CUADERNO DE TRABAJO N° 13 / DICIEMBRE 2019

# Democracia y Protección de Datos Personales en la Era Digital

CONSEJO PARA LA TRANSPARENCIA

consejo para la Transparencia

CUADERNO DE TRABAJO N° 13 / DICIEMBRE 2019

# Democracia y Protección de Datos Personales en la Era Digital

CONSEJO PARA LA TRANSPARENCIA



Ediciones Consejo para la Transparencia, Santiago Chile
Diciembre, 2019

Elaborado por Carlos Carrasco,
Analista Dirección de Estudios CPLT

Diseño y Composición: Natalia Royer
ISSN 0719-4609

# Índice de Contenidos

# I. Presentación

Hoy nos encontramos en pleno proceso de transformación de amplios sectores económicos, políticos y sociales, mediante la digitalización de la información. Sin duda, es la era de la digitalización. Esto supone grandes desafíos para la sociedad en general. Uno de ellos es la pérdida de privacidad producto del explosivo aumento de artefactos tecnológicos que recaban constantemente información personal de los ciudadanos, lo que, a su vez, supone otro desafío: los datos recolectados pueden ser utilizados para manipular nuestras decisiones, tanto las del diario vivir, como las políticas. Así, los mecanismos y canales por los cuales los candidatos comunican sus mensajes al electorado se van modificando conforme avanza la incidencia de las tecnologías de la información. De los discursos en las plazas públicas se ha llegado al uso de redes sociales con mensajes directos a los usuarios.

Recientes investigaciones científicas de perfil psicológico confirman que se puede caracterizar individualmente a las personas utilizando sus datos personales y usar de manera muy eficaz esos datos, logrando transmitir mensajes diseñados a medida, con un alto grado de personalización y obteniendo la respuesta esperada por el destinatario. Esta que es una gran herramienta para conocer mejor a los electores y consumidores también puede representar un riesgo si es utilizada de manera inescrupulosa. Por de pronto, puede constituir un riesgo para la democracia, toda vez que los equipos de campañas electorales pueden manipular la información que obtienen de esos datos y que hoy tiene una profundidad, exactitud y variedad de fuentes de información nunca antes vista en la historia.

Los datos sobre nuestros ingresos, hábitos de compra, perfiles en redes sociales, empleo, preferencias y opiniones, entre otros, pueden juntarse, sintetizarse y venderse. Llevado al extremo, este proceso podría generar un perfil digital duradero que permita a quien lo construye conocer de mejor forma a las personas de lo que ellas mismas se conocen. De esta manera, mal utilizados, los datos personales se pueden transformar en una herramienta efectiva para socavar nuestro derecho a la autodeterminación y afectar nuestra libertad de decisión política para votar por uno u otro candidato.

Por esta razón, profundizando nuestro rol público en materia de protección de datos personales, el Consejo para la Transparencia se ha propuesto la tarea de investigar los distintos ámbitos en los cuales se necesita una atención especial en el resguardo de la privacidad de las personas, ya sea porque es necesario garantizar el derecho fundamental a que exista protección de la vida privada, así como las repercusiones que puede suscitar la falta de regulación en nuestro sistema político y electoral, pues entendemos que la democracia no se limita sólo al período de elecciones, sino que también implica debate, participación y desarrollo de institucionalidad.

Las personas basan sus decisiones y participación democrática en la información de la que disponen y si dicha información es deliberadamente manipulada a través del uso indebido de sus datos personales, sus decisiones posteriores podrían no ser genuinas.

En el presente documento, los analistas de estudios se adentran en los principales elementos que problematizan la relación entre Democracia y Protección de Datos Personales en la era digital, reflexionando acerca de las investigaciones que comenzaron a gestarse desde las ciencias sociales, pero que se traspasaron a los actuales asesores y consultores políticos para que -con evidencia científica- fuese más probable la elección de algún candidato. También analizan el rol decisivo que han asumido los datos personales para que, a través de algoritmos y la integración de un sinnúmero de bases de datos, puedan influenciar las decisiones políticas de los ciudadanos.

También indagan en la transformación y adaptación que han asumido los partidos políticos frente a la digitalización para no perder el nexo con la ciudadanía, la identificación de sus necesidades desde el comportamiento social visible, sus deseos y motivaciones, lo que evidencia un cambio de paradigma del control ciudadano.

Exploran las herramientas para lograr influenciar las decisiones de los ciudadanos y analizan estrategias para minimizar el riesgo que conlleva la digitalización, actualizando, por ejemplo, la legislación vigente, empoderando a la ciudadanía respecto al uso de sus datos personales y generando un mayor comportamiento ético por parte de organismos o empresas que tratan esos datos personales.

Dada la utilidad y los riesgos que se observan en la relación que se establece entre Democracia y Protección de Datos Personales en la era digital, consideramos que es tiempo de ir subsanando los vacíos regulatorios e informar a la ciudadanía sobre los eventuales riesgos que conlleva el desarrollo digital, para que así cada cual pueda disfrutar de sus beneficios y aceptar conscientemente sus riesgos o evitarlos, en la construcción de una sociedad mejor.

**Jorge Jaraquemada Roblero**
Presidente Consejo para la Transparencia

# 2. Manipulación política en la era de los datos

## 2.2 MANIPULACIÓN POLÍTICA

Desde su nacimiento, uno de los mayores esfuerzos de las ciencias sociales fue producir teorías con un poder predictivo genuino (Gorton, 2016). Tal fin, proporcionaría las herramientas necesarias para resolver los problemas más acuciantes de la sociedad. Bajo el optimismo de los avances científicos demostrados por las ciencias naturales, una serie de investigadores buscaron homologar su metodología y rigurosidad científica para aplicarla al comportamiento social: "las ciencias naturales han proporcionado cierto tipo de conocimientos que les permiten controlar su medio ambiente natural haciéndolo así más hospitalario y productivo, de la misma manera que las ciencias sociales permitirán a los hombres controlar su entorno social, haciéndolo más armonioso y congruente con las necesidades y deseos de sus miembros" (Gorton, 2016, p. 5). El intento de predecir el comportamiento de las personas levantó alertas entre quienes visualizaban este proyecto como una forma de dominación. La escuela de Frankfurt -liderada por Theodor Adorno[1]- planteó que tratar de comprender el entorno social mediante técnicas positivistas conllevaría solo a un conocimiento superficial de la realidad social. Además, definir las políticas sociales en base a la experimentación en ambientes controlados, crearía finalmente una sociedad de tecnócratas. La ciencia, en vez de emancipar al hombre de su ignorancia mediante el uso de la razón, se transformaría en una herramienta de manipulación, conteniendo en sí misma una profunda vocación antidemocrática (Ibíd.). No quedaba del todo clara la diferencia entre el poder de predicción y la manipulación.

Las críticas, sin embargo, no surtieron el efecto esperado. Para 1950 el desarrollo de un movimiento a favor de la experimentación para predecir del comportamiento humano era cada vez más importante al interior de las universidades. Un grupo de investigadores -liderados por David Easton- comenzaron a utilizar la observación controlada y la cuantificación del comportamiento político, a través de una serie de variables, como el voto, la formación de la opinión, el comportamiento de los grupos de interés, los partidos políticos y el proceso legislativo. Pese a ello, las investigaciones no ayudaron a comprender el comportamiento político de la ciudadanía debido a una serie de factores, tales como la falta de delimitación de los problemas políticos, la incapacidad para especificar la magnitud de las relaciones entre las variables o la imprecisión en la definición de éstas (Gorton, 2016). Así, los problemas políticos eran demasiado complejos como para reducirlos solo a modelos causales, por lo que a pesar de que las investigaciones aportaron una visión general del sistema político, la imposibilidad de los cientistas sociales para descubrir las leyes generales de la política y del comportamiento humano -tal como lo hacían las ciencias naturales- socavaron los intentos para predecir y controlar los fenómenos sociales en este ámbito.

Ahora bien, los intentos iniciales de predecir y controlar fenómenos sociales que no surtieron los resultados esperados en el siglo pasado, hoy comienzan a ser una realidad a través de la manipulación del comportamiento político de los ciudadanos realizada por consultores, técnicos e investigadores que trabajaban en campañas políticas modernas, los que utilizando las técnicas experimentales del siglo pasado y complementadas con las nuevas tecnologías empleadas en las campañas, están logrando una eficacia nunca antes vista para influenciar las creencias y conductas de los ciudadanos de cara a las elecciones democráticas.

Las investigaciones realizadas por los politólogos Alan Gerber y Donald Green en torno a la participación electoral, marcaron un precedente para basar las decisiones de campañas mediante evidencias científicas. En el año 2000, publicaron los resultados del estudio *"The effects of Canvassing, Telephone Calls, and Direct Mail on Votant Turnout"*[2] en el cual buscaban definir el método más efectivo para incitar a los ciudadanos a participar en las elecciones[3]. Los investigadores seleccionaron al azar a ciudadanos de la localidad de New Heaven, Estados Unidos, y utilizaron tres métodos para animarlos a votar: "puerta a puerta", "correo postal" y "llamadas telefónicas". El grupo de tratamiento se dividió en base a estos tres métodos. Pero además, cada grupo se subdividió para que recibieran diferentes mensajes: "deber cívico", "elección cerrada" y

[1] Para ver a Theodor Adorno y su vinculación con la Escuela de Frankfurt: https://www.uaeh.edu.mx/scige/boletin/prepa3/n8/m11.html

[2] Gerber & Green, 2000, Yale University.

[3] En términos de campañas políticas, un paradigma de estudio acerca de la influencia de los debates en las inclinaciones de voto, es lo sucedido en Nixon v/s Kennedy, donde el candidato demócrata, salió favorecido. https://www.abc.es/historia/abci-nixon-contra-kennedy-debate-si-cambio-historia-television-y-politica-201904240158_noticia.html

"solidaridad vecinal". A los destinatarios del mensaje "deber cívico" se les dijo que votar era su deber cívico y que la democracia dependía de la participación de la ciudadanía. A los que recibieron el mensaje "elección cerrada", se les dijo que cada año algunas elecciones sólo se deciden por unos pocos votos y que ellos podían marcar esa diferencia. Por último, a los que recibieron el mensaje "solidaridad vecinal", se les señaló que los políticos a veces ignoran los problemas de una comunidad si es que las personas de dicha comunidad no van a votar (Gorton, 2016). Los resultados del estudio determinaron que el método "puerta a puerta" fue un 13% más eficaz para incitar a los ciudadanos a votar que su símil del grupo de control. El contacto por correo postal sólo aumentó unos pocos puntos porcentuales, mientras que no se estipularon diferencias entre ambos grupos de llamados telefónicos. Además, dentro de los subgrupos, los que recibieron el mensaje "elección cerrada", tuvieron un 3% más de probabilidades de votar respecto a los que recibieron el mensaje "deber cívico" y un 7% más que los que recibieron el mensaje "solidaridad vecinal". Las conclusiones sugieren que incitar a los electores puerta a puerta era el método más eficaz para que los ciudadanos votasen. Además, esta condición se maximizaba si iba acompañada de un *slogan* que les dijese que el desenlace de la elección dependía de cada uno de ellos, debido a lo estrecha de la votación.

El estudio, basado en un experimento de campo, resultó innovador para la época, llamando la atención de varios asesores políticos, pues con él, las ciencias sociales pasaban a ser de gran ayuda para estudiar el comportamiento de los electores y obtener una mayor eficiencia en el proceso de las campañas políticas. Fue así que asesores e investigadores políticos se volcaron a estudiar diversas técnicas de investigación de las ciencias sociales, como el uso masivo de grupos focales para diseñar mensajes precisos que incentivasen a los ciudadanos a votar, o la indagación, mediante experimentos, de estructuras subconscientes que respondiesen a estímulos o frases correctamente delineadas. De todas estas investigaciones, destacó la publicación del libro *Get Out the Vote*[4], el cual resultó ser una guía -con evidencia científica- sobre la rentabilidad de diversas tácticas para publicitar anuncios políticos, dependiendo del grupo al cual iban dirigidos.

Si bien la aplicación de la ciencia a los problemas políticos fue rechazada por parte de académicos e investigadores durante sus primeros años, las campañas políticas modernas han comenzado a utilizar los hallazgos científicos para tratar de controlar y manipular a los electores de una manera precisa y efectiva. Las tácticas que hoy en día se utilizan para influir en los votantes se centran en la formación de opiniones políticas y de creencias de los ciudadanos, identificando o desencadenando procesos inconscientes. Con los experimentos de campo realizados, los asesores de campaña saben el tipo de público al cual enviar el mensaje y el tipo de mensaje correcto para incitar a los ciudadanos a votar. Los grandes volúmenes de datos que hoy se recolectan de las personas resultan fundamentales para generar perfiles exactos de ellos. Así se sabe cuál mensaje apretará el botón del inconsciente e incitará a los ciudadanos a votar por algún candidato.

## 2.2 BIG DATA

El predecir, controlar y manipular nuestras decisiones se hace más fácil si se tiene información respecto a cómo nos sentimos, cuáles son nuestros gustos o cuáles son nuestras expectativas futuras. Precisamente, hoy en día nos situamos en una era donde el flujo de información y la cantidad de datos que se generan es impresionante[5]. Tal es la magnitud del flujo de datos, que en 2016 se produjeron tantos como en toda la historia de la humanidad hasta 2015 (Helbing, 2017). Se generan navegando en sitios web, en el uso de plataformas como Facebook, WhatsApp o YouTube e, inclusive -la última tendencia- a través de nuestros artefactos cotidianos: el internet de las cosas. Todo está conectado a la red. Se estima que en 10 años más habrá 150.000 millones de sensores produciendo una infinidad de datos. Ya no solo habrá teléfonos inteligentes, sino también casas inteligentes, empresas inteligentes y ciudades inteligentes. Es tanta la cantidad de datos que ni si quiera los humanos podemos procesarlos. Esa función la están asumiendo los algoritmos informáticos.

El desarrollo de algoritmos inteligentes proviene desde la década de los cuarenta del siglo pasado. Norbert Wiener se abocó al estudio de los sistemas de comunicación y control de seres complejos, la denominada cibernética. Advirtió que los fenómenos de retroalimentación y la sincronización, mediante una secuencia ordenada de instrucciones, son posibles de encontrar en la naturaleza, en la sociedad y en las máquinas, puesto que estos procesos -los algoritmos- son necesarios para mantener la organización y estabilidad de cualquier organismo, independiente de su naturaleza (Rajsbaum & Morales, 2016). El impulso de algoritmos aplicados a las máquinas ha sido fundamental para desarrollar y diagnosticar sistemas complejos adaptables al entorno, como la emergencia de la Inteligencia Artificial, al punto de emular las operaciones cerebrales, lo que hoy se conoce como las "redes neuronales". Incluso, existen corrientes filosóficas -que cada vez tienen mayor preponderancia en la comunidad científica- basadas en los algoritmos: el "Dataísmo". Esta corriente sostiene que "el universo consiste en flujos

[4] Green & Gerber 2015.

[5] En un minuto, en el mundo se realizan 3.877.140 búsquedas en Google, se reproducen 97.222 horas de videos en Netflix, se miran 4.333.560 videos en YouTube, se escriben 473.400 tweets en Twitter, se publican 49.380 fotos en Instagram, se generan 73.249 transacciones en internet, entre otros datos. https://business-intelligence.grupobit.net/blog/cuantos-datos-se-producen-en-un-minuto

de datos y que el valor de cualquier fenómeno está determinado por su contribución al procesamiento de datos" (Harari, 2018, p.400). Al igual que Wiener, plantean que las mismas leyes matemáticas rigen tanto para los seres vivos como para las máquinas. Por lo tanto, el mundo puede ser entendido a través de los algoritmos y los flujos de información. Así, cosas tan diversas como la economía, la música o la astronomía, tienen un denominador común: una estructura basada en un flujo de datos y del cual se puede estudiar y sacar provecho.

Para Han (2018), el "Dataísmo" sería algo así como un totalitarismo digital. Toda la vida se vuelve cuantificable: la temperatura corporal, la glucosa en la sangre, el consumo de calorías, la cantidad de horas dormidas, el rendimiento corporal, los estados emocionales y un largo etcétera. El "Dataísmo" considera que los datos liberan al conocimiento de cualquier intuición, conduciéndolo a una plenitud. La teoría, entonces, empieza a sobrar: "Adiós a toda teoría del comportamiento humano, desde la lingüística hasta la sociología. Olvida la taxonomía, la ontología, la psicología. ¿Quién sabe por qué la gente hace lo que hace? La cuestión es que lo hace y que podemos seguirlo y medirlo con una fidelidad sin precedentes. Con suficientes datos, los números hablan por sí mismos" (Anderson en Han, 2018). La presunción de entender todo mediante los números es para Han algo vacuo, pues, los números no implican necesariamente una "narración".

Para los asesores políticos, los datos representan infinitas posibilidades. Las clásicas encuestas de opinión no reflejan en tiempo real las motivaciones y necesidades de la cambiante sociedad. Resulta costoso realizar permanentemente encuestas para tratar de inferir las necesidades y preferencias de los ciudadanos. Además, los rápidos avances en el poder de los procesadores desde la mitad de la década de 1990, el surgimiento de la banda ancha desde el 2000, la explosión de los teléfonos inteligentes en el 2007 y la popularización de las redes sociales desde el 2010, abrieron las puertas para el tránsito del enorme flujo de información. Los investigadores ya no tienen la necesidad de invertir grandes sumas de dinero para recabar información. Son los mismos ciudadanos los que la ponen a disposición: "cada vez que prendemos el teléfono, que hacemos *"clic"* o seleccionamos uno u otro botón en la pantalla, estamos generando información. Los datos pueden ser usados de maneras muy distintas: para vendernos algún producto, para conectarnos con ciertas personas, para diseñar ciertas políticas públicas y, también, para manipularnos" (Luna, 2019). Es cada vez más común que en política se utilice el análisis de datos para dirigir a los ciudadanos hacia un comportamiento específico. Es lo que se conoce como *Nudding* o "pequeño empujón": una forma moderna de paternalismo. Sus defensores consideran que las personas no toman buenas decisiones, por lo tanto, hay que ayudarlas. Sin embargo, *Nudding* explota las debilidades psicológicas para conducirnos a comportamientos específicos. Es una forma moderna de conductismo (Helbing, 2017). Pero a diferencia de un sistema de recompensas y castigos, el "pequeño empujón" se sostiene, a juicio de Helbing, mediante una burbuja: con información personalizada se controla nuestro pensamiento. Con precios personalizados podemos ser castigados o compensados. Con el análisis de la información que se encuentra en la red se influencia a los individuos a tomar decisiones que comúnmente no tomarían.

*Big Data* es la integración y análisis, mediante algoritmos complejos, de un entramado gigantesco de datos de diversa naturaleza. A diferencia de la estadística, el *Big Data* trasciende la mera percepción u opinión, logrando -a través de un análisis de minería de datos- un poder predictivo mucho mayor, más fiable y con mayor exactitud. Cada acción que una persona realice en el mundo digital deja una huella. No es difícil, por lo tanto, triangular cada fuente de datos para generar perfiles e influenciarnos a realizar alguna acción mediante tácticas de inducción. Nuestra huella digital está definiendo lo que pensamos, lo que sentimos y lo que somos. Han está en lo cierto cuando asemeja el *Big Data* al *Big Brother* de Orwell. Los datos siguen aumentando. La vigilancia política, cual panóptico[6], se ejerce sutilmente, pues somos nosotros mismos los que ponemos a disposición nuestros datos personales.

[6] Según Foucault, el panóptico o panoptismo, en un contexto carcelario, es "inducir en el detenido un estado consciente y permanente de visibilidad que garantiza el funcionamiento automático del poder. Hace que la vigilancia sea permanente en sus efectos, incluso si es discontinua en su acción" (Foucault, 2012, p. 233).

# 3. Datos personales y vigilancia política

## 3.1 PARTIDOS POLÍTICOS: DE LO TRADICIONAL A LO TECNOLÓGICO

La vigilancia electoral es parte de la evolución de las campañas políticas. Desde los cimientos de la democracia moderna en el siglo XIX, los partidos políticos han recabado información de sus electores como una forma de conexión, de compromiso y entendimiento de sus necesidades (Rosanvallon, 2017). De otra forma, se corre el riesgo de que canalicen demandas escindidas de lo que plantean sus miembros. Sin embargo, en las últimas décadas, los partidos han perdido influencia como un canal legítimo de representación ciudadana. Como ocurre con otras instituciones políticas, se ha perdido la confianza en ellos[7].

Los partidos han enfrentado, con distintas estrategias, la desconfianza ciudadana (y la respectiva pérdida de adherentes), adaptándose a las nuevas formas de comunicación, transformándose la explosión tecnológica en una disyuntiva para su legitimidad política. Los partidos más tradicionales, han visto a Internet como una forma de descentralización de la comunicación política, por lo tanto, como una pérdida de control y poder (Gerl, 2017). Son los que presentan mayor conflicto con las expectativas de los ciudadanos -considerando que éstos utilizan la tecnología para canalizar sus deseos y necesidades- al no aprovechar "la comunicación instantánea" e informarse en tiempo real de las demandas ciudadanas. Pero otros han sabido leer estratégicamente el surgimiento de tecnologías como Internet, aprovechando de contrarrestar la distancia existente con la ciudadanía, ofreciendo nuevas formas de interacción social, organización y participación, por ejemplo, mediante el análisis de redes sociales. Precisamente, son estos partidos los que han utilizado el poder del *Big Data,* los algoritmos y el *Microtargeting,* innovando en la recolección de información de los ciudadanos. En todo esto hay una delgada línea entre el tratamiento de datos de forma impersonal o estadística y la comercialización de metadatos de forma ilícita, tal como lo afirma la Comisionada del Instituto Nacional de Acceso a la Información y Protección de Datos Personales de México, Patricia Kurzcyn[8]: "el problema es que se recaban los datos a través de las credenciales de un elector con el objetivo de reunir firmas para formar partidos políticos. Y ahí hay quienes venden los bancos de datos (...). Es muy famoso en México, como se encontró hace varios años, una persona en un mercado que vendía una base por 10 mil pesos (mexicanos) y que contenía la información de millones de mexicanos que teníamos credencial de elector[9]".

Lo cierto es que comienza a vislumbrarse una tendencia general de los partidos políticos para modificar sus estructuras internas y adaptarse a los nuevos desafíos tecnológicos: desde la creación de sitios web hasta la generación de equipos para producir material audiovisual que pueda ser puesto a disposición de seguidores o partidarios para distribuirlo por redes sociales. Otra tendencia, que cada vez ocupa un rol más importante para los partidos, apunta a la participación *online* de los ciudadanos, pero sólo como un "proceso de afiliación de primer nivel" (Ibíd.), ya que la participación utilizando medios tecnológicos no significa necesariamente adhesión, pero sí un medio para inscribir o captar militantes.

## 3.2 CONTROL Y VIGILANCIA POLÍTICA

La vigilancia política no es algo nuevo. En el transcurso de la historia se ha vigilado políticamente a los ciudadanos para la consecución de diversos fines. Por ejemplo, en el seno de la industrialización, para aumentar el rendimiento y la producción, se vigilaba a los sujetos para someterlos a un "código de normas, preceptos y prohibiciones, eliminando desviaciones y anomalías" (Han, 2018). Foucault (2012), describió a esta sociedad como "disciplinaria", cuyo ámbito de vigilancia y control se ejercía en todas las esferas de la vida: reproducción, tasas de natalidad y mortalidad, nivel de salud, esperanza de vida, etc. A este férreo control, Foucault lo denominó la "Biopolítica": una forma de poder político que administra a la población, la adiestra o disciplina en función del modo del producción industrial. Pero, en la actualidad, el

[7] De acuerdo a MORI (mayo 2019), un 5% de los encuestados confía en los partidos políticos, un 7% en Senadores y Diputados. https://m.elmostrador.cl/media/2019/05/INFORME-BAROMETRO-DE-LA-POLITICA-2019-compacto.pdf

[8] Patricia Kurzcyn, Comisionada INAI. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019.

[9] En Chile una situación similar genera debate cada cierto tiempo: la publicación de datos personales por el Servicio Electoral (RUN, sexo, domicilio electoral) en el marco de la Ley Sobre Inscripciones Electorales; pues en base a ello se ha abierto un flanco para la emergencia de sitios web que publican estos datos y los vinculan a otros. Para mayor información ver: https://datosprotegidos.org/servel-y-proteccion-de-datos-personales/

modo de producción ha cambiado. Ya no se necesita controlar el cuerpo y sus movimientos para obtener el máximo rendimiento. Cada vez más se producen cosas "intangibles". Se ofrecen servicios y experiencias. El control del cuerpo cede ante el control de la psiquis. "Para incrementar la productividad no se superan resistencias corporales, sino que se optimizan procesos psíquicos y mentales" (Han, 2018, p.42). En base a ello, Han sostiene que la noción de Biopolítica -junto con el control y vigilancia poblacional en base a mediciones estadísticas- ya no es adecuada para la sociedad digital. La Biopolítica es reemplazada por la Psicopolítica. La estadística como forma de control poblacional se reemplaza por el *Big Data:* ahora es posible escudriñar lo que antes no se podía: nuestros deseos y motivaciones.

La estrategia de la vigilancia política actual, por lo tanto, no se ejerce para delimitar (o disciplinar), sino para fomentar, en palabras de Han, un "desnudamiento voluntario". El antiguo panóptico de Bentham, que desde una torre central observaba privilegiadamente a todos los prisioneros, sin saber estos si efectivamente eran vigilados o no, ya no es efectivo, pues está ligado a un "medio óptico": se puede vigilar el comportamiento, el movimiento del cuerpo, pero no puede acceder al pensamiento o las necesidades internas. En razón de ello, se ha desarrollado un panóptico digital, donde Internet es el repositorio de los datos que, voluntariamente, las personas alimentan con su información. En este sentido, a la vigilancia política ya no es posible vincularla con la noción de Estado Vigilante. Con el panóptico digital, surge la "autovigilancia". Así, con la digitalización y el *Big Data*, la vigilancia es mucho más eficiente, posibilitando la observación no sólo lo que está a la vista, sino también de nuestras motivaciones, deseos, proyectos o incluso nuestros estados de ánimo, que voluntariamente ponemos públicamente a disposición mediante la red.

La efectividad de la Psicopolítica para vigilar a los ciudadanos culmina con el uso utilitario de las emociones humanas. Aparte de comunicarse con otras personas, realizar compras en línea o la búsqueda de información sobre intereses, la red se ha utilizado para una repentina descarga de afectos. Las emociones, al ser más rápidas, volátiles y situacionales, permiten estimular de mejor forma el consumo. De ahí que hoy en día ya no se consuman cosas (o candidatos), sino "emociones". La racionalidad se opone a que los sujetos puedan descargar sus deseos o motivaciones personales en la red. En cambio, la emoción -más impulsiva- otorga el acceso a la vigilancia política de nuestra psiquis. Con los repositorios modernos de información, como Facebook, Twitter, Amazon o WhatsApp, un candidato, fácilmente mediante el análisis de datos, puede alinearse con las emociones de un electorado para hacer más probable su candidatura.

## 3.3 FACTORES QUE CONTRIBUYEN A MÁS VIGILANCIA POLÍTICA

En algunos países existe una mayor tendencia a la vigilancia en periodos electorales. Si bien es un tema difícil de generalizar, dado el halo de secretismo que puede rodear a los partidos políticos, la tendencia de vigilancia política proviene principalmente de Estados Unidos, por una serie de factores. Algunos de ellos pueden, probablemente, extrapolarse a otras realidades (Bennett, 2013).

**a) Ausencia de una ley integral de protección de datos personales.** Sin una legislación integral que regule el tratamiento, uso y tráfico de los datos personales, se posibilita que entidades privadas o agencias gubernamentales controlen el comportamiento de la sociedad. El seguimiento de todas las actividades de las personas, a causa del registro de sus datos, puede afectar la dignidad humana de un ciudadano, puesto que sus decisiones ya no serían libres y la autodeterminación informativa de los sujetos sería abolida. Un ejemplo de ello es el sistema de puntos que se está implementando en China (Helbing, 2017): en dicho país, y desde 2018, todos los ciudadanos son clasificados en un sistema de crédito social. Si un ciudadano sigue un tipo de comportamiento impulsado por el gobierno, se le asignan puntos, en caso contrario, se le descuentan. Los registros que determinen que una persona en China sea buen ciudadano o no, "pueden ser sus hábitos cívicos, su estilo de vida, los sitios web navegados, lo que se compra por Internet y otros datos como las multas de tráfico"[10]. Sin una regulación integral que proteja la información personal de los ciudadanos, las decisiones equivocadas desde la perspectiva de los gobiernos o las empresas, tendrían consecuencias negativas, lo que restringiría su comisión y, por lo tanto, el grado de libertad para tomarlas. Otro problema descrito por Helbing sería que el principio de presunción de inocencia estaría obsoleto; pues los algoritmos -no exentos de errores- pondrían en tela de juicio la equidad y la justicia, siendo estos conceptos reemplazados por un nuevo tipo de arbitrariedad. El pluralismo democrático también se vería afectado y la cultura local y el comportamiento ya no serían dependientes del contexto.

**b) Leyes liberales sobre el financiamiento de campañas políticas.** En algunos países que poseen un sistema permisivo de financiación de campañas, es probable que se utilice el dinero donado para una mayor táctica de vigilancia política (Bennett, 2013). Al no existir restricciones sobre la cantidad de dinero que pudiese gastar un candidato para sus campañas electorales, ni la cantidad de dinero que aportan personas naturales o jurídicas, aumentarían considerablemente los fondos disponibles para que los partidos políticos

[10] https://www.elmundo.es/tecnologia/2018/10/31/5bd8c1bfe2704e526f8b4578.html

construyan y actualicen un sistema de gestión de electores y efectúen una mayor vigilancia política, por ejemplo, generando perfiles de electores utilizando e integrando múltiples bases de datos públicas y privadas. Así, sin una Ley de Protección de Datos Personales que regule el procesamiento de datos políticos y comerciales, sumado a pocas restricciones sobre el financiamiento de campañas políticas, se fomentaría el uso de vigilancia política.

**c) Mercado de datos personales y sensibles.** El uso extensivo de bases de datos obtenidas del marketing comercial complementan la información de datos políticos, como la afiliación y el comportamiento partidario. Existen empresas dedicadas exclusivamente a extraer datos personales de fuentes "no políticas" mediante sofisticados algoritmos que permiten inferir el comportamiento electoral. Una de estas empresas es *Aristotle*[11], que ofrece servicios de microtargeting en base a una lista de más de 5 millones de electores que están suscritos a diversas revistas de una variada gama de temáticas: religiosas, de salud, financieras o culinarias (Bennett, 2013). La integración entre datos políticos y comerciales permite el desarrollo de mensajes personalizados (microtargeting) mediante plataformas digitales como el correo electrónico, banners publicitarios en sitios web y las redes sociales[12].

**d) Uso de herramientas analíticas y de minería de datos *(Data-mining).*** En los últimos años ha proliferado una variada gama de programas informáticos, cuyo fin es recolectar datos personales -desde los registros electorales de ciudadanos a los datos sensibles- para elaborar perfiles y categorías políticas; y establecer contactos directos con los "interesados". Los partidos políticos cada vez más utilizan el software informático con el fin de identificar grupos de interés o electores indecisos para dirigir los mensajes políticos (ICO, 2018). Diversos partidos políticos de Estados Unidos, Canadá y Reino Unido utilizan estos programas. *"Voter Vault", "Liberalist" "Contact Creator", "Electrac"* o *"Feedback"* son softwares de este tipo. Las empresas "venden" a los partidos completísimas herramientas analíticas. Google, con su *"Political Campaing Software"*, indica que su programa "permite dirigir el mensaje de su campaña a las personas adecuadas en el momento adecuado; llegar a los electores comprometidos de todo el mundo en una sola cuenta; dirigir sus anuncios geográficamente o por demografía y crear mensajes únicos para electores, donantes o voluntarios (Bennett, 2013). *"NationBuilder"* es otra herramienta de gestión de campañas que indica que su software es necesario porque "la gente ya no está prestando atención a los anuncios, sino que está prestando atención a otra gente real" (Ibíd.). Éste también ofrece una función que permite a los partidos comparar la información de contacto con los datos de software de redes sociales como Facebook o Twitter (ICO, 2018). En Chile, la empresa *"Instagis"* fue utilizada en las elecciones municipales y parlamentarias en 2016 recabando datos diversos como el RUN, domicilio y preferencia política para efectuar microtargeting electoral[13].

[11] Empresa Estadounidense que ofrece servicios de microtargeting y análisis de datos: http://aristotle.com/

[12] De acuerdo a la Encuesta Protección de Datos Personales 2018 del Consejo para la Transparencia, 10% de los organismos públicos que contestaron han celebrado convenios de entrega y/o acceso de Datos Personales, de estos, la principal información intercambiada en los convenios corresponde a antecedentes comerciales de las personas (31%).

[13] https://ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/

# 4. Nuevas formas de manipulación y vigilancia política

## 4.1 CAPTURA E INTEGRACIÓN DE DATOS PERSONALES

Históricamente, los partidos políticos han mantenido un registro de sus miembros para diversos fines, como aportar con ideas para el desarrollo de un programa político; recaudar fondos para campañas; operaciones para captar electores "puerta a puerta"; reclutamiento de voluntarios, etc. Hoy en día estos registros se están ampliando, incluyendo personas que no son -ni serán- miembros de un partido. Empresas dedicadas a esta tarea, aparte de usar información de fuentes tradicionales -como el padrón electoral- han complementado esa información con encuestas telefónicas, cartas a periódicos, base de donantes y registro de direcciones. También han fusionado esos registros con otros provenientes de buscadores de Internet, como *Google*, datos de *Facebook; Twitter, Youtube, Whatsapp,* etc., además de listas georreferenciadas para correo electrónico y mensajes de texto a telefonía móvil, generando completas bases de datos de electores que, posteriormente, se venden a interesados: "Una vez que la información de mis datos la están recopilando empresas, después asesoran con los datos la construcción de encuestas, y luego las manipulan. Este tipo de información les permite conocer cuáles son las preferencias electorales de las personas y sus preocupaciones" (Comisionada INAI, Patricia Kurzcyn).

Según Bennett (2015), existen cuatro tendencias en las cuales los partidos podrían aprovechar las tecnologías de información y recabar datos de los ciudadanos para elaborar perfiles y categorías, y con ello, persuadir a segmentos cada vez más acotados, pero claves para ganar una elección. La diversidad de fuentes desde donde se puede obtener información personal va a depender de la rigurosidad de las leyes sobre el tratamiento de datos personales, así como la regulación de fondos disponibles para las campañas que permiten actualizar permanentemente las bases de datos de electores.

### 4.1.1 Información personal extraída de las redes sociales

Los partidos políticos están apostando por el uso de las "redes sociales" como una forma más económica de comunicarse con la ciudadanía (Lobo, 2017). Extraen datos por la propia información que generan los usuarios en sus perfiles. Sin embargo, uno de los mayores valores que otorga la publicidad por medio de estas redes es la credibilidad cuando apuntan a electores específicos o nichos de ciudadanos que comparten ideas. Esto hace aumentar el número de seguidores que tiene un candidato, cautivando a otros electores indecisos. Otro valor potencial de las campañas por redes sociales es la utilización de las conexiones de los usuarios (listas de amigos) para compararlas con bases de datos de electores. Así, en vez de enviar publicidad a un solo elector, se le puede enviar a todo su círculo de amigos bajo la evidencia que los electores se ven influidos, más que por el mensaje en sí, por las decisiones de su grupo de pares.

No obstante, las redes sociales presentan algunos riesgos para la comunicación y diseminación de información verídica y confiable. Es el caso de las noticias falsas *(Fake News)*. Éstas son una forma tecnificada de rumor que son facilitadas por la proliferación de artículos instantáneos que se pueden subir a un servidor de una red social (Lobo, 2017). Las noticias falsas actúan como formadoras de opinión "captando la atención para ganar dinero con publicidad y ejercer influencia política" (Lobo, 2017, p.41). Al contrario de lo que puede pensarse, el objetivo de las noticias falsas no es difundir información errónea, sino que ésta sería un vehículo para fortalecer lazos y reforzar ideas con personas que comparten la misma forma de pensar (Ibíd.). Es decir, generar comunidad en torno a una visión de mundo.

Otro riesgo son los llamados "burbujas de filtro", que también se encuentran presentes en las prácticas de microtargeting. Implica rodearse de personas que comparten las mismas ideas. Tanto las redes sociales como la práctica del *microtargeting,* al generar categorías de electores, crean una visión sesgada de la realidad, polarizando las posturas. Los *social bots*[14] también ponen en jaque el uso masivo de las redes sociales para fines políticos. Es una nueva forma de automatización de la agenda política al impulsar temas mediante mensajes repetitivos para generar reacciones de los usuarios. Lo anterior permite que la prensa publique artículos respecto a los temas generados por robots en las redes influyendo en la política. Por otra parte, la cantidad de seguidores en redes sociales no implica realmente que los mismos van a votar por un candidato, desvirtuando los pronósticos electorales.

[14] Social Bots es un *software* que ejecuta mensajes automatizados en Internet, defender ideas o actuar como un seguidor de usuarios. Además pueden generar cuentas falsas para captar seguidores. Se estima que entre un 9 a un 15 por ciento de las cuentas de Twitter pueden ser bots sociales: https://www.distilnetworks.com/glossary/term/social-media-bots/

### 4.1.2 Aplicaciones móviles (Apps)

La irrupción de teléfonos inteligentes junto a las aplicaciones móviles a fines de la década pasada, también está modificando la forma en que se realizan las campañas, siendo cada vez más intrusivas. Los partidos han utilizado las aplicaciones generalmente para "enviar mensajes políticos tradicionales; la prospección puerta a puerta; la gestión de eventos; fomentar donaciones y promover una mayor participación cívica" (Bennett, 2013, p. 10). Pero no sólo los partidos utilizan aplicaciones móviles[15] para efectuar propaganda o captar voluntarios de campaña, sino que los propios candidatos también han desarrollado sus propias aplicaciones para promocionar sus campañas mediante notificaciones periódicas que permiten a los seguidores mantenerse informados con las actividades de campaña[16].

El desarrollo de las aplicaciones plantea un riesgo a la privacidad de los usuarios y sus datos personales en la medida que las listas de contactos, fotografías o datos de geolocalización pueden fácilmente difundirse sin el consentimiento de los usuarios[17]. Además, las características actuales de las aplicaciones móviles permiten a los desarrolladores, proveedores de servicios y las empresas de publicidad, acceder a información personal. La información sobre afiliación política puede ser utilizada, sin consentimiento expreso, por parte de voluntarios y trabajadores de campaña. Por ello, los desafíos en esta materia se encuentran en informar a los usuarios -mediante un consentimiento informado- sobre sus derechos de privacidad y motivar a las plataformas móviles que incorporen requisitos de privacidad en el contrato de uso de dichas plataformas.

### 4.1.3 Internet de las cosas

Hoy en día las direcciones web son prácticamente ilimitadas. Cada cosa u objeto se puede vincular a una dirección web. Por ello se sostiene que "las cosas se convierten en proveedores activos de información" (Han, 2018, p. 95). Con la irrupción de la web 3.0 las cosas también nos vigilan. Por ejemplo, en Chile se estimó un proyecto para dotar a las casas con "medidores inteligentes"[18] con la promesa de mejorar la gestión energética de los hogares. Esto se realizaría, a través de un completo monitoreo y traspaso de información hacia un sistema central para realizar diversos procesos comerciales y técnicos[19]. En otras palabras, se mejoraría la eficiencia energética capturando nuestros hábitos de consumo eléctrico.

Al principio, los motores de búsqueda estaban orientados a buscar información mediante directorios. Había que saber la dirección web para ingresar a algún sitio. El ranking de búsqueda patentado por Google, *PageRank*[20], fue el primer indicio para saber las preferencias de las personas. Así, las empresas empezaron a ofrecer sugerencias personalizadas de productos y servicios. Con la acumulación de datos, los algoritmos de búsqueda se volvieron cada vez más sofisticados, permitiendo ya no solo recabar información de las páginas web que visitamos, sino también, de las cosas. Según Evans (2011), en el año 2003 había aproximadamente 6,3 mil millones de personas en el planeta y una cantidad de 500 millones de dispositivos conectados a Internet (0,08 dispositivos por personas). En 2010 la población mundial aumentó a 6,8 mil millones y había una cantidad de 12,5 mil millones de dispositivos conectados a internet (1,84 dispositivos por persona) superando los dispositivos la cantidad de personas por primera vez. Se proyecta que para el 2020 habrá una cantidad de 7,6 mil millones de personas y 50 mil millones de dispositivos (6,58 dispositivos por persona).

La proliferación de hogares, edificios, e inclusive ciudades inteligentes, pone a disposición de las empresas de análisis de datos una cantidad inimaginable de datos personales[21]. De ahí surge para Han (2018) la idea de que nos encontramos ante un nuevo Panóptico Digital que posibilita la vigilancia desde todos los ángulos, incluso, de nuestra psiquis. Esta pérdida de privacidad significa la pérdida de la libertad, como ya se ha planteado.

### 4.1.4 Comercio digital

La vigilancia traspasa las fronteras meramente relacionadas con los asuntos de Estado, deviniendo también en un negocio. "Los datos personales se capitalizan y comercializan por completo" (Han, 2018, p. 98). En este sentido, la vigilancia, mediante la recolección de información,

[15] Por ejemplo: The Obama of America App (Estados Unidos); Mi PSOE (España); Lágora (Chile).

[16] https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0719-367X2017000200019

[17] Comúnmente, los usuarios no leen los términos de uso de las aplicaciones, en los ítems que faculta el uso de datos que los mismos usuarios generan. https://tecnobitt.com/legalidad-en-apps-moviles/

[18] La Ley 21.076, aprobada en enero de 2018, estableció que los medidores inteligentes y empalmes pasarían a ser propiedad de las empresas (históricamente los dueños de los medidores habían sido los usuarios) y los clientes deberían pagar por dichos dispositivos, a través de las tarifas. Frente a los reclamos ciudadanos por esta situación, se decidió posponer la instalación de los medidores inteligentes. Finalmente, el gobierno despachó un proyecto de ley (Ley de Distribución Eléctrica) para solventar el tema que se encuentra en segundo trámite constitucional en el Senado. https://ciperchile.cl/2019/03/01/instalaran-nuevos-medidores-inteligentes-de-electricidad-el-costo-de-us1-000-millones-sera-asumido-por-clientes/

[19] https://www.electricas.cl/medicioninteligente/

[20] https://www.link-assistant.com/news/google-page-rank-2019.html

[21] Por ejemplo, algunos refrigeradores inteligentes, pueden recomendar recetas acorde a las preferencias alimentarias, informar la caducidad de los alimentos, mostrar ofertas para agregarlas a una canasta de compra y comunicarse con otros artefactos del hogar. Para más información ver: https://www.xataka.com.mx/domotica/el-nuevo-refrigerador-inteligente-de-samsung-ahora-podra-controlar-toda-la-casa-recomendar-recetas-y-servir-como-altavoz-hi-fi

difumina lo político con lo económico. Han sostiene que la empresa Acxiom comercializa los datos personales de aproximadamente 300 millones de ciudadanos estadounidenses, agrupando a los individuos en más de 70 categorías: "Aquellos con un valor económico escaso se les denomina *Waste,* es decir, "basura". Los consumidores con un valor de mercado superior se encuentran en el grupo *Shooting Star.* Son dinámicos, de 36 a 45 años, se levantan temprano para hacer *footing,* no tienen hijos, están casados, les gusta viajar y la serie de televisión *Seinfeld*" (Han, 2018, p.99).

Hasta el 2018, el comercio digital influyó hasta el 56% de las ventas en las empresas (ProChile, 2018). Y una de las mayores tendencias actuales en las transacciones electrónicas es el pago mediante aplicaciones móviles, utilizando huellas dactilares y reconocimiento facial. Empresas como Starbucks, Amazon, PayPal, Samsung, Visa ya están implementando los pagos mediante aplicaciones móviles. El uso de Inteligencia Artificial para recabar información en este tipo de transacciones permitirá la segmentación del comercio minorista para dirigirse a grupos predefinidos cada vez más acotados: "A medida que las marcas y los minoristas mejoran el aprovechamiento de los datos de consumo y de comportamiento, las iniciativas de comercio electrónico se dirigirán de forma mucho más específica, acercándose a la idea, antes imposible, del marketing uno a uno" (ProChile, 2018, p.11). El comercio digital se transforma así en un gran repositorio de datos financieros que puede ser aprovechado para generar no sólo perfiles económicos, sino que también para complementar los perfiles políticos.

## 4.2 MICROTARGETING: MANIPULACIÓN Y DESINFORMACIÓN TÁCTICA PARA SOCAVAR LA DEMOCRACIA

### 4.2.1 ¿Qué es el *microtargeting* político?

"En 2012 *The New York Times* informó que tanto la campaña presidencial de Obama como la de Rommey en Estados Unidos estaban utilizando el *microtargeting* para desarrollar perfiles de electores con el objetivo de identificarlos e influir en su decisión política" (Gorton, 2016). Las campañas políticas utilizan cada vez más sofisticadas estrategias para influir en los electores basándose en su información personal. El *microtargeting* consiste en ello: recopilar información sobre los posibles electores y utilizarla para mostrarles, a través de medios electrónicos, anuncios políticos específicos (Zuiderveen, 2018). Se podría decir que el *microtargeting* es una forma moderna de marketing político. También podría ser definido como una herramienta que utilizan los partidos políticos para focalizar segmentos acotados de la población e influir en la elección de un candidato particular. Sin embargo, para que el *microtargeting* sea efectivo debe contener dos supuestos: analizar el segmento correcto de la población a la que se debe enviar información y definir cuál es el mensaje indicado para incidir lo máximo posible en la votación. Para dicho objetivo, los partidos, asesores y colaboradores políticos basan su estrategia en el análisis de datos obtenidos de la información personal de los electores: datos sociodemográficos (registro electoral, dirección, sexo, edad, tamaño familiar); datos comerciales (ingresos, hábitos de gasto de tarjetas de crédito, número de automóviles, tiendas visitadas, suscripciones a revistas) y datos del comportamiento *online* (búsqueda y visitas a sitios web, compras en línea, interacciones en redes sociales, usos del botón "me gusta"), son habitualmente utilizados para efectuar campañas personalizadas, el cual -mediante un complejo entramado de algoritmos- orienta al analista de datos a decidir la forma correcta de marketing político. Así, el *microtargeting* se efectúa en base a un modelo probabilístico aplicado a los electores en el cual cada elector obtiene un puntaje que refleja la probabilidad de que exhiba el comportamiento que se ajusta a la categoría de electores (Ibíd.). Lo anterior permite a las campañas focalizar mensajes persuasivos en aquellos electores que -probablemente- están indecisos respecto a qué candidato votar y establecer estrategias de comunicación efectivas en base a los recursos de la campaña. En países donde existen pocas leyes de protección a la privacidad es más fácil adquirir bases de datos políticas y comerciales para poder extraer inferencias precisas respecto a la posible afiliación política. "Una periodista encontró cómo la publicidad se va dando diferente para su papá, para su abuelo y para ella. Entonces con esto se van formando las estadísticas, se van formando las encuestas, son datos que se van recopilando y luego se hace una publicidad que va muy direccionada para que una persona pueda cambiar su preferencia de voto" (Comisionada INAI, Patricia Kurzcyn).

Cada vez es más frecuente que las elecciones se decidan en base a electores indecisos o circunscripciones claves. Los partidos están cambiando la forma de comunicarse con los electores. En vez de hacerlo mediante medios de comunicación masivos, han optado por "personalizar los mensajes e interactuar y atraer a los electores de forma individualizada" (Bennett, 2015, p. 6). Dicha segmentación, por grupos o categorías, permite que las campañas comprendan a los grupos de ciudadanos necesarios para ganar una elección. Raymond Duch, investigador de la Universidad de Oxford, nos plantea cómo opera el *microtargeting:* "Hay muchos estudios que evidencian que los electores pueden ser influenciados a través del microtargeting. Tú puedes seleccionar un set de mensajes personalizados a un grupo con bajo nivel educacional, bajos ingresos, con condiciones precarias de vida y ver cuál mensaje funciona mejor. También puedes enviar a otro grupo completamente distinto, con mayor educación, nivel cultural o riqueza, un set de mensajes completamente diferentes y observar cuál mensaje es mejor. Entonces, no importa la diferencia de caracterización socioeconómica, ya que los mensajes son absolutamente personalizados al grupo que se envían, haciendo más probable la manipulación"[22].

[22] Entrevista realizada a Raymond Duch, Universidad de Oxford.

El *microtargeting* es posible hoy en día gracias a que se han perfeccionado las técnicas de persuasión del comportamiento provenientes de las ciencias sociales, el moderno marketing comercial y el desarrollo de las tecnologías de información (TI). Sin duda, las TI dieron al *microtargeting* político el empujón necesario -debido a la enorme capacidad de procesar y almacenar datos- para lograr analizar información de los ciudadanos, no sólo del tradicional padrón electoral y de los clásicos datos sociodemográficos, sino que se incluyó en el análisis datos que antes no era considerada, como la geolocalización, información biométrica e internet de las cosas, por nombrar algunas. La información basada en datos personales permite generar modelos de preferencias y comportamiento predictivo. Hay un sinnúmero de empresas en la actualidad dedicadas a obtener información personal de los ciudadanos para generar dichos modelos. Una de ellas es Acxiom "que se basa en unos 1.500 puntos de datos para producir modelos predictivos de comportamiento de consumidores mediante un conjunto de 23.000 servidores que le permiten analizar alrededor de 50 millones de transacciones de datos producidas por 500 millones de individuos cada año" (Gorton, 2016). Los datos procesados se sistematizan generando categorías de consumidores prediciendo de esta forma sus hábitos de compra.

De esta forma, las campañas políticas imitan la lógica del marketing comercial utilizando el *Big Data* para generar categorías de electores y así predecir su comportamiento político. Un caso ejemplificador de *Microtargeting* descrito por Gorton (2016) es el de la ciudadana estadounidense Debbie Palos: enfermera de clase media cuyos datos sociodemográficos y su estilo de vida fue analizado por el programa de *Big Data LifeTargeting* para la campaña de Bush en 2004. Palos tenía una postura catalogada de "progresista": estaba a favor del aborto, se oponía a la privatización del seguro social y se identificaba como demócrata. Sin embargo, el análisis de *Big Data* realizado por el equipo de Bush consideraba que existía un 95% de probabilidades de que Palos votara por Bush. Aunque nunca se había hablado con esta ciudadana, por el sólo hecho de recabar información sobre su estilo de vida y posteriormente analizarla, los asesores políticos confiaron plenamente en los datos como para tratar de persuadirla y capturar su voto. El programa de inteligencia artificial estipulaba que la forma en que vivía Debbie Palos se asemejaba más a una votante republicana que a una demócrata. En efecto, Palos votó por Bush. Y cuando la entrevistaron un año más tarde, "no supo esclarecer por qué había votado por ese candidato" (Gorton, 2016), el objetivo del *microtargeting* estaba cumplido. Lo anterior se replicó en otros ciudadanos con características similares. La Directora de la Fundación Ciudadanía Inteligente, Renata Ávila, refleja el microtargeting de la siguiente forma: "Un gran porcentaje de personas se informa mediante las Redes Sociales *(Facebook, Twitter, YouTube),* por lo tanto, la información política se dispone en forma segmentada en dichas plataformas. El problema de todo esto es que las plataformas digitales o las redes sociales son poco auditables, por lo que las empresas, detrás de las plataformas, pueden entregar información manipulada al usuario. Los partidos políticos con mayores recursos, con mayor posibilidad de insertar algoritmos o propaganda política e ideológica en la red, generan un quiebre, una desigualdad respecto a partidos más pequeños. La falta de regulación al respecto, conlleva a que los ciudadanos se dejen influenciar por lo grandes volúmenes de publicidad que insertan partidos políticos y empresas poderosas en las redes sociales, tomando decisiones sesgadas"[23].

### 4.2.2 Utilidades y riesgos del microtargeting político

Sin duda, existe y existirá un aumento de candidatos que basan sus campañas políticas en el *microtargeting,* debido -principalmente- a cuatro factores (Bennett, 2015): las bases de datos electorales tienden a estar cada vez más integradas; la posibilidad de utilización de bases de datos con fines comerciales para fines políticos; la factibilidad de recolección de información mediante las redes sociales y la descentralización de los datos de las campañas locales, a través de aplicaciones móviles. También podríamos añadir el componente de que cada vez más afloran empresas privadas que ofrecen el *microtargeting* político, como por ejemplo, Emerdata[24]. Ello ha derivado en el análisis de la utilidad y los riesgos que pueden surgir de esta nueva forma de publicidad, enfocado en tres segmentos: ciudadanos, partidos políticos y la opinión pública (Zuiderveen, 2018).

Uno de los factores que mayormente debilitan a la democracia es la falta participación electoral[25]. Tradicionalmente, han sido los medios de comunicación masivos los que promueven la participación política en tiempos de elecciones, a través de las franjas electorales. No obstante, se estipula que el *microtargeting* podría promocionar la participación electoral y fortalecer la democracia, pues "permitiría a los políticos atraer a las audiencias mediante anuncios relevantes" (Ibíd.): los electores recibirían justamente la información que les interesa. Los anuncios de televisión enfocados en un público masivo, no convence a todos los ciudadanos, pues a muchos no les interesa la propaganda política. En cambio, el *microtargeting* se enfoca en conectar al público objetivo con anuncios de su interés político proveniente del análisis de datos, captando a ciudadanos desinteresados de la política, pero que cada vez más utilizan los nuevos medios de comunicación como las redes sociales o plataformas de Internet.

[23] Renata Ávila, Ciudadanía Inteligente. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019.

[24] https://newsweekespanol.com/2018/05/emerdata-cambridge-analytica/

[25] De acuerdo al Índice de Calidad de la Democracia 2018, Chile se ubica en el lugar 23°, teniendo como como debilidad la participación política, la que alcanza un puntaje de 4.44, de 10 posibles. https://pages.eiu.com/rs/753-RIQ-438/images/Democracy_Index_2018.pdf?mkt_tok=eyJpIjoiTUdFMII6SmhObVprT1RGaCIsInQiOiIxT3RLUXNETUpmR3YxZjlcL2hUK1JiMU9oK1wvMm83cTRFUjRzajdNZ08rd3cyNUpPVTV3M05RYUQxWjVNMUIQNHU3aG53STh1Zk16Y0RmSFVoQ21HMkw5dE14MVFkZE5UVVNnTXczdk9QcSt3alA2Vk9uTzFsOGhETDBNM1gxTlwvTCJ9

Los partidos políticos también pueden verse beneficiados con el *microtargeting,* pues es una forma de publicidad económica y efectiva. La propaganda política tradicional puede ser sumamente costosa para los partidos pequeños. En cambio, las campañas dirigidas a públicos acotados a través de redes sociales son menos costosas y pueden llegar a ser más efectivas, ya que existe mayor probabilidad que la información efectivamente persuada a ciudadanos a los que se dirige la propaganda[26]. De esta forma, las campañas pueden centrarse en destinatarios que efectivamente votan en periodo de elecciones así como ciudadanos potenciales. Por último, el *microtargeting* eleva la oportunidad de que partidos con pocos recursos compitan con los de mayor tamaño por los electores, diversificando la oferta política.

El que exista mayor diversidad de partidos políticos compitiendo por imponer su agenda ayuda a diversificar las ideas respecto a un problema político en particular. Las campañas tradicionales -por ejemplo, mediante televisión- sólo pueden tratar un número acotado de temas y en forma superficial. En cambio, el *microtargeting* diversifica la información y también la puede profundizar, llegando a públicos especializados sobre alguna materia.

En resumen, el *microtargeting* puede ser útil para aumentar la participación ciudadana mediante la promoción del programa político a públicos específicos; permite que los partidos políticos obtengan réditos -por un menor costo- del marketing político focalizado; y es una forma efectiva de diversificar y profundizar la información en tiempos de elecciones. No obstante, el *microtargeting* también trae aparejado riesgos, que si no se toman en cuenta, pueden poner en peligro la democracia.

Para los ciudadanos, el mayor peligro que trae aparejado el *microtargeting,* sin duda, es la pérdida de privacidad. Para que éste sea posible hace falta la recopilación de una gran cantidad de información personal, ya que así se pueden generar perfiles y categorías de electores. Las personas tienden a entregar fácilmente su información personal. En un estudio realizado por Sarah Spiekermann[27], se constató la disonancia entre lo que se cree respecto a la protección de datos personales comparada con el comportamiento real de los ciudadanos: a pesar de que algunos ciudadanos consideran de suma importancia proteger sus datos, en la práctica, entregan constantemente información personal a terceros[28]. También se ha descubierto por parte de la *Federal Trade Comission*[29], que las empresas obtienen y manejan grandes cantidades de información personal proveniente de transacciones comerciales y que posteriormente son vendidos a compañías que realizan campañas de marketing. Existen otros casos donde la obtención de datos personales se hace sin consentimiento de los titulares, mediante filtraciones de datos o vulneración a los sistemas de seguridad. Un ejemplo de ello, es la filtración de datos de más de 40 mil tarjetas de crédito y débito de diversos emisores bancarios en Chile, informada por la Comisión para el Mercado Financiero[30] (CMF), que se suma a otros casos de este tipo. Regular la pérdida de privacidad entregando voluntariamente o no la información personal es el gran objetivo de las leyes de protección de datos personales.

La manipulación política es otro riesgo asociado al *microtargeting.* El caso de *Cambridge Analytica,* comenzó con un test de personalidad en la red social, recabando -sin conocimiento de los titulares- información personal de más de 50 millones de usuarios que fue utilizada para manipular psicológicamente a los votantes de las elecciones de 2016 en Estados Unidos[31] y en el Brexit[32]. La manipulación se puede efectuar de diferentes formas: un partido político o grupo de interés podría entregar mensajes "a medida" dependiendo de cada elector conllevando a una opinión sesgada respecto a las promesas políticas del partido, fomentando la fragmentación de temas y por ende, perdiendo la globalidad de los problemas que se tienen que resolver políticamente. Inclusive, un partido -con tal de ganar votos- podría entregar dos mensajes contrapuestos dependiendo del elector. En este sentido, un ciudadano podría pensar, erróneamente, que un tema particular que le fue enviado sería la temática central de la campaña. Esto sería perjudicial para la democracia en cuanto a que el candidato -una vez electo- puede enfocarse en otras temáticas, dando la sensación al elector de incumplimiento de promesas de campañas, fomentando a la larga la abstención electoral.

Por último, el *microtargeting* puede ignorar a las personas que "no son necesarias" para ganar una elección. Si, por una parte, la manipulación se hace entregando mensajes políticos persuasivos, la otra cara es la omisión. De esta forma, para algunos grupos de ciudadanos que no se consideran relevantes, como generalmente pasa con las minorías, puede ser sumamente difícil tener alguna representación política.

[26] En una encuesta realizada en Estados Unidos, un 20% de los encuestados señalaron que se informa a través de redes sociales, por otro lado un 16%, lo hacía por medio de periódicos. https://www.eluniverso.com/larevista/2018/12/10/nota/7093074/encuesta-revela-que-personas-leen-mas-noticias-redes-sociales-que

[27] BCN, 2015.

[28] Según el IX Estudio Nacional de Transparencia (2018), un 59% de los ciudadanos se encuentra "muy preocupado" por la información privada que poseen las empresas y los organismos el Estado. Sin embargo sólo un 31% lee las condiciones de privacidad cuando instala redes sociales o servicios de Internet.

[29] Agencia estadounidense.

[30] http://www.cmfchile.cl/portal/principal/605/w3-channel.html

[31] https://www.bbc.com/mundo/noticias-43472797

[32] https://elpais.com/internacional/2018/03/26/actualidad/1522058765_703094.html

### 4.2.3 Herramientas para desarrollar el *Microtargenting: Fake News*

Las noticias falsas, o en su acepción inglesa *fake news,* refieren a "información inventada que imita el contenido de los medios de comunicación en forma, pero no en el proceso o la intención de los mismos. Además, carecen de las normas y procesos editoriales de los medios de comunicación para asegurar la exactitud y credibilidad de la información" (Lazer, 2018, p. 1). Las noticias falsas se encuentran, hoy en día, en el centro del debate producto de su utilización en las campañas presidenciales de 2016 en Estados Unidos; sin embargo, su uso proviene, al menos, desde el siglo XIX, cuando el *New York Sun* publicó una serie de artículos sobre el descubrimiento de vida en la luna (Allcott & Genzkow, 2017). Lo que caracteriza a una noticia falsa es la intencionalidad de difundir hechos verificablemente falsos que inducen a una percepción o interpretación equivocada de los hechos por parte de un lector. Se distinguen de otros tipos de noticias falsas que son producto de errores no intencionales; rumores que no se originan de una publicación periodística; teorías de conspiración; sátiras; declaraciones falsas de políticos o documentos que son sesgados, pero no totalmente falsos (por ejemplo, a partir de posturas políticas). A la premeditación de difundir una noticia falsa y los medios técnicos y tecnológicos para poder hacerlo, se suma otro punto muy importante: la alusión a las emociones y creencias personales del lector para que la noticia sea aceptada. Esto último es conocido como la "posverdad" (Fernández, 2017): a pesar de que una noticia falsa puede estar en conocimiento de las personas de su condición de falsedad, no impide que las mismas tomen decisiones basándose en ella.

Las primeras normas para lograr una mayor objetividad en la información surgen post primera guerra mundial a causa del uso generalizado de propaganda y desinformación táctica. Las normas, una vez establecidas y mantenidas por oligopolios de prensa y radiodifusión, gozaron de una alta confianza pública y credibilidad. Sin embargo, el desarrollo de internet y la entrada de nuevos competidores -dado el bajo costo que implica la digitalización- han mermado la confianza en los medios a mínimos históricos. La capacidad de difusión a través de plataformas digitales, sin la rigurosidad editorial que gozaban los medios de prensa tradicionales, ha permeado el debate público al punto de que cualquier ciudadano que tenga acceso a plataformas de información puede incidir mediante mensajes que quedan en la memoria colectiva. El libre flujo de la información permite plantear ideas y opiniones que, en palabras de Galdámez (2019), "no son inocuas" y que "calan" al interior de la sociedad. Las noticias falsas, por lo tanto, cristalizan mensajes deliberadamente erróneos con la finalidad de adulterar el proceso de formación de la opinión pública. Internet y las plataformas digitales son herramientas que, mediante el debate e intercambio de ideas, pueden ayudar a preservar la democracia. Paradójicamente, uno de los mayores peligros que dichas herramientas presentan a la democracia es el quiebre de la libertad de información, en el sentido que cualquier noticia con un alto grado de fiabilidad puede catalogarse como falsa.

Para las elecciones de 2016 en Estados Unidos, se estimó que el estadounidense promedio encontró entre una y tres noticias falsas de editores conocidos[33]. Además, las noticias falsas se difunden mucho más rápido que las noticias verdaderas cuando se trata de política.

### 4.2.4 La motivación detrás de la información falsa

Resulta difícil determinar la motivación de las noticias falsas, pues los intereses son variados: "gestionar el clima social, ganar elecciones, obtener el favor de la opinión pública, promocionar el consumo, engañar a inversores, influir en la política, etc." (Blázquez, 2018). Sin embargo, las alternativas se pueden reducir a dos motivaciones principales: económica y política. El sólo hecho de difundir artículos en las plataformas digitales ya genera un cierto tipo de ingresos por número de "clics" a un sitio web. Un caso emblemático de lucro mediante noticias falsas es el de Paul Horner, ciudadano estadounidense, que se hizo conocido por ser autor de numerosas noticias falsas pro-Trump -que difundía por Facebook- a pesar de que se oponía personalmente a Trump (Allcott & Genzkow, 2017). Horner también diseñaba sitios web falsos para difundir rumores mediante llamativos titulares, ganando dinero por cada clic que un cibernauta hiciera en la noticia. Algunos autores como Blázquez (2018) señalan que el auge de las noticias falsas (con motivación económica), se produce, en parte, para influir en las decisiones de inversión, prediciendo el comportamiento del mercado y sus tendencias, a partir del estudio de sentimientos y motivaciones que las personas registran en sus plataformas digitales. La otra arista de las noticias falsas es político-ideológica, cuando se publican artículos falsos con sesgos partidistas. Detrás de estas noticias están sitios web falsos que se crean antes de las elecciones para que, una vez consumadas, vuelvan a desaparecer. Su motivación principal es posicionar a candidatos para ganar elecciones realzando virtudes del candidato o denostando al adversario.

Estas aristas, por supuesto, se entremezclan. Según medios como *The Guardian,* para las elecciones de 2016 en Estados Unidos, más de 100 sitios web que publicaban noticias falsas eran administrados por adolescentes, que favorecían indistintamente a Trump como a Clinton y que recibieron miles de dólares de ganancias (Allcott & Genzkow, 2017).

### 4.2.5 Bots

Los *bots* o las cuentas automatizadas en redes sociales, juegan un rol importante en contribuir al desarrollo de noticias falsas. La función de los bots es la inundación de propaganda política, generalmente en

[33] En 2017 en Chile, se detectaron alrededor de 20 sitios que crearon por lo menos 80 noticias falsas, y que fueron vistas y compartidas más de 3,5 millones de veces. En libro 10 años Consejo para la Transparencia. CPLT.2019.

redes sociales, para influir o alterar los resultados de las elecciones (Fernández, 2017). En razón de ello, han surgido iniciativas para desenmascarar este tipo de cuentas, como por ejemplo, *BotorNot,* que, a través de su página web, puede insertar el nombre de la cuenta e identificar si la cuenta es un *bot* o no. A pesar de estos esfuerzos, aún faltan métodos más representativos para determinar con exactitud la prevalencia de bots en las noticias falsas. El Senador de la República de Chile, Felipe Harboe, describe la función de los bots de la siguiente forma: "Generalmente existen algoritmos que producen noticias falsas por robots *(bots)* o personas que intencionan la información falsa *(trolls).* Los algoritmos de plataformas como *Youtube* -una de las más utilizadas para informarse por jóvenes y adolescentes- privilegian las noticias novedosas *(breaking news)* sobre otro tipo de información. Esto ha sido aprovechado por *bots* y *trolls* para introducir noticias falsas (videos falsos), pero novedosas, e influir a los usuarios más jóvenes, con menos criterio o discriminación respecto a noticias verdaderas, a que tomen decisiones erróneas"[34].

Los investigadores del Instituto de Internet de Oxford han concluido que la propaganda por redes sociales más intensa se realiza mediante los bots (Morgan, 2018).

### 4.2.6 Burbujas de filtro

Aparte del peligro que representan las noticias falsas para la libertad de información, existen pocas evaluaciones de impacto de su propagación fuera de los ámbitos electorales. Sin duda, las noticias falsas aumentan la desconfianza generalizada, el cinismo, la apatía. Pero un efecto interesante es el fomento del extremismo, producto de las llamadas "burbujas de filtro". Éstas refieren al "aislamiento informativo en el cual estarían quedando atrapados los ciudadanos como consecuencia de un diseño algorítmico" (Rossi, 2018, p. 265). Tiene que ver con la personalización de contenidos hacia un usuario que previamente ha buscado información o se ha suscrito a una temática particular. Los algoritmos analizan y categorizan estas búsquedas para poder construir un perfil de usuario e "intentar predecir cuáles contenidos desea ver y a cuáles publicidades podría ser permeable" (Ibíd.). El problema de todo ello es la atomización informativa, pues son los algoritmos y no los usuarios los que deciden qué "ver" y qué no. La libertad de información y la democratización mediante Internet genera un contrasentido: el ciberespacio, en vez de ser compartido mediante una agenda informativa común, es soslayado y encapsulado, promoviendo las posturas extremas. Las noticias falsas contribuyen a esta delimitación. Por ello, dos personas que busquen la misma información en internet pueden recibir resultados diferentes en cuanto a su perfilamiento. El individuo ya no puede hacer el ejercicio de informarse, analizar y discriminar la información según sus creencias, sino que esta información viene preconfigurada o filtrada de antemano.

[34] Felipe Harboe, Senador de la República de Chile. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019.

# 5. La protección a la privacidad como derecho fundamental

La crisis de credibilidad y confianza no sólo ha afectado a instituciones como los partidos políticos, los parlamentos u órganos administrativos. Los medios de comunicación también la están padeciendo. La información que transita por las redes sociales se comparte tan rápido que no se comprueba su veracidad. Además, el volumen de la información es tan grande, que sobrepasa la revisión exhaustiva de cada noticia publicable. Para enfrentar este problema, ha surgido el *fact checking* o verificación de datos. "Se trata de una operación que aplica técnicas del periodismo de datos para desenmascarar errores, ambigüedades, mentiras, falta de rigor o inexactitudes de algunos contenidos publicados en los medios de comunicación" (Ufarte, et. al, 2018). Mediante herramientas tecnológicas -incluyendo a sitios web- se contrastan fuentes fiables, documentos oficiales o investigaciones comprobadas para desnudar inconsistencias no sólo de noticias en la red, sino que también declaraciones públicas o la veracidad de cifras o datos expresados en ellas. Su objetivo es mejorar la información que está disponible para los ciudadanos, mejorando la democracia. En 2017, había 126 sitios web en el mundo dedicados a verificar noticias falsas. Además, existen encuentros internacionales como Global Fact y la *International Fact-Checking Network* (Palau, 2018) que apoyan el desenmascaramiento de este tipo de noticias[35].

El combate a la desinformación es complejo. Hay cada vez más sitios web que pueden disponer contenido falso. La última tendencia son las *deepfakes,* que suplantan rostros de políticos. No obstante, la desinformación sólo funciona si los electores tienen dudas sobre un candidato. Además, cada vez hay una mayor conciencia sobre el uso de información falsa, por lo que es fundamental develar este tipo de actos mediante la red de contactos. Como sostiene Reis (2019), los medios sociales no cambian los fundamentos tradicionales que se utilizan en campañas políticas, como diseñar un mensaje central para los electores, sino que cambian los lazos de retroalimentación para probar qué es lo que funciona y convence. Para el Senador Harboe, se necesita una mayor legislación respecto a este tipo de noticias: "La democracia no se limita sólo al periodo electoral, también implica debate, participación o el desarrollo de instituciones. Las personas basan sus decisiones y participación democrática en la información que disponen. Si la información que dispone la ciudadanía es falsa o errónea, las decisiones posteriores no son las más adecuadas. Lo que se debe hacer es generar mecanismos, en la legislación, que ayuden a las personas evitar tomar decisiones basadas en información falsa"[36].

La información personal nunca había estado disponible para ser difundida masivamente como ocurre actualmente. Por ello, el derecho a la privacidad adquiere una importancia fundamental. Este derecho implica la ausencia de obstáculos para poder tomar nuestras decisiones libremente. Es el espacio que necesita una persona para llevar a cabo una vida autónoma, sin coacciones por parte de una autoridad u otro tipo de entidad. Así, proteger la privacidad es proteger la dignidad humana.

La privacidad no se trata de una propiedad objetiva, sino de una definición jurídica. Es un derecho que establece el límite con lo público (Escalante, 2008). Si bien la privacidad implica tomar decisiones sin la intervención de alguna autoridad, paradójicamente, la privacidad se constituye jurídicamente desde el Estado. Por lo tanto, son las leyes las que pueden restringir o delimitar las circunstancias en que se justifica una intervención estatal. De esta manera, la privacidad no se debe pensar como algo estático, sino que cambia acorde a las condiciones de organización de una sociedad. Por ejemplo, debido a la emergencia de la tecnología y la masificación de la información privada de los ciudadanos se ha hecho necesaria la promulgación de leyes o la actualización de ellas.

Son muchas las leyes que, actualmente, amparan la privacidad[37]: la Declaración Universal de los Derechos Humanos (1948, artículo 12); el Convenio para la Protección de los Derechos y las Libertades Fundamentales (1953, artículo 8); el Pacto Internacional de Derechos Civiles y Políticos (1966, artículo 17); la Convención Americana de Derechos Humanos (1978, artículo 11.2), la Convención Internacional sobre la Protección de los Derechos de los Trabajadores Migratorios y sus Familiares (1990, artículo 14) y el Convenio 108+ (2018). En 2018 también entró en vigor el Reglamento General de Protección de Datos de la Unión Europea (GDPR

[35] En Chile, debido al "estallido social" en octubre de 2018, los principales medios de comunicación han debido verificar constantemente los hechos noticiosos para evitar la difusión de noticias falsas.

[36] Felipe Harboe, Senador de la República de Chile. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019.

[37] CPLT, 2019

en inglés). Se trata de una normativa en el cual el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea actualizaron y unificaron los estándares para la protección de datos personales de todos los ciudadanos pertenecientes a la Unión Europea. Su objetivo principal es "dar el control a los ciudadanos y residentes respecto a sus datos personales y simplificar el entorno regulador de los negocios internacionales, unificando la regulación dentro de la Unión Europea"[38]. El GDPR protege a los ciudadanos cuyos datos personales son almacenados, procesados, transferidos o divulgados por organizaciones o empresas sin su consentimiento, sancionando severamente el incumplimiento de la normativa. Además, incorpora nuevas definiciones de lo que es un dato personal. Por ejemplo, las direcciones IP, la información económica, la salud mental o la información biométrica, que antes no era considerada información personal, actualmente sí lo es.

La masificación de grandes volúmenes de información o *Big Data* supone un gran reto para las legislaciones actuales, en cuanto a que sus algoritmos permiten la identificación de las personas, aun cuando esos datos son considerados anónimos o "estadísticos" (Gil, 2016). Muchas veces los datos recopilados por organismos gubernamentales o empresas exceden la finalidad para el cual fueron recabados, obteniendo una gran cantidad de datos personales, por ejemplo, para realizar *microtargeting.* Debido a esto las entidades carecen de la capacidad para especificar en qué serán utilizados los datos, repercutiendo en una pérdida de control de los titulares de ellos. Un pilar central de la protección de datos refiere al consentimiento o permiso que un ciudadano concede para el tratamiento de sus datos personales. No obstante, resulta complejo informarse acerca de los múltiples consentimientos y autorizaciones que las entidades solicitan para el tratamiento de sus datos personales, dada la diversidad de fuentes del cual provienen los datos. Para solucionar este problema, y a petición de Microsoft, en 2012 se comenzó a trazar un cambio de enfoque en las normas de protección de datos personales, traspasando la responsabilidad del uso de los datos desde el individuo hacia los "usuarios" de los datos, es decir, las entidades que realizan el tratamiento de datos. Así, ya no es el usuario -por aceptar, por ejemplo, los términos y condiciones de uso de una aplicación- el responsable de lo que pueda suceder con ellos, sino el que los trata. "El foco de atención ya no debe ser el momento de la recolección de los datos, sino en el momento de utilización de los datos" (Gil, 2016, p. 134). Los ciudadanos pocas vecen se informan de las condiciones de ocupar un servicio digital y generalmente dan puerta ancha para que alguna institución o empresa utilice los datos como le plazca. De esta manera, el consentimiento informado sólo debe reservarse para alguna acción relevante como, por ejemplo, renunciar al tratamiento de datos.

Si bien, se pueden discutir aspectos para poder optar a una mejor regulación y proteger de mejor forma la privacidad, aún existe un déficit cultural respecto al cuidado de los datos personales[39]. Una de las causas de vulneración del derecho a la privacidad es la falta de conciencia ciudadana respecto al uso de los datos personales que no se ciñe, únicamente, a aspectos de ciberseguridad. Existe una carencia generalizada respecto al conocimiento de cómo los datos personales serán tratados adecuadamente, según su finalidad y propósito. Aunque las campañas informativas son de gran ayuda para que las personas reconozcan y garanticen su derecho a la protección de datos personales, una medida concreta para empoderar a ciudadanos en la materia es la autodeterminación digital mediante el derecho a una copia digital de todos sus datos personales que están siendo tratados. Con el derecho a copia, cada ciudadano tendría un mayor control respecto a sus datos y podría decidir la transferencia de estos a un tercero. Además, conociendo los datos personales que se encuentran en manos de entidades externas, es más fácil gestionar y conceder el permiso de los datos personales que serán compartidos. Por lo tanto, ya no serían las entidades quienes tratarían los datos personales, sino los propios individuos fomentando una cultura de cuidado de su privacidad. Algunas propuestas de empoderamiento proponen transformar a los ciudadanos en sujetos activos, añadiendo valor a sus datos personales, a través de diversas medidas[40]:

**1.** El individuo es el centro del sistema de recolección, gestión y uso de datos.

**2.** El individuo decide qué información revelar, de forma selectiva.

**3.** Control sobre los fines para los que se usan los datos, así como su duración, a través de contratos.

**4.** El individuo tiene mecanismos para comunicar lo que demanda de forma abierta y flexible, sin estar ligado a ninguna organización concreta.

**5.** Altas medidas de seguridad.

**6.** Portabilidad de datos, de modo que los individuos puedan obtener todos sus datos y moverlos de un proveedor de servicios a otro.

**7.** Medidas para que las empresas sean responsables de la seguridad de los datos personales, de acuerdo a los distintos niveles de permiso que el individuo ha decidido otorgar.

[38] https://www.powerdata.es/gdpr-proteccion-datos

[39] En Chile, sólo un 18% de los ciudadanos sabe que existe una normativa que regula la protección de datos personales y un 11% sabe de la existencia de una institución que vele por ellos (Estudio Nacional de Transparencia, CPLT, 2018).

[40] Rubinstein en Gil, 2016, p. 141.

Como podemos observar, el derecho a una copia de toda la información personal posibilita un mayor control a las personas de la información personal que comparten, otorgando -además- una nueva valorización a ésta, en cuanto a que es posible transformar el dato personal en un activo económico.

Para que los individuos sean realmente sujetos activos en el resguardo de sus datos personales, deben obtener las competencias necesarias para poder prever los riesgos asociados y utilizar las garantías que establecen las leyes de protección de datos personales. En esta línea, Helbing (2017) apunta hacia una alfabetización digital en materia de riesgos que implicaría el poder aprovechar las tecnologías digitales sin depender de ellas ni ser manipuladas por ellas. La finalidad es lograr un autocontrol digital educando a los ciudadanos desde la infancia, en las escuelas, y las familias. Un ciudadano informado, crítico y consciente de los riesgos de la tecnologización y la difuminación de los datos personales puede volcar a su favor la utilización de estos.

Por último, para complementar, es necesario también un comportamiento ético por parte de las entidades que tratan grandes cantidades de información personal. La iniciativa *Data for Humanity,* trata de difundir un código ético para que el uso del *Big Data* sea a favor de los grandes problemas sociales existentes, tales como el cambio climático, las migraciones masivas, las guerras o conflictos prolongados y el deterioro de la privacidad personal[41]. Mediante una carta de compromiso, la iniciativa propone los siguientes principios:

**1.** No hacer daño: aquellos que tienen un mayor conocimiento gracias al *Big Data* no deben perjudicar a terceros.

**2.** Utilizar los datos para ayudar a crear una coexistencia pacífica: las corporaciones, empresas, entidades gubernamentales y los científicos de datos deben ser conscientes de su responsabilidad de proporcionar un acceso equitativo e imparcial a los datos.

**3.** Utilizar los datos para ayudar a las personas vulnerables y necesitadas: el análisis de *Big Data* no sólo sirve para ganar elecciones o inducir a comprar artefactos, sino que se debe velar por el uso social de los datos mejorando la calidad de vida de las personas más desprotegidas.

**4.** Utilizar los datos para preservar y mejorar el medio ambiente natural: el *Big Data* puede ofrecer desarrollo solo si éste comulga en la mantención de un entorno natural saludable.

**5.** Utilizar los datos para crear un mundo justo y sin discriminación: el objetivo del análisis de datos se debe enfocar en el bien común basándose en los principios de justicia y equidad.

Frente al cada vez más frecuente uso masivo de datos personales y los riesgos que puede implicar su mal uso para la estabilidad democrática, la vulneración de la privacidad y la manipulación política, una regulación adecuada que conceda mayor control de los datos a los ciudadanos, la alfabetización digital de la ciudadanía frente a los riesgos y la conducta ética de entidades que tratan datos personales para que éstos sean utilizados con un enfoque social, se transforman en pilares fundamentales para el resguardo de una buena convivencia democrática, sin perder de vista los beneficios que trae aparejada la era digital.

[41] http://www.bigdata.uni-frankfurt.de/dataforhumanity/

# Bibliografía

**Libros y revistas científicas:**


- Allcot, H. & Gentzkow, M. (2017) *Social media and fake news in the 2016 election. Journal of Economics Perspectives,* Vol. 31, N°2.
- Bennet, C. (2015) *Trends in voter surveillance in western societies: privacy intrusions and democratic implications. University of Victoria,* Canada.
- Bennet, C. (2013) *The politics of privacy and the privacy of politics: parties, elections and voter surveillance in western democracies. First Monday* 18.
- Biblioteca del Congreso Nacional (2015), Protección de Datos Personales y Derecho a la Privacidad. Observatorio de Programa Europa de la Biblioteca del Congreso Nacional. https://www.bcn.cl/observatorio/europa/noticias/proteccion-de-los-datos-personales-y-derecho-a-la-privacidad-parte-2
- Blázquez, M. (2018) El problema de las noticias falsas: detección y contramedidas. XV Seminario Hispano-Mexicano de Investigación en Biblioteconomía y Documentación, Ciudad de México, 16-18 de mayo de 2018.
- Escalante, F. (2008) El Derecho a la Privacidad. Serie Cuadernos de Transparencia, IFAI, México.
- Evans, D. (2011) Internet de las cosas: cómo la próxima evolución de Internet lo cambia todo. Informe Técnico de Cisco Internet Business Solutions Group. California. Estados Unidos.
- Fernandez, N. (2017) Fake News: una oportunidad para la alfabetización mediática. Revista Nueva Sociedad, N°269, Buenos Aires, Argentina.
- Foucault, M. (2012) Vigilar y Castigar: nacimiento de la prisión. Editorial Siglo XXI. Buenos Aires.
- Galdámez, A. (2019) Posverdad y crisis de legitimidad: el creciente impacto de las fake news, Revista Española de Transparencia, número 8.
- Gerber, A. & Green, D. (2000) *The effects of canvassing, telephone calls, and direct mail on votante turnout: a field experiment. American Political Sciencie Review,* Vol. 94, N° 3, Yale University.
- Gerl, K. (2017) Política 2.0: Internet y el trabajo de los partidos. Revista Nueva Sociedad N° 269. Buenos Aires, Argentina.
- Gil, E. (2016) *Big Data,* Privacidad y Protección de Datos. Agencia Española de Protección de Datos, Madrid, España.
- Gorton, W. (2016) *Manipulating citizens: how political campaings' use of behavioral social science harms democracy, New Political Science,* 38:1, 61-80. Michigan, USA.
- Green, D. & Gerber, A. (2015) *Get Out the Vote: How to Increase Voter Turnout. Brookings Institution Press.* Recuperado http://www.jstor.org/stable/10.7864/j.ctt1657t5x
- Han, B. (2018) Psicopolítica. Herder Editorial, Barcelona, España.
- Harari, Y. (2018) *Homo Deus:* Breve historia del mañana. Penguin Random House Editorial. Santiago de Chile.
- Helbing, D., Et. Al. (2017) *Will democracy survive Big Data, Scientific American,* Zurich, Suiza.
- *Information Commissioner´s Office* (2018) *Democracy disrupted? Personal information and political influence.*
- Lazer, D., Et Al. (2018) *The science of fake news.* Revista *Science* N°359, Estados Unidos.

• Lobo, S. (2017) Cómo influyen las redes sociales en las elecciones. Revista Nueva Sociedad, N° 269. Buenos Aires, Argentina.

• Morgan, S. (2018) *Fake News, desinformation, manipulation and online tactics to undermine democracy, Journal of Cyber Policy.*

• Palau, D. (2018) *Fact-Cheking* y vigilancia del poder: la verificación del discurso público en los nuevos Medios de América Latina. *Communication & Society.* Universidad de Valencia, España.

• ProChile (2018) Las 10 tendencias del *e-commerce* en el mundo. Absolunet: http://10ecommercetrends.com/

• Rajsbaum, S. & Morales, E. (2016) Norbert Wiener y el origen de la Cibernética. Revista Ciencia. México D.F.

• Rosanvallon, P. (2017) La democracia del siglo XXI. Revista Nueva Sociedad N°269. Buenos Aires, Argentina.

• Rossi, A. (2018) ¿Burbujas Filtro? Hacia una fenomenología algorítmica. Revista Inmediaciones, Universidad Abierta Interamericana, Argentina.

• Ufarte, M., Et. Al. (2018) Fact Cheking: Un nuevo desafío del periodismo. El Profesional de la Información, Vol. 27, N°4. España.

• Zuiderveen, F., Et. Al. (2018) *Online political microtargeting: promises and threats of democracy.*

**Notas de Prensa:**

• Luna, J. (2019) Entrevista en: https://ciperchile.cl/2019/09/23/big-data-en-campanas-para-los-politicos-es-mas-facil-ganar-una-eleccion-pero-les-resulta-muy-dificil-gobernar/?fbclid=IwAR2zPLiVACVKOo0n313UY-HOmLutNmi-nh1SKuq3Dco9neHZ0HZY5TmSwO9A

• Reis, J. (2019) Entrevista en: https://www.latercera.com/aniversario/noticia/jessica-reis/752556/

**Entrevistas Seminario “Sigue la Huella de Tus Datos”:**

• Renata Ávila, Directora Ciudadanía Inteligente.

• Felipe Harboe, Senador de la República de Chile.

• Patricia Kurzcyn, Comisionada Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México.

• Raymond Duch, *Official Fellow en Nuffield College,* Universidad de Oxford y Director de *Nuffield Centre for Experimental Social Sciences* (CESS) Oxford.

DEMOCRACIA Y PROTECCIÓN DE DATOS PERSONALES
EN LA ERA DIGITAL