA), parte de Strategic Communications Laboratories (en adelante, SCL)[12]. El tema no era nuevo[13], pero sí escandaloso. Las investigaciones revelaron como CA/SCL ofrecía 'innovadoras' campañas electorales a través del uso intensivo de tecnologías digitales, datos personales y perfiles psicológicos de millones de usuarios[14].

Los informes periodísticos denunciaban que CA/SCL había utilizado estas novedosas herramientas en más de 200 campañas en todo el mundo: en particular, y más cercanas en el tiempo, en las elecciones norteamericanas de 2016 (con una participación a favor de Donald Trump) y, en el mismo año, en el referéndum del Reino Unido (donde apoyaron activamente la posición del Brexit)[15]. Al tomar estado público rápidamente surgieron campañas en su contra[16] y varias investigaciones en todo el mundo[17]. A los pocos días se fueron conociendo algunos detalles operativos. Los datos y perfiles de los usuarios de Facebook Inc. habían sido recolectados por CA/SCL a través de la empresa Global Science Research (GSR)[18]. Esta última fue fundada por Aleksandr Kogan, un psicólogo social ruso que trabajaba en la Universidad de Cambridge (Reino Unido).

8 Canal público de televisión comercial del Reino Unido, controlado por Channel Four Corporation (C4C), una corporación pública dedicada a televisión, cine e internet, y relacionada con la Oficina de Comunicaciones (Ofcom) del Reino Unido.

9 Diario norteamericano fundado en 1851.

10 Es el diario dominical más viejo del mundo. Fue publicado por primera vez en 1791.

11 Facebook Inc. es una corporación norteamericana dueña de la red social más grande del mundo (Facebook) y otras empresas (Instagram, Messenger, Oculus, Whatsapp). Sus oficinas centrales están en Menlo Park, California. La red social vio la luz el 4 de febrero de 2004 y comenzó a cotizar en bolsa en 2012. La plataforma Facebook se caracteriza por enlazar gente 'amiga' (o conocidos) mostrando sus actividades sociales (es decir, textos, fotos, videos sobre qué hacen). Sus principales ingresos se deben al rubro publicidad. Se estima que a principios de 2018 Facebook tenía cerca de 2 200 millones de usuarios en todo el mundo. En promedio, los usuarios activos le dedican a Facebook unos cincuenta minutos diarios (Stewart, 2016). Facebook Inc. es considerado, según criterios de uso y adopción, el negocio más exitoso en la historia de la humanidad (Galloway, 2017).

12 Cambridge Analytica (en adelante, CA) era una empresa británica (con oficinas en Londres, New York y Washington D.C.) dedicada a las consultorías de mercado y campañas electorales. Pertenecía a la familia Mercer (Robert y Rebekah) y fue presidida por Steve Bannon (director de campaña de Donald Trump en 2016). CA fue fundada en 2012 como una filial de Strategic Communications Laboratories (en adelante, SCL). SCL provee datos, análisis y estrategia para gobiernos y organizaciones militares: se dedica a colectar y analizar cuál es la opinión sobre los servicios militares y diplomáticos de Estados Unidos y el Reino Unido en todo el mundo. Trabaja principalmente con los ministerios de defensa de los países de la Organización del Tratado del Atlántico Norte (OTAN) (Briant, 2018). SCL se describe a sí misma como la primera empresa privada proveedora de operaciones psicológicas. Entre sus técnicas, se destacaban la propaganda política y la posibilidad, en tiempos de crisis, de sobreescribir las transmisiones de los medios de comunicación, además, la colecta de grandes datos y de su duplicación y segmentación.

13 En julio de 2015 la Revista Politico publicó una nota sobre la estrategia de campaña de Ted Cruz: resaltaban la promiscua relación de la familia Mercer (financista de Cruz) y empresas de su propiedad (CA/SCL) que lo asesoraban (Vogel & Parti, 2015). En diciembre de 2015, The Guardian ya denunciaba el uso de datos personales y la creación de perfiles psicológicos para la campaña en los EE. UU. (Davies, 2015). En 2017, The Intercepter denunciaba algo similar (Schwartz, 2017).

14 Las cámaras ocultas mostraban a directivos de CA/SCL ofreciendo campañas de desprestigio: escándalos sexuales, noticias falsas (*fake news*), sobornos, trabajos de inteligencia.

15 Se denomina así a la campaña del año 2016 en el Reino Unido para influir en el referéndum del 23 de junio por la salida de Gran Bretaña de la Unión Europea. Al respecto ver Glenncross (2016).

16 El 22 de marzo uno de los fundadores de Whatsapp, Brian Acton, se manifestó contra la Facebook Inc. y llamó a un boicot en su contra: *#DeleteFacebook* y *#BoycottFacebook*.

17 Se iniciaron múltiples investigaciones (políticas, administrativas y judiciales) sobre violaciones a la protección de datos personales y a las leyes electorales. En EE. UU. denunciaron a CA/SCL ante la Comisión Federal Electoral y el Departamento de Justicia. En el Reino Unido las investigaciones fueron tomadas principalmente por la Cámara de los Comunes (Digital, Culture, Media and Sport Committee, 2018; 2019). En Brasil estuvieron a cargo del Ministerio Público del Distrito Federal y Territórios (Brito, 2018; Ministério Público, 2018). En Argentina se encargaron la Cámara Nacional Electoral y la Dirección Nacional de Protección de Datos Personales (Carelli, 2018). También hay investigaciones iniciadas en Israel, Perú e India.

18 La página web de Global Science Research fue dada de baja. La información solo es disponible a través de Internet Archive: https://web.archive.org/web/20160317171729/http://www.globalscienceresearch.com

El tema de investigación de Aleksander Kogan era 'felicidad y amabilidad' (*happiness and kindness*) en las redes sociales y usaba desarrollos del Centro de Psicometría de la Universidad de Cambridge. Entre otras, investigaciones sobre psicografía[19] y predicción de la personalidad provenientes de los trabajos de Michal Kosinski y David Stillwell (Youyou *et al.*, 2015; Sumpter, 2018)[20]. Estos investigadores (Kosinski *et al*., 2013), habían advertido que la personalidad de un usuario podía predecirse fácilmente a través de los datos públicos que se extraían de sus rutinas de navegación (páginas web, redes sociales, etc). En CA/SCL estaban interesados en poder usar los datos personales y los perfiles psicográficos de los usuarios de Facebook Inc. para diseñar campañas electorales microsegmentadas.

Inicialmente, Kogan desarrolló una aplicación (un cuestionario de personalidad llamado *this is my digital life* [esta es mi vida digital]), validada en la *application programming interface* (en adelante, API) de Facebook Inc.[21], a través de la cual los usuarios consentían hacer un estudio psicográfico. Al hacerlo, permitieron voluntariamente que la aplicación recolecte todo tipo de información sobre su perfil (ubicación, género, cumpleaños, preferencias, me gusta). Incluso, al aceptar el cuestionario, por la configuración de Facebook Inc., también permitieron que la aplicación recolecte los perfiles de sus amigos (contactos)[22]. Cerca del 80% de los voluntarios ofrecieron sus datos (y los de sus amigos) por un dólar (tenían en promedio 353 amigos). Entre 2014 y 2015, aceptaron participar unos 857 usuarios de Facebook Inc. y, gracias a los 'permisos de los amigos', se recolectaron más de 287 000 perfiles (Sumpter, 2018).

En un segundo momento CA/SCL le ofreció a Aleksandr Kogan ampliar la muestra. Esta vez el contrato fue hecho por fuera de la Universidad y se usó Qualtrics (un servicio en línea de encuestas para consumidores) (Sumpter, 2018). Según afirma Kogan, en ese momento se solicitaron todas las autorizaciones correspondientes a los encuestados y también se cumplió con la normativa de Facebook Inc. (Sumpter, 2018; Stahl, 2018). En esta oportunidad el cuestionario fue respondido por cerca de 200 000 norteamericanos (Sumpter, 2018). Según datos estimados de Facebook Inc., los perfiles recolectados a través de esta segunda encuesta podrían alcanzar entre 70 y 87 millones de usuarios (inicialmente se supuso que eran 50, luego 70 y, finalmente, 87 millones). Se estimó también que, de los 87 millones, 71 millones vivían en EE. UU. (una cantidad significativa que permitió esquematizar los rasgos psicológicos de la población norteamericana).

Es importante resaltar que los datos anteriores son solo estimaciones provisorias: no existen datos oficiales ni de Facebook Inc. ni de CA/SCL, ni de ningún Estado. ¿Es posible que el número de damnificados sea superior? Es posible. Brittany Kaiser, una exempleada de Cambridge Analytica, declaró el 17 de abril 2018 ante el Parlamento Británico que –más allá de las desarrolladas por Kogan– existían dentro de la red social numerosas encuestas con similares características: por ejemplo, "sex compass [brújula sexual]" (Collins, 2018). Incluso, el mismo Aleksandr Kogan, entrevistado por Lesley Stahl (2018), expresó que dentro de Facebook existían decenas de miles de estas aplicaciones que recolectaban datos personales. Facebook Inc. reconoció (tal vez como parte de su estrategia legal) que no podían certificar (calcular) la cantidad real de usuarios afectados.

Incluso, su representante legal, Mike Schroepfer, llegó a afirmar a la prensa que en Facebook Inc. nunca revisaban los términos y condiciones incluidos en las aplicaciones que los desarrolladores cargaban a la red (Romm, 2018). No obstante, el informe final de la investigación llevada adelante

---

19 Para la psicometría todas las personalidades humanas pueden clasificarse según rasgos. El uso de PCA (*Principal Component Analysis*) permitió sintetizar cinco grandes grupos (*big five*), el modelo OCEAN (por sus siglas): *Openness* (apertura), *Conscientiousness* (responsabilidad), *Extroversion* (extroversión), *Agreeableness* (amabilidad) y *Neuroticism* (inestabilidad).

20 Michal Kosinski y David Stillwell desarrollaron (dentro de la Universidad de Cambridge) el proyecto myPersonality recolectando, con permisos explícitos, más de tres millones de perfiles de usuarios de Facebook Inc. Muchos de estos usuarios tomaron un test de psicometría (medición de inteligencia, personalidad, alegría, orientación sexual, uso de drogas, etc.). El estudio les permitió analizar como aquello que es escrito, compartido y evaluado a través de un simple 'me gusta' permite describir la personalidad y, en parte, predecir conductas (Sumpter, 2018).

21 En 2007, la red social comenzó a ofrecer un espacio para el desarrollo de aplicaciones. Esta plataforma articuló HTML, SQL (*styled query language*), JavaScript y una serie de librerías de clientes de programación. A este espacio de desarrollo se lo llamó genéricamente API (*application programming interface*). Esta plataforma le permitió a Facebook Inc. que otros desarrolladores crearan aplicaciones (externas) para mejorar la interacción entre los usuarios.

22 Es decir, los 'amigos' no aceptaban explícitamente los términos legales de la aplicación. Esta característica, llamada 'permisos de amigos' (*friend permissions*), no era un permiso especial concedido a Kogan (u otros), sino que era una de las principales 'funcionalidades' de la plataforma orientada a desarrolladores y empresas afiliadas-asociadas. Según Kogan, era una característica general de la plataforma y no un error: "It was a feature, not a bug" (Stahl, 2018). Estas características, debido a diferentes problemas legales de Facebook Inc., fueron restringidas a partir del año 2015.

por la Cámara de los Comunes del Reino Unido desmintió a Facebook Inc. y dejó en claro que la corporación sí sabía (internamente) cuantas aplicaciones corrían en la red social y bajo qué condiciones legales lo hacían (Digital, Culture, Media and Sport Committee, 2018; 2019). Facebook Inc. nunca hizo públicos estos datos. Es importante resaltar que, si bien los perfiles de los usuarios provenientes de Facebook Inc. fueron la fuente más importante para extraer datos personales, la red social norteamericana no fue la única fuente para la empresa CA/SCL[23].

CA/SCL articuló los datos personales provenientes de Facebook Inc. con otras fuentes de información de ciudadanos de los EE. UU.: entre otras, encuestas telefónicas, cuestionarios en línea, consumo de tarjetas de crédito, datos de otras redes sociales, bases de datos de las Iglesias evangélicas de los EE. UU. (Kriel & Gellein, 2020) e, incluso, datos públicos provenientes de padrones del Partido Republicano. La triangulación de las diferentes fuentes de datos le permitió a CA/SCL alcanzar perfiles más sólidos e integrados de la población norteamericana. Se estima que estas bases de datos contenían más de sesenta campos de información sobre aproximadamente 191 millones de ciudadanos norteamericanos (Kriel & Gellein, 2020). Estos datos son los que fueron retroalimentando los algoritmos predictivos que CA/SCL utilizó en la campaña de EE. UU. en 2016 y, con ajustes poblacionales, en otras campañas electorales alrededor del mundo.

## V. EL USO DE PSICOGRAFÍA EN LAS PRESIDENCIALES DE EE. UU. Y EL BREXIT DEL REINO UNIDO

El uso intensivo de las tecnologías digitales para campañas electorales no es nuevo. El presidente Barack Obama también las usó en las elecciones de 2008 para promover y financiar su llegada a la Casa Blanca[24]. Algo similar ocurrió con las campañas electorales de 2016 en EE. UU. (elecciones presidenciales a favor de Donald Trump) y también en el Reino Unido (referéndum Brexit: Vote.Leave y Leave.EU). En ambas campañas se registró un uso intensivo de redes sociales (en especial Facebook Inc.[25]), de datos personales y perfiles de Facebook Inc. (entre otros) y de herramientas psicográficas. Así lo confirmó Theresa Hong, Directora de Contenidos de la Campaña de Trump (Rampling, 2017) y los exempleados de Cambridge Analytica, Christopher Wylie y Brittany Kaiser (Cadwalladr & Graham-Harrison, 2018; Metcalf, 2018; Digital, Culture, Media and Sport Committee, 2018; 2019; Kaiser, 2019).

Específicamente, CA/SCL en los EE. UU. comenzó a trabajar en 2015 para las campañas republicanas de pequeña escala (alcaldías y legisladores). En un segundo momento, para las presidenciales de 2016 en EE. UU. comenzaron asesorando a Ted Cruz (candidato republicano) y, luego de la interna, pasaron a la campaña del también candidato republicano Donald Trump. Para la elección general el centro de operaciones se ubicó en San Antonio, Texas, y la campaña fue bautizada como Proyecto Álamo (Rampling, 2017). La estrategia de CA/SCL para influir el voto popular fue compleja y ambiciosa. Entre otros elementos, presentes también en el Brexit, buscaron articular: (i) el uso de grandes datos (personales); (ii) con desarrollos de psicometría (y su poder predictivo); y (iii) diseñar y enviar mensajes políticos micro-segmentados. Específicamente, articularon:

a) El uso de grandes datos (personales), tal y como se analizó anteriormente, obtenidos y recolectados desde diferentes fuentes (aunque, principalmente, de Facebook Inc.), para construir diferentes bases de datos y algoritmos que permitan definir y redefinir audiencias específicas para (o solo en función de) los intereses políticos de las campañas electorales que tenían por delante;

b) Los últimos desarrollos de psicometría (y su potencial para poder predecir la conducta

[23] Para Christopher Wylie, uno de los miembros de Cambridge Analytica, según declaración ante la Comisión de Asuntos Digitales, Cultura, Medios de Comunicación y Deportes de la Cámara de los Comunes (Parlamento Británico), los datos personales recolectados de la red social fueron la base sobre la que se fundó la empresa y sobre la que se apoyaron los algoritmos utilizados (Cadwalladr & Graham-Harrison, 2018). Algo similar puede haber ocurrido con AggregateIQ (AIQ), empresa canadiense que aportó modelos psicográficos para las campañas en EE. UU. y en el Brexit del Reino Unido (Digital, Culture, Media and Sport Committee, 2018; 2019).

[24] En esa oportunidad fue Google Inc. La corporación que demostró grandes capacidades de gestión para las campañas y para acompañar en la misma gestión del gobierno demócrata en EE.UU. (incluso, volviendo porosos los límites entre lo público y lo privado) (Zuboff, 2019).

[25] Según el informe corporativo de Facebook Inc. del 2016, Year in Review (Neman, 2016), ambas elecciones tuvieron la máxima relevancia. Los diez temas más hablados a nivel global del año 2016 fueron: 1) US Presidential Election, 2) Brazilian Politics, 3) Pokemon Go, 4) Black Lives Matter, 5) Rodrigo Duterte & Philippine Presidential Election, 6) Olympics, 7) Brexit, 8) Superbowl, 9) David Bowie, 10) Muhammad Ali. Es decir, cuatro de los diez temas más 'compartidos' en Facebook Inc. involucraron campañas políticas y elecciones: EE. UU., Reino Unido, Brasil y Filipinas (Neman, 2016).

política de los ciudadanos)[26]: CA/SCL creó y configuró modelos psicográficos de comportamientos de la población según rasgos de personalidad similares (grupos de votantes o audiencias). Estos modelos se desarrollaron antes del Proyecto Álamo[27]. Podrían considerarse una creación intelectual alcanzada por derechos intelectuales (Metcalf, 2018);

c) Para diseñar y enviar todo tipo mensajes microsegmentados con la intención de afectar (influir, asegurar, modificar o evitar) el voto popular. Los modelos psicográficos permitieron definir (interactuar, controlar) las audiencias (grupos de votantes) y decidir estrategias (y medios) para enviarles mensajes microsegmentados adecuados a su perfil psicológico (ansiedades, temores, solidaridad, escepticismo, etc.).

Por tanto, a partir de la estrategia implementada por CA/SCL es posible observar un punto relevante para el presente análisis. Los datos personales de carácter político de la ciudadanía tuvieron la máxima relevancia al momento de definir y conducir las campañas. Los datos personales de carácter político fueron usados para definir, construir y enviar mensajes a las diferentes audiencias. Al respecto, la Directora de Contenidos de la Campaña de Donald Trump en 2016, Theresa Hong, señaló cuál de los atributos era el más relevante para definir el universo de personas a las que dirigir la campaña microsegmentada (Rampling, 2017). Puntualmente, entre otros datos políticos relevantes, la directora expresó que para la campaña se consideraba central conocer (de personas/grupos/poblaciones): "[…] when was the last time they voted?, who did they vote for?" (Rampling, 2017)[28].

Incluso, a partir de las investigaciones de la Cámara de los Comunes del Reino Unido (Comisión de Asuntos Digitales, Cultura, Medios de Comunicación y Deportes; en adelante, la Comisión), Chris Vickery (Director de Investigaciones sobre Cyber Risk, Upguard), entregó a la Comisión un disco externo con datos personales de 191 millones de ciudadanos norteamericanos (Kriel & Gellein, 2020). La información de cada persona estaba compuesta por aproximadamente unos 60 campos. La base de datos, según afirmó Vickery, fue expuesta públicamente (accesible vía registración) a través de la organización religiosa evangelista United in Purpose (una coalición de pastores). Se estima que originalmente podría haber sido una base datos de los afiliados al Partido Republicano (llamada *Data Trust voter vault*). Entre otros campos de datos relevantes se destacan: "[…] likely swing voter … this person is likely to vote based on this issue … kind of one-position voter based on abortion […]" (Kriel & Gellein, 2020, 20:15)[29].

El gerente general de Cambridge Analytica, Alexander Nix, en su declaración ante la Cámara de los Comunes del Reino Unido, reconoció que la consultora buscaba alcanzar una adecuación de la información similar a la antes descrita. En su testimonio, tomado antes de que se desate el escándalo internacional en marzo de 2018, describe y defiende la microsegmentación implementada por CA/SCL de la siguiente forma:

> We are trying to make sure that voters receive messages on the issues and policies that they care most about, and we are trying to make sure that they are not bombarded with irrelevant materials. That can only be good [...] for democracy [...] (Digital, Culture, Media and Sport Committee, 2018, p. 27)[30].

---

[26] Para medir la personalidad antes se usaban test o cuestionarios. En la era digital se usan las huellas digitales de navegación o uso de redes sociales. Son los pequeños datos acumulados en el tiempo los que hacen la diferencia predictiva. Este es un trabajo que las computadoras hacen mejor que los seres humanos. Los algoritmos pueden identificar detalles valiosos dentro de grandes cantidades de pequeños rastros digitales. Los perfiles de comportamiento son muy buenos para estimar datos demográficos como las tendencias políticas, el género, la ubicación y la raza (Kosinski *et al*., 2013). Los análisis, predicciones y juicios sobre la personalidad hechos por computadoras son más adecuados que los hechos por seres humanos (Youyou *et al*., 2015). Las computadoras ven lo que los psicólogos, médicos o policías no ven. Un perfil de comportamiento basado en 'me gusta' (aparentemente inofensivos) junto con otros datos crean un mapa lo suficientemente bueno para obtener mucha más información sobre una persona: a mayor cantidad de dimensiones mayor el poder para clasificación (Kosinski *et al*., 2016).

[27] Según Alexander Nix (Rampling, 2017), para la campaña de Trump no se crearon modelos psicográficos específicos. La psicografía que tenían los datos utilizados en campaña fue heredada de los modelos de datos que se venían usando en las anteriores campañas (dos o tres años atrás).

[28] Traducción libre: "[…] ¿cuándo fue la última vez que votaron?, ¿por quién votaron?".

[29] Traducción libre: "[…] votante con probable cambio […] esta persona es probable que vote a partir de este tema […] tipo de votante que posiciona en primer lugar el aborto […]" .

[30] Traducción libre:

> Estamos tratando de asegurar que los votantes reciban los mensajes sobre los tópicos y las políticas que más les interesan y estamos tratando de asegurar que ellos no sean bombardeados con materiales irrelevantes. Esto solo puede ser bueno ... para la democracia […].

Los testimonios mencionados permiten observar que los perfiles psicográficos y los datos personales de carácter político, sobre todo los vinculados al voto, resultaron de máxima relevancia para las campañas. En 2016, para la campaña presidencial de EE.UU., se llegaron a enviar más de cien avisos diarios a través de las redes sociales (entre otras, Facebook, Youtube, Twitter) (Rampling, 2017). Según Christopher Wylie, la psicometría se usó para despertar los 'demonios internos' (*inner demons*) de cada persona (Cadwalladr & Graham-Harrison, 2018). Para ciertas 'audiencias' estas campañas pueden haberse convertido en un indeseable y abusivo bombardeo de todo tipo de mensajes: incluyendo, desde noticias falsas (*fake news*), hasta noticias más 'emocionales' orientadas a despertar ansiedad, temor, empatía, desagrado, desesperanza, escepticismo, etc.[31]

A partir del escándalo desatado en 2018 por el caso de Facebook. Inc. – Cambridge Analytica, la legalidad y legitimidad de este tipo de campañas micro-segmentadas, que apuntan a audiencias según perfiles psicográficos, que solo llegan a 'las pantallas' de los votantes (sin ningún control público-comunitario) y que buscan un cambio de conducta en la población, comenzaron a ser fuertemente cuestionadas en todo el mundo. A pesar de la gravedad, aún no se avizoran soluciones. Estas no aparecieron en EE. UU., tampoco en el Reino Unido. Incluso, en muchos países regular estas situaciones podría resultar una tarea casi imposible y con serias dificultades jurídico-políticas, económicas y tecnológicas. Finalmente, más allá de las vanas promesas de autoregulación corporativa, las posibles soluciones tampoco emergieron desde las mismas corporaciones tecnológicas.

## VI. ZUCKERBERG PIDE DISCULPAS PÚBLICAS, PERO FACEBOOK INC. SIGUE SU CAMINO

En medio del escándalo, Facebook Inc. intentó esquivar responsabilidades legales. En primera instancia, acusó a Aleksandr Kogan de fraude, de haber 'vendido' los datos a CA/SCL y, sin mediación, suspendió su cuenta. Por su parte, Kogan se defendió alegando que solo recopilaba la información con fines académicos y que actuó con honestidad (aunque con cierta ingenuidad). En segunda instancia, Facebook Inc. también suspendió la cuenta de CA/SCL bajo la acusación de haber violado su política de privacidad (prohibiéndole operar publicidad). Por su parte, CA/SCL también negó haber actuado de forma ilegal. No obstante, apartó a Alexander Nix. El 2 de mayo de 2018 la empresa anunció su cierre definitivo alegando pérdida de clientes y altos costos legales (Ballhaus & Gross, 2018). La empresa CA fue rápidamente transformada en otra, llamada Emerdata.

Finalmente, Mark Zuckerberg tuvo que pedir disculpas públicas por la forma en que Facebook Inc. había manejado los datos personales de sus usuarios. Sin embargo, fueron disculpas genéricas, ambiguas, sin ofrecer información válida sobre los hechos denunciados (Zukerberg, 2018). Se comprometió a realizar una investigación interna sobre CA/SCL y sobre otras aplicaciones que podrían haber minado datos personales de la red social (Zukerberg, 2018). Sin mucha relevancia, también se pusieron a disposición de los usuarios herramientas para saber si sus perfiles habían sido recolectados por CA/SCL (Facebook Newsroom, 2018). A principios de abril de 2018 Facebook Inc. presentó una nueva 'actualización' de sus términos de servicio y de su política de datos. Sin embargo, en nada modificaron sus políticas de datos personales ni su posición frente a la privacidad.

A mediados de abril de 2018 sí pudo observarse un movimiento brusco. La negativa de adecuar su gestión de datos personales a las nuevas regulaciones de la Unión Europea llevó a que Facebook Inc. cambie repentinamente su domicilio legal (la jurisdicción) de Irlanda hacia los EE.UU. Esto afectó los derechos de millones y millones de usuarios (cerca de dos tercios de sus clientes). El cambio de jurisdicción estuvo motivado por la entrada en vigencia del nuevo Reglamento General de Protección de Datos de la Unión Europea (Reglamento 2016/679, 2016). Sin mayores explicaciones Facebook Inc. regresó a su casa matriz en los EE. UU. (Agencia Telam, 2018). Los movimientos de Facebook Inc. dejaron en claro al menos dos puntos relevantes para el análisis. Por un lado, que a Facebook Inc. poco le importa la privacidad de sus usuarios y que algunas corporaciones parecen funcionar al margen de la ley. Por el otro, tal vez lo más importante, que a nivel internacional el derecho a la privacidad vale menos de lo que podía suponerse.

Los movimientos de Facebook Inc. mostraron que, a pesar de los escándalos vinculados a CA/SCL y de sus responsabilidades jurídicas, la red social

[31] Al respecto se puede revisar los informes (provisorio y final) de la Cámara de los Comunes (Digital, Culture, Media and Sport Committee, 2018; 2019) sobre desinformación (*disinformation*) y noticias falsas (*fake news*). En Argentina, según Acordada Extraordinaria 66-18, la Cámara Nacional Electoral (CNE) creó un "registro de cuentas de redes sociales y sitios web de los candidatos, agrupaciones políticas y máximas autoridades partidarias" con la intención de concientizar a la población sobre el peligro de las noticias falsas (*fake news*) (Acordada Extraordinaria 66-18, 2018).

norteamericana no tiene pensado adecuar su modelo de gestión de datos personales ni sus configuraciones de privacidad. Mucho menos revisar su modelo de negocio de publicidad y propaganda por microsegmentación de audiencias. La materia prima de Facebook Inc. son los perfiles de usuarios y su capacidad (amplia y detallada) para poder gestionarlos según sus intereses comerciales. Día a día, segundo a segundo, Facebook Inc. interroga a millones usuarios '¿qué estás pensando?'. Sus algoritmos registran cada movimiento. Facebook Inc. devino en una plataforma comercial que, lejos de ser una inocente red social de intercambio de fotos, videos o textos, adquirió una relevancia política insospechada.

En los próximos años, cada día más, Facebook Inc. (pero también Alphabet, Amazon y otras) seguirán colectando datos personales de sus usuarios. Estas corporaciones son, claramente, máquinas de disparar con publicidades y propagandas. Una vez que el relacionamiento social pasa a estar mediado solo por intereses comerciales, resulta factible que estas corporaciones se transformen en máquinas de manipulación social y afecten la autoconciencia y la autodeterminación de las personas y poblaciones[32]. El primer objetivo de Facebook Inc. como corporación es funcionar como máquina predictiva: su modelo de desarrollo, instrumentos e inteligencias artificiales (FBLearnerFlow) van creando un mercado de "futuros conductuales" (Zuboff, 2019, p. 264) sobre la base de predecir (poder anticipar) las conductas de los individuos, grupos sociales y poblaciones.

## VII. LAS TENSIONES POR EL VOTO 'OBLIGATORIAMENTE SECRETO' EN LA ERA DIGITAL

El recorrido propuesto en el artículo permite observar que la era digital no ha traído solo cambios tecnológicos favorables. La extracción y explotación de datos personales por parte de Estados y sus corporaciones tecnológicas tiene consecuencias negativas. A partir de la constante retroalimentación de los flujos de datos personales y, sobre todo, del aprendizaje circular y recursivo en la construcción de perfiles a través de tiempo, es que las conductas de los ciudadanos, comunidades y poblaciones se pueden conocer (directamente) o predecir (deducir, inferir, presumir). Entonces, ¿qué ocurre con el secreto del voto cuando algunos Estados y sus corporaciones tecnológicas pueden saber o predecir por quién/es ha votado, vota o podría votar un/a ciudadano/comunidad/población? ¿Por qué el sufragio universal fue también construyéndose como una práctica secreta?

El sufragio universal se ha transformado, desde mediados del siglo XIX, y a partir de diferentes luchas jurídico-políticas, en una de las piezas clave en la organización de poder del Estado. En la actualidad es uno de los pilares que sustenta la soberanía popular, los sistemas de representación política y los sistemas democráticos. Puede definirse como un derecho político de todos y cada uno de los ciudadanos/as para participar (elegir y ser elegido) en la organización y en las actividades del poder en el Estado. Es por ello que, a través del voto popular, logran expresarse tanto intereses individuales como colectivos: se manifiestan tanto la voluntad política individual de cada ciudadano (a favor de algún candidato o decisión política) como la voluntad colectiva de todo un pueblo/comunidad (como mayorías y minorías).

El recorrido histórico vinculado a las formas de participación política de los últimos siglos permite identificar gran cantidad y variedad de regulaciones, tecnologías y sistemas de votación: desde los más públicos –con votos a '*viva voce*', a la vista de todos–, hasta los sistemas que garantizan el voto como un 'acto secreto'. Tal y como afirma Elster (2015), todos los sistemas electorales, con semejanzas y diferencias, combinan elementos públicos y secretos. Entre las instancias públicas es posible mencionar, entre otros, los padrones electorales, el lugar y el horario y los resultados alcanzados (por mesa, distrito, provincia, etc.). Entre sus elementos más reservados se destaca, obviamente, el voto individual. En la actualidad, la mayoría de las elecciones de representantes de los cuerpos políticos se realiza a través del voto secreto[33].

En los últimos siglos se fueron construyendo las condiciones temporales, espaciales y tecnológicas específicas para garantizar el sufragio universal, igual, secreto y obligatorio[34] (Kropf, 2016). Así lo expresa el artículo 21(3) de la Declaración Univer-

[32] La autoconciencia y la autodeterminación se relacionan con las capacidades de pensar, elegir, criticar, reflexionar, empatizar, aprender, innovar y muchas de otras capacidades necesarias para el relacionamiento social.

[33] Elster (2015) afirma que, si el secreto es la norma para elecciones de representantes y la publicidad es la norma para las asambleas, la situación entre secreto y publicidad del voto pasa a ser menos clara para jurados, cortes con múltiples miembros, agencias administrativas o en votaciones de comités de expertos. En la práctica es posible observar gran variedad de casos.

[34] El voto es obligatorio solo en algunos países del mundo y no es la regla: es obligatorio votar en la mayoría de los países de América Latina (Argentina, Brasil, Bolivia, Chile, Ecuador, Perú, Panamá, Costa Rica, República Dominicana, Venezuela), y en algunos pocos de Europa y el resto del mundo (Bélgica, Luxemburgo, Grecia, Tailandia, Egipto, Australia, entre otros).

sal de los Derechos Humanos de 1948[35]. Uno de los primeros países en reconocer y sistematizar el voto secreto fue Australia[36] (Brett, 2019). Al respecto, también pueden revisarse las experiencias de Francia, Países Bajos, Grecia, Colombia o Argentina[37]. Además del reconocimiento jurídico-político, el secreto del voto también tuvo que ser garantizado tecnológicamente: el diseño de espacios específicos y reservados para votar (cuartos oscuros y cabinas), el uso de urnas cerradas (para evitar la individualización del voto) o la designación de autoridades de mesa (para el cumplimiento de las leyes electorales).

De esta manera, con similitudes y diferencias, entre los siglos XIX y XX el voto fue construyéndose como una práctica regulada, protegida, atravesada por la dualidad público-privada. Por un lado, una práctica pública (y en muchos países obligatoria) vinculada a las capacidades de participación política democrática. Por el otro, el contenido del voto fue construyéndose como algo privado, secreto, reservado y oculto a la mirada de otros (sean pocos, muchos o todos). El voto secreto se orientó a proteger la libertad política que tiene cada ciudadano de participar en la selección de candidatos (o en la toma de otras decisiones políticas) sin que medien amenazas, influencias o presiones (de cualquier tipo y forma)[38]. Según Rosanvallón (1999; 2015), en la experiencia francesa, el secreto del voto se orientó a democratizar las elecciones y evitar la 'presión partidista' sobre la opinión popular.

El secreto del voto procura que una decisión (por un/a candidato/a A, B o C, o por una consulta popular) se mantenga solo reservada al individuo que ejerce el derecho (a su esfera íntima, privada, exclusiva). Si bien el resultado general de una elección es público, el voto secreto procura evitar que se pueda identificar el contenido del voto con cada votante. Incluso, un momento clave en esta historia, es que el voto devino también una práctica obligatoriamente secreta (es decir, no alcanzó con que el voto sea optativamente secreto). El voto obligatoriamente secreto se transformó así en una de las más simples, elegantes y extendidas medidas regulativas que se construyeron para garantizar que las decisiones y/o preferencias políticas sean solo conocidas por el votante (excluyendo a otras/os, los Estados y las corporaciones). Esta situación parece haber cambiado radicalmente.

## VIII. CONCLUSIONES: LAS TENSIONES POR EL CONTROL DEL VOTO POPULAR

El extractivismo de todo tipo de datos personales que llevan adelante algunos Estados y sus corporaciones tecnológicas y la violación masiva y sistemática de la privacidad están afectando seriamente algunas libertades políticas y debilitando a la democracia representativa. En particular, el extractivismo de datos personales políticos vinculados al voto está generando una doble violación de derechos. La información política sobre a quién/es votó, vota o votará un ciudadano, un grupo social o la población, es un dato personal sensible alcanzado tanto por el derecho a la privacidad y la protección de datos personales como por la garantía del voto secreto-obligatorio. El análisis del caso Facebook Inc. – Cambridge Analytica/Strategic Communications Laboratories (entre otras empresas) permite observar claramente este doble proceso.

---

35 El artículo 21(3) de la Declaración Universal de Derechos Humanos expresa que:

> 3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto (1948).

En igual sentido, el artículo 23 del Pacto de San José de Costa Rica expresa que

> Todos los ciudadanos deben gozar de los siguientes derechos y oportunidades: [...] b) de votar y ser elegidos en elecciones periódicas auténticas, realizadas por sufragio universal e igual y por voto secreto que garantice la libre expresión de la voluntad de los electores [...] (Convención Americana de Derechos Humanos, 1969).

36 En la segunda parte del siglo XIX, Victoria, Australia, fue uno de los primeros lugares donde se garantizó la anonimidad en la relación voto-votante y en alcanzar el voto obligatorio y secreto. El secreto del voto se transformó en una de las formas fáciles y efectivas de limitar el poder de intimidación que tenían las aristocracias terratenientes de sur de Australia (Brett, 2019).

37 En la República Argentina el sufragio no fue reconocido explícitamente en la Constitución de 1853 (aunque sí de forma implícita a través de su artículo 33). Este fue regulado, por primera vez, en la Ley Sáenz Peña (Ley 8.871, 1912), donde se estableció el voto universal, secreto y obligatorio. A su vez, la Ley 13.010 (1947) otorgó el derecho de voto a las mujeres. La Reforma Constitucional de 1949 continuó con el reconocimiento "implícito" (artículo 36 de la Constitución Nacional de 1949 con redacción idéntica al artículo 33 de la Constitución Nacional de 1853). Con la reforma constitucional de 1994, artículo 37, el sufragio fue incluido explícitamente como derecho político: "[...] El sufragio es universal, igual, secreto y obligatorio" (Const. Nac., 1994).

38 Explica Elster (2015) que la razón para que el voto sea secreto (tanto en elecciones de gobierno como en votos emitidos por tribunales) es la protección de los votantes de posibles sobornos, intimidaciones o venganzas. El voto secreto se basó en el deseo de proteger a los votantes que se oponían al poder de pequeños concejos en manos de las oligarquías. Los votos en asambleas, por el contrario, no son secretos sino (en su gran mayoría) públicos.

A partir del análisis realizado es posible afirmar que las campañas electorales microsegmentadas, que usan perfiles psicográficos (y que incluyen datos personales políticos referidos al voto) están atravesadas por esta doble violación de derechos humanos. En momentos en que las leyes electorales están peligrosamente desactualizadas a nivel global, este tipo de campañas electorales se están transformando en una guerra de datos e información orientadas a la manipulación y el control del voto popular. Cada dispositivo (computadora, teléfono, televisor, etc.) conectado a internet comienza a ser un punto de intercambio de datos que, lejos de recibir mensajes (de candidatos) políticos, está siendo bombardeado con todo tipo de mensajes generados por computadoras (y por algoritmos) de acuerdo con perfiles psicológicos, estados de ánimo o predicciones de votos.

La publicidad indirecta, opaca, engañosa, microsegmentada, los anuncios oscuros (*dark ads*), las noticias falsas (*fake news*), no tienen puntos de comparación con las antiguas campañas electorales (por televisión, radio, carteles en la vía pública o prensa escrita). Los mensajes políticos enviados a través de Facebook Inc. son intencionalmente opacos: solo pueden ser vistos por usuarios finales, no se sabe quién/es los financian y, además, son imposibles de auditar (por Estados, ciudadanos y organizaciones comunitarias). La microsegmentación psicográfica favorece la construcción de conciencias políticas atomizadas, fragmentadas, divididas y agrietadas. Estas campañas atentan contra la autodeterminación, la construcción del espacio público-común y la democracia. Adecuar y fortalecer los sistemas electorales se presenta como una tarea urgente e imprescindible.

Esta adecuación va a requerir que las diferentes autoridades electorales tengan la capacidad de poder auditar, entre otros elementos clave, cuáles son los algoritmos que se usan para realizar esas campañas. Es necesario poder auditar y discutir sus diseños internos (por lo general, están ocultos, son cajas negras, de código privativo, cerrados). Muchos de estos algoritmos se están diseñando para conocer en profundidad y poder predecir las conductas de individuos, grupos, comunidades y poblaciones. Como tales representan un serio problema político. Por ello, es necesario que el diseño y uso de estos algoritmos respeten las leyes nacionales e internacionales, los derechos humanos, y que su diseño se produzca de forma abierta, cerca de los controles público-comunitarios y a través del conocimiento libre y compartido.

En sociedades democráticas los ciudadanos tienen que poder ejercer libremente su derecho al voto. Tienen que poder votar libres de amenazas, coacciones, propaganda oculta o campañas que operan subrepticiamente para modificar y condicionar sus conductas. El voto obligatoriamente secreto se construyó (se conquistó), justamente, para evitar este tipo de presiones políticas. Lamentablemente, en la era digital, esta solución simple, elegante e inteligente comienza a desvanecerse. Por ello, es necesario que la garantía constitucional del voto obligatoriamente secreto amplíe su cobertura espacio-temporal y pase a interpretarse de forma abierta, amplia y extendida. Es necesario que esta garantía proteja el secreto del voto antes, durante y con posterioridad al ejercicio del voto. Para ello, también es necesario volver a proteger los datos personales políticos de la ciudadanía.

Las democracias representativas se encuentran frente a un punto de no retorno. Si las capacidades de conocer o predecir el voto se fortalecen en algunos Estados y sus corporaciones tecnológicas, entonces, el voto popular podría pasar a ser secreto solo para los ciudadanos entre sí (es decir, entre quienes no poseen las máquinas de extraer datos e información de la población). El escenario futuro, en este caso, no es muy alentador. El voto popular podría estar migrando rápida y peligrosamente hacia un voto de 'secreto selectivo'. Es decir, un voto que, si bien no adquiere publicidad inmediata, su secreto pasa a depender de lo que 'otros' decidan sobre la información disponible. Estas intrusiones extractivistas y predictivas anticipan un aumento de la manipulación y los fraudes electorales y una disminución de las libertades políticas y de la vida democrática.

**REFERENCIAS**

Agencia Telam (19 de abril de 2018). Un cambio en Facebook hará que 1.500 millones de usuarios estén menos protegidos que los demás. *La Voz*. https://www.lavoz.com.ar/tecnologia/un-cambio-en-facebook-hara-que-1500-millones-deusuarios-esten-menos-protegidos-que-los-d/

Assange, J. (2013). *Criptopunks: La libertad y el futuro de internet*. Marea. Trilce.

(2014). *Wikileaks: When Google Met Wikileaks*. OR Books.

Ballhaus, R., & Gross, J. (2 de mayo de 2018). Cambridge Analytica Closing Operations Following Facebook Data Controversy. *The Wall Street Journal*. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140

Bartlett, J. (2018). *The People Vs Tech: How the internet is killing democracy (and how we save it)*. Penguin Random House.

Brett, J. (2019). *From Secret Ballot to Democracy Sausage: How Australia Got Compulsory Voting.* Swann House.

Briant, E. (4 de mayo de 2018). As Cambridge Analytica and SCL Elections shut down, SCL Group's defence work needs real scrutiny. *OpenDemocracy.Net*. https://www.opendemocracy.net/uk/emma-l-briant/as-cambridge-analytica-and-scl-elections-shut-down-scl-groups-defence-work-needs-re

Brito, R. (21 de marzo de 2018). Brazil prosecutors open investigation into Cambridge Analytica. *Reuters*. https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A

Cadwalladr, C., & Graham-Harrison, E. (17 de marzo de 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

Carelli, A. (22 de marzo de 2018). El Gobierno niega haber utilizado los servicios Cambridge Analytica. *Diario Perfil*. http://www.perfil.com/noticias/politica/el-gobierno-niega-haber-utilizado-los-servicios-cambridge-analytica.phtml

Collins, K. (17 de abril de 2018). Cambridge Analytica gathered Facebook data with 'sex compass' quiz. *CNET Internet Services*. https://www.cnet.com/news/cambridge-analytica-gathered-facebook-data-with-sex-compass-quiz-brittany-kaiser/

Davies, H. (11 de diciembre de 2015). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Digital, Culture, Media and Sport Committee (2018). *Disinformation and 'fake news': Interim Report* (Fifth Report of Session 2017-19). House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

(2019). *Disinformation and 'fake news': Final Report* (Eighth Report of Session 2017-19). House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

Elster, J. (2015). *Secrecy and Publicity in Votes and Debates*. Cambridge University Press.

Facebook Newsroom (4 de abril de 2018). Hard Questions: Q&A with Mark Zuckerberg on Protecting People's Information. *Facebook Newsroom*. https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/

Foucault, M. (1991). *Vigilar y Castigar: nacimiento de la prisión*. Siglo XXI.

Francis, L., & Francis, J. (2017). *Privacy: What Everyone Needs To Know*. Oxford University Press.

Galloway, S. (2017). *The four: the hidden DNA of Amazon, Apple, Facebook and Google*. Penguin.

Glencross, A. (2016). *Why the UK Voted for Brexit: David Cameron's Great Miscalculation*. Palgrave Macmillan.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the Surveillance State*. Metropolitan.

Hao, F., & Ryan, P. (2017). *Real-World Electronic Voting: Desing, Analysis and Development*. CRC Press.

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Springer.

Kaiser, B. (2019). *The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. Harper Collins.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of the United States of America*, *110*(15), 5802-5805.

Kosinski, M., Wang, Y., Lakkaraju, H., & Leskovec, J. (2016). Mining big data to extract patterns and predict real-life outcomes. *Psychological methods*, *21*(4), 493-506.

Kriel, C., & Gellein, K. (realizadores) (2020). *People You May Know* [documental]. Metrotone Media.

Kropf, M. (2016). *Institutions and the Right to Vote in America*. Palgrave Macmillan.

Lefébure, A. (2014). *El caso Snowden: Así espía Estados Unidos al mundo*. Capital Intelectual.

Metcalf, J. (16 abril de 2018). Los efectos del escándalo de Facebook para el futuro de la democracia. *MIT Technology Review*. https://www.technologyreview.es/s/10138/los-efectos-del-escandalo-de-facebook-para-el-futuro-de-la-democracia

Neman, S. (8 de diciembre de 2016). Facebook's 2016 Year In Review. *Facebook Newsroom*. https://newsroom.fb.com/news/2016/12/facebook-2016-year-in-review/

Nix, A. (2016). Cambridge Analytica – The Power of Big Data and Psychographics. *Concordia Annual Summit in New York*. https://codingvideos.net/cambridge-analytica-the-power-of-big-data-and-psychographics/

Poitras, L. (realizadora). (2014). *Citizenfour* [documental]. Praxis Films, Participant Media, HBO Films. https://citizenfourfilm.com/.

Rampling, J. (realizador) (2017). *Secrets of Silicon Valley (I and II)* [documental]. BBC and The Open University. http://www.bbc.co.uk/programmes/b0916ghq

Reischl, G. (2008). *El engaño Google: una potencia mundial incontrolada en Internet*. Medialive Content.

Riofrío Martínez-Villalba, J.C. (2015). El derecho al secreto y la teoría del cono. *Revista Derecom*, (19), 137-163.

Romm, T. (26 de abril de 2018). Facebook didn't read the terms and conditions for the app behind Cambridge Analytica. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facebook-didnt-read-the-terms-and-conditions-for-the-app-behind-cambridge-analytica/?noredirect=on&utm_term=.a0e590fccda2

Rosanvallón, P. (1999). *La Consagración del Ciudadano: Historia del sufragio universal en Francia*. Instituto de Investigaciones Dr. José María Luis Mora.

(2015). *El buen gobierno*. Manantial.

Samuel, A. (11 de marzo de 2016). Psychographics Are Just as Important for Marketers as Demographics. *Harvard Business Review*. https://hbr.org/2016/03/psychographics-are-just-as-important-for-marketers-as-demographics

Schwartz, M. (30 de marzo de 2017). Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate. *The Intercept*. https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/

Stahl, L. (22 de abril de 2018). Aleksandr Kogan: The link between Cambridge Analytica and Facebook. *CBS News*. https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/

Stewart, J. (5 de mayo de 2016). Facebook Has 50 Minutes of Your Time Each Day. It Wants More. *New York Times*. https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html

Sumpter, D. (2018). *Outnumbered: From Facebook and Google to fake news and filter-bubbles -the algorithms that control our lives*. Bloomsbury Sigma

Troncoso Reigada, A. (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*. Civitas-Thomson Reuters.

United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2014). *Fostering Freedom Online: The Role of internet Intermediaries. United Nations Educational, Scientific and Cultural Organization (UNESCO) y internet Society*. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Vaidhyanathan, S. (2011). *The googlization of everything (And Why We Should Worry)*. University of California.

Vogel, K., & Parti, T. (7 de julio de 2015). Cruz partners with donor's 'psychographic' firm. *Politico*. https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813

Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Science of the United States of America*, *112*(4), 1036-1040. https://doi.org/10.1073/pnas.1418680112

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Furure at the New Frontier of Power*. Public Affairs Books.

Zuckerberg, M. (21 de marzo de 2018). Muro de Mark Zuckerberg. *Facebook*. https://www.facebook.com/zuck/posts/10104712037900071

**NORMATIVA, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES**

Acordada Extraordinaria No. 66-18. Ag. 16, 2018, A.L.J.A (Arg.).

A.G. Res. 68/167, Derecho a la privacidad en la era digital (18 de diciembre de 2013).

Constitución Nacional [Const. Nac.] 1949 (Arg.).

Constitución Nacional [Const. Nac.], 23 de agosto de 1994, B.O. (Arg.).

Convención Americana de Derechos Humanos (Pacto de San José), 22 de noviembre de 1969, O.A.S.T.S. No. 36.

Declaración Universal de los Derechos Humanos, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (10 de diciembre de 1948).

Ley 8.871, Ley Sáenz Peña, 26 de marzo de 1912, B.O. (Arg.).

Ley 13.010, Ley del voto femenino, 27 de septiembre de 1947, B.O. (Arg.).

Portaria No. 02/2018, Inquérito Civil Público - ICP - Cambridge Analytica / Facebook, 20 de marzo de 2018 (Bras.).

Reglamento 2016/679, del Parlamento Europeo y Consejo de la Unión Europea del 27 de abril de 2016 relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016 O.J. (L 119) 1 (UE).