Universidad de Chile
Facultad de Derecho
Departamento de Derecho Público

EL DESAFÍO REGULATORIO DE LAS NUEVAS TECNOLOGÍAS: ANÁLISIS DEL USO DE DATOS PERSONALES E INTELIGENCIA ARTIFICIAL EN EL CONTEXTO DE CAMPAÑAS ELECTORALES. UNA MIRADA NACIONAL Y COMPARADA

Memoria para optar al grado de licenciado en Ciencias Jurídicas y Sociales

SEBASTIÁN ROMERO FIERRO

PROFESOR GUÍA: CARLOS HUNEEUS MADGE

SANTIAGO- CHILE

2023

AGRADECIMIENTOS

*A Natalia, por su inconmensurable amor, comprensión y apoyo durante cada una de las etapas que atravesé en mi estancia en la Escuela, siendo un pilar fundamental para llegar hasta donde me encuentro***.**

A mi abuela, que sin estar presente me acompaña en todo momento, entibiando mi alma al más mínimo recuerdo.

A mis hermanos, por llenar de gozo mi espíritu.

A mis amadas Lilo, Azula y Bimba, quienes se acurrucaron en mis pies fielmente mientras pasaba largas horas investigando.

A mis amigas y amigos de la Facultad, por acompañarme enérgicamente en todo momento y a quienes admiro profundamente intelectualmente.

Al profesor Carlos Huneeus, referente intelectual, por permitirme cultivar una relación académica desde mi primer año en la Escuela y darme la confianza para poder desarrollar un tema de mi completo interés.

A Constanza Pasarin, por su genuino interés en ayudarme y aportarme su vasto conocimiento profesional en la materia.

ÍNDICE

INTRODUCCIÓN: EL ASCENSO DE LA ERA DIGITAL Y LA PRESENCIA DE LAS NUEVAS TECNOLOGÍAS EN LA ARENA POLITICA

En las últimas décadas hemos sido testigos de un notable y acelerado auge en el desarrollo y la adopción de tecnologías que revolucionan diversos ámbitos de la sociedad. En este sentido, la creciente accesibilidad a internet, sistemas informáticos y tecnologías de la información y comunicación dotadas muchas veces de Inteligencia Artificial, han redefinido la forma en que nos comunicamos y nos percibimos como sociedad.

Sin embargo, todos los avances necesitan ser analizados con cautela. La gran cantidad de datos que requieren las nuevas tecnologías para operar han puesto de manifiesto un serio riesgo para la intimidad que supera con creces el que se advertía respecto de los medios de comunicación de masas tradicionales[1]. Esto, desde hace años, se ha materializado en el creciente reconocimiento constitucional del derecho fundamental a la protección de datos personales y la vida privada por parte de un gran número de países, sobre todo del ala occidental.

Ahora bien, la sola positivización constitucional no agota ni satisface un problema jurídico contingente que relaciona el Derecho y la tecnología y que va mucho más allá. Hoy en día, el debate legislativo nacional e internacional se centra en la suficiencia de los cuerpos legales para responder a tecnologías dinámicas que se valen de distintos medios dentro de los cuales destaca el Internet -pilar fundamental de la conexión digital- el cual se ha transformado en un espacio completamente construido en base a datos, donde destacan aquellos de carácter personal. Este gran volumen de datos disponible de forma no estructura es lo que comúnmente se conoce como *big data,* combustible por excelencia para los sistemas dotados de Inteligencia Artificial que los modelan, clasifican y analizan, permitiendo establecer patrones de comportamiento con diferentes utilidades.

Este contexto excesivamente digitalizado es lo que para algunos pensadores se conoce como "el régimen de la información" o "infocracia" en que la explotación de datos personales marca la pauta en los procesos sociales, económicos y politicos, y donde no solo el mundo privado se aprovecha de la exposición de la vida, sino que igualmente el Estado y otros actores relevantes en la democracia, como los partidos politicos[2], los cuales -en razón de su debilitamiento y rechazo popular- han tenido que redefinir la forma en que se comunican con su electorado.

---

[1] **CERDA, A.** Autodeterminación Informativa y Leyes Sobre Protección de Datos. Revista Chilena de Derecho Informático, Núm. 3, 2003. pp. 47- 75. p. 50.
[2] **HAN, BYUNG-CHUL**. *Infocracia: La digitalización y la crisis de la democracia*. Taurus, 2022.

En concreto, la presente memoria explora la incidencia de las nuevas tecnologías en la esfera democrática y, particularmente, la utilización de datos personales e Inteligencia Artificial en el contexto de campañas electorales. Este fenómeno, conocido como *microtargeting* electoral, ha causado especial revuelo e interés académico desde que salió a la luz el caso de la empresa Cambridge Analytica, abriendo las puertas a una discusión necesaria, esto es, bajo que marco jurídico se les permite y permitirá a los partidos politicos utilizar nuevas herramientas de propaganda electoral.

Cabe señalar que esta investigación toma la forma de un ensayo[3] y tiene como objetivo general dar a conocer cuál es el estado del arte en términos doctrinarios y normativos tanto en un plano nacional como comparado. Para lograrlo, se ofrece la siguiente estructura.

En el primer capítulo, de forma crítica y descriptiva, se acercará al lector a la comprensión de conceptos claves en la materia, como que es un dato personal, cuales clasificaciones son admitidas y aquello que se entiende por Inteligencia Artificial y *Big Data*.

Enseguida, en un segundo capítulo se explicará que constituye en esencia el *microtargeting* electoral, constatando las diferentes posturas que adoptan los expertos en la materia respecto de su impacto en la arena democrática; cuales son las plataformas que se utilizan para recopilar datos personales sensibles ligados a la ideología politica; y como su utilización trae aparejada consigo otras problemáticas éticas, como el desarrollo de *fake news* y *bots* propagadores de información, que distorsionan la realidad de los hechos que acaecen. Para dar cierre al capítulo, se analizarán las elecciones presidenciales que tuvieron lugar el año 2017 en Chile, caso de estudio paradigmático ya que se tomó conocimiento público de la utilización de herramientas de automatización y perfilamiento.

El tercer capítulo estará dedicado al analisis de la realidad normativa de Chile en lo referido a la protección de datos personales. En primer lugar, realizando un examen critico de la vigente Ley N° 19.628 Sobre Protección de la Vida Privada, constatando sus deficiencias y como estas abren la puerta al tratamiento de datos personales sensibles en un contexto desregulado. Posteriormente, se analizará el boletín N° 11.144 refundido con el boletín N°11.092-07 referidos al Proyecto de Ley que regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales, consignando sus principales innovaciones y los cambios que se materializarían desde su entrada en vigencia de aprobarse el cuerpo legal, siempre en relación con el *microtargeting* electoral.

[3] Instructivo sobre la Memoria de Prueba y los Talleres de Memoria en la Carrera de Derecho Art. 1 letra b). Ensayo: Razonamiento argumental en el que sobre la base de ciertos supuestos o datos, un autor examina un tema que a su juicio es problemático, desde distintas perspectivas, tomadas con el fin de llegar a una conclusión convicente para un lector.

Adicionalmente, se revisarán los boletines N° 13.698-07 y N° 15869-19, que pretenden regular la propagación de *fake news* y la Inteligencia Artificial, respectivamente.

Para cerrar la investigación y con el fin de extender el analisis hacia un enfoque comparado, tomando en consideración un estado del arte más avanzado, en el capítulo cuarto se revisará el Reglamento General de Protección de Datos de la Unión Europea y otros instrumentos jurídicos emanados del Parlamento Europeo y el Supervisor Europeo de Datos Personales, en todo aquello referido a la automatización de datos, la elaboración de perfiles y la propaganda político-electoral. Finalmente, se revisará el caso español, elección cuyo fundamento radica en las similitudes de su actual Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales con el proyecto de Ley que se tramita en Chile y, además, el paradigmático fallo del Tribunal Constitucional Español referido a una disposición normativa que permitía el tratamiento de datos y la elaboración de perfiles por parte de los partidos politicos españoles.

Todo lo anterior, nos permitirá esbozar ciertas conclusiones para determinar, por una parte, como ha sido tratado teórica y doctrinariamente el fenómeno del *microtargeting* electoral utilizando datos personales sensibles e Inteligencia Artificial; el impacto real que tiene este tipo de manipulación política en los periodos eleccionarios y los riesgos que representa para la democracia en atención a la vulneración de derechos fundamentales. Por otra, podremos concluir si el deficiente estado de la normativa vigente en materia de protección de datos en Chile propicia este mercado; si las innovaciones presentes en los proyectos de Ley constituyen una salvaguarda en la materia de ser aprobados y, finalmente, que tan alejados estamos de acercarnos al estándar europeo de protección de datos que, como es sabido, es la dirección a la que apuntan la mayoría de las legislaciones ligadas a la tradición continental del Derecho.

CAPÍTULO I. UNA APROXIMACIÓN A LOS DATOS PERSONALES Y LA INTELIGENCIA ARTIFICIAL

I.1 Concepto y naturaleza de los Datos Personales

Otorgar una definición de datos personales ha resultado un verdadero desafío tanto doctrinario como legislativo[4]. Sin embargo, esto no impide que podamos acercarnos a un concepto de datos personales a la luz de la literatura especializada vigente.

En términos estrictamente dogmáticos, Pucinelli se refiere particularmente a los "datos" como una pequeña parte de lo que conocemos como información. En este sentido, menciona: "Valga aclarar que el vocablo 'dato' alude a un elemento circunscrito y aislado (v. gr. Nombre o Nacionalidad), que no alcanza a tener el carácter de información, pues para que se transforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta"[5]. Por lo mismo, para que los referidos datos adquieran su particularidad personal, deben tener una referencia que permita individualizar a una persona determina o determinable[6] y, solo así, informaran acerca de aquel.

En esta línea, resulta bastante completa la definición que otorga el Instituto Federal de Acceso a la Información Pública de México, organismo que define a los datos personales como "toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros"[7].

Por otra parte, en la configuración conceptual de aquello que entendemos como datos personales los cuerpos normativos extranjeros han cumplido un rol fundamental, puesto que el analisis y estudio de esta materia jurídica es más bien reciente. En este contexto, el paradigma europeo representa sin lugar a duda un pilar fundamental para el desarrollo de otros países más atrasados en el desarrollo dogmático y

---

[4] **BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE.** Regimen legal nacional de protección de datos personales. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20443/5/REG_NACIONAL_PROTECC_DATOS_PERSONALES%20(LV)_v5.pdf. 3183.

[5] **PUCCINELLI, OSCAR RAÚL**. Tipos y subtipos de hábeas data en el Derecho constitucional latinoamericano. *La Ley, Suplemento de Derecho constitucional*, 1997, pp. 28-29.

[6] **BAHAMONDE GUASCH, CRISTIÁN.** Los datos personales en Chile: concepto, clasificación y naturaleza jurídica**.** *Revista Ius Novum, Centro de Estudios 2017* no 14, p 52.

[7] **INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA DE MÉXICO. EN BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE,** *Op. Cit,* p. 2.

legal de los datos personales. En efecto, el Reglamento General de Protección de Datos Personales de la Unión Europea, que entró en vigor el 25 de mayo de 2018, se refiere expresamente al concepto en comento en el artículo 4 N°1 como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Como es posible apreciar a la luz de las definiciones expuestas, los datos personales hoy en día -de forma deliberada- se entienden en un sentido amplio, tratando de incluir la mayor cantidad de elementos, de manera tal que se confiera una protección de carácter vasto a los derechos de las personas[8]. Por lo mismo, ha sido posible clasificar y categorizar los datos personales en distintos subconjuntos, que permiten un correcto analisis de su contenido.

Así, por ejemplo, se hace un contraste entre datos personales públicos y privados en virtud del poder que tiene el particular para determinar cuáles son susceptibles de ser conocidos por terceros[9]. Se distingue igualmente en aquellos de carácter directo o indirecto, cuestión que depende exclusivamente de si es que ha sido el titular quien consiente en entregarlos, o bien, han sido recopilados a través de bancos de datos que han efectuado un tratamiento sobre los mismos. Por último, es menester referirse a los datos sensibles, materia de suma relevancia para efectos de la presente memoria, que el Comité Jurídico Interamericano ha definido como[10]:

> *"una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque,*

[8] **COMITÉ JURÍDICO INTERAMERICANO (CJI). 2021.** *Principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales, con anotaciones.* Sesión Virtual : CJI, 2021, p. 7
[9] **BAHAMONDE,** *op. cit* p. 56.
[10] **COMITÉ JURÍDICO INTERAMERICANO,** *op. cit,* p. 7.

si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria"[11].

Como queda de manifiesto, la particularidad de esta categoría de datos personales viene dada por el peligro que representa su tratamiento en forma desregulada, que podrían derivar en una transgresión al ámbito más reservado de los individuos y su esfera privada, lo que en consecuencia implica la eventual vulneración de su dignidad[12].

De hecho, el creciente temor por la utilización de datos personales cuestiona, por una parte, la fuente de acceso a aquellos y, por otra, que tipo de datos se recopilan, siendo bastante preocupante que empresas abocadas al tratamiento de datos, ya sea con fines publicitarios, de *marketing* o electorales decanten por la obtención de información sensible que permita no solo encasillar en categorías a la población para enviar mensajes específicos, sino que también inducir a un determinado comportamiento, como será analizado más adelante.

I.2 Big Data e Inteligencia Artificial

Como hemos visto, los datos -sin importar a la categoría a la que pertenezcan- son susceptibles de convertirse en información cuando se acumula una cantidad adecuada de aquellos que permite "informar" acerca de algo o alguien. Sin embargo, la sola existencia de los datos no es suficiente. Para que un usuario pueda utilizarlos necesita ubicar donde se encuentran y posteriormente analizarlos y clasificarlos para aprovechar la información al máximo.

Hoy en día, dar con su ubicación no es difícil. En efecto, en un mundo altamente interconectado a través del Internet la emisión de datos se genera por nosotros mismos a través del uso de herramientas biométricas, la web, redes sociales y realizando transacciones de todo tipo[13]. La magnitud de la transferencia de datos es tal, que resulta prácticamente imposible realizar estimaciones futuras acerca del número de los datos en las redes, puesto que cada día son más las personas que acceden a nuevas tecnologías[14] y, por ende, aportan a su crecimiento exponencial aun cuando no lo sepan[15].

Ante esta situación, la doctrina especializada se ha valido de la expresión anglo "*big data"* para referirse a la existencia de una cantidad masiva de datos, de una magnitud inabarcable para nuestra

---

[11] *Ibíd.*
[12] **BAHAMONDE,** *op. cit* pp. 56-57.
[13] **HUESO, LORENZO COTINO**. Big data e inteligencia artificial. *Una aproximación a su tratamiento jurídico desde los derechos fundamentales. Dilemata*, 2017, no 24, p. 131-150, p.133.
[14]**GUTIÉRREZ-RUBÍ, ANTONI**. Política: del 'big data'al 'data thinking'. *ACOP Papers*, 2015, no 2, p.3.
[15]**BERLANGA, ANTONIO**. El camino desde la inteligencia artificial al Big Data. *Revista Índice*, 2016, no 68, p. 11.

mente[16]. En este sentido, autores como Laney[17] explicaron conceptualmente el *big data* a través de sus características, conocidas como las "3V" [18], haciendo referencia a su: volumen, es decir, la cantidad de datos masiva; su variedad de fuentes y naturaleza; y, por último, la velocidad con la que se gestionan y se actualizan tales datos[19].

Tomando esto en consideración, el Parlamento Europeo hoy en día se refiere al *big data* como "la recopilación, análisis y acumulación constante de grandes cantidades de datos, incluidos datos personales, procedentes de diferentes fuentes y objeto de un tratamiento automatizado mediante algoritmos informáticos y avanzadas técnicas de tratamiento de datos, utilizando tanto datos almacenados como datos transmitidos en flujo continuo, con el fin de generar correlaciones, tendencias y patrones (analítica de macrodatos)"[20].

De la definición, es posible advertir una cuestión fundamental, y es que con independencia de que los datos estén o no estructurados[21], lo cierto es que para procesar tal magnitud de información no se puede depender únicamente del intelecto humano y, en estas circunstancias, es que la inteligencia artificial se ha erigido como la herramienta que permite realizarlo mediante la implementación de algoritmos, estadísticas y sesgos[22].

A diferencia de lo que se pensaba con anterioridad, la Inteligencia Artificial no debe ser entendida como la utilización de robots o elementos en extremo complejos, sino que está presente en nuestro día a día, en tecnología que hoy es prácticamente indispensable en nuestra vida y forma de relacionarnos, como los teléfonos celulares que permiten albergar una multiplicidad de aplicaciones, como Whatsapp, Faceboook, entre otras[23].

En términos generales, cuando nos referimos a la IA, según la Comisión Europea, nos estamos refiriendo a "los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción -con cierto grado de autonomía- con el fin de alcanzar objetivos

---

[16] **HUESO, LORENZO COTINO**. Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*, 2017, no 24, p. 131.
[17] **LANEY, DOUG, ET AL**. 3D data management: Controlling data volume, velocity and variety. *META group research note*, 2001, vol. 6, no 70, p. 3.
[18] **BERLANGA, ANTONIO**. El camino desde la inteligencia artificial al Big Data. *Revista Índice*, 2016, no 68, p. 11
[19] **HUESO, LORENZO COTINO**, *op. cit.* pp. 131-132.
[20] **PARLAMENTO EUROPEO.** Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225 (INI)). 2017, p.83.
[21] **HUESO, LORENZO COTINO**, *op. cit.* p. 132
[22] **MARTINEZ DEVIA, ANDREA**. La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. *Rev. Prop. Inmaterial*, 2019, no. 27, p. 8.
[23] **MARTINEZ DEVIA, ANDREA**, *op. cit.* p. 7.

específicos"[24]. En efecto, la Inteligencia Artificial, en materia de datos, permite que las tecnologías nutridas de aquella logren ubicar, categorizar y clasificar datos, incluso tomando decisiones tal como lo haría un ser humano, con la gran diferencia de que no necesitan descansar y lo están haciendo en cada segundo en que están conectados a la red[25].

Los dos elementos fundamentales para que la Inteligencia sea servil a las herramientas tecnológicas para procesar datos son el *computing power*, es decir, el desarrollo de los sistemas computacionales con amplia memoria de almacenamiento y, por otro lado, el propio *big data*, ya que alimenta la IA[26].

Así, analizada la información es posible llegar a un sinfín de resultados como "el comportamiento de las personas, sus gustos, la toma de decisiones, el reconocimiento de voz, la identificación de objetos, el diagnóstico de enfermedades, el ahorro de energía, la elaboración de perfiles para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, los intereses, la fiabilidad, el comportamiento o la ubicación, datos que se utilizan con diversos fines y se encuentran al alcance de empresas, Estados e incluso particulares"[27].

Ahora bien, como mencionan algunos expertos en la materia[28], el uso de tecnologías ligadas al Big Data como la minería de datos propiamente tal o el *machine learning* como disciplina de estudio en el ámbito de la inteligencia artificial no constituyen *per se* herramientas a las que se le atribuye una utilización moralmente incorrecta, puesto que representan avances y mejoras en varios tópicos. Lo que ocurre, es que su operatividad en ciertos Estados carece de una regulación legal adecuada y dinámica, que otorgue las respuestas necesarias a la evolución tecnológica constante. Prescindiendo de ello, las empresas dedicadas al rubro se encuentran en una posición de mayor libertad de acción, pudiendo ofrecer servicios en áreas que podrían vulnerar derechos fundamentales o bienes jurídicos protegidos y amparados por nuestro ordenamiento. Por lo mismo, la discusión debe centrarse en la necesidad de regulación en la medida de lo requerido y según el sector especifico que sea objeto de estudio, como por ejemplo el tema que nos convoca, esto es, los periodos de elecciones.

---

[24] **COMISIÓN EUROPEA**. "Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre inteligencia artificial para Europa", 2018, p. 1. Disponible en: https://eur-lex.europa.eu/legalcontent/ES/TXT/?uri=CELEX%3A52018DC0237

[25] **ROUHIAINEN, LASSE**. Inteligencia artificial. *Madrid: Alienta Editorial*, 2018, p. 17

[26] **MARTINEZ DEVIA, ANDREA**, *op. cit. pp. 7-8.*

[27] *Ibid.*

[28] En este sentido, véanse las intervenciones de Sebastián Valenzuela y Natalia González en el Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

Lo anterior, ya que estos constituyen un pilar basal en las democracias liberales y, por lo tanto, es necesario asegurar que su realización se haga en el marco del pleno respeto por los derechos fundamentales, analizando todas las variables que, hoy en día, podrían poner en riesgo aquellos. Una de estas, es el *microtargeting* electoral y la creación de decisiones automatizadas en conjunto con la elaboración de perfiles para hacer llegar mensajes altamente personalizados al electorado, cuestión que será analizada de forma pormenorizada en el siguiente capítulo y que constituye el objeto de investigación de esta memoria, dada su innegable concurrencia a nivel global[29].

CAPÍTULO II. ÁNALISIS DEL MICROTARGETING ELECTORAL Y SUS IMPLICANCIAS

II.1 ¿Qué es y cómo opera el *microtargeting*?

El denominado *microtargeting*, en su acepción más general, se refiere a una estrategia de publicidad que utiliza técnicas de modelación predictivas mediante el uso de Inteligencia Artificial y otras tecnologías que se valen de una gran cantidad de datos en línea, con el fin de hacerle llegar a los usuarios mensajes altamente personalizados que influyen en la toma de sus decisiones[30].

Ahora bien, si circunscribimos esta práctica en el ámbito político electoral, el Consejo para la Transparencia lo ha explicado como "una herramienta que utilizan los partidos políticos para focalizar segmentos acotados de la población e influir en la elección de un candidato particular"[31]. En la práctica, los partidos contratan los servicios de empresas especialistas en *Big Data* para analizar una gran cantidad de datos que hacen referencia a un vasto grupo de la población y, así, poder clasificarlo en categorías específicas[32] que permiten de manera mucho más fácil incidir en el pensamiento y la opinión del electorado, "persuadiéndolo o disuadiéndolo, informándolo o confundiéndolo, y movilizando o desmovilizando los votos"[33].

Por su parte, para explicar el fenómeno el académico Juan Pablo Luna, se refiere a aquel como una "arquitectura integrada", donde el potencial de las empresas se mide según su capacidad de "integrar y analizar con modelos (…) los datos que cada uno de nosotros generamos en nuestra interacción con el

---

[29] **AAGAARD, PETER; MARTHEDAL, SELMA.** Political microtargeting: Towards a pragmatic approach. *Internet Policy Review*, 2023, vol. 12, no 1.
[30] **EUROPEAN PARLIAMENTARY RESEARCH SERVICE.** *Key social media risk to democracy; Risk from surveillance, personalisation, desinformation, moderation, and microtargeting.* EPRS, 2021, p. 22.
[31] **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit,* p. 13.
[32] **VERGARA AMOROS, GONZALO.** Microtargeting y el futuro desarrollo de campañas políticas. *El Mostrador*, 2018. [En línea] 2022. [Citado el: 15 de enero de 2022] https://www.elmostrador.cl/agenda-pais/2018/11/02/microtargeting-y-el-futuro-desarrollo-de-campanas-politicas/
[33] **EUROPEAN PARLIAMENTARY RESEARCH SERVICE.** *Op. cit,* p. 22

mundo digital[34]. Ello permite, en definitiva, que, habiendo recopilado, georreferenciado y extraído una gran cantidad de datos de distintas fuentes, estas se puedan cruzar e integrar con algoritmos y tecnología conocida como *machine learning*, que permite estudiar los patrones obtenidos y luego usarlos como información clave para movilizar los distintos sectores del electorado, en función de sus propias cualidades y características[35].

Aun cuando esto pueda parecer en extremo novedoso, algunas voces señalan que lo anterior viene a ser una remodelación en términos tecnológicos de estrategias que se utilizan desde antaño por los partidos políticos. En este sentido, Cristóbal Huneeus, director de la empresa de *data science* llamada Unholster, menciona como ejemplo el caso del expresidente Lagos, quien durante su mandato utilizó el arquetipo chileno denominado "señora Juanita" para traducir las consecuencias concretas que tenían las eventuales fijaciones de tarifas en telefonía y agua potable, puesto que como señalaba el mandatario ella "poco entendía de finanzas internacionales"[36]-[37]. Lo anterior, como explica Huneeus, carecía de la intención misma que tiene el *microtargeting* hoy en día, pero permite entender como el mundo político -al menos desde comienzos de este siglo- comprende que deben hablarles a ciertos sectores específicos para poder entregar su mensaje, de acuerdo a la necesidad y realidad de cada uno de ellos.

Agrega Luna que el trabajo de recolección de datos y segmentación, en una escala muy inferior y menos profesional, la realizaban los lideres barriales, mucho antes de que siquiera fuese posible pensar en la irrupción de empresas en el rubro[38]. Estos, por el contacto directo que tenían con los habitantes de su territorio, tenían nociones de sus necesidades, edades, genero e información relevante que podía ser entregada a los partidos politicos en los que militaban, de forma tal que organizar visitas, discursos o proyectos con adherentes resultaba mucho más fácil.

En la actualidad, con el avance de la tecnología en lo referido a minería de datos y procesamiento de aquellos mediante inteligencia artificial, distintas empresas pudieron abrir el camino a un nuevo rubro. Ahora el escenario es completamente distinto, ya que, utilizando plataformas digitales como las redes sociales u otras páginas web, los partidos políticos envían los mensajes a través de publicidad pagada

---

[34] **LUNA, JUAN PABLO EN: ALBERT, CATALINA.** Big Data en campañas: "Para los políticos es más fácil ganar una elección, pero les resulta muy difícil gobernar**".** *CIPER, 2019.* **[**En línea] 2022. [Citado el: 02 de junio de 2022] https://www.ciperchile.cl/2019/09/23/big-data-en-campanas-para-los-politicos-es-mas-facil-ganar-una-eleccion-pero-les-resulta-muy-dificil-gobernar

[35] *Ibid.*

[36] **HUNEEUS, CRISTOBAL** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

[37] **PERALTA SAINZ, ALVARO.** ¿Aprueba o rechaza? La Señora Juanita hoy. *The Clinic 2020.* [En línea] 2022. [Citado el: 02 de junio de 2022] https://www.theclinic.cl/2020/03/06/aprueba-o-rechaza-la-senora-juanita-hoy/

[38] **LUNA, JUAN PABLO EN: ALBERT, CATALINA,** *Op. cit.*

aprovechando la comunicación bidireccional que permiten tales medios, obteniendo rápidas respuestas al estímulo previamente elaborado y configurado de forma nominada para atraerlos[39]. En efecto, no debemos olvidar que hoy en día una gran cantidad de personas tienen acceso a internet y gracias a los teléfonos inteligentes están conectados a la red la mayor parte del tiempo, informándose por redes sociales del acontecer nacional e internacional, incluyendo la información política, que suele disponerse en forma segmentada según el usuario[40].

Así, el flujo de datos manejado por los partidos politicos se amplía aún más y ya no se acota a información referida a la residencia o el nivel educativo para acercarse a grupos de la población. En esto reside lo particularmente novedoso del *microtargeting* político actual[41] ya que ahora se utilizan datos que pueden ser encontrados en línea como el historial de compra y/o navegación de los usuarios, el contenido que les gusta y, en general, sus acciones en el mundo virtual[42]; se agregan datos relativos a su condición social como su registro electoral, dirección, sexo, edad y tamaño del grupo familiar; datos que se obtienen de herramientas tecnológicas avanzadas como el GPS y/o sistemas biométricos[43]; y por último, es posible mencionar el uso de datos comerciales como ingresos, hábitos de gasto de tarjeta de crédito; número de bienes de fácil rastreo como automóviles y tiendas más concurridas[44].

Como es posible apreciar, el auge del *microtargeting* como practica utilizada por los partidos políticos en Chile y el mundo en el contexto de campañas electorales y la búsqueda de militantes guarda estrecha relación con el aumento de la capacidad tecnológica en materia de tratamiento de datos personales de distintas fuentes y, además, tal como ha constatado en Chile la institucionalidad competente en la materia, es posible agregar el avance paralelo del marketing comercial y el desarrollo de las tecnologías de la información[45].

Sin embargo, no podemos dejar de lado la profunda crisis que en las últimas décadas han atravesado los partidos políticos en su calidad de actores relevantes en la vida democrática, siendo completamente ejemplificadores para estos efectos los resultados que el año 2014 se obtuvieron por el CERC en el denominado Barómetro de la Política Chilena del CERC , donde solo un 10% de las personas

---

[39] **ARSENAULT, AMELIA.** Microtargeting, Automation, and Forgery: Disinformation in the Age of Artificial Intelligence. 2020. p.37-38

[40] **ÁVILA, RENATA.**, Ciudadanía Inteligente. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019. EN: **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit*, p. 14.

[41] **DOBBER, TOM; Ó FATHAIGH, RONAN; ZUIDERVEEN BORGESIUS, FREDERIK.** The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 2019, vol. 8, no 4, pp. 15-16.

[42] **EUROPEAN PARLIAMENTARY RESEARCH SERVICE.** *Op. cit,* p. 22

[43] **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit,* p. 14.

[44] *Ibid*, p. 13.

[45] *Ibid.*

confiaba en los partidos políticos, resulta influenciada en buena parte por una mirada crítica de estas instituciones catalogadas como deshonestas[46]-[47]. Por lo mismo, en un contexto donde el acercamiento directo con las personas no logra ser fructífero, a nuestro juicio los partidos prefieren incidir de manera indirecta sobre el electorado, influenciándolo sobre todo cuando no siguen férreamente una ideología en particular, sino que están en la búsqueda de un candidato que se adecue a sus necesidades del presente.

Para lograr algo así de sofisticado, el investigador de la Universidad de Oxford, Raymond Duch señala que "(…) 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"[48].

Dicho lo anterior, es posible sostener que el *microtargeting* y su uso en específico por partidos politicos en el contexto de campañas electorales es un hecho acreditado[49], que tras los años se ha ido profesionalizando y que ha sido objeto de estudio por académicos, investigadores de prestigiosas universidades y centros de estudio en cuanto acontecimiento cierto, permitiendo su entendimiento como un fenómeno presente a lo largo y ancho del globo[50].

Ahora bien, aun cuando la utilización de estas estrategias digitales ha llegado a tal punto de conocerse casos de gran impacto mediático como la operación llevada a cabo por Cambridge Analytica, con la misma fuerza que parte de la doctrina confirma su utilización, un sector de ella recomienda morigerar el discurso por la dificultad en el hallazgo de evidencia que permita acreditar que, además de

---

[46] **CAMACHO CEPEDA, GLADYS.** Financiamiento de los procesos electorales: examen de la ley 19.884 sobre transparencia, límite y control del gasto electoral. *Revista de derecho (valdivia)*, 2015, vol. 28, no 2, p. 127.

[47] **DEL SOLAR, BERNARDITA**. Dinero y política: ¿una mezcla explosiva? *Puntos de Referencia N°391, Edición online.* Centro de Estudios Públicos 2015, p. 2.

[48] **DUCH, RAYMOND.** Universidad de Oxford. Entrevista realizada en el contexto del Seminario "Sigue la Huella de tus Datos", organizado por el Consejo para la Transparencia, 2019. EN: **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit*, pp. 13-14.

[49] **AAGAARD, PETER; MARTHEDAL, SELMA.** Political microtargeting: Towards a pragmatic approach. Internet Policy Review, 2023, vol. 12, no 1. P.14

[50] En este sentido, **BRADSHAW, SAMANTHA; HOWARD, PHILIP N.** Challenging truth and trust: A global inventory of organized social media manipulation. *The computational propaganda project*, 2018, vol. 1 y **BENNETT, W. L., SEGERBERG, A., & YANG, Y**. The Strength of Peripheral Networks: Negotiating Attention and Meaning in Complex Media Ecologies. Journal of Communication, 2018, 68(4), pp. 659-684.

utilizarse el *microtargeting*- este tiene efectos contundentes y certeros en el resultado de las elecciones[51], punto que será analizado en un próximo acápite a propósito de los casos de estudio en nuestro país.

Con todo, procederemos a analizar los argumentos que han sido esbozados por parte de la doctrina especializada tanto a favor como en contra del uso de mensajes focalizados mediante la sistematización de datos recopilados de distintas fuentes, puntualmente en el contexto electoral, que es objeto de estudio de la presente memoria. En este sentido, se expondrán aquellos más relevantes comentando críticamente cada uno de ellos.

II.2. Posturas respecto a la utilización del *microtargeting* en campañas electorales

II.2.1 Argumentos a favor del uso del *microtargeting* en la arena democrática

Los argumentos que podemos posicionar a favor del uso del *microtargeting* tienen como común denominador el hecho de que se desarrollan en base a la falta de participación electoral característica en nuestros tiempos y, además, un analisis costo beneficio, rescatando el hecho de que la focalización en el envío de mensajes al electorado puede favorecer a los partidos políticos abaratando los costos propios del acercamiento con los ciudadanos.

Así, autores como Zuiderveen mencionan que la televisión y la radio ya no logran promover efectivamente la participación electoral, por lo que el *microtargeting* se erige como una herramienta capaz de dar vuelta dicha situación y fortalecer la democracia, en circunstancias en que no se está comunicando una generalidad a un grupo amplio de la población sino que, de forma segmentada, a cada grupo de ciudadanos se le ofrece información ligada a su interés político, captando su atención de manera mucho más sencilla y eficaz, lo que eventualmente podría aumentar la participación de las personas en la convulsionada vida democrática de nuestros días[52].

Respecto a este punto, si bien en primera instancia podría parecer una técnica al menos considerable para hacer frente a un momento en que existe una crisis de representatividad[53], claramente le subyace una pugna entre derechos fundamentales como lo son el derecho a participar en la vida democrática y el derecho a la privacidad. Más aun, debiésemos preguntarnos si efectivamente podríamos

---

[51] Véanse las intervenciones de **HUNEEUS, CRISTOBAL** y **VALENZUELA, SEBASTIÁN** en Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s. Además, en la misma línea, **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. *Cuadernos. info*, 2019, no 44, p. 61-77.

[52] **ZUIDERVEEN BORGESIUS, FREDERIK.** Online political microtargeting: promises and threats for democracy. *Utrecht Law Review*, 2018, vol. 14, no 1, p. 85.

[53] En este sentido se pronuncia **SEBASTIÁN VALENZUELA** en el Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

considerar que la recepción de mensajes configurados especialmente para el usuario en cuestión realmente implica que este esté participando activamente de la vida democrática, puesto que simplemente le serán enviados mensajes que conciernen a sus preocupaciones y/o corriente ideológica en base a una serie de datos que son extraídos de diversas fuentes, difiriendo el marco legal que permite aquello según la legislación aplicable en cada país.

Además, elevar la práctica del *microtargeting* con fines tan utilitaristas podría terminar por socavar aún más la democracia, puesto que su uso solapado es el que permite que por diversos medios -como las redes sociales- los electores "contesten" a los mensajes que se les hacen llegar en forma de publicidad o noticias mediante algoritmos. Si esta práctica se abre a la comunidad como una alternativa abiertamente conocida, muy probablemente terminaría por disgustar a la población, que tendría conciencia de que está accediendo a información sesgada por medio de técnicas eminentemente comerciales, limitando su conocimiento.

Por otro lado, el argumento relativo a la eventual diversificación de la oferta política en circunstancias en que el *microtargeting* podría ser utilizado por nuevos actores políticos[54] que deben hacer frente a cuantiosas barreras de entrada, resulta ser una hipótesis que a la fecha es difícil de comprobar puesto que se carece de estudios serios que permitan avalarlo. De hecho, a juicio de quien les escribe, sería bastante difícil poder acreditar dicha premisa en tanto las empresas especializadas en tratamiento de datos y uso del *microtargeting* tanto a nivel netamente comercial como político cobran elevadas sumas de dinero, por la novedosa tecnología que deben utilizar y los complejos *softwares* que ponen a disposición para tales fines. Por lo mismo, la profundización en el uso de dichas herramientas no terminaría aboliendo las barreras de entrada que actualmente deben sortear, sino que presumiblemente solo las reemplazarían por otras, esto es, la contratación de servicios de tratamiento de datos.

Dicho todo lo anterior, si bien en términos prácticos el *microtargeting* logra efectos interesantes a tener en consideración, deben analizarse con mesura, siendo bastante ingenuo creer que estas herramientas tecnológicas por sí mismas frenarán o revertirán la desconfianza de los ciudadanos hacia la institucionalidad. En la materia, no existen soluciones únicas y, por lo mismo, una discusión legislativa seria se hace necesaria para extraer lo positivo del acercamiento político digital, ponderando siempre los bienes jurídicos en juego, materia que será objeto de analisis en el capitulo siguiente.

[54] **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit,* p. 14.

II.2.2 Argumentos en contra del uso del *microtargeting* en la arena democrática

En la vereda opuesta, encontramos una serie de argumentos que ven con preocupación el uso del *microtargeting*. Obviamente, la amenaza se circunscribe a su aplicación en la vida democrática, particularmente las elecciones y la búsqueda de nuevos adherentes, puesto que su uso en materia comercial solo puede representar un problema en aquellos casos en que los datos que fueron extraídos para enviar los mensajes personalizados se dieron en el contexto de una vulneración de las normas de protección de la privacidad atingentes.

Uno de los estudios más recientes en esta línea, fue efectuado por el Parlamento Europeo mediante su Servicio de Investigación (EPRS), publicando el año 2021 un manuscrito que aborda diferentes problemáticas que se suscitan por la injerencia que tienen actualmente las redes sociales en la democracia contemporánea. Dicho órgano, pone énfasis especialmente en dos riesgos que son consecuencia directa del uso del *microtargeting* en la arena democrática, esto es, la manipulación política que afecta directamente a los ciudadanos y, por otra parte, la distorsión del proceso electoral[55].

Como primer riesgo, la manipulación política que puede menoscabar el ejercicio democrático de los ciudadanos se explica recordando como funciona en sí mismo el *microtargeting*, a saber, enviando por parte de los partidos políticos mensajes altamente personalizados a grupos de ciudadanos que fueron previamente perfilados en base a sus modelos de conducta[56]. Así, explican autores como Zitrain, los partidos explotan en demasía practicas usuales, conocidas y aceptadas en periodos de campaña como lo son las exageraciones y artimañas retoricas, pasando a incluso ofrecer mensajes con contenido profundamente contradictorio que muchas veces se alejan de la propia ideología del partido, con el fin de maximizar el encuentro de nuevos votos[57].

Lo anterior, es lo que el autor define como *digital gerrymandering,* que termina por desvirtuar completamente las expectativas del electorado en primera instancia y, cuando este grupo toma conocimiento de la manipulación que ha sufrido, se siente traicionado y pasado a llevar, socavando aún más las bases de la democracia[58]. Es justamente este punto lo que según Raz distingue el vicio propio del *microtargeting* que se aleja completamente de las tácitamente autorizadas técnicas de persuasión propia de los líderes políticos y sus partidos, puesto que en el contexto del *digital gerrymandering* existe una pormenorizada estrategia que pretende influenciar al electorado a ejercer una acción, como concurrir

[55] **EUROPEAN PARLIAMENTARY RESEARCH SERVICE.** *Op. cit,* p. 23
[56] *Ibid.*
[57] **ZITTRAIN, JONATHAN.** Engineering an election. *Harv. L. Rev. F.*, 2013, vol. 127, p. 335.
[58] **RAZ, JOSEPH.** *The morality of freedom*. Clarendon Press, 1986, p. 204

a votar, o bien, desmotivarlo para que no participe del proceso democrático y así deje el camino libre a un partido que ve amenazada su victoria.

En síntesis, permitir sin mayores limites que los partidos utilicen herramientas deliberadamente manipuladoras, termina por quitar al ciudadano autonomía en la vida democrática, sin tener real capacidad de decidir cómo y cuándo participar[59]. Además, al obstaculizar continuamente el potencial ciudadano para formar su propio criterio político, el *microtargeting* termina naturalmente comprometiendo la privacidad de los individuos, quienes actúan motivados por las presiones psicológicas que se ejercen sobre ellos, en base a los datos recabados con anterioridad[60].

Por otra parte, el segundo gran riesgo dice relación con la distorsión del proceso electoral que se presenta como efecto del uso sistemático del *microtargeting* político. En concreto, los expertos suelen señalar que la manipulación de la que son objeto los ciudadanos cuando el fenómeno muestra su cara más abusiva, termina difuminando las reglas democráticas referidas a la comunicación electoral, pudiendo potencialmente cambiar el resultado de una elección en base a engaños[61].

Obviamente, el impacto negativo que puede causar el *microtargeting* en el proceso electoral varía dependiendo del sistema electoral. El equipo de investigación del Parlamento Europeo explica este punto de la siguiente forma:

> *"In winner-takes-all systems (where the political party or group with the most votes gets all the seats within a given district), political microtargeting that focuses on small but key segments of society (e.g. 'swing voters') may be determine election results. For example, the use of political microtargeting by Cambridge Analytica has been credited as one of the key elements of Trump's electoral success in 2016. In hindsight, it appears that campaigners needed to persuade only a small fraction of voters to achieve the result, as it took about 80 000 votes in three key states to tip the scales. Whereas this situation is less likely to occur in proportional electoral systems (where seats are distributed among parties according to the share of the votes received), even there a significant microtargeting campaign directed to the right sectors of society might be able to tip the balance of an election".*

Sin embargo, aun cuando los riesgos referidos a la manipulación política y la distorsión electoral parecieren resultar argumentos suficientes para quitar terreno a cualquier practica de microsegmentación

---

[59] **SUSSER, DANIEL; ROESSLER, BEATE; NISSENBAUM, HELEN**. Technology, autonomy, and manipulation. *Internet Policy Review*, 2019, vol. 8, no 2. pp. 4-5.
[60] **EUROPEAN PARLIAMENTARY RESEARCH SERVICE.** *Op. cit,* p. 24.
[61] **ARAL, SINAN**. The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health--and How We Must Adapt. *Currency*, 2021, p. 224.

en procesos claves de la democracia como son las elecciones, lo cierto que es que desde nuestro punto de vista las consecuencias negativas no pueden ser estudiadas en base a relatos carentes de evidencia empírica, tal como señala Cristóbal Huneeus y Sebastián Valenzuela[62]. De hecho, este último especialista en un seminario organizado el año 2021 por el Consejo para la Transparencia de Chile, menciona que no existen estudios serios que permitan corroborar que el *microtargeting*, -más allá de su concurrencia efectiva- ha influido en elecciones nacionales o internacionales de forma determinante.

Por lo mismo, tomando en consideración los eventuales problemas que pueden generarse y que han sido expuestos líneas arriba, conviene más bien discutir una regulación lo suficientemente amplia para hacer frente al acelerado proceso de evolución tecnológica, de forma tal que pueda ser aplicada por órganos competentes en la materia y, así, resolver posibles conflictos que puedan suscitarse a este respecto de forma dinámica.

Una completa prohibición sin un articulado que establezca sanciones y fiscalice a los partidos politicos y otros actores que participan desde la sociedad civil en las campañas electorales, a juicio de quien les escribe, podría fomentar el uso de estas herramientas de manera más bien clandestina, sin establecer limitaciones claves referidas a lo preocupante que resulta la transferencia, registro y analisis de nuestros datos sensibles en diferentes espacios digitales con fines electorales.

Así las cosas, en la presente memoria se opta por seguir una postura pro regulatoria como se ha hecho en el territorio europeo, en que teniendo a la vista las consecuencias nocivas que podrían afectar la democracia en el ámbito de las elecciones y el hecho de que el uso de la tecnología vino a reemplazar lo que en antaño se hacía de forma rudimentaria para conocer al público elector (pero con fines en extremo similares como se ha señalado), se ha reglamentado de forma novedosa la aplicación de la inteligencia artificial y, en cuanto a datos personales, se da una respuesta contundente en cuanto a cómo obtenerlos, conservarlos y transferirlos, lo que en definitiva mitiga el desconocimiento de los usuarios respecto a la huella de sus datos.

II.3 Plataformas y métodos para recopilar datos personales sensibles de corte ideológico

Lograr acceder a plataformas que resultan ser fuente de una gran cantidad de datos, a pesar de lo que ingenuamente podría creerse, no es una tarea en extremo difícil. En efecto, en la era digital en que vivimos, constantemente introducimos datos personales consentidamente sin prestar atención a los detalles o incluso al momento exacto en que lo efectuamos. Esto, como se ha dicho, guarda relación con

[62] **HUNEEUS, CRISTOBAL** y **VALENZUELA, SEBASTIÁN** en Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

el auge de internet y la masiva adquisición de dispositivos inteligentes que permiten la subida y descarga de información en cuestión de segundos.

En este escenario, presentaremos algunas de las plataformas digitales donde probable y presumiblemente las empresas especialistas en datos que son contratadas en el contexto de campañas electorales por partidos políticos o candidatos independientes logran capturar e integrar datos personales de los electorales para posteriormente perfilarlos en base a sus preferencias.

II.3.1 Aplicaciones digitales (APP'S)

Las aplicaciones digitales, o como también se les conocen abreviada y comúnmente *APPs*, se refieren a "toda aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles"[63]. En su faz hibrida, es posible incluso su ejecución en equipos de escritorio y, en cualquier caso, prescindiendo de conexión a internet[64]. En términos generales, el concepto aplica para referirse a softwares relativamente simples que se destinan a su uso en dispositivos móviles inteligentes y, para acceder a ellas[65], se suele acudir a los distribuidores que coincidentemente son administradas por las compañías creadoras de los sistemas operativos móviles[66].

Una vez descargadas, el usuario por regla general debe ingresar una serie de datos que van desde el nombre, edad, sexo y domicilio a ciertas preferencias que puedan estar ligadas a la finalidad de la aplicación. Sin embargo, existe un déficit en materia de transparencia de carácter generalizado referido a que hacen las empresas detrás de las aplicaciones con la información personal que recopilan[67]. Lo anterior, es facilitado por marcos regulatorios que son diversos de país en país, explotándose las posibilidades de acceder a una gran cantidad de información personal en Estados que tienen menos desarrollo en una cultura legal de protección de datos[68]. Sin embargo, tal como apuntan Truong y Phu, "la razón fundamental parece ser la disponibilidad de los usuarios a disfrutar de ciertos servicios y aplicaciones sin coste alguno asociado, aunque resulte obvio que el principal incentivo para sus desarrolladores sea la rentabilidad ligada al valor estratégico o de mercado que extraen de los datos y estadísticas de uso a gran escala"[69].

---

[63] **SANTIAGO, RAÚL; TRABALDO**, Susana. *Mobile learning: nuevas realidades en el aula*. Digital-Text, 2015, p. 8
[64] **MUÑOZ, MIGUEL MORENO**. Privacidad y procesado automático de datos personales mediante aplicaciones y bots. *Dilemata*, 2017, no 24, p. 3
[65] *Ibid.*
[66] **SANTIAGO, RAÚL; TRABALDO.** *Op. cit,* pp. 8-9.
[67] **TRUONG, HONG-LINH; PHUNG, PHU H.; DUSTDAR, SCHAHRAM**. Governing bot-as-a-service in sustainability platforms–issues and approaches. *Procedia Computer Science*, 2012, no. 10, p 564.
[68] *Ibid.*
[69] *Ibid.*

En el mismo sentido se pronuncia María Paz Canales, Directora de la ONG Derechos Digitales, quien explica que este tipo de modelos de negocio, donde se permite a los usuarios acceder de manera gratuita a la plataforma o servicio ofrecido, busca generar rentas principalmente de la publicidad y, por lo tanto, se espera una interacción con la aplicación lo más continua posible, lo que permite a su vez extraer datos, ya sea para aumentar la constancia de dicha interacción, como otros fines[70].

En efecto, la proliferación de información confidencial y/o datos personales desde las aplicaciones a sistemas distribuidos de datos que conforman lo que conocemos como *Big data*[71], constituyen el soporte principal de las empresas que se dedican al tratamiento y analisis de datos personales para perfilar. Al mismo tiempo, esta práctica que se aprovecha de las zonas grises del marco regulador y que da pie al mercado de datos personales termina por favorecer escenarios de abuso para los usuarios[72], que como señalamos introduciendo al tema, no solo son perfilados para registrar pautas de consumo que pueden servir a modelos de negocio comercial, sino que también a instituciones u organismos integrantes de la vida pública, como los partidos políticos.

Por lo mismo, la regulación en materia de aplicaciones móviles resulta un verdadero desafío para proteger la privacidad de los consumidores y sus datos personales, toda vez que, como señala el Consejo para la Transparencia del Estado "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"[73], esto, obviamente con el fin de maximizar sus posibilidades electorales.

II.3.2 Redes sociales

Durante la primera mitad del siglo XX las redes sociales, en términos conceptuales, se relacionaban con la sociología producto al trabajo de Frigyes Karinthy que explicaba la teoría de "los seis grados de separación", que se fundamentaba en el hecho de que cualquier persona puede interaccionar con otra persona del planeta utilizando solo seis enlaces[74]. Esto, fue posteriormente recogido y reafirmado por Watts el año 2004, quien -desde nuestro punto de vista- influenciado por el

[70] **CANALES, MARÍA PAZ** en Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s
[71] **MUÑOZ, MIGUEL MORENO**. *Op. cit*, pp 8-9.
[72] *Ibid*, p. 17.
[73] **CONSEJO PARA LA TRANSPARENCIA.** *Democracia y protección de datos personales en la Era Digital*. Santiago : Ediciones Consejo para la Transparencia, 2019, Cuaderno de trabajo N° 13, p. 12.
[74] **BARRIUSO RUIZ, CARLOS**. Las redes sociales y la protección de datos hoy. *Anuario de la Facultad de Derecho (Universidad de Alcalá)*, 2009, no.2, p. 302.

auge en las tecnologías, explicó que el número de conocidos que tenemos crece exponencialmente con el número de enlaces en nuestra cadena de contactos y, con pocos enlaces, se puede llegar a toda la población humana[75].

Hoy en día, hablar de redes sociales es parte común de nuestro lenguaje en términos estrictamente digitales, y cuando mencionamos dicho genero hacemos referencia a distintas especies como Facebook, Whatsapp, Twitter, solo por mencionar algunos ejemplos. Para autores como Cabrera, estas comunidades virtuales que interconectan a personas con afinidades comunes son uno de los mejores paradigmas de lo que conocemos como Web 2.0[76], término que acuñó Tim O'Reilly para referirse justamente a una de las características principales de la tecnología Web se nuestro siglo, esto es, la posibilidad de intercambiar información ágilmente entre los usuarios de una red social[77]. Es justamente esto último lo más atractivo, ya que como bien expone Barriuso:

> *"Hay grupos de interés o de poder que atesoran los contenidos de las redes sociales, entre ellos, datos personales, como información muy valiosa. No es altruismo lo que permite que estos servicios funcionen gratuitamente, quitando los beneficios por publicidad; a cambio pueden obtener información de la 'inteligencia colectiva' del 'neuromundo'. Información que siendo monitorizada, controlada, analizada y segmentada puede evaluar ratios de todo tipo. Esta información de los "medios sociales" sometida a algoritmos de análisis, selección y extracción de contenidos, con seguimiento de palabras clave de forma selectiva permite obtener perfiles de alto significado, con las tendencias por edades, profesiones, aficiones, etc."*[78].

Sin embargo, aun con estos riesgos cada vez son más las personas que acceden a las redes sociales día a día[79], y como señalamos introduciéndonos al tema que nos convoca, los partidos políticos no han estado alejados de este verdadero fenómeno en términos de cantidad de usuarios. En efecto, los medios de comunicación de masas "tradicionales" como la televisión y la radio, que caracterizan por ser unidireccionales y con poca capacidad de retorno que eran utilizados fuertemente desde la segunda mitad del siglo anterior, están poco a poco siendo reemplazados por

---

[75] *Ibid.*
[76] **CABRERA, A**. Evolución tecnológica y cibermedios. *Zamora: Comunicación Social*, p. 117.
[77] **BARRIUSO RUIZ, CARLOS**. *Op. cit*, p. 302.
[78] *Ibid*, p.304
[79] Solo en Chile en enero del 2021 las empresas WE ARE SOCIAL y HOOTSUITE evidenciaron alrededor de 16.000.000 de cuentas ligadas a redes sociales. La totalidad de resultados puede consultarse en https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-chile-en-el-2020-2021/

los *social media* que, superan las deficiencias comentadas ya que son bidireccionales y permiten una comunicación participativa[80], en que los usuarios opinan activamente acerca de sus intereses.

Así, es como por medio de especialistas, capturan y analizan los datos que ofrecen las redes sociales, e incluso, cuando no es posible extraer información de un grupo de población, mediante el uso de *Fake News,* y publicaciones o comentarios hechos por *Bots* se puede inducir a los usuarios a que den su opinión, recolectando valiosos datos relativos a su postura política o preferencia electoral, ejerciendo influencia política, en definitiva.[81].

En síntesis, utilizando estas herramientas en redes sociales. el abanico de posibilidades para manipular datos se amplía, pudiendo perfilar a los usuarios tal como ocurrió en las elecciones presidenciales del año 2016 en Estados Unidos. Así, eventualmente, como señala cierto sector de la literatura, se podría cautivar electores indecisos; acceder a las listas de amigos de aquellos perfiles que manifestaron una inclinación política, bajo el supuesto de que aquellos comparten sus ideales; crear encuestas sesgadas y/o distorsionar el apoyo a un candidato haciendo creer que un gran número de personas votará por él por la cantidad de seguidores que posee (los cuales pueden ser meros *bots*)[82].

II.3.3 Bases de datos administradas por organismos públicos: El ejemplo del SERVEL

La gestión pública no ha estado exenta de la incorporación de las nuevas tecnologías para dotar de mayor eficiencia y transparencia los procesos burocráticos propios de los servicios públicos[83]. Como es posible apreciar en el día a día, cada vez más son los tramites que es posible realizar en línea, desde postulación a becas y créditos universitarios hasta la actualización de la ficha de acreditación del nivel socioeconómico. Esto, tiene como consecuencia que los diversos organismos públicos cuenten con bases de datos de gran envergadura donde almacenan la información que es proporcionada por los ciudadanos.

Si bien su tratamiento queda regulado en el caso chileno por disposición del inciso primero del artículo 1 de la Ley N°19.628 Sobre la Protección de la Vida Privada[84], lo cierto es que de todas formas

---

[80] **BARRIUSO RUIZ, CARLOS**. *Op. cit,* p. 308.
[81] **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit,* p. 12.
[82] *Ibid.*
[83] Para mayor profundidad en el tópico en comento véase: **MONSALVE, DANIELA; GÓMEZ DOMÍNGUEZ, JOSÉ GREGORIO.** Transformación digital: la gestión pública de la nueva era. *Debates IESA,* 2021, vol. 25, no 2.
[84] **Artículo 1º.-** El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política.

la normativa da pie a ciertas fuentes accesibles al público, vale decir, de acceso no restringido o reservado a los solicitantes.

En efecto, el mencionado cuerpo legal -siguiendo la tónica de la regulación comparada[85]- en su artículo 4 inciso quinto otorga una excepción a la regla general relativa al consentimiento en materia de acceso a datos personales y su transferencia. Además, define las fuentes de acceso público en términos amplios, sin establecer un catálogo taxativo de aquellas fuentes como se ha hecho en la legislación española[86], por ejemplo. Alvarado, advierte sobre este punto que la consecuencia directa que deriva de este hecho se traduce en que "se pueden obviar otras obligaciones estipuladas para el tratamiento de datos personales, como obligaciones de información o de mantener reserva de los datos"[87].

En el caso de las bases de datos en poder de la administración pública, las dudas surgen en aquellas circunstancias en que la normativa no expresa directamente la privacidad ni la posibilidad de su publicidad, lo que según Enrique Rajevic deviene en el examen casuístico entre el interés de retener la información y el interés de divulgarla, de cara al daño que podría provocar su revelación[88], lo cual –cómo es posible concluir analizando su jurisprudencia- ha sido el camino que ha seguido el Consejo para la Transparencia como autoridad competente al pronunciarse sobre estos casos[89].

En este contexto de zonas grises, uno de los organismos en torno al cual se ha generado polémica en materia de protección y tratamiento de datos personales es el SERVEL, institución administradora y fiscalizadora de los procesos electorales que tienen lugar en nuestro país. En efecto, hasta el año 2010 dicho servicio ofrecía el padrón electoral en el mercado a un precio que superaba los 20 millones de pesos[90], siendo posible que los privados compraran toda esa información.

Si bien está situación cambio el año 2008 con la dictación de la Ley 20.285 Sobre Acceso a la Información Pública, ya que se determinó por parte del Consejo para la Transparencia que los datos de los ciudadanos contenidos en el padrón electoral eran de carácter público y gratuito, aquello no vino a solucionar la problemática central referida a la circulación de datos sensibles, puesto que se seguía

---

[85] **ALVARADO, FRANCISCO.** Internet y las fuentes de acceso público a datos personales. *Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales*. Taller Sobre Privacidad y Tecnologías, Facultad de Derecho, Universidad de Chile, 2011, p. 86

[86] **ALVARADO, FRANCISCO.** *Op. cit,* p. 40.

[87] **ALVARADO, FRANCISCO.** *Op. cit,* p. 87.

[88] **RAJEVIC, Enrique; AA. VV**. Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación. *Varios autores, Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago: Expansiva*, 2011, p.155

[89] **ALVARADO, FRANCISCO.** *Op. cit,* p.116.

[90] **GARRIDO, ROMINA.** *Datos personales e influencia política en Chile.* Fundación Datos Protegidos, 2018, p.8.

interpretando erróneamente los principios de finalidad y proporcionalidad, que constituyen verdaderas directrices en la materia[91].

Cabe recordar que, en ese entonces, la Ley Orgánica Constitucional 18.556 sobre el Sistema de Inscripciones Electorales y Servicio Electoral fue modificada por la Ley 20.568 del año 2012 relativa a la Inscripción Automática Electoral. A mayor abundamiento, este último cuerpo legal mandató se incorporarán una serie de artículos en la LOC, en los que destacan para estos efectos aquellos contenidos en el párrafo tercero del título primero y en el párrafo uno del título segundo, todos referidos a datos electorales.

Puntualmente, el artículo 8 de la Ley 18.556 dispuso que debía crearse un Registro Electoral que contuviera los siguientes datos de los inscritos: nombre completo, Rut, fecha y lugar de nacimiento, nacionalidad, sexo, profesión, domicilio y circunscripción electoral[92]. Posteriormente, en los artículos 30 y siguientes se señalaba que el SERVEL debía crear dos padrones electorales en los que se acompañara la información contenida en el Registro Electoral, publicándose un documento auditado en la página web del organismo 90 días antes de la elección o plebiscito, siendo expresamente públicos aquellos datos personales[93].

---

[91] **GARRIDO, ROMINA.** *Op. cit.* p.9.

[92] **Artículo 8 de Ley 18.556 anterior a la reforma del año 2021:** *"El Registro Electoral deberá contener los nombres y apellidos de los inscritos, e indicará para cada uno el número de rol único nacional, la fecha y el lugar de nacimiento, la nacionalidad, el sexo, la profesión, el domicilio electoral, la circunscripción electoral que corresponde a dicho domicilio con identificación de la región, provincia y comuna, o del país y ciudad extranjera, según corresponda, a que pertenezca, el número de la mesa receptora de sufragios en que le corresponde votar y el cumplimiento del requisito de avecindamiento, si procede.*
El Registro Electoral también deberá contener los antecedentes necesarios para determinar si la persona inscrita ha perdido la ciudadanía, el derecho a sufragio o se encuentra éste suspendido.
Se entenderá por datos electorales los señalados en este artículo y cualquier otro que sea necesario para mantener actualizado el Registro Electoral".

[93] **Artículo 31 de Ley 18.556 anterior a la reforma del año 2021:** "*Para cada uno de los padrones electorales, el Servicio Electoral determinará un Padrón Electoral con carácter de provisorio, ciento veinte días antes de una elección o plebiscito. Éste contendrá una nómina de las personas inscritas en el Registro Electoral que, conforme a los antecedentes conocidos por el Servicio Electoral antes de los ciento cuarenta días previos al acto electoral, reúnan a la fecha de la elección o plebiscito correspondiente los requisitos necesarios para ejercer el derecho a sufragio.*
Cada Padrón Electoral con carácter de provisorio será objeto de auditorías conforme al Párrafo 2° de este Título. Estos padrones se ordenarán en forma alfabética y contendrán los nombres y apellidos del elector, su número de rol único nacional, sexo, domicilio electoral con indicación de la circunscripción electoral, comuna, provincia y región a la que pertenezcan, o del país y ciudad extranjera, según sea el caso, y el número de mesa receptora de sufragio en que le corresponde votar.
Junto con cada Padrón, y dentro del mismo plazo, el Servicio Electoral elaborará dos nóminas provisorias de Inhabilitados, que incluirá a las personas inscritas que se encuentren inhabilitadas para votar en la correspondiente elección o plebiscito, y que sufraguen dentro o fuera de Chile, según corresponda, con indicación de la causal que dio lugar a dicha condición.

Ante esta particular situación, la Fundación Datos Protegidos el año 2018 solicitó al SERVEL información relativa a la cantidad de veces que entregó el padrón electoral desde el año 2013 vía Ley de Transparencia[94]. La respuesta del organismo fue nada menos que 143 veces, siendo lo más grave el hecho de que en ningún caso se cumplió con la supervigilancia en términos de trazabilidad de los datos solicitados, cuestión que es ordenada por el artículo 5 de la Ley N°19.628 relativa a la protección de la vida privada[95], ya sea que los datos sean públicos o privados. Así, tal como esgrime la Fundación " se terminó configurando una base de datos de fuente accesible al público, un concepto que ha sido debatido por los expertos en cuanto a su origen e interpretación, y que para Datos Protegidos no admite mayor análisis: el SERVEL es responsable de los datos y de su comunicación y los titulares de los datos pierden todo posible control sobre éstos, pues la fuente de acceso al público constituye una de las excepciones al consentimiento y al principio de finalidad (artículo 4° y 9° de la Ley N°19.628, respectivamente)"[96].

El panorama no cambió sino hasta hace poco, específicamente el 16 de febrero del año 2021, en que se publicó la Ley 21.311 que vino a modificar la legislación electoral vigente en aquel momento. Específicamente, se dispuso que se agregará un inciso final a los artículos 33 y 34 del siguiente tenor *"Con todo, la publicación a que se refiere el inciso anterior no contendrá la información relativa al número de rol único nacional, sexo ni domicilio electoral de los electores"*, vale decir, se excluyeron aquellos datos del Registro Electoral (base del padrón en cuanto a información) a los que hacía referencia la norma anteriormente, cuestión que se aplicó durante las elecciones que tuvieron lugar el año 2021.

Los padrones electorales y las nóminas provisorias de Inhabilitados son públicos, sólo en lo que se refiere a los datos señalados en el inciso tercero, debiendo los requirentes pagar únicamente los costos directos de la reproducción. Los partidos políticos recibirán del Servicio Electoral, dentro de los cinco días siguientes a su emisión, en forma gratuita, copia de ellos en medios magnéticos o digitales, no encriptados y procesables por software de general aplicación. Lo mismo se aplicará para los candidatos independientes, respecto de las circunscripciones electorales donde participen.
Sólo las personas inhabilitadas podrán conocer, además, la respectiva causal que las inhabilita".
Artículo 32 de Ley 18.556 anterior a la reforma del año 2021: *Para cada uno de los padrones electorales, el Servicio Electoral determinará un padrón electoral con carácter de auditado, noventa días antes de una elección o plebiscito. Éstos corresponderán a los padrones electorales con carácter de provisorio, después de ser auditado por las empresas de auditoría a las que se refiere el título II y que haya sido modificado sólo como consecuencia de las correcciones sugeridas por las empresas de auditoría en sus informes, si las hubiere, y que, conforme a lo señalado en el artículo 43, sean aceptadas por el Servicio Electoral. Los padrones electorales con carácter de auditado podrán ser objeto de reclamación de conformidad a lo establecido en la presente ley. Junto con cada Padrón, y dentro del mismo plazo, el Servicio Electoral elaborará dos nóminas auditadas de inhabilitados, modificando las anteriores en base a las correcciones sugeridas por las empresas de auditoría que haya aceptado, si las hubiere. Los padrones electorales con carácter de auditado y las nóminas auditadas de inhabilitados deberán ser publicados por el Servicio Electoral en su sitio web con noventa días de antelación a la fecha que deba verificarse una elección o plebiscito. Serán aplicables a los padrones y nóminas antes mencionados las disposiciones contenidas en los incisos tercero, quinto y sexto del artículo anterior.*
[94] **GARRIDO, ROMINA.** *Op. cit.* p.9.
[95] *Ibid.*
[96] *Ibid,* p.10.

Aun cuando esta modificación constituya un antecedente relevante en materia de protección de datos, lo cierto es que durante una gran cantidad de años los padrones electorales contenían información sensible que fue utilizada sin que se tenga conocimiento efectivo de la finalidad con la que fueron solicitados al SERVEL[97]. Ello, permite que hoy en día existan preocupaciones fundadas acerca de aquellos datos, puesto que con dicha base los privados que se dedican a su tratamiento solamente deben corroborar la información, siendo una tarea notoriamente menos dificultosa.

Sin perjuicio de lo anterior, en otras áreas como la relativa a datos comerciales de los ciudadanos, la pugna entre los principios de transparencia y vida privada sigue estando bastante latente. Como es sabido, los denominados datos económicos, financieros, bancarios y/o comerciales, son un fuerte componente del mercado de carácter público. Tal como señala Alvarado, el legislador decidió regular de esta manera con el fin de hacer funcionar correctamente la economía, debido a que la información en cuestión resulta tener un innegable valor en materia de evaluación de riesgos, por ejemplo, para otorgar créditos a los usuarios[98]. En concreto, la Ley N°19.628 se refiere a este tipo de datos pudiendo distinguirse entre aquellos de carácter patrimonial positivo y negativo, siendo estos últimos los que más relevancia cobran, ya que se refieren a información referida a incumplimiento de obligaciones crediticias[99].

Si bien la Ley 20.575 publicada el año 2012 vino a establecer el principio de finalidad en el tratamiento de este tipo de datos, señalando que -salvo puntuales excepciones[100]- la comunicación de estos solo tiene el fin de evaluar el riesgo comercial de los usuarios para los procesos de crédito, lo cierto es que los deudores morosos de los fondos solidarios de créditos universitarios se ven sometidos a otro tratamiento. En efecto, el artículo 15 de la Ley 19.287 dispone que las nóminas de los deudores morosos de aquellos créditos serán públicas y, de hecho, en virtud del artículo 13 bis de la Ley 19.848 no le son aplicables a aquellos lo establecido en la Ley de Protección de la Vida Privada. Así, fácilmente y en pocos minutos es posible descargar los datos personales de los insolventes desde la página web del CRUCH, específicamente su nombre completo, RUT, monto de la deuda y casa de estudios[101].

---

[97] *Ibid, p. 9*
[98] **ALVARADO, FRANCISCO.** *Op. cit,* p.48.
[99] *Ibid,* p. 49
[100] Una de las excepciones está contenida en el artículo 5 de la referida Ley 20.575, el cual dispone: "En caso que el titular de los datos personales de carácter económico, financiero, bancario o comercial, requiera presentar información contenida en los registros o bancos de datos a que se refiere esta ley para fines diferentes a la evaluación de riesgo en el proceso de crédito, podrá solicitar al responsable de éstos una certificación para fines especiales, el que deberá entregarla considerando únicamente las obligaciones vencidas y no pagadas que consten en él".
[101] Los referidos datos pueden ser descargados en el siguiente enlace https://www.consejoderectores.cl/fondo-solidario-de-credito-universitario/

En definitiva, a pesar de la preocupación que surge sobre todo en el caso de tratamiento de datos personales recepcionados por organismos públicos, lo cierto es que sea cual sea la fuente de la información, los partidos políticos y candidatos pueden utilizar estas variables para perfilar a los ciudadanos y abaratar los costos propios de la campaña que deben soportar, tal cual lo hacen las empresas del comercio digital para acercar publicidad a los usuarios. Ahora bien, en cuanto a la determinación del grado de licitud que existe en tal tratamiento, nos remitimos al próximo capitulo.

II.4 Otras problemáticas asociadas al *microtargeting* electoral: *Fake news*, *bots*, donación de servicios de *microtargeting* por grandes compañías a los partidos políticos y otros planteamientos morales frente al fenómeno

Si bien hemos expuesto los riesgos asociados a la microsegmentación desde un escenario en que los datos son recopilados de distintas fuentes, donde la problemática propiamente tal viene dada por el hecho de que un cuerpo legal obsoleto no da respuesta ni protección a los casos en que la procedencia de la información puede ser encuadrada en un contexto de infracción legal, lo cierto es que existen otros riesgos que es menester exponer al menos de forma sucinta.

En efecto, las empresas dedicadas al rubro no siempre se valen de datos obtenidos a través de bancos de información públicos o privados, sino que, en una faceta mucho más activa, haciendo uso de sofisticadas herramientas digitales crean estímulos suficientes en los usuarios con el objetivo de que estos actúen y, así, tomar nota de su modelo de comportamiento[102]. En este sentido, cobran relevancia las noticias falsas (popularizadas conceptualmente en inglés como *fake news*) y el uso de *bots* en redes sociales y otras plataformas[103].

Respecto de las *fake news*, estas son entendidas por Bennet y Livingston como "falsedades, intencionalmente creadas y distribuidas en formato de noticias o documental"[104] y si bien su origen se remonta al siglo XIX debido a la popularidad de los periódicos[105], el fin perseguido en aquel entonces era aumentar los réditos económicos producto de las ventas[106]. Sin embargo, hoy en día también existen

---

[102] **RAMÓN FERNÁNDEZ, Francisca**. Microtargeting, transparencia, datos y propiedad intelectual: una reflexión sobre los nuevos retos de la inteligencia artificial. *Microtargeting, transparencia, datos y propiedad intelectual*, 2021, p. 1-136.

[103] **ARSENAULT, AMELIA.** Microtargeting, Automation, and Forgery: Disinformation in the Age of Artificial Intelligence. 2020.pp 43-48

[104] **BENNETT, W. L. & LIVINGSTON, S. EN: SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. *Cuadernos. info*, 2019, no 44, p. 64.

[105] Respecto a una historia más acabada del origen y desarrollo de las fake news **BERKOWITZ, DAN; SCHWARTZ, DAVID ASA. MILEY, CNN AND THE ONION**: When fake news becomes realer than real. *Journalism practice*, 2016, vol. 10, no 1, p. 1-17 y **UBERTI, DAVID.** The real history of fake news. Columbia Journalism Review, 2016, vol. 15.

[106] **GARCÍA, MARC AMORÓS**. *Fake News: La verdad de las noticias falsas*. Plataforma, 2018.

motivaciones ideológicas detrás de la producción de las mismas, que permiten reforzar ideas preconcebidas y presentes en la opinión pública, o bien, derechamente manipular a la población para que actúe de cierta manera[107].

Su masificación, como sugieren Santana y Huerta, puede ser explicada a través de las teorías de información y de decisión bayesiana, en tanto la atención humana es atraída por lo novedoso, componente clave en la formulación de noticias falsas y que sobrepasan la consideración de los datos objetivos[108]. Además, hoy en día la propia inteligencia artificial permite que con solo el ingreso de una palabra a un *software* se pueda generar una noticia falsa a partir de modelos predictivos del lenguaje, necesitándose muchas veces un analisis acucioso de la información para verificar su veracidad[109]. A ello, se suma el hecho de que las plataformas digitales, dotadas de algoritmos de visualización, reconocen los contenidos más populares y aumentan su tráfico, masificándose a gran escala en cuestión de segundos[110].

Ahora bien, su fundamento como herramienta utilizada para dar vida al *microtargeting*[111] cobra sentido si consideramos el tipo de contenido que las personas comparten de manera voluntaria en redes sociales, de corte eminentemente moral e ideológico puesto que constituye una forma de expresar opinión en sus perfiles o grupos.[112] y, por lo tanto, de forma implícita están dando a conocer datos sensibles. Así, la información es recogida por *social bots,* concepto que hace referencia a cuentas de redes sociales controladas de forma autónoma por un programa computacional[113].

De hecho, estos se utilizan tanto como para esparcir noticias falsas como para apoyar a un candidato en los espacios de opinión digital (como las secciones de comentarios), de forma tal que se cree "la idea de un consenso público en un tema en el que no existe tal consenso"[114] y logren detectar de forma automática a los usuarios que apoyan tales ideas o han recibido y compartido la información falsa que se ha esparcido, operando de lleno el *microtargeting* con posterioridad. Lo anterior, puede llegar al punto de crear verdaderas burbujas entre públicos sumergidos en redes poco heterogéneas, lo que facilita la focalización del contenido a enviarles con el fin de que refuercen sus ideas y para darles la seguridad

---

[107] **GARCÍA, MARC AMORÓS**, *Op, cit.*
[108] **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. Cuadernos. info, 2019, no 44, p. 64.
[109] **KREPS SARAH, McCAIN MILES.** Not Your Father's Bots AI Is Making Fake News Look Real. *FOREIGNS AFFAIRS, 2019.* [En línea] 2022. [Citado el: 02 de junio de 2022] https://www.foreignaffairs.com/articles/2019-08-02/not-your-fathers-bots
[110] Ibid.
[111] Así lo entiende, **CONSEJO PARA LA TRANSPARENCIA.** *Op. cit,* p. 16.
[112] **VALENZUELA, PIÑA y RAMÍREZ EN**: **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. Cuadernos. info, 2019, no 44, p. 64.
[113] **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA, *Op. cit. p. 64***
[114] *Ibid*, p.65

de actuar de una forma determinada, aun cuando tengan dudas[115]. Lo anterior, es lo que se conoce como la teoría del *big nudging*[116].

La aplicación real y las consecuencias negativas provenientes de la utilización de las *fake news* y *social bots* con estos fines han sido estudiadas y documentadas[117], puesto que la mayor cantidad de propaganda electoral se da hoy en día en redes sociales [118]. Así, en primer lugar podemos manifestar que se crean bases de datos a partir de datos sensibles de los usuarios que han sido inducidos a expresarlos, con el objetivo de poder segmentarlos y seguir nutriéndolos con contenido o desecharlos si poseen ideas radicalmente contrarias; en segundo lugar, claramente existe una dificultad propia del mundo digital, puesto que dar con quienes originan las *fake news* y los *social bots* es prácticamente imposible aun utilizando tecnología sofisticada para su persecución, lo que constituye un problema para la institucionalidad competente en materia de elecciones[119]; por último, el hecho de que se utilicen este tipo de herramientas para conocer la opinión de las personas causa un daño profundo al debate público, distorsionan la legitimidad de la participación[120] y como señaló Natalia González en su calidad de Consejera del CPLT, resulta ser un tipo de comportamiento contrario a los derechos humanos y los principios democráticos occidentales[121].

En segundo lugar, y de la mano con el primer riesgo señalado, la propagación de desinformación utilizando datos sensibles en el contexto de estrategias de *microtargeting* mediante IA puede tener como consecuencia una polarización digital que se hace presente de forma posterior en el mundo real, al explotar los temores de los usuarios[122]. Esta opinión es compartida por expertos, como Marcelo Mendoza, investigador del instituto milenio, quien explica la situación de la siguiente manera:

> *"Es muy importante indicar que el perfil determina un umbral de reacción, es decir, una persona en función de su sistema de creencias está más o menos dispuesto a propagar una determinada información. Hay algo que se llama el sesgo de confirmación, si yo conozco cual es el*

---

[115] **CIANCI, LICIA; ZECCA**, **DAVIDE**. Polluting the Political Discourse: What Remedies to Political Microtargeting and Disinformation in the European Constitutional Framework?. *European Journal of Comparative Law and Governance*, 2023, vol. 1, no aop, pp 16-17.

[116] **GONZALEZ, NATALIA.** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

[117] El Inventario Global de Manipulación Organizada en Redes sociales posee evidencia de la práctica en países de todos los continentes, como señalan **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA,** *Op. cit.* p.66

[118] **MORGAN, SUSAN. EN: CONSEJO PARA LA TRANSPARENCIA,** *Op. cit.* p.17

[119] **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA,** *Op. cit.* p. 65

[120] *Ibid.* p. 63

[121] **GONZALEZ, NATALIA.** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

[122] **BARRET, PAUL; HENDRIX, JUSTIN; SIMS, J.GRANT,** Fueling the fire: how social media intensifies u.s political polarization and what can be done about it. NYU STERN, 2021.

perfilamiento de un grupo de usuarios y lo expongo a un determinado contenido, esos usuarios van a tener una probabilidad de compartir esos mensajes que es mucho mayor que si yo lo dirigiera a una audiencia más amplia (…) Como se da el proceso de información selectiva, básicamente lo que va ocurriendo es que estos grupos que están muy bien perfilados van recibiendo cierta información que es muy de nicho por decirlo así, y por lo tanto, se empieza a formar una especie de burbuja de información en la cual se maneja una visión muy parcial de la información que es de interés de esos grupos específicos."[123].

Lo anterior, convierte a los usuarios en receptores de mensajes con alto componente emocional para disminuir la capacidad de razonamiento lógico[124], condicionando su comportamiento al miedo y sus aflicciones. Esto mismo fue lo que puso en tela de juicio la operación económica que terminó haciendo que uno de los controladores de la empresa Sosafe sea Instagis Spa, empresa dedicada al tratamiento y modelamiento de datos contratada en varias ocasiones por los partidos politicos del medio nacional[125]. En efecto, el software desarrollado por Sosafe permite georreferenciar lugares donde se cometen delitos, permitiendo denunciar los hechos en línea a ciertas autoridades como municipio o policías[126], lo criticado, es que una empresa que analiza datos en el contexto de campañas electorales, pueda tener acceso a datos personales que fueron entregados para un *software* de seguridad en particular, siendo difícil controlar si efectivamente se ha dado ese traspaso de información y, por lo tanto, los miedos han sido un factor relevante al micro focalizar contenido político.

La preocupación en el contexto internacional no ha sido menor y, de hecho, como se verá más adelante a propósito de la regulación comparada de datos e IA, el parlamento de la unión europea como pionera en dichas materias, se encuentra discutiendo el último borrador del reglamento de inteligencia artificial, en que se dispone expresamente en su título segundo que constituyen herramientas de IA prohibidas aquellas que "tienen un gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos"[127].

---

[123] **MENDOZA, MARCELO.** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

[124] Ibid.

[125] **SEPÚLVEDA, NICOLAS.** Alguien te mira: así funciona el gigante de las campañas políticas que controla Sosafe. *CIPER 2019.* [En línea] 2022. [Citado el: 20 de julio de 2022] https://www.ciperchile.cl/2019/09/11/alguien-te-mira-asi-funciona-el-gigante-de-las-campanas-politicas-que-controla-sosafe/

[126] Las funciones de Sosafe pueden ser visualizadas en su página web https://es.sosafeapp.com/

[127] El reglamento puede ser encontrado en el siguiente link https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

En tercer lugar, para finalizar, cabe mencionar los riesgos que implica la normalización del uso de estas herramientas sin una institucionalidad que tenga la competencia para supervigilar que se respete el marco normativo, de haberlo y ser adecuado. Lo anterior, considerando lo señalado en el acápite anterior, esto es, el alto costo en la contratación de los servicios, que termina por privilegiar a los partidos más poderosos adquisitivamente[128]. Además, como menciona el International Institute for Democracy and Electoral Assistance, la legislación de financiamiento de partidos podría ser fácilmente burlada si consideramos que las herramientas digitales pueden ser contratadas en el exterior sin dejar rastro[129], o bien, podemos arriesgarnos a que grandes compañías como Facebook o Google (poseedores de una infinidad de datos a gran escala), donen servicios de *microtargeting* a candidatos afines a su ideología, parcializando el contenido digital y socavando la libertad informativa[130] que es un pilar fundamental de la democracia.

II.5 Posible uso de *microtargeting* en campañas electorales chilenas: caso de estudio

Chile no ha estado ajeno al influjo y auge de las tecnologías en la vida cotidiana. Además, como es relevante con motivo de esta investigación, nuestro país es uno de los tantos Estados en que el fenómeno de la crisis partidaria[131] y el impacto de sus efectos en la democracia es notoria hace más de una década, generando problemas que son constante motivo de estudio y que, como algunos postulan, fue una de las causas del "estallido" o "revuelta social" que tuvo ocasión en octubre del año 2019[132].

En este contexto, que podríamos catalogar de desapego generalizado por la política institucional – o como llaman algunos autores "desafección política" [133] – es que la disminución de la participación ciudadana en la política convencional e incluso no convencional se haya agudizado en las últimas décadas, cuestión que se acentuó aún más con la implementación del voto voluntario el año 2012. Por

---

[128] **INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE.** Digital Microtargeting, Political Party Innovation Primers, 2018, p.18. Disponible en: https://www.idea.int/sites/default/files/publications/digital-microtargeting.pdf

[129] Ibid. 19

[130] **ZITRAIN, JONATHAN.** Engineering an Election, Digital Gerrymandering poses a threat to democracy. Disponible en: https://harvardlawreview.org/2014/06/engineering-an-election/. En el mismo sentido **SUSSER, DANIEL; ROESSLER, BEATE; NISSENBAUM, HELEN**. 2019. "Technology, autonomy, and manipulation". Internet Policy Review 8, p.2. Disponible en: https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation. y policyreview-2019-2-1410.pdf

[131] Un comentario más acabado se puede encontrar en **HUNEEUS, CARLOS**. Malestar y desencanto en Chile. Legados del autoritarismo y costos de la transición. *Papeles de Trabajo-Programa de Estudios Prospectivos*, 1998, vol. 54, p. 1-72. Véase también **HUNEEUS, CARLOS**. Partidos en Chile: debilidad y crisis. *Mensaje*, 2009, vol. 58, no 580, p. 6-10.

[132] En este sentido, véase **WAISSBLUTH**, **MARIO**. Orígenes y evolución del estallido social en Chile. *Santiago de Chile: Centro de Estudios Públicos Universidad de Chile*, 2020.

[133] **PAVLIC, RODOLFO; ARÉVALO, ROBERTO MARDONES**. Chile 2010: la desafección política y su impacto en la participación política convencional y no convencional. *Revista del CLAD Reforma y Democracia*, 2019, no 73, p. 189-226.

consiguiente, ha sido una tarea importante para los partidos políticos poder movilizar a los ciudadanos no militantes para que estos concurran a las urnas en los periodos de elecciones, utilizando diversos tipos de herramientas, siendo lo más novedoso el uso de aquellas ligadas a la microsegmentación del electorado.

Si bien la efectividad de su utilización en el medio nacional está en tela de juicio y ciertos expertos como Sebastián Valenzuela, han llegado a señalar que la "evidencia empírica de que todo (…) opere es bastante cuestionable"[134], la elección presidencial del año 2017 ha sido objeto de estudio y revuelo mediático por la utilización de herramientas tecnológicas de procesamiento de datos y segmentación de electores, por lo que serán revisadas separadamente a la luz de la literatura vigente.

II.5.1 Elecciones presidenciales del año 2017

Las elecciones presidenciales que tuvieron lugar el año 2017 en nuestro país fueron objeto de revisión por parte de centros de estudios especializados en el tratamiento de datos, como la Fundación Datos protegidos, que en un artículo publicado el año 2018 hizo presente la posible utilización de herramientas de *microtargeting* para movilizar votos, siendo prácticamente uno de los pocos materiales académicos que se refieren a la situación en términos pragmáticos en nuestro país[135].

En concreto, Datos Protegidos da especial énfasis a la cantidad de votos emitidos en favor de los entonces candidatos Alejandro Guillier y Sebastián Piñera, quienes en primera vuelta obtuvieron 1.498.040 y 2.418.540 votos respectivamente[136], lo que les consagró como primeras mayorías para disputar el balotaje. Luego, los resultados de la segunda vuelta dieron por ganador al expresidente Piñera, quien obtuvo 3.796.918 votos, casi un 10% más que Guillier, quien obtuvo 3.160.628 votos según datos otorgados por SERVEL[137], en unas elecciones marcadas por la abstención ciudadana.

Como se señala en el documento emanado desde la fundación en comento[138], fueron estos antecedentes los que motivaron a los periodistas de la Tercera, María José Ahumada e Ignacio Bazán, a elucubrar ciertas hipótesis pocos días después de los resultados electorales que permitieran desenmarañar

---

[134] **VALENZUELA, SEBASTIÁN.** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

[135] **GARRIDO, ROMINA.** *Datos personales e influencia política en Chile.* Fundación Datos Protegidos, 2018.

[136] Datos extraídos desde el sitio web oficial del SERVEL: https://historico.servel.cl/servel/app/index.php?r=EleccionesGenerico&id=187

[137] Datos extraídos desde el sitio web oficial del SERVEL: https://historico.servel.cl/servel/app/index.php?r=EleccionesGenerico&id=216

[138] **GARRIDO, ROMINA,** *Op. cit,* p.15

la estrategia detrás de una victoria que, en sus palabras, "no solo motivó gente no había votado en primera vuelta, sino que fue capaz de robarle votos al mismo Guillier"[139].

El sustento de la tesis propuesta por ambos dice relación con una supuesta planificación descentralizada por parte de Rodrigo Ubilla (RN), encargado territorial del comando de Piñera en ese entonces, quien optó por nombrar coordinadores regionales que propusieran planes de acción adecuados para los distintos territorios bajo su supervisión, en el entendido de que debían acercarse de diferente modo a cada grupo de votantes según sus características como habitante[140].

Ahora bien, para Datos Protegidos la estrategia utilizada no es en sí misma relevante, sino que las herramientas que fueron aplicadas para poder conocer a los distintos tipos de electores según su ubicación en el territorio nacional. En particular, lo que sirvió de base para esgrimir por parte del equipo de la Tercera que las elecciones presidenciales del año 2017 fueron objeto de *microtargeting* electoral y, más aún, que aquello favoreció la victoria de Sebastián Piñera en la segunda vuelta, fue la contratación de la empresa de tratamiento de datos InstaGis por Renovación Nacional para las elecciones municipales del año 2016, quienes suscribieron un contrato de prestación de servicios con aquella empresa el 05 de septiembre de ese mismo año, según es posible confirmar en el portal de transparencia del partido, que da acceso al contrato propiamente tal[141].

En dicho documento, se consigna que Instagis SPA es una empresa que se dedica a las consultorías en el marco general de las tecnologías de la información, desarrollando, arrendando y vendiendo softwares[142]. Además, se señala que el contrato celebrado tiene por objeto el "perfilamiento de votantes de las comunas objetivo del CLIENTE, detalladas en el anexo del contrato 'Detalle de los Servicios', en base a la información pública electoral disponible a la fecha del contrato y las interacciones políticas reveladas públicamente en Facebook, con el fin de que terceros efectúen acciones segmentadas a los votantes de la comuna, en base a sus características y preferencias individuales, a través de dos medios; 1) audiencias personalizadas de Facebook (Facebook custome audiences) y 2) Call Center"[143].

Dicha empresa, fue contratada en diciembre del año 2017 por el equipo de Sebastián Piñera, según consta en la planilla de gastos rendida al SERVEL, individualizando la factura que asciende a la

---

[139] **AHUMADA, MARIA JOSÉ; BAZÁN, IGNACIO.** Piñera: Viaje al corazón del triunfo. *La tercera, 2017.* [En línea] 2022. [Citado el: 26 de julio de 2022] https://www.latercera.com/noticia/pinera-viaje-al-corazon-de-su-triunfo/

[140] Ibid.

[141] El documento en cuestión puede ser visualizado en el siguiente link: http://transparencia.rn.cl/wp-content/uploads/2017/02/01.-Intagis-SPA.pdf.

[142] Ibid.

[143] Ibid.

suma 10.053.425 como "Licencia de software de comunicaciones"[144]. Esto, en el marco de la victoria electoral, motivó a otros medios a indagar en los servicios prestados por la empresa de comunicaciones, como una forma de verificar su rol en el resultado de los votos, cuestión que es recogida como información fundamental en el estudio realizado por la fundación Datos Protegidos.

En razón de ello, el medio periodístico CIPER decidió contactarse con el entonces secretario general de Renovación Nacional, Mario Desbordes, quien explicó el *modus operandi* y los objetivos que como partido tenían al contratar los servicios de Instagis, ya que señaló "Ocupamos intensamente la herramienta de Instagis en las municipales de 2016. A través de Facebook, por ejemplo, se perfilan a los electores de una comuna determinada y se detectan cuáles son abiertamente de derecha, de centro o de izquierda, y cuáles son neutros. Con eso trabajamos un mensaje específico para los de derecha, otro para los neutros, no molesto ni pierdo tiempo con los de izquierda, y si tengo los recursos puedo traducir eso en un trabajo de campo también aplicado con las mismas lógicas"[145].

Por su parte, Pablo Matamoros, director de la campaña digital de Renovación Nacional reconoció abiertamente que "Lo que hizo Instagis en estos dos años de campaña fue entregarnos audiencias segmentadas para Facebook, para que nosotros pudiésemos incluir o excluir audiencias y ejecutar inversiones en esa plataforma"[146]. De hecho, desde la propia empresa se reconoció que utilizaron datos para tales fines, sosteniendo eso sí, que obtendrían información de la inclinación ideológica de los usuarios en grupos de acceso público en Facebook, cruzando dichos datos con otros obtenidos, por ejemplo, del padrón electoral[147].

Así, los dichos expuestos anteriormente llevaron a concluir a la fundación Datos Protegidos que "el perfilamiento de votantes es un negocio al alza"[148] y constituye un hecho. En la misma línea se han pronunciado centros de estudio abocados a la materia como en la ONG Derechos Digitales y desde el propio Consejo para la Transparencia de Chile[149]. Sin embargo, como mencionamos escuetamente en acápites anteriores, el que efectivamente existan empresas especializadas en este tipo de estrategias y

---

[144] Datos extraídos desde el sitio web oficial del SERVEL: https://www.servel.cl/ingresos-y-gastos-de-candidatos/
[145] **CIPER.** Instagis: el "gran hermano" de las campañas políticas financiado por Corfo. *CIPER 2018.* [En línea] 2022. [Citado el: 20 de julio de 2022] https://www.ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/
[146] **GARRIDO, ROMINA,** *Op. cit,* p.19
[147] *Ibid*, p.23
[148] *Ibid* p.28
[149] **VALENZUELA, SEBASTIÁN.** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

que, además, estas sean contratadas por partidos de todo el espectro político, no tiene como consecuencia directa que se haya influido con éxito en la votación de los electores.

En primer lugar, como menciona Sebastián Valenzuela, porque se carece de estudios serios en el medio nacional e internacional que puedan establecer una causalidad entre la operación del *microtargeting* y el resultado final de las elecciones[150]. En segundo lugar, como explica certeramente Cristobal Huneeus respecto a las elecciones del 2017, porque tendría que demostrarse que las 800.000 personas que votaron en primera vuelta y no votaron en segunda, junto con las 1.500.000 personas que no votaron en primera vuelta, pero si en segunda, recibieron mensajes que pudieron haber desalentado o alentando su voto, sin poder conocer en realidad por quien votaron en circunstancias en que el sufragio es secreto[151]. Continua el experto señalando que el problema para estudiar estas variables es que los datos son de baja calidad y se suma la volatilidad de la participación en escenarios politicos complejos como el nuestro, atribuyéndose consecuencias en los resultados de elección al *microtargeting* mediante relatos mediáticos exentos de evidencia empírica[152].

De hecho, en uno de los pocos estudios que midieron la difusión de *fake news* y mensajes de apoyo a candidatos por *social bots* en espacios digitales como Facebook y Twitter durante la campaña presidencial del año 2017, sus autores señalaron que "como conclusión general, se puede decir que no existe evidencia que la discusión eleccionaria presidencial en Chile estuviera cooptada o secuestrada por ciber-tropas, es decir, no hubo grandes grupos de individuos mandatados por partidos politicos, candidatos presidenciales o por el gobierno cuyo objetivo fuera desvirtuar la conversación"[153].

Por lo tanto, para efectos de la discusión atingente a la presente memoria, debemos manifestar que no es posible, al día de hoy, acreditar que realmente el *microtargeting* tenga incidencia directa en el resultado de una votación. Sin embargo, lo anterior no implica que la discusión legislativa en materia de protección de datos e IA tenga que dejarse de lado y, por el contrario, la regulación europea constituye el escenario más avanzado hacia donde debiésemos dirigirnos, teniendo siempre presente que la tecnología avanza mucho más rápido que la técnica jurídica. Esto justamente, será analizado en los próximos acápites.

---

[150] *Ibid.*
[151] **HUNEEUS, CRISTOBAL** Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s
[152] *Ibid.*
[153] **VALENZUELA, PIÑA y RAMÍREZ EN**: **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. Cuadernos. info, 2019, no 44, p. 73.

CAPÍTULO III. ANALISIS CRÍTICO DEL MARCO NORMATIVO NACIONAL PARA EL TRATAMIENTO DE DATOS PERSONALES Y OTROS PROYECTOS DE LEY COMPLEMENTARIOS

En Chile, hasta el año 1999, se carecía de protección legal especializada en materia de protección de datos. De hecho, ante la ausencia de una consagración constitucional expresa, parte de la doctrina y jurisprudencia de la época, en un claro esfuerzo interpretativo para sortear las dificultades propias de este vacío, señaló que podía deducirse tal protección en el artículo 19 N°4 de nuestra Constitución, en tanto se garantiza "el respeto y la protección a la ida privada y a la honra de la persona y su familia"[154].

Sin perjuicio de lo anterior, desde el comienzo de los años 90', la discusión parlamentaria referida a la creación de un cuerpo legal que regulara de forma específica la protección de datos personales comenzó a tomar fuerza, lo que varios años más tarde traería la dictación de la Ley N°19.628 Sobre Protección de la Vida Privada, vigente hoy en día. Sin embargo, tal como retrata Viollier, las críticas no tardaron en llegar, argumentándose por autores como Jijena y Cerda, que el éxito de su promulgación viene dado por el hecho de ser una de las primeras leyes de protección de datos en la región latinoamericana, mas no por su contenido, el cual fue catalogado como fragmentario e insuficiente para lograr sus objetivos[155].

Esto, causa problemas hasta el día de hoy, aun cuando tras 4 años de discusión legislativa el año 2018 se hiciera efectiva la inclusión de la protección de los datos personales en el artículo 19 N°4 de nuestra Constitución. En efecto, el mencionado precepto dispone que *"El respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"*. Como es posible apreciar, la protección constitucional no tiene efectos prácticos si la Ley a la que se remite es deficiente.

Comprendiendo este escenario, la importancia de examinar la Ley N°19.628 para efectos de la presente memoria es determinar si su insuficiencia en términos de protección de datos personales es una de las causas que permite que el mercado de datos prolifere de forma acelerada, haciendo mucho más fácil para las empresas dedicadas al rubro utilizar información con fines, por ejemplo, de perfilamiento electoral, sin existir mecanismos de cumplimiento efectivos, ni sanciones que conduzcan a la aplicación de la normativa.

---

[154] **VIOLLER, PABLO.** El estado de la protección de datos en Chile, 2017. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf, p. 7

[155] *Ibid.*

III.1 Historia de la Ley N° 19.628 Sobre Protección de la Vida Privada

La Ley N°19.628 Sobre Protección de la Vida Privada, se origina gracias a la moción del ex Senador Eugenio Cantuarias Larrondo, el día 05 de enero de 1993, con la finalidad de dar protección civil al derecho a la privacidad de las personas, en caso de que se produjeran eventuales intromisiones o transferencia de los mismos por parte de terceros[156].

En la misma moción, se declara que los "parámetros orientadores" del proyecto se encuentran en el Derecho Comparado, y que particularmente vienen dados por los tratados internacionales de Derechos Humanos suscritos y ratificados por Chile y, además, otros cuerpos legales vigentes en aquella época en diversos Estados, como España, Francia, Reino Unido y Noruega, bastantes avanzados en la materia[157].

El fundamento, se entiende tomando en consideración las palabras del ex Senador, quien señalaba que "la informática debe estar al servicio de las personas y que su desarrollo deberá realizarse respetando el derecho a la vida privada de las mismas"[158]. De esto, se puede desprender la preocupación que existía ante la irrupción de la tecnología computacional y el internet, medios que en ese entonces eran utilizados principalmente por bancos, administradoras de fondos de pensiones, aseguradoras, instituciones de salud, casas comerciales, entre otras instituciones del mismo tipo.

Teniendo en cuenta lo anterior, el contenido del proyecto comprendía un desarrollo legal de lo que se entendía comprendido en el artículo 19 N° 4 de nuestra Constitución Política de la República, esto es, el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. En efecto, se caracterizó el derecho a la privacidad y aquellos derechos contenidos en aquel; posteriormente se desarrollaron principios aplicables a la materia; se incluyeron hipótesis de intromisión considerados antijuridicos y aquellos que no y, por último, se articularon los mecanismos civiles procesales donde se comprendían acciones indemnizatorias y civiles de protección de los datos personales.

Ya en aquel entonces, conforme consta en el boletín N° 896-07 correspondiente al primer informe recibido por la Comisión de Constitución del Senado el año 1995, se daba cuenta desde un punto de vista constitucional que "el proyecto de ley no trata ni aborda todas las materias que pueden o podrían en el futuro estar comprendidas en la protección del artículo 19, Nº 4º, de la Constitución Política"[159].

---

[156] **BIBLIOTECA DEL CONGRESO NACIONAL,** Historia de la Ley 19.628 Protección de la vida Privada. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf, p.4
[157] *Ibid,* p.5
[158] *Ibid,* p. 7
[159] *Ibid*, p.19

Además, el profesor Gómez Bernales señaló que el proyecto permitía concluir que toda intromisión en la vida privada era -en principio- ilegitima, siendo sumamente difícil determinar de forma clara aquellas hipótesis en que los datos pueden ser almacenados y entregados a terceros y los casos en que no, haciendo difícil la fiscalización sobre este punto[160].

Durante los años siguientes, la discusión parlamentaria tuvo por objeto limitar los tópicos tratados por la ley, aun cuando existía un consenso generalizado en la necesidad de regular la materia de forma amplia. Por ello, sin perjuicio del intento inicial de regular los alcances de la protección de la vida privada en términos generales, lo cierto es que finalmente la Ley terminó por regular únicamente el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares[161]-[162], no siendo concordante esto con el propio título que se da a la ley en comento.

Por otra parte, se prescindió del catálogo de intromisiones ilegitimas en la vida de las personas e igualmente de la presunción de ilegitimidad de las intromisiones en el caso de conductas contrarias al espíritu de la ley. Como señala Viollier, estas limitaciones de contenido se explican por la decisión del legislador de optar por una Ley de carácter general, "aplicables a distintas circunstancias relativas al tratamiento de datos personales"[163].

En palabras de Jijena, la causa de este cambio se debe principalmente a dos factores[164]. En primer lugar, el desconocimiento de una materia altamente técnica y poco desarrollada en la época, lo que no permitió una discusión legislativa elevada y con miras a la tecnología. Por otra parte, el poder económico por medio de empresas y gremios tuvo una gran incidencia, lo que relegó al cuerpo legal a la regulación del negocio acerca del procesamiento de datos personales de forma laxa, sin tomar en consideración el futuro ni mucho menos el objetivo principal de la moción, la protección de la vida privada y, dentro de aquella garantía, el tratamiento de la información personal de los ciudadanos.

Así las cosas, termina por publicarse la Ley N° 19.628 el 28 de agosto de 1999, modificándose sustantivamente el contenido de la moción parlamentaria original y, de hecho, distando bastante de las leyes comparadas supuestamente tenidas en consideración al momento de su redacción, como, por

[160] *Ibid,* p.20
[161] **VIOLLER, PABLO.** *Op, cit.* p.10
[162] **VIAL, FELIPE.** Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 23-36, 2001, p. 23.
[163] **VIOLLER, PABLO.** *Op, cit.* p.16
[164] *Ibid,* p.7

ejemplo, la ley francesa, española y británica[165], cuestión que permita explicar por qué se tramita una nueva ley para regular la materia.

III.2 Análisis crítico de la Ley vigente N° 19.628 Sobre Protección de la Vida Privada

Como fue señalado líneas arriba, el legislador optó por aprobar una Ley que no regula orgánicamente todos los aspectos de la vida privada de los ciudadanos limitándose de manera muy específica al tratamiento de datos personales por bancos de datos por sujetos de derecho público y privado, excluyendo únicamente del ámbito de aplicación los datos personales que circulen en ejercicio de la libertad de información y opinión consagradas constitucionalmente en el artículo 19 numero 12[166].

Dentro de las disposiciones normativas más relevantes en la Ley podemos distinguir las definiciones de dato personal, dato personal sensible, bases de licitud a estos y otras clasificaciones analizadas al comienzo de esta memoria. Además, puede desprenderse del espíritu del cuerpo legal que: es necesaria la autorización del titular o la ley al momento de transferir datos personales; debe concurrir una finalidad determinada, legitima y explicita en el tratamiento de datos; las transferencias de datos personales deben no pueden ser vulneradoras de las garantías constitucionales[167].y, por último, se explicita uno de los principios rectores en materia de Derecho Privado, como lo es la responsabilidad de las personas que comercializan bases de datos personales.

Cabe agregar que, doctrinariamente se articularon los principios que se entienden consagrados en la Ley, los cuales son fundamentales como directriz interpretativa al momento de suscitarse problemáticas asociadas a la transferencia de datos. Como bien resume Peña, los principios aplicables son los de: libertad en el tratamiento de datos personales; información y consentimiento del titular; calidad de los datos; protección especial a los datos sensibles; seguridad de datos; confidencialidad respecto a la información recibida y el principio de finalidad[168].

Ahora bien, las principales críticas que se realizan a la Ley N° 19.628 se fundamentan en la baja eficacia de esta, en términos de protección. En efecto, como puede desprenderse del principio de libertad en el tratamiento de datos personales y recordando las criticas esbozadas por Jijena relativas al lobby empresarial y gremial en el proceso de creación del cuerpo legal[169], se propició un mercado flexible de

---

[165] *Ibid.*
[166] **VIAL, FELIPE.** *Op, cit.* p. 23-24.
[167] Ibid. 33-34
[168] **PEÑA YAÑEZ, SEBASTIÁN.** Régimen de indemnización de perjuicios de la ley 19.628 y la seguridad de datos personales. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, 2019, pp. 19 y ss.
[169] **CIPER.** Instagis: el "gran hermano" de las campañas políticas financiado por Corfo. *CIPER 2018.* [En línea] 2022. [Citado el: 03 de agosto de 2022] https://www.ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/)

datos personales en Chile, basado en la utilidad económica que genera el flujo de información tanto para los organismos públicos como privados[170]. Dentro de las principales razones para sostener lo deseable que es contar con información personal de terceros encontramos: determinación del riesgo en mercados crediticios; disminución de costos de búsqueda en el mercado de datos con fines publicitarios y de *marketing;* y, el caso del Estado disminuye los costos asociados a la planificación de una política pública orientada a sectores determinados de la sociedad[171].

Sin embargo, permitir la comercialización de información personal por parte de terceros requiere -entendiendo el bien jurídico en juego- que la libertad dada al mercado se circunscriba dentro de límites establecidos en el marco normativo aplicable, en nuestro caso, la N° Ley N°19.628. Empero, esto no logra materializarse, pudiendo sistematizarse las criticas emanadas desde la doctrina especializada de la siguiente manera:

- **Ausencia de un órgano de control especializado:** La creación de un cuerpo normativo que brinde protección en la materia supone necesariamente que, para hacer efectiva la tutela, se pueda recurrir a un órgano de carácter administrativo en caso de una vulneración relativa a los datos personales de los ciudadanos, con facultades fiscalizadoras y sancionatorias. Sin embargo, en nuestro país esto no se contempló en la discusión legislativa, transcurriendo casi 10 años desde la publicación de la Ley N°19.628 sin un órgano competente.

  No fue sino hasta la dictación de la Ley N° 20.285, el año 2008, que se le otorga la función de "velar por el adecuado cumplimiento de la Ley Nº 19.628, , por parte de los órganos de la Administración del Estado" al recién creado Consejo para la Transparencia ("CPLT")[172].

  Aun cuando lo anterior constituía un intento por superar una de las críticas más contundentes y coetáneas a la entrada en vigencia de la Ley N° 19.628, lo cierto es que no cumple con las características fundamentales que requiere un órgano administrativo competente, ya que el CPLT no se ajusta al principio de especialidad, autonomía y eficiencia[173]. Además, no está

[170] **JERVIS, PAULA.** La regulación del Mercado de datos personales en Chile. Tesis para optar al grado de Magíster en Derecho, Universidad de Chile, 2006, p.189
[171] Ibid. 191-192
[172] **VIOLLER, PABLO.** *Op, cit.* p.27
[173] **ASESORÍA TÉCNICA PARLAMENTARIA.** Consulta experta sobre la Ley de Protección de la vida privada de las personas, 2018. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26703/2/BCN_Consulta_experta_sobre_la_Ley_de_Proteccion_de_la_vida_Privada.pdf, p.9

dotado de capacidad regular a nivel administrativo ciertas materias ni tampoco cuenta con facultades sancionatorias que permitan garantizar el cumplimiento de la Ley[174].

De esta forma, como afirma el académico Gonzalez Hoch, la ausencia de recursos en sede administrativa para dirimir conflictos obliga al titular de los datos personales, en calidad de víctima, a tener que accionar en sede judicial, con los excesivos costos que aquello implica[175].

- **Ausencia de un registro público de bancos de datos personales privados:** Una de las omisiones más graves en la Ley N° 19.628 es que no obliga a los bancos de datos personales privados a registrarse, por lo cual, no se puede saber realmente hoy en día cual es la cantidad de aquellos operando en nuestro país. La única excepción con respecto a este punto es el mandato a que los organismos públicos comuniquen la creación de bancos de datos, en conjunto con la finalidad y tipos de datos recopilados[176]. Como expone Jijena, el legislador no reguló este aspecto bajo el argumento de no tornar excesivamente burocrático el mercado[177], lo que refleja aún más el punto tratado líneas arriba, esto es, la influencia del poder económico en la creación de una ley bastante liberal en lo que se refiere al comercio de datos.

- **Insuficiencia de los mecanismos de tutela y sanciones:** La doctrina esta conteste en que la acción jurídica para resguardar a las personas en casos de tratamientos abusivos de sus datos personales era el Habeas Data[178], entendido en Chile bajo su función de amparo de los derechos del titular de los datos tratados de manera ilegitima[179]. En concreto, su procedencia deriva de la infracción de los derechos de acceso, información, modificación, bloqueo y cancelación consagrados en el artículo 15 de la Ley N° 19.628[180].

Sin embargo, resolver la contienda en sede judicial es excesivamente oneroso para el titular , máxime si consideramos que la responsabilidad que se persigue contra el banco de datos

---

[174] *Ibid.*
[175] **GONZALEZ HOCH, FRANCISCO.** Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 153-174, 2001, p. 177.
[176] **VIAL, FELIPE.** *Op, cit.* p. 34
[177] **JIJENA, RENATO.** Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 85-112, 2001, p. 96.
[178] **ASESORÍA TÉCNICA PARLAMENTARIA.** Consulta experta sobre la Ley de Protección de la vida privada de las personas, 2018. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26703/2/BCN_Consulta_experta_sobre_la_Ley_de_Proteccion_de_la_vida_Privada.pdf, p.7
[179] **PEÑA YAÑEZ, SEBASTIÁN.** *Op, cit,* p. 146
[180] **CORRAL TALCIANI, HERNAN.** Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 39-57, 2001, p. 50.

es de carácter extracontractual (según la doctrina generalizada)[181], por lo que no es aplicable la presunción de culpa del artículo 1547 inciso 3 del Código Civil, ni tampoco se establece un sistema de responsabilidad objetiva, siendo -tal como menciona Gonzalez Hoch- "prácticamente imposible de acreditar esa culpa o negligencia"[182].

Ahora bien, aun cuando se cumplan los requisitos que hacen procedente la responsabilidad del banco de datos, las multas establecidas, debido a su bajo monto, no incentivan a cumplir la ley, siendo más conveniente y eficiente para las empresas de datos pagar las sanciones mientras continúan infringiendo debido a los réditos que esto les genera en el mercado[183]-[184].

- **Precisión y desarrollo conceptual:** Una de las falencias que reconoce la doctrina especializada en la Ley N°19.628 guarda relación con la técnica conceptual, puesto que es clave en materias altamente complejas como la que se analiza, claridad respecto a las definiciones y sus alcances[185], como ocurre con los datos sensibles[186]. A modo de ejemplo, y siendo sumamente importante para efectos de esta memoria, se ha criticado la definición de fuentes accesibles al público porque termina por convertir en regla general a aquello que, en principio, iba a constituir la excepción[187]. Como afirma Gonzalez Hoch "su regulación debe ser detallada para que el libre acceso que permite a ciertos datos no se transforme en la regla general y conlleve una pérdida en la privacidad de las personas"[188].

Esto, sumado a la falta de desarrollo conceptual de lo que se entiende por inteligencia artificial, *big data*, internet, informática, el tratamiento de datos biométricos o biológicos, y otros conceptos claves, sepultan a la Ley vigente por su anacronismo, al desatender elementos claves hoy en día en el mundo digital y la protección de datos personales[189].

- **Regulación deficiente del mercado de transferencia de datos:** Por último, podemos mencionar la problemática referida propiamente al mercado de transferencia de datos[190], que debe ser diferenciada entre la transferencia local y la transfronteriza.

---

[181] En este sentido, **CORRAL TALCIANI, HERNAN.** *Op. cit.*
[182] **GONZALEZ HOCH, FRANCISCO.** *Op, cit.* p. 178
[183] *Ibid.*
[184] **ASESORÍA TÉCNICA PARLAMENTARIA.** *Op, cit.* p.9
[185] *Ibid*, p.7
[186] *Ibid*, p.9
[187] **VIOLLER, PABLO.** *Op, cit.* p.46
[188] **ASESORÍA TÉCNICA PARLAMENTARIA.** *Op, cit.* p.9
[189] *Ibid.* p.9 y 10
[190] *Ibid.*

La Ley N° 19.628 se refiere únicamente a la primera y de forma preocupante amplia. En efecto, el artículo 2 letra c) se refiere a ella como "comunicación o transmisión de datos, es dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas", homologando conceptos que realmente no constituyen sinónimos y que generan incerteza[191].

En el caso de la transferencia transfronteriza, organismos internacionales como la ONU y OCDE exigen que el país receptor de los datos ofrezca garantías similares en cuanto a protección de la vida privada[192]. Sin embargo, como expone Peña, en el caso chileno el Senado prefirió rechazar el precepto que regulaba la materia, bajo el argumento de que esto debía ser resuelto mediante tratados internacionales[193], sin haberse salvado la situación hasta nuestros días[194].

Expuestas y desarrolladas las críticas que se efectúan a la Ley N° 19.628, no se puede sino concluir que el mercado de datos personales en Chile está, en gran medida, desregulado. Lo anterior, se traduce en el desconocimiento por parte del Estado y de las empresas que transfieren y tratan datos personales, propiciando vulneraciones al derecho fundamental de la privacidad y el derecho a la autodeterminación informativa. Así, aun cuando no se pueda asegurar al día de hoy que el *microtargeting* pueda incidir en las elecciones y la conducta del votante de manera fehaciente, lo cierto es que una legislación débil y carente de organismos de control, genera un incentivo para el surgimiento de empresas que logran grandes réditos con nuestra información personal, a muy bajo costo.

III.3 Proyecto de reforma Ley N° 19.628: Boletines 11.144 refundido con Boletín N°11092-07

Debido a las deficiencias mencionadas en el acápite anterior, las críticas a la vigente Ley Sobre Protección de la Vida Privada no se hicieron esperar y se acrecentaron en la última década producto del auge de las nuevas tecnologías que se alimentan de bases de datos y las empresas dedicadas a la transacción de los mismos. En este contexto, el año 2017 son presentados dos proyectos de ley de suma relevancia con un objetivo en común, derogar completamente la Ley N° 19.628 para dar paso a un nuevo cuerpo legal encargado de regular los aspectos relativos a la protección de los datos personales y la vida privada, implementando además un órgano encargado de fiscalizar y supervigilar el cumplimiento de esta.

---

[191] **PEÑA YAÑEZ, SEBASTIÁN.** *Op, cit,* p. 94
[192] *Ibid,* pp. 91.93
[193] Ibid.
[194] **ASESORÍA TÉCNICA PARLAMENTARIA.** *Op, cit.* p.9

El primer proyecto de reforma es presentado en enero del año 2017[195]y se origina gracias a la moción de los senadores Pedro Araya, Alfonso De Urresti, Alberto Espina, Felipe Harboe y Hernán Larraín. La motivación detrás del proyecto de Ley en comento fue poder materializar el compromiso asumido por Chile el año 2010 al haber ingresado a la OCDE, esto es, adecuar el marco normativo nacional a estándares internacionales de protección de datos, cuestión que hoy en día aún no se cumple. Además, los legisladores en el mensaje del proyecto reconocen expresamente la ineficacia de la ley vigente sobre todo en lo referido al mercado de datos, expresando que "la magnitud de la recogida y del intercambio de datos personales también ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas por su parte también difunden un volumen cada vez mayor de información personal. La tecnología ha transformado tanto la economía como la vida social y si bien debe facilitarse la libre circulación de los datos, debe garantizarse un adecuado nivel de protección a los mismos"[196].

El segundo proyecto, data del mes de marzo del año 2017 y comienza su tramitación en el congreso en virtud del Mensaje 001-365 emanado del gobierno de la expresidenta Michelle Bachelet, aduciendo motivos bastante similares al proyecto antes expuesto, esto es, hacer frente a la explosión de los agentes de mercado que comercializan datos con diferentes fines. En concreto, se expone que -con miras a asegurar de manera efectiva el derecho fundamental a la vida privada- el proyecto de ley "busca balancear y equilibrar las diferentes miradas y opciones técnicas, económicas, jurídicas y políticas que se promueven por los diversos actores, instituciones y grupos de interés que participan de este debate, proponiendo un marco regulatorio que proteja los derechos y libertades de las personas, garantice el tratamiento lícito de los datos personales por parte de terceros, sin entrabar ni entorpecer la libre circulación de la información y, en definitiva, se alcance una legislación moderna y flexible que permita enfrentar los desafíos del país de cara al Siglo XXI"[197].

Finalmente, en razón de la estrecha similitud en cuanto objetivos e ideas matrices, ambos proyectos son refundidos por acuerdo del Senado con fecha 22 de marzo de 2017, autorizando a la Comisión para discutirlos en general y en particular durante el primer informe. En cuanto a su contenido

---

[195] Boletín 11092-07

[196] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, pagina 4. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[197] Ibid.

-sin ánimos de realizar una sistematización intensiva del proyecto que se aleje del objeto de la presente investigación- podemos mencionar las siguientes principales innovaciones del proyecto:

- **Cambio de nomenclatura en la ley:** Tomando en consideración que el proyecto de ley se caracteriza por una técnica legislativa orientada a la derogación y sustitución de la mayor parte del corpus de la Ley N° 19.628 sobre "protección de la vida privada"[198], es necesario resaltar la primera disposición contenida en el artículo 1 del proyecto. En esta, se modifica el nombre de la ley vigente por "protección de los datos personales", con tal forma de materializar uno de los objetivos que es posible extraer del mensaje 001-365 del proyecto emanado del gobierno de la expresidenta Bachelet, esto es, "regular el tratamiento de los datos personales, asegurando el respeto y protección de los derechos y libertades fundamentales de los titulares de datos (personas naturales), en particular el derecho a la vida privada"[199].

Sin embargo, a pesar de intentar poner el acento en la protección de los datos personales siguiendo el mandato constitucional a través del cambio de nomenclatura, para autores como Vergara "persiste en su redacción la mentalidad de considerarlos como algo transable, en vez de poner como idea principal los derechos de los titulares de los datos"[200].

- **Consagración efectiva de los derechos ARCO**: Los derechos ARCO, en virtud de sus siglas, hacen referencia a los derechos de acceso; rectificación; supresión (anteriormente llamado de cancelación)[201] y oposición de los que gozan los titulares de datos personales en todo lo referido a su tratamiento por terceros[202]. La importancia de su consagración pretende amparar la libertad personal desde dos frentes[203]. Por una parte, materializando la autodeterminación informativa, esto es, que una persona pueda decidir arbitrariamente que información quiere dar

---

[198] **VERGARA ROJAS, Manuel**. Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. Revista chilena de derecho y tecnología, 2017, vol. 6, no 2, p. 137

[199] Mensaje 001-365 de S. E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín 11144-07

[200] **VERGARA ROJAS,** *Op. cit.* p. 138

[201] Tal como consta en el informe, la explicación de este cambio de nomenclatura se debe a que "se generaron confusiones respecto del concepto "CANCELACIÓN", pues en materia civil cancelar es la operación que hacen los acreedores cuando ha sucedido el pago efectivo de una deuda.
El deudor paga, el acreedor cancela. Dadas las innecesarias confusiones que el uso de este concepto generó, se optó por cambiar el nombre de "derecho de cancelación" a "derecho de supresión".
Invita a la Comisión a hacer lo mismo, de forma tal que utilicemos un lenguaje normalizado, y así como en Europa y en las nuevas normas a nivel mundial ya no se habla del derecho de cancelación, sino que derecho de supresión, nosotros hagamos lo mismo" **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO,** *Op. cit.* pp.103-104

[202] **FUNDACIÓN DATOS PROTEGIDOS**. Una propuesta a la ley de datos personales en Chile, 2017, p.5. Disponible en: https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf

[203] *Ibid, p.7*

a conocer y cuando. Por otra, permite la libertad informática, estableciendo normativamente bajo que contexto se permite la transferencia de datos personales[204].

En este contexto, un gran avance en el proyecto de ley en tramitación es que, en su artículo segundo destinado a definir ciertos conceptos, agrega los derechos en comento y, además, adiciona el derecho del usuario a la portabilidad de sus datos, pudiendo exigir una copia de los mismos para los fines que crea convenientes. Además, se incluye igualmente el derecho de bloqueo en el artículo 8 bis ter, legitimando al titular de los datos a solicitar la suspensión temporal de la operación de tratamiento en casos de vigencia dudosa o inexactitud. Lo anterior, para autores como Vergara, implica un claro esfuerzo del legislador por sistematizar y delinear ciertos conceptos que, si bien en parte están incluidos en la vigente ley, "se presentaban desordenados y no muy delineados"[205].

- **Creación de una Agencia de Protección de Datos:** El proyecto en comento, tal como su nombre indica, ordena la creación de una Agencia de Protección de Datos que, tal como sistematiza Orellana[206] teniendo en miras los artículos 30 y siguientes del proyecto, tiene como principales funciones: proponer normativa de carácter técnico; interpretar los cuerpos legales destinados a la protección y tratamiento de datos personales; prevenir la transgresión de los derechos contenidos en la ley estableciendo programas con diversos organismos para apuntar en dicha dirección; resolver las consultas relativas al marco jurídico que ofrece el proyecto de ley; fiscalizar el cumplimiento de la normativa, los derechos y principios contenidos en el cuerpo legal; determinar las infracciones en el tratamiento de datos personales u otras disposiciones contenidas en la ley, imponiendo los mecanismos de sanción que la ley ofrece.

De esta forma, al día de hoy parece zanjarse uno de los puntos centrales en el debate legislativo, esto es, la determinación del órgano que se encargaría de cumplir con la función eminentemente fiscalizadora del proyecto de ley y las futuras leyes sectoriales que puedan complementar la protección de datos en Chile. Así, termina por desecharse la idea de extender las facultades de un órgano ya existente como la Contraloría General de la República, el SERNAC o el Consejo para la Transparencia del Estado[207].Una decisión en contrario, sobre todo si se consideraba el CPLT, podía incluso representar una paradoja, ya que como explica Vicencio "se trata de un órgano que vela por el cumplimiento del principio de publicidad propio de la

[204] *Ibid.*
[205] **VERGARA ROJAS,** *Op. cit.* p. 139
[206] **ORELLANA VILCHES.** Agencia de protección de datos personales. *Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales*. Facultad de Derecho, Universidad de Chile, 2011, p. 55 y ss.
[207] **VERGARA ROJAS,** *Op. cit.* p. 141

actividad pública, mientras que la protección de datos debe velar por la privacidad de las personas"[208].

Con todo, de aprobarse el proyecto, la efectividad del órgano -como argumenta la doctrina especializada- estará supedita a la creación de una ley orgánica, un adecuado financiamiento y una correcta distribución de cargos interna[209], de modo que se supere la principal preocupación que se hizo presente en la discusión parlamentaria de manera transversal, esto es, el excesivo gasto en la creación de un nuevo órgano que podría ser inocuo[210].

- **Readecuación del tratamiento de datos personales a nivel nacional e internacional:** El proyecto de ley, en su artículo 2 letra o) define el tratamiento de datos personales como "cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales". En este sentido, cabe señalar que el proyecto descansa sobre el pilar fundamental del consentimiento, entendido como "toda manifestación de voluntad libre, específica, inequívoca e informada, otorgada a través de una declaración o una clara acción afirmativa, mediante la cual el titular de datos, su representante legal o mandatario, según corresponda, autoriza el tratamiento de los datos personales que le conciernen"[211]. Si bien la normativa vigente igualmente hace referencia a este principio y sus excepciones (aun en el caso de datos personales sensibles), la creación de un órgano fiscalizador y una batería de sanciones permite hacer efectivo el control respecto del consentimiento de los titulares de datos personales en el medio nacional, sin que el marco legal sea inaplicable en términos facticos, como muchas veces ocurre hoy.

Por otra parte, en materia de transferencias internacionales de datos, el legislador ha optado por seguir la tónica internacional como es posible evidenciar en el proyecto, permitiendo que se ejecuten estos actos sólo si el país hacia donde se transfiere los datos tiene un nivel de

---

[208] **VICENCIO ZOLEZZI.** Nueva ley de datos personales para Chile. Proyecto de ley para la modernización normativa en la protección de datos personales en Chile: análisis evaluativo y desafíos. *Tesis presentada para obtener el grado académico de Magíster en Políticas Públicas.* Escuela de Gobierno, PUC. P.19

[209] **VERGARA ROJAS,** *Op. cit.* p. 150

[210] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, pp. 18 y ss. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[211] Articulo 2 letra p) del proyecto.

"protección al menos tan bueno como el que establece la legislación nacional"[212]. En cualquier caso, tal como queda patente de la lectura del proyecto de ley en su artículo 27, la Agencia de Protección de Datos Personales será la encargada de elaborar una lista de Estados que cuentan con un nivel de protección adecuado y, en cualquier otro caso, podría permitir la transferencia de datos siempre y cuando "el transmisor y el receptor de los datos otorguen las garantías adecuadas en relación con la protección de los derechos de las personas que son titulares de estos datos y la seguridad de la información transferida, de conformidad con la presente ley"[213].

- **Aplicación de diversos procedimientos y sanciones:** Por último, es menester mencionar el desarrollo legal de procedimientos de distinta naturaleza que constan en el proyecto de ley, como una forma de dar cierre a una normativa que tiene por objetivos modificar el estado del arte actual en materia de protección de datos y, lograr que, los responsables de infracciones sean sancionados de manera efectiva y sin mayores dilataciones que obstaculicen el proceso para los titulares de datos, preocupación planteada por la fundación Datos Protegidos hace varios años[214].

Los principales procedimientos se distinguen entre aquellos de carácter administrativo -llevados a cabo ante la Agencia de Protección de Datos- y aquellos que podemos denominar como propiamente judiciales[215]. Dentro de los primeros, se pueden distinguir dos finalidades, por una parte, un procedimiento administrativo de tutela de los derechos que otorga el proyecto a los titulares de datos personales, que en ningún caso puede durar más de seis meses[216]. El segundo procedimiento administrativo, que puede comenzar de oficio o a petición de parte, tiene por finalidad aplicar las sanciones correspondientes en el caso de infracciones a la ley, que se traducen en incumplimiento de principios derechos y obligaciones que consten en el cuerpo legal[217]. Ahora bien, los articulos 38 bis y siguientes hacen referencia expresa a las conductas que constituyen infracciones, graduándose como aquellas consideradas leves; graves y gravísimas, con sanciones efectivas que van entre 1 y hasta 20.000 UTM, según sea el caso[218].

---

[212] **CONDE, B; HERNÁNDEZ, L**. Evaluación del Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales en Chile. *Documento de Trabajo No 65 (CLAPES UC)*, 2019. P, 10.
[213] Artículo 27 del proyecto.
[214] **FUNDACIÓN DATOS PROTEGIDOS**. Una propuesta a la ley de datos personales en Chile, 2017, p.11. Disponible en: https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf
[215] **VERGARA ROJAS,** *Op. cit.* p. 142
[216] **ORELLANA VILCHES.** *Op. cit.* p. 65.
[217] *Ibid*, p. 66
[218] Artículo 38 bis; ter y siguientes del proyecto

Respecto de estos procedimientos administrativos, cabe destacar que la discusión parlamentaria hubo ciertas reticencias. En efecto, en la sesión N°2 del 23 de marzo del año 2022 de la Comisión de Constitución, Legislación, Justicia y Reglamento, el diputado Sánchez opinó que un procedimiento de tales características era "vulneratorio del derecho constitucional del debido proceso y la igualdad ante la ley"[219]. Sin embargo, se decidió mantener este tipo de procedimientos bajo el correcto argumento de que aquel "tiene como propósito dar un orden previo a la instancia judicial, ya que el propio artículo 47 del cuerpo legal que se propone establece un procedimiento judicial en caso de que la persona se sienta afectada o menoscabada por la respuesta, sanción o vulneración de derechos realizada por la Agencia. Siendo así, no son excluyentes, sino complementarias"[220].

Finalmente, el procedimiento judicial se encuentra regulado en el artículo 47 del proyecto de ley, radicándose la competencia en las Cortes de Apelaciones nacionales en todos aquellos casos en que las personas naturales o jurídicas resulten agraviadas por la resolución administrativa dictada por la Agencia de Protección de Datos y quieran interponer un reclamo de ilegalidad[221]. Así, si la magistratura estima que existió agravio o que en un procedimiento sancionatorio la resolución no se ajusta a Derecho, podrá ordenar la rectificación del acto impugnado o, bien, modificar la sanción impuesta al responsable, incluso absolviendo, dependiendo del caso concreto[222].

Habiendo expuesto los principales pilares en los que se sustenta el proyecto de reforma, ampliamente debatidos durante la tramitación del proyecto, cabe analizar -sin olvidar el objeto de esta investigación- la manera en que el perfilamiento es abordado normativamente y como la inclusión o reformulación de nuevos derechos, conceptos y órganos institucionales permite otorgar protección a los titulares de datos en dicho contexto, en circunstancias en que hoy se encuentran parcialmente desprotegidos, ya que solo se puede recurrir a las reglas generales de la Ley N° 19.628.

---

[219] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p.19. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[220] *Ibid.*, p.22

[221] **ORELLANA VILCHES.** *Op. cit.* p. 70-71

[222] *Ibid*. p. 71

En este sentido cobra relevancia el articulo 2 letra o) del proyecto, toda vez que nos ofrece una definición de tratamiento de datos en que se contempla aquel que implica operaciones automatizadas[223]. Además, el citado artículo -de forma innovadora y en atención a las nuevas tecnologías- en su letra w complementa lo señalado anteriormente estipulando que la elaboración de perfiles consiste en *"toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural"*[224]. Este marco conceptual incluido en el proyecto debe ser valorado positivamente, toda vez que, luego de las reiteradas críticas al cuerpo normativo vigente por su desactualización, finalmente pone el acento en la regulación de ciertas prácticas que se desarrollan profusamente día a día.

A mayor abundamiento, durante la discusión legislativa que tuvo lugar el 11 de mayo del año 2022 en lo que fue la sesión N°14, el señor Gencarelli, en su calidad de jefe de la denominada Unidad de Protección y Flujo de Datos Internacionales en la Comisión Europea, expuso que el proyecto debía "abordar ciertos sesgos, formas de discriminación en el contexto de ciertos usos de inteligencia artificial y toma de decisiones automatizadas. Se requiere asegurar la transparencia y el derecho de los individuos para solicitar intervención humana cuando las decisiones se tomen con base en un proceso automático de datos"[225].

En la misma dirección se pronunció la directora de GobLab de la Universidad Adolfo Ibáñez, María Paz Hermosilla, aportando datos claves en la materia y exponiendo que la utilización de algoritmos es una práctica recurrente por parte de privados, pero igualmente por el Estado, donde hasta un 78% de sistemas públicos hace uso de datos personales, por ejemplo, para detectar fraudes en licencias médicas, otorgar subsidios o bien, implementar asistentes virtuales[226] , siendo necesario regular todo tratamiento de información de forma automatizada con el fin de perfilar personas, para que no ocurran filtraciones inesperadas como ocurrió en el caso SERVEL.

A mayor abundamiento, los expertos en la materia recomendaron sentar las bases de la discusión legislativa en torno a la regulación de sistemas algorítmicos y de perfilamiento teniendo presente la

---

[223] 2 letra o) proyecto "Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales".
[224] Art. 2 letra w) del proyecto.
[225] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p. 77. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY
[226] *Ibid*, p.79

necesidad de: analizar el estándar de transparencia aplicable los responsables en el tratamiento de datos de forma automatizada y articular hipótesis en que los derechos ARCO se hacen específicamente aplicables en el contexto de la elaboración de perfiles[227].

Así las cosas, los aportes técnicos de estos y otros expertos que fueron parte de la discusión en el Congreso Nacional permiten que, en atención al proyecto, el análisis de perfilamiento se realice sobre la base de los principios inspiradores del mismo y los derechos que se confiere a los titulares de datos. Como mencionamos líneas arriba, uno de los pilares sobre los cuales descansa el proyecto es la consagración de los derechos "ARCO" en el título primero, donde existen claras referencias directas a la hipótesis de automatización en el tratamiento de datos y a la elaboración de perfiles en algunos de estos derechos, pudiendo desglosarse aquellas menciones del proyecto de la siguiente manera:

- **Derecho de acceso:** Este confiere al titular de los datos la potestad de solicitar al responsable del tratamiento que responda, en primer lugar, si aquel se encuentra actualmente operando sus datos. Si aquello es afirmativo, le permite solicitar al mismo sujeto información acerca de los datos tratados; de donde los obtuvo; cual es la finalidad perseguida; a quien pretende ceder o cedió los datos; duración del tratamiento y, además, los intereses legítimos del responsable en aquellas hipótesis en que no se requiere consentimiento expreso del titular.[228]

Para el caso del tratamiento automatizado de datos, existe una hipótesis contemplada de manera clara, toda vez que el responsable debe aportar "información significativa sobre la lógica aplicada en el caso de que el responsable realice tratamiento de datos de conformidad con el artículo 8 bis" del proyecto, esto es, el caso de decisiones individuales automatizadas, donde se incluya expresamente la elaboración de perfiles.

De esta forma, como señala Bordachar se consagra "la salvaguardia más importante del derecho a la autodeterminación informativa, lo que se explica por su carácter habilitante, en tanto posibilita el ejercicio de los demás derechos que se puedan otorgar a los titulares de datos personales"[229], máxime si consideramos que se encuentra consagrado en la Carta de Derechos Fundamentales de la Unión Europea[230]. Adicionalmente, cabe comentar que el proyecto, que

[227] *Ibid.* p. 80
[228] Art 5 Proyecto de ley.
[229] **BORDACHAR BENOIT.** Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO. *Revista chilena de derecho y tecnología*, 2022, vol. 11, no 1, p.399.
[230] *Ibid*.

originalmente contenía excepciones al ejercicio de este derecho[231], fue enmendado para adecuar la normativa al estándar europeo, ajustando la limitación a una causal tal como establece el artículo 5 inciso final, a saber, en el caso de que una ley lo disponga[232], superando las criticas esgrimidas por ciertos autores[233].

Con respecto al derecho de acceso, podemos concluir que, gracias a la referencia expresa en torno al tratamiento automatizado de datos y la elaboración de perfiles, todos aquellos sujetos que sean objeto de este tipo de prácticas podrán ejercitar un derecho que les permite tener pleno conocimiento de la información que estuviesen manejando. Sin perjuicio de lo anterior, una de las críticas que podemos esbozar al proyecto es que, tal como se extrae del artículo 14 y siguientes, a propósito de los deberes de los responsables de tratamiento, no queda claro si es que existe lo que la doctrina ha denominado un "deber de transparencia activa"[234], esto es, si es que el responsable debe notificar acerca de información relativa a los derechos de los titulares; política de tratamiento de datos personales; fuente de los datos; medidas de seguridad; la existencia de decisiones automatizadas y elaboraciones de perfiles, entre otras comunicaciones en atención al artículo 14 ter[235], o por el contrario, si es que la "facilitación de información" que mandata la norma se traduce en "imponer al titular la carga de buscar la información sobre el tratamiento que terceros pudieran hacer de sus datos, incluso aquella que resulta necesaria para

---

[231] Los casos en que el responsable del tratamiento de datos se encontraba eximido de permitir el ejercicio del derecho de acceso se daba en los siguientes casos: i) cuando el titular ya dispusiera de la información requerida; cuando su comunicación resultara imposible o su entrega exigiera un esfuerzo desproporcionado; ;cuando su entrega imposibilite u obstaculice gravemente un tratamiento de datos con fines históricos, estadísticos o científicos, para estudios o investigaciones que atiendan fines de interés público o vayan en beneficio de la salud humana; y, por ultimo cuando lo disponga expresamente la ley.

[232] Art. 5 inciso final del proyecto "El responsable siempre estará obligado a entregar información y a dar acceso a los datos solicitados excepto cuando una ley disponga expresamente lo contrario".

[233] **BORDACHAR BENOIT.** *Op. cit.* p.400

[234] *Ibid.* p.402-403

[235] **Artículo 14 ter**.- Deber de información y transparencia. El responsable de datos debe mantener permanentemente a disposición del público, en su sitio web o en cualquier otro medio de información equivalente, al menos, la siguiente información:
a) La política de tratamiento de datos personales que haya adoptado, la fecha y versión de la misma;
b) La individualización del responsable de datos y su representante legal y la identificación del encargado de prevención, si existiere;
c) El domicilio postal, la dirección de correo electrónico, el formulario de contacto o la identificación del medio tecnológico equivalente mediante el cual se le notifican las solicitudes que realicen los titulares;
d) Las categorías, clases o tipos de datos que trata; la descripción genérica del universo de personas que comprenden sus bases de datos; los destinatarios a los que se prevé comunicar o ceder los datos, las finalidades de los tratamientos que realiza y los tratamientos que se basan en la satisfacción de intereses legítimos;
e) La política y las medidas de seguridad adoptadas para proteger las bases de datos personales que administra;
f) El derecho que le asiste al titular para solicitar ante el responsable, acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, de conformidad a la ley, y g) El derecho que le asiste al titular de recurrir ante la Agencia, en caso de que el responsable rechace o no responda oportunamente las solicitudes que le formule.

el pleno ejercicio de su derecho a la protección de los datos personales, la que solo podría llegar a conocer mediante la consulta constante, de los sitios de cada uno de los responsables que pudieran estar tratando sus datos personales, como bien apuntó el senador Harboe durante la discusión de estos artículos"[236].

En este sentido, y siguiendo lo expuesto por la Ministra Uriarte durante la Sesión N° 41 de 27 de septiembre de 2022 en el Congreso, será deber de la Agencia eventualmente determinar el alcance del deber de información de los responsables[237], esperando que esto no implique una judicialización a gran escala por existir imposibilidad de cumplimiento para los responsables. En cualquier caso, dado que a lo largo de esta memoria se ha constatado que la elaboración de perfiles con distintos fines -incluso electorales- es un hecho y existen grandes agentes económicos incursionando en este ámbito, el derecho en comento permite que los titulares puedan, en definitiva, tomar conocimiento integral de los datos personales que están siendo tratados, traduciéndose a todas luces en un avance que necesita ser analizado en la práctica.

- **Derecho de oposición**: El artículo 8 del proyecto establece el denominado derecho de oposición, señalando al respecto que *"el titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan (...)"*[238]. Gracias a la consagración de este derecho en términos positivos, se le otorga una facultad de cierre a los titulares de datos personales, toda vez que correlativamente al acceso que se les garantiza a aquellos, indudablemente es necesario permitirles decidir libremente si es que quieren permitir que se realice el tratamiento de información que les compete.

Ahora bien, cabe señalar que la aplicación práctica de este derecho está circunscrita a ciertas hipótesis en específico, destacando la segunda de aquellas que se enumeran ya que contempla aquellos casos en que *"(...) el tratamiento se realiza exclusivamente con fines de*

---

[236] *Ibid.* p. 403

[237] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p. 253. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[238] Artículo 8 inciso primero del proyecto

mercadotecnia o marketing directo de bienes, productos o servicios, incluida la elaboración de perfiles, de conformidad con el artículo 8 bis de la presente ley"[239].

La inclusión de esta figura resulta relevante dado el contexto digital en el que nos encontramos inmersos, máxime si reiteramos que una de las críticas que se efectúa a la ley vigente es justamente su anacronismo. En efecto, la experta María Paz Hermosilla en la comentada sesión N°14 que tuvo lugar el 11 de mayo del año 2022, puso sobre la mesa que una de las maneras de avanzar en el fortalecimiento del derecho de los ciudadanos frente a los sistemas algorítmicos -sobreabundantes hoy en día-, era consagrando "la facultad de poder impugnar la decisión y la correlativa obligación del responsable de garantizar el ejercicio de este derecho"[240].

De esta forma, se agrega el referido artículo 8 bis. - que complementa el citado artículo 8 y se refiere al caso de decisiones individuales automatizadas y la elaboración de perfiles en relación al derecho de oposición, como comentamos líneas arriba. En concreto, se dispone en la disposición normativa que:

> **Art. 8 bis***"El titular de datos tiene derecho oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente.*
>
> *El inciso anterior no se aplicará en los siguientes casos:*
>
> *a) Cuando la decisión sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable;*

---

[239] Artículo 8°.- Derecho de Oposición. El titular de datos tiene derecho a oponerse ante el responsable a que se realice un tratamiento específico o determinado de los datos personales que le conciernan, en los siguientes casos:
a) Cuando la base de licitud del tratamiento sea la satisfacción de intereses legítimos del responsable. En dicho caso podrá ejercer su derecho de oposición en cualquier momento, debiendo el responsable del tratamiento dejar de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.
b) Si el tratamiento se realiza exclusivamente con fines de mercadotecnia o marketing directo de bienes, productos o servicios, incluida la elaboración de perfiles, de conformidad con el artículo 8 bis de la presente ley
c) Si el tratamiento se realiza respecto de datos obtenidos de una fuente de acceso público y no existe otro fundamento legal para su tratamiento. No procederá la oposición al tratamiento cuando este se realice con fines de investigación científica o histórica o fines estadísticos, siempre que fueran necesarios para el cumplimiento de una función pública o para el ejercicio de una actividad de interés público.

[240] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p. 83. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

b) Cuando exista consentimiento previo y expreso del titular en la forma prescrita en el artículo 12 de la presente ley,

y c) Cuando lo disponga la ley, en la medida en que ésta disponga el empleo de salvaguardas a los derechos y libertades del titular.

En todos los casos de decisiones basadas en el tratamiento automatizado de datos personales, inclusive aquellos señalados en las letras a), b) y c) precedentes, el responsable deberá adoptar las medidas necesarias para asegurar los derechos, libertades del titular, su derecho a la información y transparencia, el derecho a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión.

Cabe señalar que durante el debate legislativo que se suscitó respecto de esta norma, la asistente del Ministerio de Secretaría General de la Presidencia, Lizzy Seaman, recomendó que se modificará la redacción original del inciso primero que versaba de la siguiente manera: *"El titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le conciernan, basadas únicamente en el hecho de realizarse a través de un tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles".* Básicamente, se decidió suprimir la palabra "únicamente", permitiendo que el supuesto factico previsto por la disposición normativa incluya aquellos casos en que interviene un humano de alguna manera[241], como lo haría un programador de un software que constituya una herramienta coadyuvante para estos efectos.

Ahora bien, con respecto a la redacción del artículo propiamente tal, existe un balance positivo, considerando que en la actualidad la mayoría de los Estados tienen como modelo el Reglamento General de Protección de Datos de la Unión Europea. En efecto, durante la discusión parlamentaria se discutió cuidadosamente el alcance que debía tener el derecho de oposición en el contexto de la elaboración de perfiles y decisiones automatizadas, optando por circunscribir la aplicación del derecho a aquellos casos en que las comentadas acciones "produzca efectos jurídicos en él o le afecte significativamente de modo similar" al igual que en el RGPD, tal como lo recomendó la experta invitada Paula Silva, secretaria ejecutiva de la Mesa de Regulaciones Digitales, en representación de la Cámara Chilena Norteamericana de Comercio [242].

---

[241] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p.207 y ss. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[242] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE**

Además, si se pone el foco en el inciso final del artículo 8 bis. podemos percatarnos de que obliga al responsable del tratamiento de datos personales a *"adoptar las medidas necesarias para asegurar los derechos, libertades del titular, su derecho a la información y transparencia, el derecho a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión"*, cuestión que incluso se extiende a las tres hipótesis -en principio- exceptuadas por la norma. Esto, nos permite concluir que, en el caso de decisiones automatizadas, el legislador ha optado por elevar la protección con respecto a los titulares de datos personales en atención a los derechos que los amparan, con el objetivo de que las libertades individuales no se vean coartadas.

Por último, en cuanto a las referencias del proyecto a hipótesis de elaboración de perfiles en términos generales, cabe hacer mención del título segundo del cuerpo legal denominado "Del tratamiento de los datos personales y de las categorías especiales de datos". Específicamente el artículo 15 regula la cesión de datos personales por parte de los responsables del tratamiento, sin embargo, el artículo 15 ter va más allá y dispone que en ciertos casos podría ser necesaria una "evaluación de impacto en protección de datos personales". Es decir, el legislador ha establecido procedimientos previos que evitan una posición meramente reactiva de la institucionalidad, anticipándose a los efectos negativos que podrían radicarse en los titulares de datos personales. A mayor abundamiento, la disposición normativa en comento dispone que:

> **Art. 5 ter** *"Cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, se pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales, el responsable del tratamiento deberá realizar, previo al inicio de las operaciones del tratamiento, una evaluación del impacto en protección de datos personales. La evaluación de impacto se requerirá siempre en casos de:*
>
> *a) Evaluación sistemática y exhaustiva de aspectos personales de los titulares de datos, basadas en tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos.*
>
> *b) Tratamiento masivo de datos o gran escala.*
>
> *c) Tratamiento que implique observación o monitoreo sistemático de una zona de acceso público.*
>
> *d) Tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento.*

PROTECCIÓN DE DATOS PERSONALES. Boletines N°s 11.144-07 y 11.092-07, refundidos, p.94. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

> *La Agencia de Protección de Datos establecerá y publicará una lista orientativa de los tipos de operaciones de tratamiento que requieran o no una evaluación de impacto relativa a la protección de datos personales.*
>
> *La Agencia también establecerá las orientaciones mínimas para realizar esta evaluación, considerando a lo menos en dichos criterios, la descripción de las operaciones de tratamiento, su finalidad, la evaluación de la necesidad y la proporcionalidad con respecto a su finalidad, la evaluación de los riesgos y medidas de mitigación. Los responsables podrán consultar a la Agencia de Protección de Datos, cuando en virtud del resultado de la evaluación, el tratamiento demuestre ser de alto riesgo a efectos de obtener recomendaciones de parte de dicha entidad*"[243]

De la redacción de la norma, se vislumbra claramente que la naturaleza de la elaboración de perfiles es potencialmente peligrosa, por lo que el legislador analiza con recelo este tipo de acciones, sin que por supuesto ello implique prohibirlas del todo. Además, los casos enumerados no son excluyentes, ya que como se ha explicado a lo largo de esta memoria, en la elaboración de perfiles con fines electorales se entrecruzan variables de peso a considerar, ya que estamos en presencia de tratamiento de datos sensibles como lo es una preferencia política; analizando datos a gran escala y que podrían estar inmersos en fuentes de libre acceso, uniéndose las hipótesis que son tratadas de forma separada en la norma y, por lo tanto, siendo materia digna de evaluación previa.

Así, grandes agentes del mercado del perfilamiento social, como por ejemplo la citada agencia Instagis ya contratada por ciertos partidos politicos en el contexto de campañas electorales, deberán adecuarse a un marco normativo sólido y concorde a un mundo altamente digitalizado.

in embargo, es importante señalar a este respecto que el avance tecnológico lleva aparejado consigo una etapa de desregulación inevitable, toda vez que avanza de forma sustancialmente más acelerada que cualquier discusión legislativa. Por lo mismo, hay que hacer presente que cualquier evaluación con respecto al proyecto es meramente estimativa y comparativa y, debido a ello, un analisis en concreto requerirá -además de la promulgación del proyecto, por cierto- examinar el rol que adopte la Agencia de Protección de Datos como órgano competente para fiscalizar el cumplimiento de la ley e interpretarla.

Ahora bien, ante la probable aparición de casos de alta complejidad que escapen de las hipótesis reguladas en el proyecto en cuestión, es que los principios consagrados se erigen como un pilar coadyuvante. En efecto, no se debe olvidar que estos constituyen -siguiendo la clásica idea de Dworkin- la respuesta jurídica en aquellos casos en que las reglas no ofrecen una solución en concreto, al ser

[243] Articulo 15 ter del proyecto

medidas de optimización, integración e interpretación de los ordenamientos jurídicos[244]. Por eso, podemos tachar de acertada la inclusión de una lista de principios aplicables a la protección de datos personales en el artículo 3 del proyecto, consagrando los principios de: licitud y lealtad; finalidad; proporcionalidad; calidad; responsabilidad, seguridad y confidencialidad. Estos, probablemente constituyan una herramienta útil para la Agencia, que, en el caso de desarrolladores de tecnologías de la información y perfilamiento, permitirán por sobre todo, determinar si es que el tratamiento es lícito y, en segundo lugar, si es leal[245] con los titulares[246], esto es que "quienes no necesariamente tengan los conocimientos técnicos también les pueda ser fácil la comprensión del uso de datos"[247].

Finalmente, contestando la pregunta central que motiva este capítulo, esto es, si el marco normativo vigente propicia la proliferación de agentes que perfilan datos electorales al no existir una fiscalización adecuada al respecto, podemos concluir que efectivamente no existen incentivos ni limitaciones legales claras para evitar las malas prácticas en que han incurrido algunos en el contexto de campañas electorales y comerciales, siendo especialmente necesario promulgar el Proyecto de Ley de reforma.

Ahora bien, cabe señalar que a pesar de los riesgos que han sido presentados en esta memoria, el *microtargeting*, sin importar su fin, difícilmente desaparecerá y su prohibición absoluta solo podría fomentar su aplicación al margen de la ley, siendo aún más difícil su fiscalización. De hecho, aun cuando la opinión de variados expertos citados en acápites anteriores como Cristobal Huneeus, denoten desconfianza en la efectividad del perfilamiento para influir de lleno en una elección, podemos decir que seguir la senda regulatoria de los Estados Europeos permite controlar anticipadamente escenarios en los que, evolucionado el estado del arte, pueda afirmarse que el *gerrymandering* electoral es efectivo y representa una amenaza tangible para la democracia.

---

[244] **ALEXY, ROBERT.** Sistema jurídico, principios jurídicos y razón práctica, 1988, p. 139 Disponible en https://rua.ua.es/dspace/bitstream/10045/10871/1/Doxa5_07.pdf

[245] El principio de lealtad adopta esta nomenclatura por ser una traducción aceptada del término *fairness*, que como principio se recoge en el Reglamento Europeo y fue ejemplificado de la siguiente forma por **BORDACHAR.** "El caso que describe ocurrió en Europa, una empresa de televisión escuchaba las conversaciones de las personas a través del control remoto. En el juicio, la empresa se defendió argumentando que el mecanismo era transparente porque lo informaron en su política de privacidad, y lícito, porque las personas dieron el consentimiento; pero, gracias al principio de lealtad, se resolvió que no era leal, pues, nadie podría pensar que a través de un control remoto se podría estar escuchando su conversación" **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO,** *Op.cit* p. 177

[246] **BORDACHAR** en cuanto a este punto mostró su preocupación en la Sesión N° 16 de 18 de mayo de 2022, señalando que el desarrollo del principio de licitud y lealtad (sobre todo este último), era en extremo necesario para dar garantías de seguridad a los titulares de datos, como ocurre en Europa.

[247] Intervención del Ministro Giorgio Jackson 176 informe sesión Sesión N° 26 de 6 de julio de 2022. **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO,** *Op.cit* p. 176

En este sentido, para cerrar este apartado, destacamos las palabras del señor Carlos Reusser Monsálvez, académico de Derecho de la Información y Derechos Digitales de la Universidad Alberto Hurtado quien expuso ante el congreso que "El camino no era la prohibición, sino la transparencia algorítmica, es decir que sí se puede usar Inteligencia Artificial para resolver múltiples asuntos en forma automatizada — en los que hay involucrados datos personales—, pero lo que debe hacerse es establecer la obligación de transparentar los algoritmos que se utilizan para tomar decisiones, de forma de conocer cuál es la lógica del razonamiento que utilizan dichos sistemas. Y si la lógica es cuestionable, probablemente también lo sea el resultado de la decisión"[248].

III.4 Proyecto de Ley que limita el acceso de los partidos a información personal y que regula la propagación de "fake news" en política: Boletín N° 13.698-07

En el apartado tercero de esta investigación se desarrolló el concepto de noticias falsas o *fake news*, y se explicó, por una parte, que su utilización constituye una herramienta auxiliar para lograr captar la atención de grupos importantes de la población que responden al estímulo compartiendo datos personales. Por otra parte, se explicó que los métodos de diseminación de las mismas pueden ser más bien tradicionales, esto es, la disposición de capital humano que las redacta y las propaga manualmente, o bien, pueden ser más sofisticados, valiéndose de sistemas dotados de IA que rápidamente pueden crear cientos de *fake news* y propagarlas a través de *bots* automatizados en distintas plataformas digitales donde están conectados día a día los ciudadanos.

Ahora bien, sin perjuicio de que sea un tema de larga data como quedó demostrado anteriormente -aunque con mayor impacto el ultimo siglo por el auge de la Tecnología de la Información y Comunicación (TIC'S)-, en nuestro país la crítica social y académica no se había materializado en un intento legislativo por regular la problemática sino hasta el año 2020 en que los Honorables Senadores señor Harboe, señora Rincón y señor Pugh presentaron el proyecto de ley que *"limita el acceso de los partidos a información personal y que regula la propagación de "fake news" en política"*, boletín N° 13.698-07.

El proyecto, tiene por objetivo, en palabras de sus autores, el tratamiento de datos por los partidos políticos y la difusión de *fake news*[249]. Además, es importante destacar que, [250]en la introducción del proyecto, los Senadores hacen referencia directa al *microtargeting electoral* como una realidad que requiere regulación, manifestando su preocupación por la creación de algoritmos que reducen a los

[248] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO,** *Op.cit* p. 104
[249] Ibid.
[250] **Boletín N° 13.698-07**

ciudadanos a una etiqueta que permite enviarles propaganda ideológica personalizada que contribuye a la formación de sesgos y burbujas, en una tónica concordante con la literatura que se ha expuesto en está investigación, toda vez que ponen el acento en la ligazón que existe en las técnicas de perfilamiento y la proliferación de noticias falsas.

Las modificaciones que propone el proyecto se centran en reformar ciertas disposiciones normativas de los principales cuerpos legales que regulan a los partidos politicos y los periodos eleccionarios, siguiendo la tónica que, han adoptado países pertenecientes a la Unión Europea respecto del tema[251]. En concreto, las modificaciones propuestas son:

- **Modificación Ley N°18.603, Orgánica Constitucional de los Partidos Políticos**: En este caso se propone agregar un nuevo artículo 18 bis, el cual dispondrá: *"Los partidos políticos tendrán prohibido el tratamiento de datos personales con el objeto de inferir la ideología política de alguna persona, por tratarse de un dato sensible de conformidad al artículo 2º letra g) de la ley Nº 19.628, Sobre Protección a la Vida Privada.*

Esta prohibición incluye la realización de perfiles a través de datos ideológicos, sexuales, religiosos o de cualquier otro tipo que se desprenda a partir del comportamiento de una persona en línea, sean redes sociales u otras fuentes de acceso público, a menos de contar con su consentimiento expreso.

En forma adicional, los partidos políticos al momento de tratar los datos personales de sus afiliados deberán respetar el principio de finalidad del dato."

Además, en el caso del artículo 20 numero 1° -que regula derechos y deberes de los afiliados y consagra en favor de ellos el deber de que los estatutos de los partidos expliciten los derechos de aquellos-, se agregaría el literal m) que versa así: *"Manifestar el consentimiento para el tratamiento de la información relativa a la afiliación al partido político respectivo. Asimismo, ejercer respecto de todos sus datos personales los derechos de acceso, rectificación, cancelación, oposición y portabilidad, conforme a lo previsto en las leyes Nºs 19.628 y 21.096."*

- **Modificación Ley N°19.628 sobre Protección a la Vida Privada**: Se agrega al artículo 3 referido a los datos obtenidos en sondeos, encuestas o similares, un nuevo inciso final, que consagra derechos en favor de los titulares de datos personales, señalando que *"Con todo, el tratamiento de datos sensibles relativos a las convicciones ideológicas, filosóficas o políticas*

[251] Véase **PEÑA DANIELA, VARGAS FERNANDA.** *Análisis y desafíos que plantean las fake news para el derecho a la libertad de expresión y la información.* Memoria para obtener el grado de Licenciatura en Ciencias Jurídicas. Facultad de Derecho y Ciencias Sociales, Universidad de Valparaíso.

siempre requerirá del consentimiento expreso del titular, y no serán aplicables respecto de éste las excepciones a la obligación de requerir consentimiento consagradas en el artículo 4º de la ley".

- **Modificación Ley N°18.665 Orgánica Constitucional sobre Sistema de Inscripciones Electorales y Servicio Electoral**: En este caso, se ordena la modificación del actual artículo 31 del cuerpo legal en comento[252], agregando un nuevo inciso segundo. Además, se modificaría completamente el inciso quinto, teniéndose por resultado la siguiente disposición normativa:

> *"Para cada uno de los padrones electorales, el Servicio Electoral determinará un Padrón Electoral con carácter de provisorio, ciento veinte días antes de una elección o plebiscito. Éste contendrá una nómina de las personas inscritas en el Registro Electoral que, conforme a los antecedentes conocidos por el Servicio Electoral antes de los ciento cuarenta días previos al acto electoral, reúnan a la fecha de la elección o plebiscito correspondiente los requisitos necesarios para ejercer el derecho a sufragio.*
>
> ***Para los efectos del inciso anterior, se deberá tener especialmente presente las disposiciones aplicables a cada dato personal según su propia naturaleza.***
>
> *Cada Padrón Electoral con carácter de provisorio será objeto de auditorías conforme al Párrafo 2° de este Título.*
>
> *Estos padrones se ordenarán en forma alfabética y contendrán los nombres y apellidos del elector, su número de rol único nacional, sexo, domicilio electoral con indicación de la circunscripción electoral, comuna, provincia y*

[252] **Artículo 31 Ley N°18.665 vigente:** Para cada uno de los padrones electorales, el Servicio Electoral determinará un Padrón Electoral con carácter de provisorio, ciento veinte días antes de una elección o plebiscito. Éste contendrá una nómina de las personas inscritas en el Registro Electoral que, conforme a los antecedentes conocidos por el Servicio Electoral antes de los ciento cuarenta días previos al acto electoral, reúnan a la fecha de la elección o plebiscito correspondiente los requisitos necesarios para ejercer el derecho a sufragio.
Cada Padrón Electoral con carácter de provisorio será objeto de auditorías conforme al Párrafo 2° de este Título.
Estos padrones se ordenarán en forma alfabética y contendrán los nombres y apellidos del elector, su número de rol único nacional, sexo, domicilio electoral con indicación de la circunscripción electoral, comuna, provincia y región a la que pertenezcan, o del país y ciudad extranjera, según sea el caso, y el número de mesa receptora de sufragio en que le corresponde votar.
Junto con cada Padrón, y dentro del mismo plazo, el Servicio Electoral elaborará dos nóminas provisorias de Inhabilitados, que incluirá a las personas inscritas que se encuentren inhabilitadas para votar en la correspondiente elección o plebiscito, y que sufraguen dentro o fuera de Chile, según corresponda, con indicación de la causal que dio lugar a dicha condición.
Los padrones electorales y las nóminas provisorias de Inhabilitados son públicos, sólo en lo que se refiere a los datos señalados en el inciso tercero, debiendo los requirentes pagar únicamente los costos directos de la reproducción. Los partidos políticos recibirán del Servicio Electoral, dentro de los cinco días siguientes a su emisión, en forma gratuita, copia de ellos en medios magnéticos o digitales, no encriptados y procesables por software de general aplicación. Lo mismo se aplicará para los candidatos independientes, respecto de las circunscripciones electorales donde participen.
Sólo las personas inhabilitadas podrán conocer, además, la respectiva causal que las inhabilita.

región a la que pertenezcan, o del país y ciudad extranjera, según sea el caso, y el número de mesa receptora de sufragio en que le corresponde votar.

Junto con cada Padrón, y dentro del mismo plazo, el Servicio Electoral elaborará dos nóminas provisorias de Inhabilitados, que incluirá a las personas inscritas que se encuentren inhabilitadas para votar en la correspondiente elección o plebiscito, y que sufraguen dentro o fuera de Chile, según corresponda, con indicación de la causal que dio lugar a dicha condición.

Los datos personales de cada elector contenidos en los padrones electorales y las nóminas provisorias de inhabilitados no serán públicos. El Servicio Electoral será, por tanto, responsable de proteger y resguardar estos datos personales en conformidad a la legislación vigente

Sólo las personas inhabilitadas podrán conocer, además, la respectiva causal que las inhabilita".

Se agrega, además, un nuevo inciso respecto de las auditorias de las que son objeto los registros y padrones electorales, reguladas en el artículo 39, de la siguiente manera:

"Las auditorías serán practicadas por dos empresas independientes de auditoría externa, de niveles equivalentes, inscritas en el registro que al efecto lleva la Superintendencia de Valores y Seguros, las cuales deberán cumplir con los requisitos de capacidad, tamaño, confiabilidad y garantía que, mediante una norma general, determinará el Consejo del Servicio Electoral.

La auditoría deberá respetar las disposiciones aplicables según la naturaleza de cada dato personal tratado. Queda prohibida la divulgación de los datos respecto de los cuales los auditores tengan conocimiento en virtud de la prestación del servicio

El presupuesto del Servicio Electoral deberá contemplar los fondos necesarios para financiar los procesos de auditorías"

- **Modificación Ley N°18.700 Orgánica Constitucional sobre Votaciones Populares y Escrutinios**: Respecto del actual artículo 31 que sienta las bases de aquello que es considerado propaganda electoral, se agrega un nuevo inciso tercero y cuarto que delimita conceptualmente de la siguiente manera: *"En ningún caso se considerará como propaganda electoral aquellas acusaciones, imputaciones o noticias que se refieran a hechos que sean capaces de alterar la sinceridad de la próxima votación y sean difundidos de forma deliberada, artificial, automatizada y masiva a través de un canal de comunicación masivo o red social"*.

"Se prohíbe la realización de propaganda electoral vía telemarketing en cualquier horario, así como la mensajería instantánea masiva sin el consentimiento expreso del destinatario".

- **Modificación Ley N° 19.884 sobre Transparencia, Límite y Control del Gasto Electoral**: Se agregaría un nuevo artículo 29 bis, en el marco de las sanciones que impone

dicha Ley, disponiendo que: *"El que, durante el período legal de campaña electoral, a sabiendas, difunda acusaciones, imputaciones o noticias que se refieran a hechos que sean capaces de alterar la sinceridad del proceso electoral en curso o del próximo y sean difundidos de forma deliberada, artificial, automatizada o masiva a través de un canal de comunicación masivo o red social, será sancionado con la pena de presidio menor en su grado mínimo a medio y multa de 10 a 100 UTM.*

Tratándose de un candidato a un cargo de elección popular, quedará además inhabilitado para proceso electoral en curso.

La autoridad electa que incurra en la conducta descrita en el inciso primero durante el periodo de campaña electoral cesará en su cargo."

En síntesis, podemos señalar que las modificaciones constatadas satisfacen los fines del proyecto de Ley explicitados por sus promotores, readecuando la normativa vigente para prohibir ciertas conductas que pueden ser lesivas con respecto a los derechos fundamentales de los ciudadanos y que implican en concreto una violación a su libertad de conciencia, opinión e información. Sin embargo, el proyecto en cuestión se encuentra estacando en su tramitación, ya que aun se encuentra en primer su prime trámite constitucional en el Senado, pasando con fecha 11 de agosto de 2020 a la Comisión de Constitución, Legislación, Justicia y Reglamento, sin que existan nuevos avances.

Sin perjuicio de lo anterior, estimamos que, de momento, no vale la pena avanzar con su tramitación sin antes promulgar la nueva Ley de Protección de Datos personales que se encuentra en su fase final como comentamos en el segundo acápite de este capítulo. Lo anterior, toda vez que no tendría sentido mandatar la modificación de la Ley N° 19.628 si está será derogada y, en paralelo, será necesario armonizar todos los cambios que se pretenden realizar respecto de las leyes electorales adecuándolas a la sustancia normativa que está contenida en el proyecto de Ley de Datos Personales para nuestro país.

De hecho, es posible percatarse que el artículo primero del proyecto, al modificar la Ley Orgánica Constitucional de los Partidos Políticos les prohíbe la elaboración de perfiles compuestos de datos personales sensibles como los ideológicos, sexuales, religiosos aun cuando la información en cuestión sea recopilada de fuentes de acceso público. Este punto, de aprobarse el proyecto de Ley de Protección, a juicio de quien escribe, debería ser incluido en este, puesto que constituye una excepción a las reglas dispuestas para el caso de la recopilación de fuentes de acceso público, en atención al artículo 14 bis. relativo al deber de confidencialidad de quien trata datos personales que recopiló de dicha forma[253], estableciéndose una prohibición a todo evento para los partidos politicos de forma particular.

[253] **Artículo 14. Bis del proyecto:** Deber de secreto o confidencialidad. El responsable de datos está obligado a mantener secreto o confidencialidad acerca de los datos personales que conciernan a un titular, salvo cuando el

III.5 Proyecto de ley que regula los sistemas de Inteligencia Artificial en Chile: Boletín N°15869-19

Como ha quedado de manifiesto a lo largo de esta memoria, la utilización de datos personales con el fin de perfilar segmentos de la población y eventualmente incidir en su toma de decisiones requiere de la utilización de sistemas dotados de inteligencia artificial (en adelante IA, por sus siglas) que, en definitiva, ejecuten las operaciones metódicamente y, a su vez, estos sistemas requieren de una amplia gama de datos personales para poder nutrirse de "conocimiento". En este sentido, no resulta para nada desconocida la irrupción constante de softwares dotados de IA que permiten crear imágenes a partir de textos; redactar artículos periodísticos o literarios; e incluso contestar a las más variadas preguntas como ocurre con el paradigmático caso de ChatGPT.

En este contexto de revolución tecnológica, el Ministerio de Ciencias, Tecnologías, Conocimiento e Innovación formuló la denominada Política Nacional de Inteligencia Artificial, que fue publicada en octubre del año 2021. El entonces ministro de Ciencias Andrés Couve enfatizó durante su lanzamiento en que "la Inteligencia Artificial es un ámbito de la revolución tecnológica que se ha incorporado a nuestra vida cotidiana. Esta Política Nacional nos permite promover la construcción de capacidades para su desarrollo y uso responsable y apunta a empoderar a la ciudadanía, a comprender las oportunidades y ventajas que nos brinda, así como los riesgos asociados"[254].

Siguiendo la línea de los objetivos de dicha política, esto es, situar a Chile para el año 2031 como uno de los países sobre el estándar OCDE en materia de IA en la región latinoamericana[255], con fecha 26 de abril del 2023 el Honorable Diputado Dr. Tomás Ignacio Lagomarsino Guzmán presentó el proyecto

---

titular los hubiere hecho manifiestamente públicos. Este deber subsiste aún después de concluida la relación con el titular. En caso de que el responsable haya realizado alguna acción sobre datos personales obtenidos de fuentes de acceso público, tales como organizarlos o clasificarlos bajo algún criterio, o combinarlos o complementarlos con otros datos, los datos personales que resulten de dicha acción se encontrarán protegidos bajo el presente deber de secreto o confidencialidad.
El deber de secreto o confidencialidad no obsta a las comunicaciones o cesiones de datos que deba realizar el responsable en conformidad a la ley, y al cumplimiento de la obligación de dar acceso al titular e informar el origen de los datos, cuando esta información le sea requerida por el titular o por un órgano público dentro del ámbito de sus competencias legales.
El responsable debe adoptar las medidas necesarias con el objeto de que sus dependientes o las personas naturales o jurídicas que ejecuten operaciones de tratamiento de datos bajo su responsabilidad, cumplan el deber de secreto o confidencialidad establecidos en este artículo.
Quedan sujetas a la obligación de confidencialidad las personas e instituciones y sus dependientes a que se refiere el artículo 24, en cuanto al requerimiento y al hecho de haber remitido dicha información.

[254] Véase https://www.gob.cl/noticias/chile-presenta-la-primera-politica-nacional-de-inteligencia-artificial/

[255] **MINISTERIO DE CIENCIAS, TECNOLOGÍAS, CONOCIMIENTO E INNOVACIÓN.** Politica Nacional de Inteligencia Artificial, 2021, p.6. Disponible en: https://www.minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf

de Ley boletín N°15869-19 que *"regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación"*. El proyecto en cuestión, tal como se consigna en su primer considerando, tiene por objetivo regular aspectos sustantivos ligados a las nuevas tecnologías que utilizan inteligencia artificial, con tal de evitar riesgos y la radicación de efectos negativos en los usuarios de tales sistemas, resguardando los derechos fundamentales de los ciudadanos. Por lo mismo, resulta necesario analizar en el contexto de esta memoria, si el presente proyecto de ley esta dotado de la potencialidad necesaria para regular los sistemas dotados de IA que se utilizan complementariamente para perfilar al electorado y que, desde luego, pueden afectar derechos fundamentales como la libertad de opinión y conciencia, la vida privada y sus datos personales, y a un desarrollo científico y tecnológico que esté al servicio de las personas y se llevé a cabo con respeto a la vida y a la integridad física y psíquica, tal como prescribe la Constitución vigente.

En este sentido, resumimos que los pilares sobre los cuales descansa el proyecto en comento son los siguientes:

1. Ofrece un catálogo de definiciones de conceptos comúnmente utilizados en las relaciones jurídicas en que participa una IA.
2. Establece una enumeración taxativa de sistemas de IA que son consideradas de riesgo inaceptable y de alto riesgo.
3. Mandata al Ministerio de Ciencia, Tecnología, Conocimiento e Innovación la creación de la Comisión Nacional de Inteligencia Artificial, cuyas funciones se compondrán de labores preventivas, administrativas fiscalizadoras y sancionadoras en todo aquello relacionado al uso de sistemas de IA.
4. Establece un procedimiento administrativo para que los desarrolladores y/o usuarios de sistemas de IA soliciten autorización a la Comisión Nacional de Inteligencia Artificial para el desarrollo, distribución, comercialización y utilización de aquellos, decidiendo la Comisión en cuestión si autoriza en un plazo de 30 días.
5. Establece un catálogo de sanciones en el caso de que -en el marco del desarrollo, distribución, comercialización y utilización de sistemas de IA- se incumplan las normas contenidas en el proyecto.

Ahora bien, sin perjuicio de lo novedoso del proyecto se hace imperioso mencionar que -tal como se explicita en el considerando segundo del boletín N°15869-19[256]- en la creación del cuerpo legal,

[256] Disponible en: https://www.camara.cl/legislacion/comisiones/proyecto_ley.aspx?prmID=3303

se utiliza como referencia la propuesta de Reglamento de Inteligencia Artificial del Parlamento Europeo, pero de forma extremadamente acotada.

En cuanto a tal proyecto de derecho comparado, como puede desprenderse de la lectura de la exposición de motivos que fundamentan la creación del Reglamento Europeo, el objetivo de dicho Parlamento es dotar de un marco regulatorio que permita fiscalizar *ex ante* y *ex post* los sistemas dotados de IA, siempre en atención al potencial riesgo que estos representan y a los conflictos éticos que pueden derivar de la utilización de estas nuevas tecnologías. En concreto, los objetivos específicos de esta política europea son:

- *"Garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;*

- *Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;*

- *Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;*

- *Facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado"*[257].

Dicho esto, cabe destacar que, en línea con la comentada clasificación de riesgos que resulta ser un pilar fundamental para la Comisión Europea, el proyecto presentado por el Diputado Lagomarsino establece en su artículo tercero cuales sistemas dotados de IA son catalogados como inaceptables, estipulando que lo son:

Art. 3:

1. *Aquel que se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.*

2. *Aquel que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra.*

3. *Aquel utilizado por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas naturales durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad*

---

[257] **PROPUESTA REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN**, *Comisión Europea*, 2021, P.3. Disponible en español en: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

conocidas o predichas, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:

a. Un trato perjudicial o desfavorable hacia determinadas personas o colectivos en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente.

b. Un trato perjudicial o desfavorable hacia determinadas personas o colectivos que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de éste.

4. Aquel de identificación biométrica remota en tiempo real o diferido en espacios de acceso público, salvo y en la medida que dicho uso sea estrictamente necesario para alcanzar uno o varios de los siguientes objetivos:

a. La búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos.

b. La prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas o de un atentado terrorista.

c. La detección, localización, identificación o enjuiciamiento de la persona que ha cometido, o se sospecha que ha cometido alguno de los delitos incluidos en el Código Penal.

Por su parte, el artículo cuarto menciona cuales sistemas serían aceptables, pero calificados como de alto riesgo y, por tanto, dignos de tratamiento especial:

Art. 4

Serán calificados como sistemas de IA de alto riesgo los destinados a utilizarse en:

1. *La identificación biométrica remota en tiempo real o diferido de personas en espacios privados.*
2. *La utilización en gestión del suministro de agua, electricidad y gas.*
3. *La asignación y determinación del acceso a establecimientos educacionales y la evaluación de estudiantes.*
4. *La selección y contratación de personas en trabajos.*
5. *La asignación de tareas y el seguimiento y evaluación del rendimiento y la conducta de trabajadores.*
6. *La evaluación de las personas para acceder a prestaciones y servicios de asistencia pública.*
7. *La evaluación de la solvencia de personas o establecer su calificación crediticia.*
8. *La utilización en situaciones de emergencia y desastre, particularmente en el envío o establecimiento de prioridades para el envío de servicios de intervención (ejemplo, bomberos o ambulancias).*
9. *La utilización de ellas para determinar el riesgo de que personas cometan infracciones penales o reincidan en su comisión, así como el riesgo para las potenciales víctimas de delitos.*
10. *La utilización de ellas en cualquier etapa de investigación e interpretación de hechos que pudieran constituir un delito en el contexto de un juicio.*
11. *La utilización de ellas para gestión de la migración, el asilo y el control fronterizo.*

Igualmente, serán calificados como sistemas de IA de alto riesgo aquellos que conlleven

el riesgo de causar un perjuicio a la salud y la seguridad, o el riesgo de tener repercusiones negativas para los derechos fundamentales, cuya gravedad y probabilidad sean equivalentes o mayores de los riesgos de perjuicio o de repercusiones negativas asociados a los sistemas de IA señalados en el inciso primero de este artículo.

Tomando en consideración los artículos en comento, podemos darnos cuenta de que resultan ser una reproducción parcial de las disposiciones normativas contenidas en el proyecto europeo en su titulo segundo referido a "practicas de inteligencia artificial prohibidas" y a su título tercero relativo a "sistemas de IA de alto riesgo", destacando que estos últimos no se prohíben, sino que se regulan de forma especial, debido al impacto que pueden tener en los usuarios.

Si bien el estado de la discusión legislativa es extremadamente incipiente, resulta necesario esbozar ciertas recomendaciones que eleven el debate y, por cierto, permitan explorar la posibilidad de incluir ciertas hipótesis que digan relación con aquellos sistemas que utilizan grandes volúmenes de datos para perfilar al electorado, al menos dentro de una figura más general.

De hecho, del examen del articulado, cabe preguntarse si aplicaciones dotadas de IA que tienen por objetivo manipular al electorado para incitarlos a optar por determinadas conductas en el marco de un proceso democrático constituyen sistemas de riesgo inaceptable por valerse de técnicas subliminales para inmiscuirse en la conciencia de una persona provocando perjuicios que pueden ser psicológicos, siguiendo la terminología del artículo tercero antes expuesto. Bien podría también argumentarse que la tecnología que lleva a cabo el *microtargeting* electoral aprovecha la vulnerabilidad de un grupo en específico, si, por ejemplo, se ejecuta en grupos de la población ya segmentados por cuestiones físicas, como aquellos ciudadanos que presentan discapacidades.

En razón de estas dudas, cobra relevancia la técnica legislativa utilizada en el proyecto europeo, toda vez que no ofrece una lista taxativa e invariable de hipótesis en que los sistemas dotados de IA son prohibidos o considerados de alto riesgo, sino que, se le otorga el poder a la Comisión Europea en el mismo proyecto para poder ampliar el catalogo de manera más expedita, sobre todo si un sistema o *software* puede tener consecuencias negativas con respecto a los derechos fundamentales de los ciudadanos[258]. Así, aun cuando de la interpretación del proyecto se consigne que, en principio, un sistema

[258] Art. 7. Se otorgan a la Comisión los poderes para adoptar actos delegados de conformidad con el artículo 73 al objeto de modificar la lista del anexo III mediante la adición de sistemas de IA de alto riesgo cuando se reúnan las dos condiciones siguientes:
a) los sistemas de IA estén destinados a utilizarse en cualquiera de los ámbitos que figuran en los puntos 1 a 8 del anexo III; y
b) los sistemas de IA conlleven el riesgo de causar un perjuicio a la salud y la seguridad, o el riesgo de tener repercusiones negativas para los derechos fundamentales, cuya gravedad y probabilidad sean equivalentes o mayores a las de los riesgos de perjuicio o de repercusiones negativas asociados a los sistemas de IA de alto riesgo que ya se mencionan en el anexo.

de IA que perfila al electorado no constituye un riesgo, esto podría ser modificado de manera expedita en atención a la vulneración de derechos fundamentales.

En conclusión, resulta extremadamente necesario que el desarrollo legislativo del boletín N° 15869-19 permita que el proyecto en comento se convierta en un cuerpo legal dinámico. Lo anterior, a juicio de quien les escribe, se logrará en la medida de que trascienda ciertas deficiencias propias de un proyecto de ley que es presentado en un formato tremendamente acotado y que se inspira en un reglamento de mucha mayor extensión y envergadura, como el europeo. Además, de aprobarse el proyecto de ley de datos personales en Chile, será necesario que ambos cuerpos legales estén en armónica sintonía y las hipótesis de sistemas dotados IA considerados inaceptables o de alto riesgo se basen en los peligros que pretenden ser regulados desde la arista de los datos personales. Lo anterior es importante, toda vez que el estado del arte actual demuestra fehacientemente que la inteligencia artificial requiere de volúmenes de datos ostensibles para operar de forma adecuada.

CAPÍTULO IV. ÁNALISIS DE LA SITUACIÓN COMPARADA

Como se ha señalado a lo largo de esta memoria, el *microtargeting* electoral representa una preocupación de carácter internacional, abriendo un debate ético y político-legal acerca de cómo los partidos politicos perfilan a sus votantes para dotarlos de información de campaña, o bien, para derechamente influir en el sufragio. Por lo mismo, la presente investigación no puede sino cerrar analizando el panorama comparado, toda vez que ha quedado patente que la discusión y regulación más sofisticada a propósito de los datos personales y la inteligencia artificial -en términos generales- ha sido promovida fuera del país, en el territorio europeo principalmente.

Las razones por las cuales se produce esta diferencia regulatoria son varias, pero, a juicio de quien les escribe, principalmente vienen dadas por la eficiencia y voluntad de La Comisión Europea y los países miembros y, por otro lado, debido a los paradigmáticos casos de *microtargeting electoral* que marcaron la pauta mediática en la Unión Europea.

En cuanto a la primera razón esbozada, cabe señalar que el Parlamento Europeo ha desarrollado una serie de reglamentos y directrices que han sido adoptados por los países miembros. Un ejemplo claro del punto anterior es la creación del Reglamento General de Protección de Datos de la Unión Europea que se encuentra vigente desde el año 2018, el que constituyó un innovador intento por otorgar una regulación armonizada, homogénea y altamente efectiva en cuanto a la salvaguarda de los derechos fundamentales de los ciudadanos de la Unión. En este sentido, el considerando decimo del referido Reglamento es bastante revelador:

> *"Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas*

sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito"[259]

En cuanto al segundo punto, resulta especialmente paradigmático el caso de Cambridge Analytica, corporación que fue objeto de estudio e investigación por su participación en la recopilación de datos que fueron utilizados en campañas electorales que tuvieron lugar en Estados Unidos y Europa, como, por ejemplo, la campaña de Donald Trump y el Brexit, respectivamente.

A mayor abundamiento, la empresa en cuestión (de ahora en adelante, CA), resultó ser una consultora británica fundada el año 2013 y dependiente del grupo Strategic Communications Laboratories (SCL Group), proveedora de datos y analisis de los mismos para gobiernos y organizaciones militares, principalmente relativo a miembros de la OTAN[260] que ya tenía experiencia en el manejo de propaganda política, a través de la empresa especializada SCL Elections, parte del grupo económico.

La creación de la empresa contó con el financiamiento de los republicanos Robert Mercer y Steve Bannon, y desde que comenzó a operar se compuso de una mayoría de integrantes que resultaban ser investigadores de la Universidad de Cambridge, inspirando el nombre definitivo que adquirió la consultora[261]. Ahora bien, para comenzar a operar en el mundo de las asesorías de campaña política, requerían una gran cantidad de datos que fueron comprados a una tercera empresa llamada Global Science Research, que tenía como líder a Aleksander Kogan, un psicólogo ruso que creó una aplicación llamada "This is my digital life" que ofrecía una predicción psicográfica de la personalidad[262]. La forma en que operaba era a través de una conexión obligada a la red social Facebook, solicitando el permiso para acceder a datos personales, pero no solo eso, sino que igualmente a los datos personales de los

[259] **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS,** Considerando 10. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

[260] **VERCELLI, ARIEL**. La (des) protección de los datos personales: análisis del caso Facebook Inc.-Cambridge Analytica. En *XVIII Simposio Argentino de Informática y Derecho (SID)-JAIIO 47 (CABA, 2018)*. 2018. P 2

[261] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

[262] **VERCELLI, ARIEL.** *Op. cit* P.2

usuarios agregados como amigos en la plataforma[263]. De esta forma la actividad constituyó una verdadera minería de datos que les permitió manejar datos personales de un aproximado de 50 millones de usuarios[264], habiendo accedido inicialmente a la plataforma directamente solo unos 370.000[265].

El caso salió a la luz gracias a la investigación llevada a cabo por los medios periodísticos británicos Channel 4 y The Observer (The Guardian), además del The New York Times, quienes expusieron igualmente las negociaciones internas que llevaron a cabo las empresas que trataban los datos con Facebook, que al tomar conocimiento de los hechos solo les ordenó eliminar los datos sin tomar una posición activa denunciando lo ocurrido, ni tampoco verificando que realmente se materializara[266].

De ahí en más, como constatan los investigadores de Dinamarca Selma Marthadal y Peter Aagaard en un artículo que tiene por objeto dar a conocer el estado del arte referido a la literatura académica europea y norteamericana que analiza el uso de datos personales e IA en campañas electorales, se concluyó que desde el año 2016 hubo un aumento sostenido en las publicaciones, que solo cesó el año 2021 y siguientes, probablemente porque para esa fecha la regulación del tópico -que adoptó diferentes formatos según el Estado- había avanzado considerablemente[267].

Si bien los enfoques respecto al *microtargeting* varían según los artículos de estudio y apuntan en diferentes direcciones, como por ejemplo, la afectación de derechos fundamentales; el esparcimiento de noticias falsas; el analisis de cuerpos normativos en materia de protección de datos; entre otros, existe un consenso generalizado en que el tema si bien es controversial por la dificultad que se suscita al momento de verificar científicamente si es que existe movilización de los votos luego de aplicada la técnica de manipulación, lo cierto es que -como se verá en los próximos acápites- la regulación europea hace referencias al uso de datos por los partidos politicos en las campañas electorales de forma clara y expresa.

En atención a lo comentado, el estudio comparado de la temática se realizará, en primer lugar, a partir del analisis del Reglamento General de Protección de Datos de la Unión Europea que, lejos de ser un examen pormenorizado y exhaustivo, tendrá por objeto comparar las reglas relativas a las hipótesis

---

[263] **SCHNEBLE, CHRISTOPHE OLIVIER; ELGER, BERNICE SIMONE; SHAW, DAVID**. The Cambridge Analytica affair and Internet-mediated research. EMBO reports, 2018, vol. 19, no 8, p. e46579. P.1
[264] **BOLDYREVA, ELENA L.,** et al. Cambridge analytica: Ethics and online manipulation with decision-making process. European Proceedings of Social and Behavioural Sciences, 2018, vol. 51. P.96
[265] **SCHNEBLE, CHRISTOPHE OLIVIER; ELGER, BERNICE SIMONE; SHAW, DAVID.** *Op. cit* p.3
[266] **BOLDYREVA, ELENA L.** *Op. cit.* p.*96*
[267] **AAGAARD, PETER; MARTHEDAL, SELMA**. Political microtargeting: Towards a pragmatic approach. *Internet Policy Review*, 2023, vol. 12, no 1. P.7

de tratamiento automatizado de datos y la elaboración de perfiles con aquellas contenidas en el proyecto de ley de Protección de Datos que se tramita en nuestro país.

En segundo lugar, se analizará la situación en que se encuentra España frente al tema, país que ha sido escogido dado que su regulación de Derecho Interno ha servido de modelo en la discusión parlamentaria que sigue llevándose a cabo en nuestro territorio y, además, porque existen significativos casos de estudio en conjunto con un fallo del Tribunal Constitucional Español que se pronuncia sobre el tema y amerita ser comentado.

IV.1 Análisis del Reglamento General de Protección de Datos de la Unión Europea y su regulación frente al tratamiento automatizado de datos personales

El Reglamento General de Protección de Datos Europeo (en adelante, RGPD) es el resultado de una concatenación de acuerdos politicos de la Unión Europea dirigidos a salvaguardar y proteger activamente los derechos fundamentales de los ciudadanos de los países miembros. Así, uno de los antecedentes más importantes es la proclamación de la Carta de Derechos Fundamentales de la Unión Europea el año 2000, que pasó de un documento declarativo de carácter eminentemente político a ser jurídicamente vinculante y catalogado como Derecho Primario para la UE, una vez que entró en vigor el Tratado de Lisboa del año 2009[268].

En dicha Carta, se consagra en el artículo octavo como derecho fundamental la protección de los datos personales, en línea con el instrumento jurídico de la Unión Europea que imperaba en ese momento en materia de protección de datos, esto es, la Directiva 95/46/CE del Parlamento Europeo y del Consejo 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para aquél entonces, la mayoría de Estados miembro tenían regulaciones de Derecho interno y, por lo mismo, en la década del noventa se intentó lograr una armonía que, en ese entonces, más que proteger a los ciudadanos buscaba regular el mercado entre los países pertenecientes a la UE.[269]

No fue sino hasta el año 2012 en que la voluntad política de la Comisión Europea se traduce en la aprobación de una propuesta de Reglamento que modificara la regulación europea de protección de datos personales vigente en la época, derogándola con el objetivo de que se erigiera como la cúspide de la regulación a nivel internacional. Así, termina por promulgarse el RGDP el 04 de mayo del año 2016 -mismo año en que se dan a conocer los casos de Cambridge Analytica y Facebook- y entra en vigor de

[268] **MANUAL DE LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS**. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019 Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf, p, 31- 32

[269] *Ibid p.33*

forma definitiva el 25 de mayo del año 2018, habiéndose otorgado un plazo de adecuación a los actores europeos.

Pasando al analisis concreto del cuerpo legal en comento, es posible constatar en su artículo segundo relativo al ámbito de aplicación material del Reglamento que se aplica al tratamiento total o parcialmente automatizado de datos personales, así como el tratamiento no automatizado. Lo anterior, responde a la idea de bases regulatorias que protejan a los ciudadanos sin importar los mecanismos que se utilizan, lo que el Parlamento define como "una regulación tecnológicamente neutra"[270].

Posteriormente, se ofrece un listado de definiciones conceptuales que resultan atingentes a la sustancia del Reglamento, y que, por supuesto incluyen la automatización de datos y la elaboración de perfiles, punto que claramente sirvió de inspiración para el proyecto de Ley que se encuentra en tramitación en nuestro país.

Más importante aún, el RGDP en su artículo 9 se refiere al Tratamiento de categorías especiales de datos personales, dentro de las cuales se encuentran las opiniones políticas. La particularidad de estas categorías es que como señala el inciso primero de la referida disposición normativa, no son susceptibles de tratamiento, salvo que se cumpla algún supuesto previsto en la norma, como por ejemplo si el tratamiento utilizará datos personales que el interesado ha hecho manifiestamente públicos[271], supuesto que igualmente se recoge en el proyecto chileno[272], con la diferencia de que en nuestro caso se agrega la frase final "y su tratamiento esté relacionado con los fines para los cuales fueron publicados", lo que, para expertas como Matus, tiene una ligazón con el principio de finalidad[273].

Por su parte, en el marco de los deberes de información, quien trate los datos personales deberá informar la fuente de a partir de la cual se recopilaron los datos personales y, además, si se está en un supuesto de decisiones automatizadas que incluya la elaboración de perfiles[274]. Adicionalmente, se establecen correlaciones entre los derechos ARCO y las hipótesis de automatización y perfilamiento,

---

[270] **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS,** Considerando 15. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

[271] **REGLAMENTO (UE) 2016/679 Articulo 9 letra e)**

[272] **Artículo 16 Proyecto de Ley de Protección de Datos Chile**

[273] **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos, p. 108. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[274] **REGLAMENTO (UE) 2016/679 Artículo 14**

toda vez que los interesados tienen derecho a obtener del responsable una respuesta en torno a si se están tratando o sus datos, y la forma en que lo realiza. Lo mismo ocurre a propósito del derecho de portabilidad de datos provenientes del mismo contexto y el derecho de oposición a la elaboración de perfiles.

Hasta ahora, sin necesidad de excedernos en la revisión del RGPD, podemos constatar que el proyecto de Ley de Protección de Datos en Chile -latamente analizado en el capítulo anterior- recoge abiertamente la gran mayoría de disposiciones normativas de aquél, sin necesidad de que todos los alcances regulatorios sean reproducidos nuevamente. Sin embargo, eso no quiere decir que en Europa no se abra la discusión algunos artículos en particular.

En este sentido, resulta interesante la lectura que realiza del RGPD el académico finlandés Jukka Ruohonen, quien en un artículo publicado el presente año 2023 establece un nexo problemático entre los artículos 6, 9 y 22 del Reglamento, los cuales, desde su punto de vista requieren ser armonizados. En efecto, el artículo noveno -a propósito de los datos personales sensibles- señala que queda prohibido su tratamiento siempre y cuando no se esté en alguna de las hipótesis de excepción del inciso segundo. Así, en palabras del autor *"con respecto a la elaboración de perfiles políticos basados en fuentes públicas, como en los estudios académicos de informática señalados, una debilidad notable es la exención en el artículo 9 (2) (e) del RGPD*[275] *según el cual se permite el procesamiento en caso de que una persona haya hecho manifiestamente sus datos personales sensibles sean públicos. Los políticos y partidos políticos europeos también podrían tratar de justificar la elaboración de perfiles políticos sobre la base de que mantienen la democracia y tienen intereses legítimos con fines electorales, como se señala en el considerando 56 del RGPD, y luego utilizar la exención del RGPD en el artículo 9(2)(g)*[276] *sobre intereses públicos sustanciales como base jurídica junto con el artículo 6 (…)* "[277].

[275] **REGLAMENTO (UE) 2016/679 Art. 9.2.e)** Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: (…) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

[276] **REGLAMENTO (UE) 2016/679 Art. 9.2.g)** Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: (…) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado

[277] **RUOHONEN, JUKKA.** A Note on the Proposed Law for Improving the Transparency of Political Advertising in the European Union. *arXiv preprint arXiv:2303.02863*, 2023. P.8

En la misma línea, se explica la problemática asociada al 22 del RGPD puesto que regula expresamente las decisiones individuales automatizadas e incluye la elaboración de perfiles, disponiendo que "*todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar",* salvo que: sea necesaria para la ejecución de un contrato entre ambas partes; exista autorización por el Derecho de la Unión y se establezcan medidas adecuadas para salvaguardar sus derechos y libertades; o bien, que tenga por base el consentimiento explícito del interesado.

Además, el apartado cuarto del artículo 22 señala que si la decisión automatizada se basa en categorías especiales de datos personales que se contemplan en el artículo 9 del Reglamento (como información referida a ideología política), se requiere: o bien, el consentimiento expreso del titular, o que el tratamiento se base en razones de un interés público esencial, en ambos casos tomando las medidas adecuadas para salvaguardar los derechos, libertados e intereses legítimos del titular.

Para algunos académicos, la redacción -compuesta en su mayoría por conceptos jurídicos indeterminados-[278] no permite vislumbrar el verdadero alcance de la norma que está contenida en el artículo 22, existiendo ciertos problemas que son necesarios resolver doctrinariamente[279], ya que -a la fecha- no existen pronunciamientos del Tribunal de Justicia de la Unión Europea referidos al *microtargeting* electoral que permitan analizar el alcance de ciertas disposiciones normativas que podrían causas conflicto[280].

En primer lugar, para cierto sector de la doctrina genera poca seguridad jurídica que la oposición a las decisiones automatizadas y elaboración de perfiles se habilite siempre y cuando produzca efectos jurídicos o afecte significativamente al titular, toda vez que no se ofrece una ejemplificación de los casos de bajo y alto impacto que permita orientar en sus derechos al usuario[281]-[282].

---

[278] **PALMA ORTIGOSA, ADRIÁN**. Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. 2019. P.8

[279] **NIŠEVIĆ, MAJA, ET AL.** Understanding the legal bases for automated decision-making under the GDPR. En *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, 2022. p. 450

[280] **BRKAN, MAJA.** EU fundamental rights and democracy implications of data-driven political campaigns. *Maastricht Journal of European and Comparative Law*, 2020, vol. 27, no 6, p. 781

[281] **NIŠEVIĆ, MAJA, ET AL.** *Op. cit.* p. 451

[282] Una pequeña guía orientadora en este sentido podría ser el considerando 75 del RGPD que dispone "Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional,

En segundo lugar, no queda claro si el artículo 22, y particularmente su primer apartado, constituye un derecho para el titular de los datos personales o una prohibición para quien es el responsable del tratamiento. Si se mira como una prohibición, la lectura completa del artículo (incluyendo los apartados dos y tres), resulta más conveniente, ya que los responsables no podrían ejecutar decisiones automatizadas y elaboración de perfiles sin que exista una base legal, es decir, las excepciones que están contenidas en el primer apartado (un contrato; autorización del Estado miembro; o consentimiento explicito)[283].

Por último, se destaca el hecho de que el artículo 22 disponga que "todo interesado tendrá derecho a no ser objeto de una decisión basada **únicamente** en el tratamiento automatizado (el subrayado es nuestro)", lo cual abre la posibilidad a una defensa sustentable por los responsables del tratamiento de datos que podrían argumentar la intervención humana para que no les sea aplicable la comentada norma (aun cuando en la realidad material son los humanos quienes alimentan de datos a los sistemas dotados de IA y quienes delegan a ellas), o bien, que la decisión no fue completamente automatizada y, por lo tanto, los titulares de los datos personales nada pueden objetar[284]. Cabe destacar con respecto al último punto que, como se vio en el capitulo anterior, el legislador chileno prefirió seguir las recomendaciones de expertos que hicieron presente la problemática que surgió en el contexto europeo y eliminar la palabra "únicamente" para sortear futuras dificultades.

Con todo, aunque el RGPD constituya la piedra angular en materia de Protección de Datos de los ciudadanos de los Estados miembros de la UE y efectivamente regule el marco general respecto de las decisiones automatizadas y la elaboración de perfiles, lo cierto es que no regula de forma particular y pormenorizada el perfilado de carácter netamente ideológico, ni tampoco se refiere al rol que pueden

---

reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados"

[283] **NIŠEVIĆ, MAJA, ET AL.** *Op. cit.* p. 452

[284] **NIŠEVIĆ, MAJA, ET AL.** *Op. cit.* p. 453

jugar los partidos politicos como sujetos activos en la operación durante las campañas electorales, dejando encomendada la regulación al Derecho Interno de los países miembros[285].

Hernandez explica que *"el RGPD se encargó, principalmente, de lo referente a la exigencia de base jurídica para la recopilación y tratamiento, y de resolver ausencias normativas internas (...) Esto es así porque la definición de datos personales que recoge el RGPD —y que asume el legislador nacional— es amplia y con intención de omnicomprensividad. Abarca cualquier tipo de información que identifique o permita identificar a una persona física. El perfilado y la microsegmentación electoral encajan en esta definición, y alcanza también —al menos, desde nuestra opinión— la información inferida acerca de preferencias políticas recurriendo a técnicas de analítica avanzada (e. g., machine learning o deep learning). Además, esta actividad supone recopilación y tratamiento de datos de categorías especiales, por lo que se somete a cautelas y salvaguardas adicionales que reflejan un estándar de protección más elevado, ex art. 9 RGPD"*[286].

Aun cuando al momento de la entrada en vigencia del RGPD el propio Parlamento señalaba que este nuevo *legalis corpus* era suficiente para regular el tratamiento de datos personales en campañas electorales[287], desde algunos años la tónica regulatoria ha cambiado y, en un intento por nivelar la regulación de los países miembros en lo referido a la regulación de sistemas digitales el Parlamento Europeo ha ampliado su agenda legislativa, con importantes avances en la materia.

Los antecedentes que motivaron el impulso legislativo en comento se consignan en resoluciones dictadas por el Parlamento, que ponían el acento en las problemáticas asociadas a las nuevas tecnologías. Así, por ejemplo, el año 2017 se dictaba la Resolución 2016/2225 sobre las implicancias de los macrodatos en los derechos fundamentales, que para ese entonces reconocía el creciente número de empresas privadas abocadas al tratamiento de datos entre tantos otros fines, "(…) para influenciar las elecciones y los resultados políticos, por ejemplo, mediante comunicaciones específicas"[288]. Por otra parte, el 03 de mayo de 2022 se dictó una Resolución respecto la Inteligencia Artificial en la era digital

---

[285] **PEÑA, JUAN CARLOS HERNÁNDEZ**. Campañas electorales," big data" y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos. *Revista española de derecho constitucional*, 2022, vol. 42, no 124, p. 52

[286] *Ibid.*

[287] **ORIENTACIONES DE LA COMISIÓN RELATIVAS A LA APLICACIÓN DE LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EN EL CONTEXTO ELECTORAL.** COMISIÓN EUROPEA, 2018. Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52018DC0638

[288] Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley. Considerando f). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html

(como precedente de la ya comentada Propuesta de Reglamento de Inteligencia Artificial para la UE)[289], donde se expresaron los riesgos que representaba la IA como vehículo de desinformación; contaminación del debate político y herramienta de manipulación procesos democráticos[290].

Empero, en una faz mucho más vinculante y obligatoria en la regulación de medios digitales, con fecha 19 de octubre del año 2022 se publicó el Reglamento del Parlamento Europeo y del Consejo Relativo a un mercado único de servicios digitales[291] que tendrá plena vigencia el año 2024. Por otra parte, actualmente se discute la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la transparencia y la segmentación de la publicidad política, cuerpo legal de especial interés para esta memoria ya que, de aprobarse, constituirá un modelo que sin lugar a dudas será adoptado en otros territorios, tal como ocurrió con el RGPD.

En cuanto al Reglamento ya aprobado que regula los Servicios Digitales, son destacables dos considerandos que ponen énfasis en la problemática explorada en esta memoria, y que se citan enseguida:

- **Considerando 69**: *"Cuando se presentan a los destinatarios del servicio anuncios basados en técnicas de segmentación optimizadas para responder a sus intereses y apelar potencialmente a sus vulnerabilidades, los efectos negativos pueden ser especialmente graves. En algunos casos, las técnicas de manipulación pueden afectar negativamente a grupos enteros y amplificar perjuicios sociales, por ejemplo, contribuyendo a campañas de desinformación o discriminando a determinados grupos. Las plataformas en línea son entornos especialmente delicados para tales prácticas y plantean un riesgo mayor para la sociedad. Por consiguiente, los prestadores de plataformas en línea no deben presentar anuncios basados en la elaboración de perfiles como se definen en el artículo 4, punto 4, del Reglamento (UE) 2016/679, utilizando las categorías especiales de datos personales a que se refiere el artículo 9, apartado 1, de dicho Reglamento, ni utilizando categorías de elaboración de perfiles basadas en dichas categorías especiales. Esta prohibición se entiende sin perjuicio de las obligaciones aplicables a los prestadores de plataformas en línea o a cualquier otro prestador de servicios o*

[289] Véase, capitulo III

[290] **Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia De Inteligencia Artificial (Ley De Inteligencia Artificial).** Considerando 54 Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52021PC0206

[291] **Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales.** Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2065

anunciante que participen en la difusión de los anuncios en virtud del Derecho de la Unión en materia de protección de datos personales"[292].

- **Considerando 94:** *"Las obligaciones en materia de evaluación y reducción de riesgos deben desencadenar, en función de cada caso, la necesidad de que los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño evalúen y, en caso necesario, adapten el diseño de sus sistemas de recomendación, por ejemplo adoptando medidas para evitar o minimizar los sesgos que den lugar a la discriminación de personas en situaciones vulnerables, en particular cuando dicha adaptación sea conforme con el Derecho en materia de protección de datos y cuando la información esté personalizada sobre la base de categorías especiales de datos personales a que se refiere el artículo 9 del Reglamento (UE) 2016/679. Además, y como complemento de las obligaciones de transparencia aplicables a las plataformas en línea en lo que respecta a sus sistemas de recomendación, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben garantizar sistemáticamente que los destinatarios de su servicio disfruten de opciones alternativas que no se basen en la elaboración de perfiles, en el sentido del Reglamento (UE) 2016/679, para los parámetros principales de sus sistemas de recomendación. Estas opciones deben ser directamente accesibles desde la interfaz en línea en la que se presentan las recomendaciones"*[293].

Vale la pena decir que la importancia de ambos considerandos radica en que, por una parte, nuevamente existe un reconocimiento del órgano supranacional respecto de las potenciales amenazas que representa una incorrecta utilización de IA y del *big data* en la arena política, pudiendo distorsionar procesos en una clara vulneración de derechos fundamentales. Por otro lado, en un sentido más técnico y resolutivo, el considerando 94 mandata a los intermediarios -quienes ofrecen el medio para que las empresas de propaganda política-, a que adopten medidas de mitigación en la creación de sesgos que puedan derivarse de la elaboración de perfiles en base a datos personales sensibles, o especiales como señala el RGPD.

Sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la Transparencia y la segmentación de la publicidad política nos referiremos en el próximo acápite.

[292] **Reglamento (UE) 2022/2065** Considerando 69
[293] **Reglamento (UE) 2022/2065** Considerando 94

IV.2 Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la Transparencia y la Segmentación de la Publicidad Política

Con fecha 25 de noviembre del año 2021 la Comisión Europea, Dirección General de Justicia y Consumidores despachó la propuesta de Reglamento para regular la Transparencia y la Segmentación de la Publicidad Política con el objetivo de "contribuir al buen funcionamiento del mercado interior de la publicidad política mediante el establecimiento de normas armonizadas que garanticen un nivel elevado de transparencia de la publicidad política y los servicios conexos"[294], aplicándose tanto a los proveedores de servicios de publicidad políticas como a los demás responsables del tratamiento de datos personales en la cadena[295], lo cual ayuda a complementar el Reglamento de Servicios Digitales comentado líneas arriba[296]

El Parlamento reconoce que los cambios tecnológicos acelerados han agregado complejidad, y escasa posibilidad de vigilancia a los procesos electorales en los que operan sistemas de perfilamiento, y más aún, expone su preocupación en torno a la fragmentación regulatoria dentro de los países miembros, que no ofrece seguridad jurídica y que permite que los agentes económicos tratantes de datos personales en el contexto de periodos eleccionarios evadan la regulación aprovechándose de las lagunas de ejecución transfronteriza de los servicios, sobre todo si consideramos que estos podrían operar fuera del Estado en que se llevaron a cabo elecciones[297].

Se resalta además que regular el tópico es un imperativo que deriva, por una parte, de la Carta de los Derechos Fundamentales de la Unión Europea, toda vez que el artículo 8 consagra el derecho a la protección de datos personales, lo que en caso alguno implica una ponderación de derechos como el referido a la libertad de expresión -como han explorado algunos autores-[298], ya que normar el *microtargeting electoral* implica reglamentar la forma en que se hacen llegar mensajes al electorado y no el contenido del mensaje propiamente tal[299]. Por otro parte, se recuerda que la germanización de la

---

[294] **Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la Transparencia y la Segmentación de la Publicidad Política COM/2021/731 final.** Disponible: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0731 P.1

[295] *Ibid. p. 4*

[296] *Ibid.*

[297] *Ibid. p. 3 y 4*

[298] **CIANCI, LICIA; ZECCA, DAVIDE.** Polluting the Political Discourse: What Remedies to Political Microtargeting and Disinformation in the European Constitutional Framework?. *European Journal of Comparative Law and Governance*, 2023, vol. 1, no aop, p. 12-13

[299] **Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la Transparencia y la Segmentación de la Publicidad Política COM/2021/731 final.** Disponible: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0731 P.13

transparencia es un objetivo público legítimo que deriva de los valores compartidos por los Estados miembros de la UE, como queda reflejado en el artículo 2 del Tratado de la Unión Europea[300].

En concreto, dentro de las principales innovaciones que constan en la propuesta, podemos señalar las siguientes:

- **Consagra definiciones atingentes en la materia**[301]: En efecto, en el artículo 2 se ofrecen ciertos conceptos -dentro de los cuales destacamos el de publicidad política definida como "la preparación, inserción, promoción, publicación o difusión, por cualquier medio, de un mensaje: a)por un actor por un actor político, en su nombre o por su cuenta, a menos que sea de carácter estrictamente privado o estrictamente comercial; o b) que pueda influir en el resultado de una elección o referéndum, en un proceso legislativo o reglamentario o en el comportamiento electoral". Por otra parte, se señala que el concepto de "actor político" no solo engloba a los partidos politicos, sino que a organizaciones de campaña política con o sin fines de lucro, siéndoles aplicables el reglamento. Por último, cabe mencionar que igualmente se define lo que constituyen técnicas de segmentación o amplificación como "técnicas que se utilizan para dirigir un anuncio político personalizado únicamente a una persona o grupo de personas específicos o para aumentar la circulación, el alcance o la visibilidad de un anuncio político".

  En cualquier caso, es necesario mencionar que para ciertos autores como Ruohonen, es esperable que se incluya una referencia expresa a los ciudadanos que voluntariamente realizan esparcimiento de publicidad política, toda vez que pareciera que las hipótesis contempladas en la propuesta están vinculadas únicamente a relaciones comerciales onerosas[302].

- **Limita el Derecho Interno de los Estados miembros**: Para asegurar un nivel de armonización adecuado, el artículo 3 dispone que "Los Estados miembros no mantendrán ni introducirán, por motivos de transparencia, disposiciones o medidas que difieran de las establecidas en el presente Reglamento".

- **Consagra obligaciones de transparencias aplicables a los servicios de publicidad política:** En cuanto a este punto regulado en el capítulo segundo de la propuesta, es posible opinar que resulta ser uno de los enclaves de control más importantes del proyecto, ya

[300] Ibid.
[301] Una pequeña critica respecto de ciertas definiciones puede ser revisada en **NME NEWS MEDIA EUROPE** Posición sobre la Comisión Europea Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre Transparencia y Focalización de la Publicidad Política. 2022. Disponible en: https://ec.europa.eu/ info/law/better-regulation/have-your-say/initiatives/12826-Politicaladvertisingimproving-transparency/F2820204 es)
[302] **RUOHONEN, JUKKA.** *Op cit.* p.6

que obliga a los proveedores de servicios publicitarios, por una parte, a que declaren expresamente si aquellos son de corte político y, además, a que en el contenido del contrato se estipule la manera en que se dará cumplimiento a las disposiciones del Reglamento. Enseguida, el artículo sexto mandata que los proveedores conserven por cinco años los anuncios politicos creados; la especificación de los servicios prestados; los importes facturados y la identidad de quien los solicitó.

Los artículos siguientes se refieren a los requisitos de transparencia de cada anuncio político (declarar que se trata de un anuncio político, la identidad de quien patrocina y el contexto del anuncio); la obligación de que editores de publicidad política dejen registro anual de los importes de las prestaciones y el poder conferido a las autoridades para solicitar a los servicios de publicidad la información transmitida.

- **Agrega un capitulo referido especialmente a la segmentación y amplificación de la publicidad política**: Estableciendo un reenvío al RGPD, el artículo 12 dispone expresamente que se prohíben las técnicas de segmentación y amplificación donde se involucre la categoría de datos referidos en el artículo 9 del Reglamento General de Protección de datos[303], como aquellos referidos a opiniones políticas.

Sin embargo, se establece una excepción a la prohibición del *microtargeting*, en aquellos casos en que el tratamiento de datos personales sensibles se haga con consentimiento del titular (artículo 9.2.a del RGPD) o bien, el tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro (artículo 9.2.d del RGPD).

En este caso, se vuelve al mismo problema que mencionamos al inicio de este capítulo, esto es, la posibilidad de que los partidos politicos se excusen en conceptos jurídicos indeterminados como “actividades legítimas” y “debidas garantías”, que podrían aducir como finalidad los partidos politicos para exonerarse de responsabilidad, aún cuando el apartado tercero del artículo 12 de la propuesta en cuestión ordene que los tratantes cuenten con registros

[303] **REGLAMENTO (UE) 2016/679 Artículo 9.1**: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

de las labores de segmentación y adopten políticas internas de resguardo, facilitando el acceso de los titulares.[304]

- **Se establecen mecanismos de fiscalización y sanción por incumplimiento del Reglamento:** En cuanto a los órganos encargados de supervigilar, el artículo 15 apartado segundo menciona que cada Estado miembro designará aquellos que serán competentes en su territorio. Además, en cuanto la batería de sanciones igualmente corresponderá a cada país perteneciente a la UE, donde se incluyen multas administrativas y pecuniarias.

Como ha sido posible apreciar, al menos a nivel europeo, el órgano supranacional ha demostrado materialmente a través del proyecto en comento que existe voluntad política para regular la publicidad política en todas sus formas, estableciendo un estándar armónico que le sea aplicable a los países miembros de la UE. Sin embargo, cabe mencionar que, respecto de ciertos puntos en particular, la institucionalidad no está conteste.

A mayor abundamiento, el Supervisor Europeo de Protección de Datos (SEPD), Wojciech Wiewiórowski, a comienzos del año 2022 emitió una opinión formal respecto a la propuesta que debate el Parlamento Europeo, expresando su preocupación -entre muchos otros- respecto a las excepciones que se consagran respecto al *microtargeting* en el artículo 12 del proyecto, en los siguientes términos:

> *"(...) El SEPD está convencido de que deben reforzarse aún más las garantías de la Propuesta con respecto al tratamiento de datos personales en el contexto de la publicidad política y, en particular, el uso de técnicas de focalización y amplificación. Con este fin, el SEPD recomienda:*
>
> *1) Disponer una prohibición total de la microfocalización con fines políticos, es decir, seleccionar los mensajes y/o la audiencia prevista de la publicidad política de acuerdo con las características percibidas, los intereses o las preferencias de las personas en cuestión; y*
>
> *2) Introducir más restricciones de las categorías de datos que pueden procesarse con fines de publicidad política, incluida la orientación y la amplificación, en particular prohibiendo la publicidad dirigida basada en el seguimiento generalizado, es decir, el procesamiento de información sobre el comportamiento de una persona en sitios web y servicios. con vistas a la publicidad dirigida sobre la base de perfiles".*[305]

Así las cosas, quedará pendiente y sujeto a modificación por el Parlamento si es que se toman en consideración los consejos del SEPD, marcando un hito que sería aún más estrictos y que podría

---

[304] **RUOHONEN, JUKKA.** *Op cit.* p.8

[305] **EUROPEAN DATA PROTECTION SUPERVISOR.** Opinion 2/2022 on the Proposal for Regulation on the transparency and targeting of political advertising. P.10 Disponible en: https://edps.europa.eu/system/files/2022-01/edps_opinion_political_ads_en.pdf

cambiar todo el estado del arte actual, borrando por completo la posibilidad de que se realicen operaciones de *microtargeting* por parte de agentes responsables del tratamiento de datos personales que presten servicios de publicidad política y elaboración de perfiles, reduciendo todo riesgo de que puedan suscitarse nuevos casos de gran impacto como el de Cambridge Analytica, en un entorno desregulado. Eso sí, a juicio de quien les escribe, si es que se produce un avance en la prohibición, solo será factible si se cuenta con los recursos necesarios para fiscalizar el mercado publicitario de forma integral, sin que existan incentivos para operar desde las sombras.

IV.3 España y el pronunciamiento del Tribunal Constitucional Español respecto al *microtargeting* electoral

Para finalizar el estudio del estado normativo y académico en el Derecho Comparado, hemos seleccionado a España como objeto de analisis. El fundamento de la elección radica en que, en primer lugar, su Ley de Protección de Datos nacional, fue uno de los modelos a seguir en la tramitación del proyecto de Ley de reforma en Chile[306]. En segundo lugar, en el contexto de la proliferación de contrataciones de servicios de *microtargeting* electoral y analisis de datos por parte de los partidos politicos españoles[307]-[308], su Agencia de Protección de Datos ha emitido resoluciones frente a los hechos e, incluso -en cuanto a su Ley de Protección de Datos- el Tribunal Constitucional español ha tenido la posibilidad de pronunciarse particularmente al respecto de las disposiciones normativas que guardan relación con los partidos politicos.

Expuestas las razones se procederá, en primer lugar, a analizar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD-GDD), particularmente en lo referido a la utilización de datos personales sensibles por partidos politicos. Enseguida, se revisará el paradigmático fallo del Tribunal Constitucional Español que se pronuncia acerca del artículo 58 bis. N°1 de la Ley de Protección de Datos.

---

[306] Véase, **INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES**. Boletines N°s 11.144-07 y 11.092-07, refundidos. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

[307] **RODRÍGUEZ, AITOR FERNÁNDEZ; ARAMBURU, DAVID VARONA**. Elecciones 2021 en la Comunidad de Madrid: Movilización del votante de partidos de izquierdas en Telegram. *[RMd] RevistaMultidisciplinar*, 2023, vol. 5, no 2, p. 57-77.

[308] **BAVIERA, TOMÁS; CANO-ORÓN, LORENA; CALVO, DAFNE.** Tailored messages in the feed? Political microtargeting on Facebook during the 2019 General Elections in Spain. *Journal of Political Marketing*, 2023, p. 1-20.

La LOPD-GDD del año 2018 es una ley aprobada por las Cortes Generales de España, cuyo objeto principal fue adecuar la normativa vigente en aquella época al Reglamento General de Protección de Datos del Parlamento Europeo[309], permitiendo la operatividad complementaria de ambas, toda vez que en palabras del Tribunal Constitucional español "configuran conjuntamente, de forma directa o supletoria, el desarrollo fundamental a la protección de datos que exigen los artículos 18.4 y 81.1 de la Constitución española"[310].

Sin embargo, llama la atención la técnica legislativa utilizada, toda vez que a pesar de la vocación reformista de la LOPD-GDD - tal como queda de manifiesto si se analizan los considerandos preliminares que sirven como guía orientadora para entender las razones de la reforma- lo cierto es que no derogó cada aspecto de la Ley Orgánica 15/1999 de Protección de Datos Personales, ya que aun se encuentran vigentes para regular algunos aspectos, aunque menores[311]-[312]. Por otra parte, cabe mencionar que, naturalmente, se constatan una gran cantidad de reenvíos al RGPD en materias ya estudiadas a lo largo de esta investigación.

Así, por ejemplo, respecto de las categorías especiales de datos reguladas en el artículo 9 de la LOPD-GDD, se señala que *"a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico",* cambiando el criticado enfoque que fue revisado a propósito de la habilitación de tratamiento

---

[309] **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS,** Considerando 10. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

[310] **PEÑA, JUAN CARLOS HERNÁNDEZ**. Campañas electorales," big data" y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos. *Revista española de derecho constitucional*, 2022, vol. 42, no 124 p.51

[311] **Disposición adicional decimocuarta de la LOPD-GDD.** Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE. Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas

[312] **Disposición transitoria cuarta**. Tratamientos sometidos a la Directiva (UE) 2016/680.- Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva. y modifica toda una serie de legislación especial conexa con la materia.

de datos sensibles contenida en el artículo 9.2.a) del RGPD, basado en el consentimiento del titular de los datos. Para algunos autores, esta exclusión podría estar justificada en la dificultad inherente de probar si es que efectivamente se ha otorgado consentimiento en atención al artículo 7 del RGPD y las dificultades que podrían tener que soportar los titulares de datos personales[313].

Sin embargo, se establece enseguida que las demás hipótesis reguladas en el artículo 9.2 del Reglamento de la UE si son aplicables, y, por lo tanto, la responsable del tratamiento de datos personales podría excusarse en una de aquellas, como, por ejemplo, el caso de que el interesado haya hecho manifiestamente públicos los datos personales sensibles[314], o bien, que exista una razón de interés público esencial siempre y cuando se adopten garantías adecuadas para proteger los derechos fundamentales del interesado [315] . Nuevamente, la controversia relativa a estos conceptos jurídicos indeterminados contenidos en el artículo 9.2 letra g) del RGPD tiene lugar, pero ahora en España.

En efecto, como bien explica Hernández "el interés público al que hace referencia ha de conectarse con la previsión del considerando 56 del propio Reglamento, esto es, el funcionamiento del Estado democrático puede exigir que se recopilen y traten datos relacionados con opiniones políticas, aunque sujetos a restricciones y salvaguardas. Lo dicho exige, por una parte, la mediación de una norma jurídica que concrete las circunstancias y justificaciones del interés público (…) Por otra, que esa norma determine, con garantías adecuadas y suficientes, el marco en el que se podría realizar el tratamiento. Entre otros aspectos, la justificación del tratamiento excepcional, el arco temporal en que se admite, los sujetos autorizados y posibles límites"[316].

Ahora bien, la crítica precedente es más bien coetánea a nuestros tiempos, ya que al momento de promulgarse la LOPD-GDD el año 2018, se incluyó la disposición final tercera, que ordenaba la modificación de la Ley Orgánica 5/1985 referida al Régimen Electoral General añadiendo el artículo 58 bis. en los siguientes términos:

Artículo 58 bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.*

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

---

[313] **PEÑA, JUAN CARLOS HERNÁNDEZ.** *Op. cit.* p.54
[314] Supuesto contenido en el artículo 9.2.e) del **REGLAMENTO (UE) 2016/679**
[315] Supuesto contenido en el artículo 9.2.g) del **REGLAMENTO (UE) 2016/679**
[316] **PEÑA, JUAN CARLOS HERNÁNDEZ.** *Op. cit.* p.54

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

Vale decir, que se permitía a los partidos politicos de forma expresa excusarse en el tratamiento de datos personales sensibles demostrando que tenían un interés público, aun cuando no se diera una explicación sustancial del concepto, más allá de lo dispuesto en el considerando 56 del RGPD.

En atención a los riesgos que representaba una interpretación laxa y permisiva del artículo 58 bis, la Agencia Española de Protección de Datos dictó la circular 1/2019 con fecha 07 de marzo, referida al "tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General"[317].

En dicha circular se expresó que *"el interés público actuaría como fundamento, pero también como límite. Por tanto, la aplicación del mismo debe interpretarse siempre en el sentido más favorable a la consecución de dicho interés público, por lo que en ningún caso podrá amparar tratamientos, como el microtargeting, que puedan ser contrarios a los principios de transparencia y libre participación que caracterizan a un sistema democrático"*[318], siempre en atención a los derechos fundamentales referidos a la libertad ideológica, la libertad de expresión e información y a la participación política positivizados en la Constitución Española.

De esta manera, la Agencia de Protección de Datos Española en atención a sus facultades regulatorias en virtud del artículo 55 de la LOPD-GDD, decidió fijar criterios expresos a los que respondería el órgano en todos aquellos casos que tuviese que conocer en relación a los alcances del

---

[317] **Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General**. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-11672

[318] **Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.** p.2 Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-3423

artículo 58 bis incluido en la Ley Orgánica 5/1985 del Régimen Electoral General[319]. En síntesis, la circular 1/2019 dispuso que:

- El tratamiento de datos personales referidas a opiniones políticas por los partidos politicos conforme a lo dispuesto en el artículo 58 bis de la Ley Orgánica del Régimen Electoral General es dable si concurre un interés público esencial y se ofrecen conforme al comentado artículo 9.2 letra g) del RGPD. Empero, es la Agencia la que por medio de la circular establece cuales son las garantías adecuadas que se deben satisfacer para proteger los derechos fundamentales del titular de los datos, como una forma de otorgar certeza jurídica. [320]
- El tratamiento de datos personales sensibles de corte político solo es licito durante el periodo electoral y respecto de actividades de propaganda y actos de campaña electoral[321].
- Los datos personales sensibles referidos a la ideología de sus titulares tienen como base de licitud en cuanto a su tratamiento el hecho de haber sido dados a conocer públicamente por aquellos y fuentes de acceso público, prohibiéndose expresamente utilizar tecnologías dotadas de Inteligencia Artificial para "llegar a inferir la ideología política de una persona"[322]
- Queda excluido del tratamiento a realizar la preparación de perfiles individuales demasiado específicos, admitiéndose únicamente aquellos de corte general.
- En el caso de que se viole la seguridad de los datos personales sensibles referidos a opiniones políticas, los responsables deben dar conocimiento a la Agencia de inmediato, al igual que a los afectados[323].
- La mensajería de propaganda política no tiene el carácter de comunicación comercial[324]
- En todos estos casos, se debe abrir la posibilidad de forma expedita de que los titulares ejerzan sus derechos ARCO.
- Por último, ponemos el acento en la complementación que se realiza en favor del artículo 9.2 letra g) que hace reenvío al artículo 9 de la LOPD-GDD. Esto ya que la Agencia

[319] **RAMÓN FERNÁNDEZ, F.:** Microtargeting, transparencia, datos y propiedad intelectual. Una reflexión sobre los nuevos retos de la inteligencia artificial, Tirant lo Blanch, Valencia, 2021
[320] **Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos.** Articulo 3
[321] *Ibid.* Articulo 4
[322] *Ibid.* Articulo 5
[323] *Ibid.* Articulo 10
[324] *Ibid.* Articulo 11

Española de Protección de datos establece que son garantías adecuadas para proteger los interés y derechos fundamentales de los afectados por el tratamiento[325]:

Artículo 7. Garantías adecuadas.

1. Conforme a lo previsto en el artículo 9.2.g) del RGPD tendrán la consideración de medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados, en todo caso, las siguientes, sin perjuicio de cualquier otra que estime el responsable del tratamiento y las que puedan exigir otros órganos en el ámbito de sus competencias:

- *1.º Atendiendo al principio de responsabilidad desde el diseño y por defecto previsto en el artículo 25 del RGPD, deberán adoptarse, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, e incluso la agregación y anonimización. Además, deberá garantizarse que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento y que no serán accesibles, sin intervención de la persona, a un número indeterminado de personas.*
- *2.º Será obligatorio designar a un delegado de protección de datos conforme a lo previsto en el artículo 37.1.c) del RGPD, al realizarse un tratamiento a gran escala de categorías especiales de datos personales. El delegado de protección de datos desempeñará las funciones que le atribuyen el artículo 39 del RGPD y los artículos 36 y 37 de la LOPDPGDD con especial diligencia atendiendo al alto riesgo asociado a estos tratamientos.*
- *3.º Deberá llevarse un registro de las actividades de tratamiento con el contenido señalado en el artículo 30 del RGPD, debiendo ser precisos y claros, conforme a los principios de lealtad y transparencia, en la descripción de los fines del tratamiento, y de las categorías de interesados y de datos personales objeto de tratamiento. La llevanza de dicho registro resultará en todo caso obligatoria al incluir categorías especiales de datos personales del artículo 9.*
- *4.º Se deberá realizar una evaluación de impacto relativa a la protección de datos al realizarse un tratamiento a gran escala de las categorías especiales de datos conforme a lo dispuesto en el artículo 35.3 del RGPD.*
- *5.º Deberá consultarse a la AEPD antes de proceder al tratamiento conforme al artículo 36.1 del RGPD al tratarse de tratamientos que entrañan un alto riesgo, a no ser que el responsable justifique la adopción de medidas para mitigarlo. En este último caso deberá remitirse a la AEPD el análisis de riesgos y la evaluación de impacto junto a la justificación de las medidas adoptadas, al amparo de lo previsto en el artículo 58.1. a) y e) del RGPD. La solicitud de consulta a la AEPD o, en su defecto, la remisión de la documentación anteriormente indicada deberá realizarse al menos 14 semanas antes del inicio del periodo electoral.*

[325] **Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos.** Articulo 7

- *6.º Deberán adoptarse las medidas de seguridad necesarias conforme a lo previsto en el artículo 32 del RGPD, que deberán ser lo más rigurosas que permita el estado de la técnica teniendo en cuenta que se están tratando datos referentes a las opiniones políticas cuyo tratamiento es excepcional y que suponen un alto riesgo para los derechos y libertades de las personas físicas.*
- *7.º Cuando el tratamiento se vaya a realizar por un encargado del tratamiento, deberá seleccionarse uno que ofrezca garantías suficientes y haberse suscrito un contrato con el contenido del artículo 28 del RGPD, en el que deberá quedar plenamente garantizado que el encargado actuará solo siguiendo instrucciones del responsable, debiendo dichas instrucciones contemplar todas las garantías adecuadas a las que se hace referencia en la presente circular.*
- *8.º Deberá facilitarse, de un modo sencillo y gratuito, el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, conforme a lo previsto en el artículo 12 del RGPD y, en cuanto al derecho de oposición, conforme a lo previsto en el apartado 5 del artículo 58 bis de la LOREG.*
- *9.º En el caso de que se pretenda obtener los datos de terceros que no actúen como encargados del tratamiento, el responsable deberá comprobar que dichos datos fueron obtenidos de manera lícita y cumpliendo con todos los requisitos del RGPD, especialmente que el tercero tiene una legitimación específica para obtener y tratar dichos datos y que ha informado expresamente a los afectados de la finalidad de cesión a los partidos políticos, cumpliendo de este modo con el principio general de responsabilidad proactiva consagrado en el artículo 5.2 del RGPD, y singularmente para actuar conforme a lo previsto en sus artículos 24 y 25.*
- *10.º El responsable deberá cumplir con lo dispuesto en el artículo 22 del RGPD si los afectados van a ser objeto de decisiones automatizadas, incluida la elaboración de perfiles, siempre que el tipo de tratamiento que prevea, por sus características y teniendo en cuenta de nuevo la naturaleza de los datos tratados, pueda afectar significativamente a los ciudadanos.*

2. El responsable del tratamiento y, en su caso, el encargado, deberán ser capaces de acreditar documentalmente la adopción de las anteriores garantías.

Sin embargo, la controversia en torno al artículo 58 bis no quedó ahí y la amplitud con la que fue redacta dicha disposición normativa permitiendo que los partidos politicos pudiesen tratar datos personales sensibles referidos a la ideología de los titulares no pudo ser morigerada ni siquiera por la circular dictada por la Agencia Española, que pretendía dar certeza jurídica al artículo 58 bis con la extensa lista de garantías expuesta precedentemente.

A mayor abundamiento, el año 2019 se interpuso un recurso de inconstitucionalidad contra el artículo 58 bis numeral 1 de la Ley Orgánica del Régimen Electoral General, incorporada en este cuerpo normativo en virtud de la disposición final tercera de la LOPD-GDD. El sujeto activo que promovió la

acción constitucional fue el Defensor del Pueblo, fundamentando que existe una clara vulneración a los derechos fundamentales contenidos en la Constitución Española referidos a la protección de datos personales y la libertad ideológica[326]. Además, apunta a la desfavorable situación en que quedan los titulares de datos personales si se persiste en la vigencia de hipótesis habilitantes del tratamiento de datos personales sensibles en circunstancias que dependen de la concurrencia de requisitos no definidos de forma clara como los ya comentados "intereses públicos" y las "garantías adecuadas"[327].

Tales argumentos fueron acogidos por el Tribunal Constitucional Español, que con fecha 22 de mayo de 2019 dictó sentencia declarando -con unanimidad del pleno- la inconstitucionalidad del apartado primero del artículo 58 bis. Como acertadamente apunta Francisca Ramón[328], los considerando diez de la sentencia resulta ser en extremo ilustrativo para entender la decisión del tribunal, ya que en este se señala:

> **Considerando 10** *"La declaración de inconstitucionalidad y nulidad se basa, como se ha dicho en el fundamento jurídico anterior, en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el artículo 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear. Por lo que, en coherencia con este fundamento, y con plena coincidencia con el suplico del recurso de inconstitucionalidad, la declaración de inconstitucionalidad y nulidad debe extenderse a la totalidad del apartado 1 del artículo 58 bis LOREG, incorporado a esta por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales"*[329].

Finalizando la revisión del panorama legal español en lo referido al tratamiento de datos personales sensibles que pueden ser utilizados por los actores politicos en el marco de campañas electorales, debemos concluir que si bien es cierto que la LOPD-GDD como estatuto de Derecho Interno presenta ciertas mejoras, como por ejemplo, la exclusión del consentimiento como base de legitimación

---

[326] **Sentencia 76/2019, de 22 de mayo de 2019. Recurso de inconstitucionalidad 1405-2019.** Tribunal Constitucional Español. Disponible en: https://boe.es/diario_boe/txt.php?id=BOE-A-2019-9548

[327] *Ibid.*

[328] **RAMÓN FERNÁNDEZ, F.:** Microtargeting, transparencia, datos y propiedad intelectual. Una reflexión sobre los nuevos retos de la inteligencia artificial, Tirant lo Blanch, Valencia, 2021

[329] **Sentencia 76/2019, de 22 de mayo de 2019. Recurso de inconstitucionalidad 1405-2019.** Tribunal Constitucional Español. Disponible en: https://boe.es/diario_boe/txt.php?id=BOE-A-2019-9548

en aquellos tratamientos que tienen por principal finalidad identificar -entre muchos aspectos- la ideología política conforme al artículo 9.1 de la LOPD-GDD, lo cierto es que *"Ni el legislador europeo, ni tampoco el nacional, han afrontado el tratamiento de las categorías especiales con el debido nivel de detalle. En efecto, estando previstas en el art. 9.2 RGPD las circunstancias en que los datos especiales pueden tratarse —existencia de base de legitimación para ello mediante—, sin embargo, no se han regulado las garantías específicas que demanda el contenido esencial del derecho. Como puede constatarse, no todos los tratamientos en los que se utilizan datos de las categorías especiales cuentan con una ley sectorial que los regule y, menos aún, que incorpore garantías específicas. Por otra parte, las leyes existentes se limitan a hacer referencias generales a la necesidad de observancia de la normativa de protección de datos, sin establecer mayores cautelas o precisiones (...)"* como apunta Jove[330].

Por lo mismo, será necesario estar atentos al desarrollo legislativo de las propuestas que alcanzan a todos los países miembros de la Unión Europea, dentro de los cuales destaca el Reglamento sobre Transparencia y la Segmentación de la Publicidad Política, máxime si recordamos que -en dicha discusión legislativa- no se ha zanjado aquello que ha hecho presente el Supervisor Europeo de Datos Personales Señor Wojciech Wiewiórowski, esto es, avanzar hacia una prohibición completa del *microtargeting* electoral en razón del ulterior fin de manipulación ciudadana que engloba la práctica. En un supuesto así de tajante, corresponderá analizar cual sería el tratamiento de datos personales sensibles que podrían lícitamente llevar a cabo los partidos politicos de los distintos Estados parte de la UE y, más aún, con que fines sería permitido.

[330] **VILLARES, DANIEL JOVE**. La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de Mayo. *Revista Española de Derecho Constitucional*, 2021, no 121, P 327-328

V. CONCLUSIONES

La presente investigación, como fue señalado a un comienzo, tenía por objetivo general dar a conocer el estado del arte en términos doctrinarios y normativos en todo aquello referido a la utilización de datos personales e Inteligencia Artificial en el contexto de campañas electorales.

Tomando esto como base, hemos podido analizar -a la luz de la literatura especializada- cuales son los elementos que definen por esencia al *microtargeting* electoral, dejando constancia, por una parte, que su existencia y utilización es efectiva, existiendo numerosos ejemplos en que partidos politicos han contratado a experimentados responsables de tratamiento de datos personales. Por otra parte, ha sido posible recabar y contrastar los principales argumentos referidos, en específico, a la probabilidad de que la microfocalización del electorado tenga un impacto certero en la distribución de votos y, en definitiva, la elección de un candidato u opción. Respecto a este punto, nos permitimos concluir que ninguna investigación a la fecha ha podido demostrar fehacientemente que aquello ocurra, comprobándose el riesgo mas no un daño con resultado concreto.

Sin perjuicio de lo anterior, es posible constatar que el debate se traslada -acertadamente- a los conflictos ético-politicos que se suscitan en torno al tópico, más allá de su efectividad, esto es, cuáles son los limites aceptables dentro de los cuales los partidos politicos y otros actores relevantes de la vida publica pueden hacer uso de herramientas que manejan tales volúmenes de información que se componen de datos personales sensibles. A juicio de quien les escribe, es el acelerado dinamismo propio de la revolución tecnológica el contexto que permite al legislador prescindir de pruebas concretas referidos a la eficiencia sustancial del *microtargeting* y, por el contrario, lo motiva a regular la materia en concreto y todos los fenómenos auxiliares que le rodean.

En cuanto al examen normativo de la Protección de Datos circunscrita al ordenamiento jurídico nacional podemos señalar lo siguiente. En primer lugar, la vigente Ley N°19.628 sobre Protección de la Vida Privada, es lisa y llanamente insuficiente para garantizar efectivamente el derecho fundamental a la Protección de Datos que se consagra en el artículo 19 N°4 de nuestra Constitución Política de la República. Lo anterior, desde nuestro punto de vista, se debe al enfoque comercial que le dio el poder legislativo al cuerpo legal, estableciendo hipótesis de transferencia de datos personales y relegando a un segundo plano los mecanismos que permitirían efectivamente proteger los datos de la sociedad, sin siquiera contar con un ente fiscalizador *ad hoc.*

Sin embargo, se evidenció que – en un claro intento por superar dichas dificultades- el Legislador desde los últimos 10 años ha presentado diversos proyectos de Ley que -de aprobarse- permitirán que Chile se acerque a los parámetros OCDE en lo referido a protección de datos y, por otra parte, siente las

bases para que las empresas de propaganda política operen en nuestro país sujetas a un estatuto mucho más rico jurídicamente.

Dentro de los proyectos revisados, destaca por supuesto aquel que Regula la Protección y el Tratamiento de los Datos Personales y crea la Agencia de Protección de Datos Personales, que incluye -como su nombre indica- la creación de un órgano fiscalizador adecuado; consagra los denominados derechos ARCO que permiten amparar de manera efectiva a los titulares de datos personales y establece procedimientos expeditos en conjunto con una batería de sanciones en el caso de que se infrinja el cuerpo legal. Todo lo anterior, sin considerar que igualmente se consignó la tramitación de proyectos de Ley que regulan proliferación de las noticias falsas y la Inteligencia Artificial, pilares fundamentales para llevar a cabo servicios de microsegmentación.

El balance que hacemos respecto al ordenamiento jurídico chileno y los proyectos de reforma nos permite concluir lo urgente que amerita ser aprobado el nuevo marco normativo, el cual se encuentra finalizando su tramitación legislativa. De entrar en vigor, la protección que se otorgaría a los ciudadanos en materia de datos será sustancialmente más completa, ofreciendo un marco jurídico amplio que regula de forma expresa la automatización de decisiones y la elaboración de perfiles, en atención a los derechos de acceso, rectificación, oposición, supresión, portabilidad y bloqueo, ya revisados pormenorizadamente.

Ahora bien, aun cuando podrían esgrimirse ciertas criticas respecto a las bases de licitud comentadas a propósito del artículo 16 del proyecto, esto es, los casos en que se autoriza el tratamiento de datos personales sensibles (como aquellos referidos a la ideología política), debido a la excesiva inclusión de conceptos jurídicos indeterminados que hacen cuestionar su redacción, lo cierto es que – a nuestro juicio- existe un balance positivo del proyecto. Esto, ya que la creación de un órgano como la Agencia de Protección de Datos, con las facultades que le confiere el proyecto, permitirá, por un lado, que sean denunciables efectivamente las transgresiones a la Ley ante un ente especializado. Por otro lado, permitirá que de forma expedita se dicten circulares informativas; se interpreten los cuerpos legales a través de resoluciones y se sienten bases jurisprudenciales que permitan examinar de forma correcta las disposiciones normativas, tal como ocurre en Europa.

Por último, con respecto a las indagaciones efectuadas sobre el escenario comparado, podemos concluir que efectivamente Chile ha utilizado como parámetro el Reglamento General de Protección de Datos Europeo y las leyes de Derecho Interno de los países miembros de la unión y, más aún, en el debate legislativo se pulieron ciertos aspectos no contemplados internacionalmente, referidos a la automatización de decisiones. Consecuencialmente, se pudo constatar que, si bien el estado del arte está mucho más avanzado y las regulaciones son de larga data, igualmente se suscitan problemáticas referidas

a los alcances de las disposiciones normativas de sus respectivos Reglamentos y Leyes, como ocurre a propósito del comentado artículo 58 bis de la Ley de Protección de Datos Personales española y las bases de licitud para tratar datos personales sensibles.

Empero, innovadores proyectos como el de Transparencia y la Segmentación de la Publicidad Política vienen a regular de manera especifica y supletoria toda deficiencia que pueda existir en cuanto al *microtargeting* electoral y el envío de propaganda política a través de medios digitales por parte de los partidos politicos europeos; sin olvidar que importantes figuras como el Supervisor Europeo de Datos Personales en una vereda mucho más restrictiva quieren prohibir de forma absoluta este tipo de prácticas.

Redondeando las ideas, para el autor de la presente memoria, será necesario -desde luego- que la doctrina y jurisprudencia nacional tome en consideración los casos planteados en el escenario comparado, adoptando un enfoque moderado frente a los mismos. En este sentido, se adopta una posición pro regulatoria que no implique una prohibición total del *microtargeting* electoral como propone el SEPD, toda vez que los riesgos del surgimiento de un mercado negro de datos sensibles son altamente probables. Resulta más conveniente, por lo mismo, que se desarrollen de forma detallada los supuestos e hipótesis habilitantes para que se proceda a la elaboración de perfiles con fines electorales, siempre desde una perspectiva de protección a los ciudadanos y la faz más intima de su vida privada.

La importancia del planteamiento precedente radica en que no solo existe un derecho fundamental involucrado (de protección de datos), sino que concurren varios otros como el de libertad ideológica y de pensamiento. Estos nos permiten en una faz activa manifestar voluntariamente nuestras creencias y, a *contrario sensu*, guardar reserva respecto de las mismas a nuestro propio arbitrio, sin que se permita la coacción de ningún sujeto u órgano para darlos a conocer. Por lo tanto, resulta previsible que los partidos politicos quieran hacer uso de las nuevas tecnologías para comunicarse con su electorado, sobre todo si consideramos que la tecnología de la información redefinió la manera en que nos comunicamos.

Sin embargo, como quedó patente en esta memoria, los esfuerzos deben estar puestos en delimitar la practica a dicha comunicación digital, fiscalizando energéticamente que no se abran las puertas a modelos predictivos que tengan por única finalidad incidir en la *psiquis* del sujeto, manipulando su comportamiento en base a información distorsionada, lo cual – en definitiva- si podría socavar las bases de la democracia y comprometer el interés público.

BIBLIOGRAFÍA

ARTÍCULOS ACADÉMICOS

AAGAARD, PETER; MARTHEDAL, SELMA. Political microtargeting: Towards a pragmatic approach. *Internet Policy Review*, 2023, vol. 12, no 1.

AHUMADA, MARIA JOSÉ; BAZÁN, IGNACIO. Piñera: Viaje al corazón del triunfo. *La tercera, 2017.* [En línea] 2022. [Citado el: 26 de julio de 2022] https://www.latercera.com/noticia/pinera-viaje-al-corazon-de-su-triunfo/

ALBERT, CATALINA. Big Data en campañas: "Para los políticos es más fácil ganar una elección, pero les resulta muy difícil gobernar**".** *CIPER, 2019.* **[**En línea] 2022. [Citado el: 02 de junio de 2022] https://www.ciperchile.cl/2019/09/23/big-data-en-campanas-para-los-politicos-es-mas-facil-ganar-una-eleccion-pero-les-resulta-muy-dificil-gobernar

ALEXY, ROBERT. Sistema jurídico, principios jurídicos y razón práctica, 1988, p. 139 Disponible en https://rua.ua.es/dspace/bitstream/10045/10871/1/Doxa5_07.pdf

ALVARADO, FRANCISCO. Internet y las fuentes de acceso público a datos personales. *Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales*. Taller Sobre Privacidad y Tecnologías, Facultad de Derecho, Universidad de Chile, 2011.

ARAL, SINAN. The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health--and How We Must Adapt. *Currency*, 2021.

ARSENAULT, AMELIA. Microtargeting, Automation, and Forgery: Disinformation in the Age of Artificial Intelligence. 2020.

ASESORÍA TÉCNICA PARLAMENTARIA. Consulta experta sobre la Ley de Protección de la vida privada de las personas, 2018. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26703/2/BCN_Consulta_experta_sobre_la_Ley_de_Proteccion_de_la_vida_Privada.pdf.

BAHAMONDE GUASCH, CRISTIÁN. Los datos personales en Chile: concepto, clasificación y naturaleza jurídica**.** *Revista Ius Novum, Centro de Estudios 2017* no 14.

BARRET, PAUL; HENDRIX, JUSTIN; SIMS, J.GRANT, Fueling the fire: how social media intensifies u.s political polarization and what can be done about it. NYU STERN, 2021.

BARRIUSO RUIZ, CARLOS. Las redes sociales y la protección de datos hoy. *Anuario de la Facultad de Derecho (Universidad de Alcalá)*, 2009, no.2.

BAVIERA, TOMÁS; CANO-ORÓN, LORENA; CALVO, DAFNE. Tailored messages in the feed? Political microtargeting on Facebook during the 2019 General Elections in Spain. *Journal of Political Marketing*, 2023, p. 1-20.

BENNETT, W. L. & LIVINGSTON, S. EN: SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. *Cuadernos. info*, 2019, no 44.

BENNETT, W. L., SEGERBERG, A., & YANG, Y. The Strength of Peripheral Networks: Negotiating Attention and Meaning in Complex Media Ecologies. Journal of Communication, 2018, 68(4).

BERKOWITZ, DAN; SCHWARTZ, DAVID ASA. MILEY, CNN AND THE ONION: When fake news becomes realer than real. *Journalism practice*, 2016, vol. 10, no 1, p. 1-17 y **UBERTI, DAVID.** The real history of fake news. Columbia Journalism Review, 2016, vol. 15.

BERLANGA, ANTONIO. El camino desde la inteligencia artificial al Big Data. *Revista Índice*, 2016, no 68.

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Régimen legal nacional de protección de datos personales. [En línea] 2014. [Citado el: 20 de diciembre de 2021.] https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20443/5/REG_NACIONAL_PROTECC_DATOS_PERSONALES%20(LV)_v5.pdf. 3183.

BOLDYREVA, ELENA L., et al. Cambridge analytica: Ethics and online manipulation with decision-making process. European Proceedings of Social and Behavioural Sciences, 2018, vol. 51

BORDACHAR BENOIT. Comentarios al proyecto de ley chileno sobre protección de datos personales: deficiencias e inconsistencias en los derechos ARCO. *Revista chilena de derecho y tecnología*, 2022, vol. 11, no 1.

BRADSHAW, SAMANTHA; HOWARD, PHILIP N. Challenging truth and trust: A global inventory of organized social media manipulation. *The computational propaganda project*, 2018, vol. 1.

BRKAN, M. (2020). Derechos fundamentales de la UE y democracia Implicaciones de Campañas políticas basadas en datos.Maastricht Journal of European and Comparative Law,27(6), 774–790.

CABRERA, A. Evolución tecnológica y cibermedios. *Zamora: Comunicación Social.*

CAMACHO CEPEDA, GLADYS. Financiamiento de los procesos electorales: examen de la ley 19.884 sobre transparencia, límite y control del gasto electoral. *Revista de derecho (valdivia)*, 2015, vol. 28, no 2.

CERDA, A. Autodeterminación Informativa y Leyes Sobre Protección de Datos. Revista Chilena de Derecho Informático, Núm. 3, 2003. pp. 47- 75.

CIANCI, LICIA; ZECCA, DAVIDE. Polluting the Political Discourse: What Remedies to Political Microtargeting and Disinformation in the European Constitutional Framework?. *European Journal of Comparative Law and Governance*, 2023, vol. 1, p. 1-46.

CIPER. Instagis: el "gran hermano" de las campañas políticas financiado por Corfo. *CIPER 2018.* [En línea] 2022. [Citado el: 20 de julio de 2022] https://www.ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/

COMISIÓN EUROPEA. "Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre inteligencia artificial para Europa", 2018, p. 1. Disponible en: https://eur-lex.europa.eu/legalcontent/ES/TXT/?uri=CELEX%3A52018DC0237

COMITÉ JURÍDICO INTERAMERICANO (CJI). 2021. *Principios actualizados del comité jurídico interamericano sobre la privacidad y la protección de datos personales, con anotaciones.* Sesión Virtual : CJI, 2021.

CONDE, B; HERNÁNDEZ, L. Evaluación del Proyecto de Ley que Regula la Protección y el Tratamiento de los Datos Personales en Chile. *Documento de Trabajo No 65 (CLAPES UC)*, 2019.

CONSEJO PARA LA TRANSPARENCIA. *Democracia y protección de datos personales en la Era Digital*. Santiago : Ediciones Consejo para la Transparencia, 2019, Cuaderno de trabajo N° 13.

CORRAL TALCIANI, HERNAN. Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 39-57, 2001.

DEL SOLAR, BERNARDITA. Dinero y política: ¿una mezcla explosiva? *Puntos de Referencia N°391, Edición online.* Centro de Estudios Públicos 2015. Disponible en: https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf

DOBBER, TOM; Ó FATHAIGH, RONAN; ZUIDERVEEN BORGESIUS, FREDERIK. The regulation of online political micro-targeting in Europe. *Internet Policy Review*, 2019, vol. 8, no 4.

EUROPEAN DATA PROTECTION SUPERVISOR. Opinion 2/2022 on the Proposal for Regulation on the transparency and targeting of political advertising. Disponible en: https://edps.europa.eu/system/files/2022-01/edps_opinion_political_ads_en.pdf

EUROPEAN PARLIAMENTARY RESEARCH SERVICE. *Key social media risk to democracy; Risk from surveillance, personalisation, desinformation, moderation, and microtargeting.* EPRS, 2021.

FUNDACIÓN DATOS PROTEGIDOS. Una propuesta a la ley de datos personales en Chile, 2017, p.5. Disponible en: https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf

GARCÍA, MARC AMORÓS. *Fake News: La verdad de las noticias falsas*. Plataforma, 2018.

GARRIDO, ROMINA. *Datos personales e influencia política en Chile.* Fundación Datos Protegidos, 2018.

GONZALEZ HOCH, FRANCISCO. Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 153-174, 2001.

GUTIÉRREZ-RUBÍ, ANTONI. Política: del 'big data'al 'data thinking'. *ACOP Papers*, 2015, no 2

HUESO, LORENZO COTINO. Big data e inteligencia artificial. *Una aproximación a su tratamiento jurídico desde los derechos fundamentales. Dilemata*, 2017, no 24.

HUNEEUS, CARLOS. Malestar y desencanto en Chile. Legados del autoritarismo y costos de la transición. *Papeles de Trabajo-Programa de Estudios Prospectivos*, 1998, vol. 54.

HUNEEUS, CARLOS. Partidos en Chile: debilidad y crisis. *Mensaje*, 2009, vol. 58, no 580.

INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO, RESPECTO AL PROYECTO DE LEY REFUNDIDO QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES. Boletines N°s 11.144-07 y 11.092-07, refundidos, p. 4. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=25447&prmTIPO=INFORMEPLEY

INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE. Digital Microtargeting, Political Party Innovation Primers, 2018, p.18. Disponible en: https://www.idea.int/sites/default/files/publications/digital-microtargeting.pdf

JERVIS, PAULA. La regulación del Mercado de datos personales en Chile. Tesis para optar al grado de Magíster en Derecho, Universidad de Chile, 2006.

JIJENA, RENATO. Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 85-112, 2001.

KREPS SARAH, McCAIN MILES. Not Your Father's Bots AI Is Making Fake News Look Real. *FOREIGNS AFFAIRS, 2019.* [En línea] 2022. [Citado el: 02 de junio de 2022] https://www.foreignaffairs.com/articles/2019-08-02/not-your-fathers-bots

LANEY, DOUG, ET AL. 3D data management: Controlling data volume, velocity and variety. *META group research note*, 2001, vol. 6, no 70.

MANUAL DE LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS. Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2019 Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf, p, 31- 32

MARTINEZ DEVIA, ANDREA. La Inteligencia Artificial, el Big Data y la Era Digital: Una Amenaza para los Datos Personales. *Rev. Prop. Inmaterial*, 2019, no. 27.

MENDOZA, MARCELO. Seminario Virtual Uso de Datos Personales en Elecciones, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

MINISTERIO DE CIENCIAS, TECNOLOGÍAS, CONOCIMIENTO E INNOVACIÓN. Politica Nacional de Inteligencia Artificial, 2021, p.6. Disponible en: https://www.minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf

MONSALVE, DANIELA; GÓMEZ DOMÍNGUEZ, JOSÉ GREGORIO. Transformación digital: la gestión pública de la nueva era. *Debates IESA*, 2021, vol. 25, no 2.

MUÑOZ, MIGUEL MORENO. Privacidad y procesado automático de datos personales mediante aplicaciones y bots. *Dilemata*, 2017, no 24.

NIŠEVIĆ, MAJA, ET AL. Understanding the legal bases for automated decision-making under the GDPR. En *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, 2022.

NME NEWS MEDIA EUROPE Posición sobre la Comisión Europea Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre Transparencia y Focalización de la Publicidad Política. 2022. Disponible en: https://ec.europa.eu/ info/law/better-regulation/have-your-say/initiatives/12826-Politicaladvertisingimproving-transparency/F2820204 es)

ORELLANA VILCHES. Agencia de protección de datos personales. *Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales*. Facultad de Derecho, Universidad de Chile, 2011.

ORIENTACIONES DE LA COMISIÓN RELATIVAS A LA APLICACIÓN DE LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EN EL CONTEXTO ELECTORAL. COMISIÓN EUROPEA, 2018 Disponible en: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52018DC0638

PALMA ORTIGOSA, ADRIÁN. Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. 2019

PAVLIC, RODOLFO; ARÉVALO, ROBERTO MARDONES. Chile 2010: la desafección política y su impacto en la participación política convencional y no convencional. *Revista del CLAD Reforma y Democracia*, 2019, no 73, p. 189-226.

PEÑA YAÑEZ, SEBASTIÁN. Régimen de indemnización de perjuicios de la ley 19.628 y la seguridad de datos personales. Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales, 2019.

PEÑA, JUAN CARLOS HERNÁNDEZ. Campañas electorales," big data" y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos. *Revista española de derecho constitucional*, 2022, vol. 42, no 124, p. 41-73.

PERALTA SAINZ, ALVARO. ¿Aprueba o rechaza? La Señora Juanita hoy. *The Clinic 2020.* [En línea] 2022. [Citado el: 02 de junio de 2022] https://www.theclinic.cl/2020/03/06/aprueba-o-rechaza-la-senora-juanita-hoy/

PUCCINELLI, OSCAR RAÚL. Tipos y subtipos de hábeas data en el Derecho constitucional latinoamericano. *La Ley, Suplemento de Derecho constitucional*, 1997.

RAJEVIC, Enrique; AA. VV. Protección de datos y transparencia en la administración pública chilena: Inevitable y deseable ponderación. *Varios autores, Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago: Expansiva*, 2011.

RAMÓN FERNÁNDEZ, F.: Microtargeting, transparencia, datos y propiedad intelectual. Una reflexión sobre los nuevos retos de la inteligencia artificial, Tirant lo Blanch, Valencia, 2021

RAZ, JOSEPH. *The morality of freedom*. Clarendon Press, 1986.

RODRÍGUEZ, AITOR FERNÁNDEZ; ARAMBURU, DAVID VARONA. Elecciones 2021 en la Comunidad de Madrid: Movilización del votante de partidos de izquierdas en Telegram. *[RMd] RevistaMultidisciplinar*, 2023, vol. 5, no 2, p. 57-77.

ROUHIAINEN, LASSE. Inteligencia artificial. *Madrid: Alienta Editorial*, 2018.

RUOHONEN, JUKKA. A Note on the Proposed Law for Improving the Transparency of Political Advertising in the European Union. *arXiv preprint arXiv:2303.02863*, 2023.

SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. Cuadernos. info, 2019, no 44.

SANTIAGO, RAÚL; TRABALDO, Susana. *Mobile learning: nuevas realidades en el aula*. Digital-Text, 2015.

SCHNEBLE, CHRISTOPHE OLIVIER; ELGER, BERNICE SIMONE; SHAW, DAVID. The Cambridge Analytica affair and Internet-mediated research. EMBO reports, 2018, vol. 19, no 8, p. e46579.

SEMINARIO VIRTUAL USO DE DATOS PERSONALES EN ELECCIONES, organizado por El Consejo para la Transparencia de Chile. Disponible en: https://www.youtube.com/watch?v=MmdhKMej2co&t=1156s

SEPÚLVEDA, NICOLAS. Alguien te mira: así funciona el gigante de las campañas políticas que controla Sosafe. *CIPER 2019.* [En línea] 2022. [Citado el: 20 de julio de 2022] https://www.ciperchile.cl/2019/09/11/alguien-te-mira-asi-funciona-el-gigante-de-las-campanas-politicas-que-controla-sosafe/

SUSSER, DANIEL; ROESSLER, BEATE; NISSENBAUM, HELEN. 2019. "Technology, autonomy, and manipulation". Internet Policy Review 8, p.2. Disponible en: https://policyreview.info/articles/analysis/technology-autonomy-and-manipulation. y policyreview-2019-2-1410.pdf

TRUONG, HONG-LINH; PHUNG, PHU H.; DUSTDAR, SCHAHRAM. Governing bot-as-a-service in sustainability platforms–issues and approaches. *Procedia Computer Science*, 2012, no. 10.

VALENZUELA, PIÑA y RAMÍREZ EN: **SANTANA, LUIS E.; CÁNEPA, GONZALO HUERTA**. ¿Son bots? Automatización en redes sociales durante las elecciones presidenciales de Chile 2017. Cuadernos. info, 2019, no 44.

VERCELLI, ARIEL. La (des) protección de los datos personales: análisis del caso Facebook Inc.-Cambridge Analytica. En *XVIII Simposio Argentino de Informática y Derecho (SID)-JAIIO 47 (CABA, 2018)*. 2018

VERGARA AMOROS, GONZALO. Microtargeting y el futuro desarrollo de campañas políticas. *El Mostrador*, 2018. [En línea] 2022. [Citado el: 15 de enero de 2022] https://www.elmostrador.cl/agenda-pais/2018/11/02/microtargeting-y-el-futuro-desarrollo-de-campanas-politicas/

VERGARA ROJAS, MANUEL. Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. Revista chilena de derecho y tecnología, 2017, vol. 6, no 2.

VIAL, FELIPE. Tratamiento de datos personales y protección de la vida privada; estudios sobre la Ley 19.628 sobre protección de datos de carácter personal. *Cuadernos de extensión jurídica* 5. Universidad de los Andes, pp. 23-36, 2001.

VICENCIO ZOLEZZI. Nueva ley de datos personales para Chile. Proyecto de ley para la modernización normativa en la protección de datos personales en Chile: análisis evaluativo y desafíos. *Tesis presentada para obtener el grado académico de Magíster en Políticas Públicas.* Escuela de Gobierno, PUC.

VILLARES, DANIEL JOVE. La inconstitucional habilitación a los partidos políticos para recabar datos sobre opiniones políticas. Comentario a la STC 76/2019, de 22 de Mayo. *Revista Española de Derecho Constitucional*, 2021, no 121, P 327-328

VIOLLER, PABLO. El estado de la protección de datos en Chile, 2017. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf,

WAISSBLUTH, **MARIO**. Orígenes y evolución del estallido social en Chile. *Santiago de Chile: Centro de Estudios Públicos Universidad de Chile*, 2020.

ZITRAIN, JONATHAN. Engineering an Election, Digital Gerrymandering poses a threat to democracy. Disponible en: https://harvardlawreview.org/2014/06/engineering-an-election/.

ZUIDERVEEN BORGESIUS, FREDERIK. Online political microtargeting: promises and threats for democracy. *Utrecht Law Review*, 2018, vol. 14, no1.

LEGISLACIÓN NACIONAL

LEY N°20.285 SOBRE ACCESO A LA INFORMACIÓN PÚBLICA

LEY N°20.575 ESTABLECE EL PRINCIPIO DE FINALIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

LEY N°19.628 SOBRE PROTECCION DE LA VIDA PRIVADA

LEY N°19.848 ESTABLECE NUEVAS NORMAS PARA LA REPROGRAMACION DE DEUDAS PROVENIENTES DEL CREDITO SOLIDARIO DE LA EDUCACION SUPERIOR

LEY N°21.311 MODIFICA DIVERSOS CUERPOS LEGALES PARA PERFECCIONAR LA LEGISLACIÓN ELECTORAL VIGENTE

LEY ORGÁNICA CONSTITUCIONAL N°18.556 SOBRE EL SISTEMA DE INSCRIPCIONES ELECTORALES Y SERVICIO ELECTORAL

BOLETÍN N°11144-07 REFUNDIDO CON BOLETÍN N°11092-07: PROYECTO DE LEY QUE REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES

BOLETÍN N°15869-19: PROYECTO DE LEY QUE REGULA LOS SISTEMAS DE INTELIGENCIA ARTIFICIAL EN CHILE

BOLETÍN N° 13.698-07: PROYECTO DE LEY QUE LIMITA EL ACCESO DE LOS PARTIDOS A INFORMACIÓN PERSONAL Y QUE REGULA LA PROPAGACIÓN DE “FAKE NEWS” EN POLÍTICA

LEGISLACIÓN COMPARADA

CIRCULAR 1/2019, DE 7 DE MARZO, DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, SOBRE EL TRATAMIENTO DE DATOS PERSONALES RELATIVOS A OPINIONES POLÍTICAS Y ENVÍO DE PROPAGANDA ELECTORAL POR MEDIOS ELECTRÓNICOS O SISTEMAS DE MENSAJERÍA POR PARTE DE PARTIDOS POLÍTICOS, FEDERACIONES, COALICIONES Y AGRUPACIONES DE ELECTORES AL AMPARO DEL ARTÍCULO 58 BIS DE LA LEY ORGÁNICA 5/1985, DE 19 DE JUNIO, DEL RÉGIMEN ELECTORAL GENERAL.

COM/2021/206: PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL).

COM/2021/731 PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO SOBRE LA TRANSPARENCIA Y LA SEGMENTACIÓN DE LA PUBLICIDAD POLÍTICA

LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES.

LEY ORGÁNICA 5/1985 DEL RÉGIMEN ELECTORAL GENERAL.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 DE ABRIL DE 2016 RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS

REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 19 DE OCTUBRE DE 2022 RELATIVO A UN MERCADO ÚNICO DE SERVICIOS DIGITALES

JURISPRUDENCIA

RESOLUCIÓN DEL PARLAMENTO EUROPEO, DE 14 DE MARZO DE 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley

SENTENCIA 76/2019, DE 22 DE MAYO DE 2019. RECURSO DE INCONSTITUCIONALIDAD 1405-2019. TRIBUNAL CONSTITUCIONAL ESPAÑOL