



PODER Y TECNOLOGÍA; EL PERFILAMIENTO Y LA PERSONALIZACIÓN RETÓRICA DEL CONTENIDO

<< Ensayo sobre un nuevo poder que debe problematizarse en el derecho. Una argumentación sobre la frustrada protección de datos personales y la tecnología que permite el perfilamiento y la personalización retórica del contenido.>>

**Memoria para optar al Grado de Licenciado en
Ciencias Jurídicas y Sociales**

IGNACIO ALFONSO TOLEDO ROBRES

Profesor Guía, Daniel Álvarez Valenzuela

A todos los que me acompañaron en este último paso por la Facultad, gracias.

ÍNDICE

Contenido

ÍNDICE	3
PRÓLOGO	7
EXPLICACIÓN PRELIMINAR	8
CONCEPTOS TECNOLOGICOS	12
ESTRUCTURA DEL RAZONAMIENTO	13
¿POR QUE NOS IMPORTA ESTE ASUNTO?; PODER Y DERECHO	15
IDEARIO INTRODUCTORIO A UNA ALERTA NECESARIA	18
EL CONTEXTO DE LA TECNOLOGÍA Y LA REVOLUCIÓN DE LA INDUSTRIA	26
TRES ASPECTOS MATERIALES: MASIVIDAD, CAPACIDAD DE CÓMPUTO Y CONECTIVIDAD	26
Capacidad de cómputo al alcance	27
Interconectividad	28
Masividad y digitalización de la vida	29
BREVE INTRODUCCION A LA IDEA DE CUARTA REVOLUCIÓN INDUSTRIAL DE KLAUS SCHWAB	31
EXPONER EL FENOMENO Y NUESTRA PROTECCIÓN	35
PRIMERAS EVIDENCIAS EXPERIMENTALES, EL EXPERIMENTO MANIPULATORIO PÚBLICO DE FACEBOOK	39
EL DILEMA DEL CONSENTIMIENTO QUE RIGE LA UTILIZACIÓN DE NUESTROS DATOS	41
LA SITUACION GENERAL DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE	46

UN DERECHO EN LA CONSTITUCIÓN DEL 2021	46
LA LEY DE PROTECCIÓN DE DATOS PERSONALES	48
DATO PERSONAL, PERSONAL SENSIBLE Y ESTADÍSTICO	51
Dato personal	51
Datos sensibles	52
Datos estadísticos	52
DERECHOS ARCO	54
EL CAUCE PROCESAL A LA PROTECCIÓN DE DATOS: HABEAS DATA	55
HIPÓTESIS DE AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS.....	57
Autorización para el tratamiento de datos personales.....	57
Autorización para el tratamiento de datos personales sensibles.....	58
SOBRE LA EXCEPCION AL CONSENTIMIENTO DEL DATO PERSONAL CONTENIDO EN UNA FUENTE DE ACCESO PÚBLICO	59
INSTAGIS, EMPRESA CHILENA DE TRATAMIENTO DE DATOS PERSONALES	62
EL APEGO A LA LEY DE INSTAGIS Y UN BREVE CONTRAARGUMENTO.....	64
REFORMA A LA LEY DE PROTECCION DE DATOS; EL BOLETÍN 11.144-07 Y 11.092-07 REFUNDIDOS	68
IDEAS CONCLUSORIAS AL CAPITULO	70
DIFICULTADES	70
SOBRE LA CAPACIDAD DEL PERFILAMIENTO	72
MIEDOS Y CASOS DE CAPTACION ILÍCITA DE DATOS	74
RED DE VIGILANCIA MUNDIAL.....	75
CAMBRIGE ANALYTICA	76
PROBLEMAS CON LA PERSONALIZACION RETÓRICA ARTIFICIAL	79
RECAPITULACIÓN	79

LA PERSONALIZACIÓN RETÓRICA ARTIFICIAL.....	80
EL CORROSIVO PODER	82
¿QUÉ TIENE ESTO DE NUEVO?.....	83
LLEGAR A LO ADECUADO PARA PERSUADIR.....	88
LA CAPACIDAD DE TRANSFORMARLO TODO	90
LA VULNERABILIDAD HUMANA, LA CONCIENCIA ES UN FENOMENO MALEABLE.....	93
EL SESGO DE LO RACIONAL Y EL INCONSCIENTE	94
EL LENTE DE LA TECNOLOGÍA, MEDIO Y FORMA DE ENTENDER LA REALIDAD	99
EL LENGUAJE Y EL CONTROL DE LA EPISTEME	101
EL PODER DE LA PERSUACIÓN Y LA UTILIDAD DE ENTENDER EL PROBLEMA COMO RETÓRICA.....	105
¿Por qué es relevante jurídicamente destacar la retórica en un problema de protección de datos?	110
CONCLUSIÓN	114
FIN	117
ANEXO	119
IDEAS INTRODUCTORIAS A LOS DISRUPTORES TECNOLOGICOS.....	119
<i>BIG DATA</i>	120
<i>LAS BIG DATA TECHNOLOGIES</i>	122
LA INTELIGENCIA ARTIFICIAL	123
<i>MACHINE LEARNING</i>	124
1. Supervised learning.....	125
2. Unsupervised self learning.....	126
3. Reinforcement Learning.....	126
REDES NEURONALES	127
DEEP LEARNING	128

Bibliografía	131
Bibliografía no académica	136
NO AUDIOVISUAL	136
AUDIOVISUAL	138

PRÓLOGO

En el contexto de la cuarta revolución industrial y el desarrollo masivo e intrusivo de la tecnología, es importante integrar al debate dentro del derecho el ejercicio de la personalización retórica con el uso de la inteligencia artificial. Un nuevo poder consistente en la capacidad de teorizar a través de la tecnología de procesamiento de datos, el estímulo adecuado para persuadir en la situación concreta.

El presente trabajo analiza esta capacidad exponiendo el contexto tecnológico, la legislación relativa a la protección de datos y distintas comprensiones del fenómeno; a la vez que caracteriza y problematiza la idea de personalización retórica artificial.

El objeto general de esta tesis es evidenciar una nueva clase de actividad retórica, o de persuasión, que escapa de las actuales formas de protección jurídica, identificando lo que permite o no limita hoy, a través de las nuevas tecnologías, la inducción del comportamiento humano a través del perfilamiento del usuario y la personalización del contenido.

EXPLICACIÓN PRELIMINAR

Lo que aquí problematizaremos es la nueva capacidad de teorizar, y ejercer, lo adecuado para convencer a determinado perfil a través de un tratamiento de datos. Esto es lo que llamamos personalización retórica artificial, o meramente, personalización retórica.

La idea de retórica se centra en buscar el medio para generar la predisposición o convicción de un individuo particular, al apelar a las formas en las cuales toma decisiones, sea esto de forma racional o inconsciente. Dado que retórica es “la facultad de teorizar lo que es adecuado en cada caso para convencer”³ (Aristóteles) o, “el arte de persuadir a una audiencia específica con acciones y creencias específicas”⁴. Esta idea es justamente lo que pretendemos controvertir como una nueva capacidad que el tratamiento de datos permite, gracias al “incremento del monitoreo del comportamiento humano y el uso de la información recolectada para mostrar información personalizada”⁵.

La búsqueda por la estrategia persuasiva que es posible mediante las nuevas tecnologías es una nueva clase de retórica, cual identificamos como retórica artificial. Esta no utiliza la intuición, sensibilidad o inventiva humana para persuadir, sino, el estímulo probabilísticamente acertado en consideración a los datos y el medio disponible. Esta clase de retórica, no la realiza la inteligencia humana, si no una inteligencia artificial⁶. De aquí el apelativo artificial en el concepto. Por esto decimos que esta capacidad, es un poder nuevo en la historia; dado que requiere de las nuevas tecnologías. Lo que diferencia la retórica artificial de la retórica humana, aun teniendo el mismo objeto; teorizar y actuar para inducir.

³ Aristóteles, *Retórica*. Editorial Gredos, Madrid. - 1. Definición y estructura lógica de la retórica. 2.1 Definición de retórica y generalidad de su aplicación. (p. 173)

⁴ Definición de Angie Hobbes, filósofa y académica británica, especializada en filosofía y ética del griego clásico. In our time - rhetoric - BBC Sounds. <https://www.bbc.co.uk/sounds/play/p004y263> (min: 1:22)

⁵ Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. <https://doi.org/10.1080/00913367.2017.1339368> (p.1)

⁶ Es la disciplina de las ciencias de la computación que busca que objetos puedan manifestar un funcionamiento similar, o que imite, al pensamiento humano. Igualmente, este funcionamiento es llamado Inteligencia Artificial.

La capacidad persuasiva de la retórica artificial se vuelve un asunto cada vez más problemático. Esto en tanto que existe una correlación entre la mejora exponencial de las nuevas tecnologías de tratamiento de datos -Big Data *Technologies* - y la progresiva captación de datos personales para hacer más persuasiva la capacidad retórica actual de la inteligencia artificial, aumentando el riesgo de una inducción automatizada. “A medida que los datos se recopilan e ingresan perfiles de usuario cada vez más complejos, el riesgo del daño aumenta con el tiempo en correlación con la tecnología y la eficiencia asociada de la personalización”⁷.

Para ejercer la retórica artificial, es necesario perfilar y personalizar el contenido. Es necesario perfilar; para teorizar qué generaría la predisposición y convicción de un individuo particular. Y es necesario personalizar; para llevar a cabo la acción, ordenando los estímulos para el caso concreto.

Para precisar que es el perfilamiento, cabe decir que es entendido un doble sentido. Es tanto la captación de los datos personales, para la detección de patrones humanos; como, la generación de un perfil clasificable. El perfilamiento es, “la interferencia o la detección de patrones mediante Data Mining -y las Big Data *Technologies* en general- y, la consiguiente clasificación de las personas”¹⁰ (Hildebrandt & Koops)^{14,15}. Perfilar es tanto, encontrar un patrón para identificar a una persona o grupo, como también, la categorización de un grupo o individuo dentro de un perfil o patrón identificado.

⁷ Skatova, A.; Lorenz-Spreen, P.; Lewandowsky, S.; Leiser, M.R.; Herzog, S. (2019) Response to the Centre for Data Ethics and Innovation: [call for a] review of online targeting. <https://hdl.handle.net/1887/83089> (p.1)

¹⁰ Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428-460. <https://doi.org/10.1111/j.1468-2230.2010.00806.x> (p. 431)

¹⁴ Para el perfilamiento, como Hildebrandt & Koops, (2010. p. 431) sintetizan: “primero, los datos se capturan, almacenan y agregan, lo que implica una traducción de eventos de la vida real a datos legibles por máquina [...] El segundo paso, aplicar la minería de datos, que consiste en aplicar algoritmos a los datos, con el objetivo de descubrir patrones (clusters, reglas de asociación, correlaciones, etc.) en los datos que no son visibles a simple vista”

¹⁵ Otra definición de Hildebrandt es: “Perfilar es el proceso de “descubrir” patrones dentro de una base de datos que se puede utilizar para identificar o representar a un ser humano o un grupo y / o, la aplicación de perfiles para individualizar y representar a un individuo o para identificar a un sujeto como miembro de un grupo”. Hildebrandt, M., & Gutwirth, S. (Eds.). (2008). *Profiling the European Citizen*. Profiling the European Citizen. Published. <https://doi.org/10.1007/978-1-4020-6914-7> (p.19)

Entendemos por personalización retórica del contenido, al sentido amplio de la adecuación del entorno con fines inductivos, en consideración a las características del sujeto. Esto incluye tanto los estímulos que se den *online* como *off line*, o aquellos estímulos que persuaden de forma explícita o implícita. Lo importante para que se entienda como personalización retórica artificial, es que sean producto de un tratamiento de datos que tenga en consideración las características particulares del usuario para inducir un comportamiento.

La personalización que nos preocupa es aquella que busca inducir un comportamiento¹⁶ en su amplio aspecto mediante las nuevas tecnologías. Nos preocupa aquel tratamiento de datos personales que busque, clasifique y adecue, con el fin de conducir a una conducta. Esto sea mediante la alteración de la presentación de las opciones existentes - adecuación del espacio de decisión, “Nudge¹⁷”-; o, aquella que busque deliberadamente alterar la predisposición utilizando sesgos cognitivos –“Framing Effect¹⁸”-; o, aquella personalización que, como la ocultación, desinformación o mentira, lleve a una falsa representación de la realidad determinada por la ignorancia o la equivocación¹⁹. Finalmente, lo que llamamos a controvertir es el uso de la retórica mediante un tratamiento de datos.

¹⁶ Una precisión. Los conceptos inducir y manipular tienen una relación género-especie. A diferencia de la inducción, la “manipulación” se ejercer en el sujeto “de forma imperceptible y con provecho de sus vulnerabilidades” biopsicosociales. Este sentido lo recogemos de la noción de “manipulación” de Susser, et al. en el artículo Online Manipulation: Hidden Influences in a Digital World (2019).

¹⁷ “Nudge”- empujón- “es cualquier pequeño rasgo en el ambiente que atrae nuestra atención e influencia el comportamiento en la decisión que tomamos”. “Nudging” - empujar- se realiza a través de lo que se denomina “choice architecture”- arquitectura decidida-, que refiere a la idea de quien diseña la experiencia de a quien se quiere influenciar. El concepto dado en el inicio fue extraído de: Richard Thaler - Nudge: An Overview - <https://www.youtube.com/watch?v=xoA8N6nJMRs> (consultado: 09 de abril del 2020).

El concepto de se popularizó en el 2008 gracias al libro “Nudge: Improving Decisions About Health, Wealth, and Happiness”, escrito por el economista conductual Richard Thaler y el jurista Cass Sunstein.

¹⁸ ‘Framing Effect’, noción que dispone que las personas llegamos a perspectivas diferentes según como se nos presente la información, generando una ponderación que depende de la perspectiva anímica o narrativa, no enteramente de la lógica pura de los elementos que la componen. El concepto fue popularizado por Tversky y Kahneman en “The Framing of decisions and the psychology of choice”(1981).

¹⁹ Hemos hecho alusión directa a la idea de ‘error de hecho’ que es recogido desde las tradiciones romanas y se consagra en nuestro Código Civil como un vicio del consentimiento.

En la literatura reciente existen distintos conceptos que pueden asemejarse a la idea de ‘personalización retórica artificial’, por tratar la intencionada afectación del mundo digital al comportamiento humano. Sin embargo, existen diferencias de alcance con muchos de ellos para describir el fenómeno. De todos modos, como señala Boerman et al., “a pesar de la atención recibida (al fenómeno - “online behavioral advertising”-) no hay una definición sólida, ni una clara acumulación de hallazgos empíricos”²⁰.

Podemos señalar como conceptos, similares a personalización retórica artificial, los siguientes términos: “online behavioral advertising”(Boerman, Kruikemeier y Zuiderveen); “Chilling effects and corporate profiling” (Büchi, Fosch, Lutz, Tamò-Larrieux, Velidi y Viljoen); “Online Manipulation” (Susser, Roessler y Nissenbaum,); “Behavioral targeting” (Bennett); “Networked information *Technologies*” (Pfaffenberger); “Hyper-nudging” (Karen Yeung); “Modulated Society” (Cohen); “Dark Patterns” (Brignull); “Values in Design” (Flanagan & Nissenbaum’s); “Dataísmo” (Harari); “Psicopolítica” (Han); “Surveillance Capitalism”, “(Com)modification” (Zuboff); “Exploitation of experienced freedom” (B. Harcourtr).

Estas aproximaciones son valiosas, pero no son iguales al concepto ‘personalización retórica artificial’; la acuñación del concepto es una propuesta novedosa y se refiere al problema concreto de la capacidad de teorizar el estímulo adecuado para persuadir en la situación concreta (retórica) a través de la tecnología de procesamiento de datos (artificial) adecuando el estímulo (personalizada). Pensamos que este concepto logra determinar lo que en él se derecho debe problematizar como afectación del mundo digital al comportamiento humano a través de las nuevas tecnologías.

El concepto propuesto, a diferencia de los vistos en la literatura, se apoya en la tradición existente en torno a la retórica para exaltar la teorización de lo adecuado para convencer y la intención inductiva. La idea de retórica es amplia, y se centra en la teoría y práctica de lo que induce, independiente del medio empleado. Al mismo tiempo, pensamos conveniente el término artificial para señalar el uso de la inteligencia artificial en la búsqueda

²⁰ Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. <https://doi.org/10.1080/00913367.2017.1339368> (p.363)

de lo adecuado para inducir²¹ (sin embargo, como este apelativo se subentiende en el contexto, no siempre lo referiremos). Finalmente, el termino personalización es crucial, pues delimita el término a aquella acción retórica que utiliza un tratamiento de datos personales, pues requiere conocer datos relativos a la persona identificable.

CONCEPTOS TECNOLOGICOS

El uso de nuevas tecnologías es central en la capacidad a problematizar. Respecto de estas tecnologías clave, es bueno tener presente desde un comienzo -al menos de forma somera-, los siguientes conceptos que utilizaremos a lo largo de este trabajo:

Algoritmos, son un conjunto de reglas que define de forma precisa, a través de especificaciones no ambiguas, un conjunto de operaciones en una secuencia definida y finita de instrucciones²².

Big Data Technologies, son las tecnologías que permiten analizar enormes volúmenes de datos para reconocer patrones, tendencias y asociaciones.

Big Data, o Macrodatos, es toda aquella información registrable o, una enorme cantidad de datos, es decir, es la fuente desde la que extraer y analizar información, e igualmente, - pues hay quienes lo entienden - es el proceso de análisis y sus resultados como *Big Data*²³.

Machine learning, o Aprendizaje Automático, es la capacidad que pueden mostrar máquinas para aprender mediante experiencia y datos²⁴.

²¹ Sin embargo, dado que este apelativo se subentiende muchas veces en el contexto, no siempre lo referiremos.

²² Definición, adecuada, de Deborah Lupton (2015), *Digital Sociology* (p.49-50).

²³ Otra definición podría ser: "información caracterizada por un alto volumen, velocidad y variedad que requieren tecnología y métodos analíticos específicos para su transformación en valor". (De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, 65(3), 122-135. <https://doi.org/10.1108/lr-06-2015-0061>)

²⁴ Definición propia. Otra definición posible, siguiendo "The *Machine learning* Dictionary" (University of New South Wales): "se dice que el aprendizaje automático ocurre en un programa que puede modificar algún aspecto de sí mismo, a menudo denominado su estado, de modo que, en una ejecución posterior con la misma entrada, se produce una salida diferente" (Este Diccionario sigue los conceptos

Neural Network, o Redes Neuronales, son un grupo de modelos algorítmicos de procesamiento de datos, que se enmarcan en el aprendizaje automático, cuales se caracterizan por utilizar perceptrones, o las denominados neuronas.

Artificial Intelligence (AI), o Inteligencia Artificial (IA), es la disciplina que busca que objetos puedan manifestar un funcionamiento similar, o que imite, al pensamiento humano. Igualmente, el resultado de esta disciplina, es llamado Inteligencia artificial.

En el anexo se expone con mayor profundidad, pero de forma introductoria, estos conceptos.

ESTRUCTURA DEL RAZONAMIENTO²⁵

Para tratar el problema central ya anunciado, este trabajo desarrolla una exposición de:

comprendidos en el compilado COMP9414 de la University of New South Wales, Sydney. <https://web.archive.org/web/20180826151959/http://www.cse.unsw.edu.au/~billw/mldict.html#aativfn>)

Finalmente, “la esencia de *Machine learning* son los algoritmos que dan a los computadores la capacidad de aprender de los datos para luego hacer predicciones y decisiones” (Machine Learning & Artificial Intelligence: Crash Course Computer Science #34. (2017, 1 noviembre). [Video]. YouTube. [https://www.youtube.com/watch?v=z-EtmaF\]ieY&ab_channel=CrashCourse](https://www.youtube.com/watch?v=z-EtmaF]ieY&ab_channel=CrashCourse))

²⁵ Este trabajo, que recibe comúnmente el nombre de tesis, está escrito en modalidad ensayo, modalidad definida por la Escuela de Derecho de la Universidad de Chile para las Tesis de Memoria como: “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 convincente para el lector”.

Esta modalidad aprobada el 2 de diciembre del 2015 por el Consejo de Facultad, se encuentra establecida en la resolución administrativa número 725 en su artículo 1, literal B. Esta resolución integra la modalidad ensayo al modificar el “instructivo sobre memoria de prueba y los talleres de memoria en la carrera de derecho” para efectos de lo dispuesto en el artículo 7° inciso final del reglamento para optar al grado de licenciado en ciencias jurídicas y sociales, D. U. N° 002441, de 1976. Puede encontrarse la resolución 725 en el siguiente enlace: <http://web.derecho.uChile.cl/documentos/Resol%20725%20Instructivo%20Memorias.pdf> [Consultado en Julio 2020]

- a) una introducción sumaria;
- b) los aspectos relevantes de la contingencia y la tecnología;
- c) la frustrada protección jurídica a los datos personales para evitar el perfilamiento;
- d) el interés tras el ejercicio de la retórica artificial, las vulnerabilidades humanas que lo permiten y una idea en torno a la retórica.

El razonamiento argumental para cumplir con estos objetivos es el siguiente:

Introducción: Brindar una exposición sumaria.

Primero: Situar el problema dentro de un contexto y técnica. Para ello, describiremos el incremento en la capacidad de cómputo, la masividad de los dispositivos inteligentes y la interconectividad, para luego abordar la idea de cuarta revolución industrial. Complementando este capítulo, en el **anexo** exponemos de forma introductoria -pero suficiente para tener un manejo conceptual-, las tecnologías de tratamiento de datos, describiendo que es Inteligencia Artificial, *Big Data*, Redes Neuronales y *Machine learning*.

Segundo: Trataremos el derecho a la protección de datos que ha dejado, en la práctica, el perfilamiento de los usuarios sin restricción efectiva. Para abordar este punto, revisaremos el experimento de manipulación social de Facebook (2012)²⁶, para cuestionar “la forma básica de enfrentar la protección de la privacidad”²⁷, el consentimiento como autorización para el tratamiento de datos. Luego, analizaremos brevemente la actual legislación sobre datos personales en Chile²⁸ exponiendo las principales categorías de la ley 19.628; en particular, las clases de datos, los derechos ARCO, la herramienta especializada de control del tratamiento de datos “Habeas Data” y las hipótesis de licitud de tratamiento. Después de esto, se comentaran los principales aspectos de la reforma a la ley de protección de datos del boletín 11.144-07 y 11.092-07. Posteriormente, analizaremos la empresa chilena

²⁶ Llevado al conocimiento público en el artículo “Experimental evidence of massive-scale emotional contagion through social networks “. Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014)

²⁷ Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. (2013) (p.1881)

²⁸ En particular destacaremos la ley 19.628 de 1999, puesto que es la ley encomendada actualmente por la Constitución de la República a determinar la forma y condiciones en la que se efectuará la protección de datos personales y el tratamiento de datos.

de perfilamiento InstaGIS (2017) contraargumentando su licitud. Finalmente, tratando dos macro escándalos, terminaremos con una reflexión general sobre las dificultades para con la protección de datos y la amenaza que esto supone.

Tercero: Entregaremos una visión general del problema. Trataremos para esto, el interés económico y político tras la inducción al comportamiento, exponiendo distintas perspectivas en la literatura. Luego, en una reflexión desde las humanidades, veremos tres aspectos de la vulnerabilidad humana que permiten predisponer la experiencia para persuadir, en los títulos “sesgo racional” -donde trataremos especialmente a Kahneman-; “el lente de la tecnología” -Heidegger-; “el control de la episteme” -Foucault-. Para finalizar, brindamos una idea general de lo que es la retórica clásica y lo pertinente de entender el problema actual como retórica.

¿POR QUE NOS IMPORTA ESTE ASUNTO?; PODER Y DERECHO.

La retórica busca inducir, e inducir es la intención y probabilidad de que una voluntad se imponga; esto es poder y por ello el derecho debe reaccionar.

Como disciplina, el derecho tiene una responsabilidad compleja frente al poder; lo tiene encomendado. Citando a Edgar Bodenheimer, “la función general de las ramas del derecho es esencialmente la misma; [...] la creación de restricciones al ejercicio arbitrario e ilimitado del poder”²⁹.

El poder puede ser definido³⁰, siguiendo la famosa definición de Max Weber, como: “la probabilidad de imponer la propia voluntad, dentro de una relación social, aún contra toda

²⁹ Bodenheimer, E. (1942). Teoría Del Derecho (2.a ed.). Fondo de Cultura Económica (p.28)

³⁰ Otras definiciones de poder con sentido similar son;

David Easton: El poder es un fenómeno de relaciones, no es una cosa que alguien posea. El poder es una relación en la cual una persona o grupo puede determinar las acciones de otro, en forma tal que satisfaga los fines del primero. Easton, David. (1968) Política Moderna. Ed. Letras, México (p. 149)

Raymond Aron: El poder es la capacidad de un individuo para determinar la conducta de otros. En su sentido más general, el poder es la capacidad de hacer, producir o destruir. Raymond, A. (1968). Democracia y Totalitarismo. Editorial Seix Barral, Barcelona. Ambas definiciones fueron extraídas de,

resistencia y cualquiera que sea el fundamento de esa probabilidad”³². Esta noción alcanza la característica del problema a describir, pues la personalización retórica artificial sobrepasa la resistencia cuando induce el comportamiento. Inducir, del latín “inducere”, es ‘conducir hacia’. Siendo el problema poder, debe ser problematizado, estudiado y encausado por el derecho.

Si el derecho es, esta vez siguiendo a Kant, “el conjunto de condiciones bajo las cuales el arbitrio de un individuo puede coexistir con el árbitro de otro bajo una ley general de libertad³³”, al evidenciarse patentemente que este asunto genera una interferencia en la capacidad que posee un agente para actuar en el mundo; el derecho debe idear el conjunto de condiciones para que prime la ley general de libertad. Es por esto, en último término, que la personalización retórica artificial debe ser un problema en el derecho.

Ante otras transformaciones económico-sociales el derecho, con tardanza y no libre de dificultades, debió abandonar antiguas soluciones obsoletas para proteger a la parte más débil. Así mismo, aparecieron áreas como el derecho del consumidor, el derecho medioambiental y el derecho laboral. Posiblemente, al igual que con otros desafíos, nos encontramos en una situación que amerita una reinención o nueva subdisciplina. Después de todo, y parafraseando a Madeleine Albright, “nos enfrentamos a la tarea de regular las tecnologías del siglo XXI, con una mentalidad del siglo XX, bajo una institucionalidad del siglo XIX”³⁴. Por ello, ante el desafío que plantea la retórica artificial, debemos pensar el futuro y abandonar los compartimentos estancos del derecho que son palabra inútil ante problemas reales; porque el derecho es la ciencia social encomendada a sortear como disciplina los cauces del poder.

Montbrun, Alberto. (2010). Notas para una revisión crítica del concepto de "poder". Polis (Santiago), 9(25), 367-389. <https://dx.doi.org/10.4067/S0718-65682010000100022>

³² Weber, Max, economía y Sociedad. Esbozo de sociología comprensiva (1922). Ed. FCE, México, 2008 (p. 43).

³³ Kant, Immanuel. Principios metafísicos del derecho. Buenos Aires: Americalee, 1943 (p.47)

³⁴ US Secretary Madeleine K. Albright, Chairman National Democratic Institute, at #DisinfoWeek (2017): “citizens are speaking to their governments using 21st century technologies, governments are listening on 20th century technology and providing 19th century solutions.” <https://medium.com/dfrlab/we-need-21st-century-responses-6b7eed6750a4>

IDEARIO INTRODUCTORIO A UNA ALERTA NECESARIA

La tecnología ha cambiado el mundo que vivimos; “hoy miles de millones de sensores incorporados a dispositivos comunes, portados por millones de individuos, registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red”³⁵. Esto ha generado un perverso escenario, “donde las empresas captan, agregan, comercializan y utilizan información personal en niveles sin precedentes, generando un acceso extenso a datos personales, sobre las características y comportamientos de miles de millones de individuos, lo que les permite monitorear, seguir, juzgar, clasificar, calificar y clasificar constantemente a las personas” (Wolfie, 2017)³⁶.

En este contexto, “los anunciantes cada vez más monitorean el comportamiento de los usuarios en línea para usar esta información recopilada y mostrar a las personas información dirigida individualmente” (Boerman et al., 2017)³⁷. Lo que “ha permitido que empresas y los partidos políticos puedan dirigirse a grupos de personas que probablemente utilicen y disfruten sus productos y servicios, pero igualmente, ha permitido inducir y sostener un

³⁵ Parafraseo del concepto internet de las cosas (IoT) contenido en el dictamen 8/2014 del Grupo de Trabajo del Artículo 29, ahora Comité Europeo de Protección de Datos.

³⁶ Wolfie (2017). How companies use personal data against people. Working paper by cracked LABS. Published. (p.4)

³⁷ Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. <https://doi.org/10.1080/00913367.2017.1339368> (p.363)

consumo innecesario o crear oportunidades para la manipulación política” (Skatova et al., 2019)³⁸

La enorme cantidad de ejemplos de comportamiento humano disponible y la constante producción de datos, ha habilitado entrenar sistemas para identificar el comportamiento y las debilidades los usuarios. Al punto que, con una pequeña interacción y las capacidades derivadas de *Big Data* y *Machine learning*, con un elevado acierto sea posible revelar asuntos como “la capacidad económica, inclinación sexual, patrones psicológicos, o afinidades políticas”³⁹. De hecho, para conocer estos sensibles asuntos, “los modelos informáticos necesitan 10, 70, 150 y 300 Me gusta (de Facebook), respectivamente, para superar a un colega de trabajo promedio, conviviente o amigo, miembro de la familia y cónyuge” (Youyou et al., 2015)⁴⁰. Como vemos, “mediante los datos de una persona se puede inferir [...] (siendo) Esta información valiosa al comercialmente, pues permite, solo por mencionar uno de sus usos más inofensivos, ofrecer publicidad personalizada.” (Ospina-Celis y Upegui Mejí, 2020)⁴¹

La mercantilización de la personalización retórica para obtener réditos políticos y económicos es un asunto problemático. Considere que, “cuando Facebook recopila los datos, los recopila para venderlos. Hoy, un político o una empresa puede directamente comprar datos personales en Facebook para efectos de su campaña política o comercial, que originalmente no era el propósito de la recolección” (Álvarez, 2021)⁴². Así mismo, considere que “Facebook, al monitorear publicaciones, imágenes, interacciones y actividad en Internet

³⁸ Skatova, A.; Lorenz-Spreen, P.; Lewandowsky, S.; Leiser, M.R.; Herzog, S. (2019) Response to the Centre for Data Ethics and Innovation: [call for a] review of online targeting. <https://hdl.handle.net/1887/83089> (p.1)

³⁹ Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15), 5802-5805. <https://doi.org/10.1073/pnas.1218772110> (p.1)

⁴⁰ Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040. <https://doi.org/10.1073/pnas.1418680112> (p.1037)

⁴¹ Op cit. Ospina-Celis y Upegui Mejí. (2020) *Festín de datos Empresas y datos personales en América Latina*. Editorial Dejusticia, ISBN 978-958-5597-31-0 (p.12).

⁴² Álvarez, Daniel (2021) “El Estado es un muy buen recolector de datos personales de los pobres”. *The Clinic*. <https://www.theclinic.cl/2021/10/29/daniel-alvarez-experto-en-derechos-digitales-y-privacidad-de-datos-el-estado-es-un-muy-buen-recolector-de-datos-personales-de-los-pobres/>

en tiempo real, permite a los anunciantes dirigirse focalizadamente a personas en momentos en los que se sienten “nerviosos”, “estresados”, “inútiles”, “ansiosos”, “abrumados”, “estúpidos” e “inseguros”⁴³. Por otro lado, político, considere el macro escándalo de Cambridge Analytica⁴⁴, que “utilizo cientos o miles de puntos de datos individuales [...] para comprender exactamente qué mensajes van a atraer a qué audiencias” (CEO Nix, 2016)⁴⁵ y a partir del perfilamiento, “creo modelos para explotar lo que sabíamos de ellos y apuntar a sus demonios internos” (ex empleado Christopher Wylie, 2018)⁴⁶.

Como consecuencia de los intereses tras este nuevo poder, “la estrecha relación existente entre el Big Data y la Inteligencia Artificial (IA) seguirán en aumento y en evolución, ya que con los macrodatos se pueden capacitar sistemas de IA que utilicen redes neuronales y modelos estadísticos, con el fin de predecir algunos acontecimientos y comportamientos” (Herrera y Viollier, 2020)⁴⁷ mejorando la capacidad de personalizar el contenido.

En esta situación se ve envuelta, prácticamente, a toda la humanidad. “En el entorno en línea, las opciones disponibles (u observables) que tenemos y la información que vemos, se generan cada vez más mediante sofisticadas e inteligentes técnicas de elaboración de perfiles, que aprovechan una comprensión detallada de nuestra huella digital” (Skatova et al.,

⁴³ Sam Machkovech, Facebook Helped Advertisers Target Teens Who Feel “Worthless,” ARS TECHNICA (consultado: 3 de febrero 2021), <https://arstechnica.com/informationtechnology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/> [https://perma.cc/BPD9-6NKP]. [Como se cito en: “Online Manipulation: Hidden Influences in a Digital World, 2019” (p. 2)]. Igualmente, Davidson, D. (2017, May 1). Facebook targets “insecure” to sell ads. The Australian. [Como se cito en: “Technology, autonomy, and manipulation, Internet Policy Review, 2019(p.6)]]

⁴⁴ Sobre Cambridge Analytica, hablaremos con mayor profundidad en el título “MIEDOS Y CASOS DE CAPTACION ILICITA DE DATOS”

⁴⁵ Nix, Alexander. Cambridge Analytica - The Power of Big Data and Psychographics. (2016, 27 septiembre). [Video]. YouTube. https://www.youtube.com/watch?v=n8Dd5aVXLCc&ab_channel=Concordia [Consultado: marzo 2021].

⁴⁶ Cambridge Analytica and Facebook: The Scandal So Far, AL JAZEERA (Mar. 28, 2018), <https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html> [https://perma.cc/PU4C-KNSN].

⁴⁷ Herrera, Paloma y Pablo Viollier. (2020) Rendición de cuentas de Facebook y otros negocios en Chile: la protección de datos personales en la era digital. ISBN: 978-958-5597-32-7 (p.123)

2019)⁴⁹. Estos “sistemas toman decisiones sobre las personas en función de sus datos, produciendo sustanciales efectos adversos que pueden limitar enormemente sus opciones y oportunidades en la vida. Estos sistemas son en gran parte opacos, no transparentes, arbitrarios, sesgados, injustos e irresponsables [...]. A través de la personalización basada en datos, las empresas y otras instituciones pueden utilizar fácilmente las asimetrías de información para explotar las debilidades personales con eficiencia calculada para generar persuasión personalizada, pudiendo influir eficazmente en el comportamiento a gran escala.” (Wolfie, 2017)⁵⁰. “Dado que todos estamos envueltos en esta situación, la premisa de partida debe ser que todo el mundo es vulnerable (“vulnerabilidad generalizada”), pues no solo afecta a grupos o personas particularmente vulnerables” (Skatova et al., 2019)⁵¹.

Tomando en cuenta todo lo anterior, el desarrollo de la economía digital y las tecnologías del *Big Data* plantean desafíos importantes para los derechos a la intimidad y a la protección de datos personales de las personas, así como para la transparencia, la seguridad de los datos y el derecho a la igualdad (Newman y Angel, 2019)⁵²; e igualmente, representa un desafío mayor, por tener “el potencial de vulnerar los derechos fundamentales de los titulares, ya sea por la asimetría de poder que crea entre el usuario y la plataforma, el eventual rastreo y monitoreo de actividades requerido para su ejecución y la personalización o manipulación del comportamiento que puede generar” (Büchi, Fosch, Lutz, Tamò-Larrieux, Velidi y Viljoen, 2019)⁵³.

Sobre todo lo anterior, tenemos al “corrosivo modelo de negocios” que afecta a las plataformas tecnológicas que ofrecen sus servicios al público de forma gratuita y masiva, pues estas compañías comúnmente, tienen su ingreso a través de servicios directamente relacionados con el perfilamiento de sus usuarios, incluso si esto conlleva a efectos sociales

⁴⁹ Op cit. (p.6)

⁵⁰ Ibid. Wolfie (2017) (p.4)

⁵¹ Ibid. (p2)

⁵² Newman y Ángel 2019, 13. Como se citó en: Ospina-Celis y Upegui Mejí. (2020) Festín de datos Empresas y datos personales en América Latina. Editorial Dejusticia, ISBN 978-958-5597-31-0 (p.14,)

⁵³ Büchi, Moritz, Eduard Fosch-Villaronga, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi y Salome Viljoen. “Chilling Effects of Profiling Activities: Mapping the Issues”. SSRN, 2019. Consultado enero 8, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379275. Como se citó en Herrera y Viollier, 2020 (p.215)

nocivos (Harris, 2020)⁵⁴. De aquí la común frase, “cuando el producto es gratis, tú eres el producto”. Para dimensionar esto, tengamos en cuenta la masividad de las aplicaciones con este modelo; a enero del 2021, Facebook cuenta con: 2.740 millones de usuarios activos; Instagram: 1.221 millones; TikTok: 689⁵⁵.

El asunto en cuestión tiene el potencial de remodelar las fuerzas del sistema económico y político. Por ello, Zuboff ha acuñado el concepto “capitalismo de vigilancia”⁵⁶ para referirse a lo que parece ser, en su opinión, la forma dominante de capitalismo de nuestra época; una evolución de la economía política caracterizada por la mercantilización de datos personales y su transformación como mercancía sujeta a la compraventa. Zuboff (2021) señala que: “El capitalismo descubrió que era posible capturar en secreto la experiencia humana privada y tratarla como materia prima gratuita para la traducción en datos de comportamiento -behavioral data- e inmediatamente, declararlos propiedad privada para vender predicciones de comportamiento”. [...] “Esto se traduce en un nuevo tipo de poder para dar forma, adiestrar, agrupar y modificar nuestro comportamiento individual y colectivamente a escala” [...] “todo esto de manera que no genera alerta a nuestra conciencia”⁵⁷.

⁵⁴ Esta conclusión es de Tristan Harris, la que ha dado en distintas charlas, pero en especial, en documental de Netflix “Social dilema” (2020). El asunto central de este documental es justamente el modelo económico que sostiene a las plataformas sociales gratuitas al público. Tristan Harris es científico informático y presidente cofundador de “Center for Humane Technology”, anteriormente, fue especialista en ética del diseño en Google.

⁵⁵Informe enero 2021 de “We Are Social” y “Hootsuite” <https://www.slideshare.net/DataReportal/digital-2021-global-overview-report-january-2021-v03> (p.93). Cabe mencionar que YouTube tiene 2.291 millones de usuarios activos, sin embargo, una parte menor, tiene una versión pagada.

⁵⁶El concepto “Capitalismo de vigilancia” fue popularizado el 2014 por la psicóloga social Shoshana Zuboff. Una conceptualización puede ser la siguiente: “sistema político económico dependiente de la mercantilización de datos personales y la transformación de información personal en una mercancía sujeta a la compraventa con fines de lucro para adecuar al sujeto y la producción.” (Zuboff da 8 acepciones al concepto en su libro en el acápite “definición”, y se ha referido al concepto de múltiples maneras en los últimos años; yo he intentado dar una síntesis)

⁵⁷ Shoshana Zuboff: We Need Rights to Protect Us from Big Data Surveillance | Amanpour and Company. (2021, 23 febrero). [Video]. YouTube. https://www.youtube.com/watch?v=D8qAGQQbZd0&ab_channel=AmanpourandCompany (min, 2:05)

Sea un nuevo capitalismo, o una reformulación del poder político para cumplir sus metas, la posibilidad de una vigilancia automatizada que reconoce y utiliza vulnerabilidades biopsicosociales para inducir el comportamiento, es un asunto complejo y de urgencia. Más si consideramos que la utilización de los datos personales y la inteligencia artificial para la predicción e inducción de los comportamientos humanos, es una capacidad sumamente rentable para intereses políticos y económicos.

“Es innegable la importancia económica que tiene el uso y análisis de datos para la economía digital —que hoy en día es una economía global transnacional—. También es innegable que la recolección masiva de datos personales, mediante internet y de dispositivos móviles, supone grandes riesgos para la sociedad y para los derechos humanos en la era digital. Así las cosas, resulta necesario regular de alguna forma la recolección, uso, análisis y tratamiento de datos personales que hacen las ‘empresas con modelos de negocios basados en datos’ (EMNBD) con el fin de salvaguardar los derechos a la protección de datos, a la privacidad y a la igualdad, entre otros” (Ospina-Celis y Upegui Mejí, 2020)⁵⁸

El perfilamiento y la personalización retórica del contenido presenta desafíos al modelo predominante de protección de datos en el mundo, en una parte importante, por lo ineficiente que ha sido ante brechas sistémicas frente a la tecnología. Por un lado, la velocidad, escala y forma en la que se tratan los datos, eluden fácilmente la fiscalización *ex ante* y *ex post*, “estamos tratando con un procesamiento de datos que tiene lugar en una escala enorme, de manera instantánea, ubicua y en una multitud de formas que eluden la observación humana” (Hildebrandt y Koops, 2010)⁵⁹. Por otro lado, debemos considerar el hecho de que los dispositivos y softwares son corrompibles, “de hecho, el objetivo de construir un sistema absolutamente seguro sería contrario a las leyes generales de la cibernética” (Kinis, 2018)⁶⁰; por lo que siempre la programación dará espacio a

⁵⁸ Ospina-Celis y Upegui Mejí. (2020) Festín de datos Empresas y datos personales en América Latina. Editorial Dejusticia, ISBN 978-958-5597-31-0 (p.6)

⁵⁹ Hildebrandt, M., & Koops, B. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428-460. doi:10.1111/j.1468-2230.2010.00806.x (p. 443)

⁶⁰ Kinis, Uldis (2018). «From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter-RVDP): The Latvian approach». *Computer Law & Security Review*, 34 (3): 508-522. Disponible en bit.ly/2MfgZ34. (p.510) Anteriormente, Kinis

vulnerabilidades de software. Finalmente, dentro de las dificultades destaca que, hacer un perfilamiento relativamente certero no requiere de muchos datos, y el poder de procesamiento para teorizar la acción retórica no requiere estar en el dispositivo; basta que se capten unos cuantos comportamientos y se tenga conexión a internet para que desde el servidor se concluya que hacer.

Como veremos en este trabajo, por antijurídico que sea, vivimos un escenario sin coto a una perjudicial afectación a la integridad del ser humano, sin embargo, la existencia de políticas y leyes de protección de datos personales. La personalización retórica del ambiente digital es un poder que existe en el mercado pese a lo corrosivo que puede llegar a ser “influir y dar forma a la experimentalidad y esencia misma de lo que significa ser humano” (Croft, 2020)⁶¹, pues no hay respuesta persecutoria, protectora y reparadora, efectivamente garantizada.

De hecho, como afirma Jijena (2020) respecto a la protección de datos personales en Chile, “hoy se está conteste que por sus errores de forma y de fondo poco y nada protege⁶²”. Esta situación es sumamente palpable en nuestro país, en buena parte porque, la protección recae en la autogestión del ciudadano común y no existe autoridad de control, pese a ser un compromiso con la OCDE y “uno de los consensos que existe en materia de protección de datos” (Álvarez , 2016)⁶³. Pero igualmente, el mundo no se encuentra en una situación muy distinta frente a las brechas sistémicas que tiene la regulación frente a la tecnología. Pareciera

citando a Oriola, ‘Bugs for sale: Legal and ethical proprietaries of the market in software vulnerabilities. (p.8) comenta que, “las vulnerabilidades del software se han definido como “errores inherentes o errores en el diseño, la especificación y la programación del software”.

⁶¹ Esta imagen, sobre el impacto en la experimentalidad de la tecnología y la inteligencia artificial en el significado de ser humano, es de Steven Croft, clérigo que ha tenido larga trayectoria discutiendo el impacto de los medios digitales en el espíritu. En particular, he seguido; The Ethics of Artificial Intelligence | Rt. Revd. Dr. Steven Croft | Stories of Impact. (2020, 13 julio). [Video]. YouTube. <https://www.youtube.com/watch?v=O6oa2kQxvRs&t=323s> [min0:40]

⁶² Jijena, Renato. Contenido y alcances del derecho fundamental a la protección de datos personales en la constitución de 1980. Tesina de Magister. 2020

⁶³ Álvarez Valenzuela, D. (2016). Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos? Revista de derecho (Coquimbo), 23(1), 51-79. <https://doi.org/10.4067/s0718-97532016000100003>.(p.56)

que “reglas legales escritas que no pueden adecuadamente hacer frente a la infraestructura tecnológica proactiva y omnipresente en tiempo real” (Hildebrandt y Koops, 2010)⁶⁴.

El desafío no es simple y no podemos quedarnos de brazos cruzados. A todas luces, sin un efectivo control, el abuso de este poder puede resultar catastrófico. Urge que este asunto sea controvertido en el derecho a fin de plantear regular el abuso de esta nueva capacidad. A fin de cuentas, el futuro no será una distopía si comenzamos a tratar seriamente los problemas que plantea la progresión de nuestro escenario. Este trabajo procura ir en esta dirección.

⁶⁴ Hildebrandt, M., & Koops, B. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428-460. doi:10.1111/j.1468-2230.2010.00806.x (p. 443)

EL CONTEXTO DE LA TECNOLOGÍA Y LA REVOLUCIÓN DE LA INDUSTRIA

La capacidad tecnológica actual permite una nueva clase de persuasión. Esta requiere, captar datos personales, detectar patrones complejos en enormes volúmenes de información, perfilar seres humanos y deducir sus vulnerabilidades -cognitivas o afectivas- para personalizar retóricamente el contenido. Esta capacidad técnica constituye un disruptivo poder que solo en los últimos años ha sido posible de ejercer, pues requiere de ciertos progresos que son propios de la cuarta revolución industrial.

Para dimensionar el problema, es importante comprender el contexto y tener una noción de los elementos técnicos que permiten esta nueva capacidad. Por ello, en los siguientes títulos trataremos de 'situar' la capacidad tecnológica describiendo brevemente: tres aspectos materiales, el poder de cómputo, la masividad y la interconectividad de los dispositivos inteligentes; y una visión de la revolución industrial en curso.

TRES ASPECTOS MATERIALES: MASIVIDAD, CAPACIDAD DE CÓMPUTO Y CONECTIVIDAD.

La revolución industrial generó condiciones nunca vistas, eso es indudable. En nuestros al menos 315.000 años como especie⁶⁵, los últimos 200 años han implicado un cambio radical

⁶⁵ Durante el año 2017, la comunidad científica cifro a 315.000 la data de los fósiles Sapiens más antiguos encontrados. Fuente online: Nature News. Hublin, J. (2017, 7 junio). Oldest Homo sapiens fossil claim rewrites our species' history. <https://www.nature.com/news/oldest-homo-sapiens-fossil-claim-rewrites-our-species-history-1.22114> (En línea octubre 2020). Revista: Nature 546, 289–292 (2017) Hublin, J., Ben-Ncer, A., Bailey, S. et al. new fossils from Jebel Irhoud, Morocco, and the pan-African origin of Homo sapiens. <https://doi.org/10.1038/nature22336>

importante⁶⁶. Durante estos años sucede la revolución industrial e inicia a una nueva era en la relación progresiva del ser humano con la técnica. Esta situación no se ha detenido, por el contrario, se agudiza y continúa generando condiciones nuevas en toda la humanidad⁶⁷, en particular con las tecnologías de la información y comunicación (TIC).

Capacidad de cómputo al alcance

En muchos lugares históricamente desolados por la pobreza, veremos hoy en las manos de cualquiera una tecnología con mayor capacidad que aquella que hace unos pocos años tenían los lugares más desarrollados. De forma notoria, ha aumentado el acceso a la tecnología a la vez que ha incrementado su potencia.

El incremento en la potencia de cómputo ha sido resultado, principalmente, por la satisfacción de la llamada “Ley de Moore”. Ley que expresa que cada dos años se duplica el número de transistores en un microprocesador, aumentando con esto la capacidad de cómputo. Desde la patente del primer circuito integrado con 6 transistores (1951), el progreso ha llevado a que hoy contemos con chips de millones y millones de transistores. Es gracias a las mejoras exponenciales en la capacidad de cómputo que los dispositivos electrónicos pueden tener el apelativo Smart o inteligente, pues operan softwares que demandan gran capacidad de cómputo.

El poder de procesamiento, o de cómputo, es que haya un mayor número de transistores, (interruptores lógicos) que permiten un estado ON/OFF que puede ser traducidos a código binario. Son, a grandes rasgos, los que permiten procesar los datos y mantener todo el mundo digital que existe.

⁶⁶ El desarrollo de la industria ha implicado un cambio gigantesco. “En materia económica, desde la primera revolución industrial, el ingreso real promedio por persona en las economías de la OCDE ha aumentado alrededor de 2.900%” (McCloskey, 2016).

⁶⁷ Así mismo, el ‘salir del subdesarrollo’ es un hecho masivo que ha sumado a millones en las últimas décadas. De hecho, entre los años 2000 y 2012, la tasa de pobreza en el mundo se redujo a la mitad, siendo el período de desarrollo económico más rápido de toda la historia. (Altraide, 2019, p.192)

En gran parte, el desarrollo tecnológico se ha logrado por esta proeza de la ingeniería que no ha tenido otro impulso más que las fuerzas del mercado, la Ley de Moore es solo una situación de facto.

Interconectividad

A la capacidad de cómputo que se ha masificado en los últimos años, debemos sumar la conectividad a Internet. En especial, el acceso que ha incrementado gracias a los *Smartphones* y otros *Smartdivices*.

En Chile, el acceso a Internet en el hogar pasó de 60,4% en 2012, a más de un 90% en diciembre del 2018⁶⁸, principalmente por el acceso vía teléfonos inteligentes. A esa fecha el 79,2% del total del acceso a internet en Chile es a través de un smartphone⁶⁹. Por otro lado, según Subtel 2018, 84,8% de los accesos a Internet son por uso de red de datos móviles (uso de señal 3G+4G); y de este total, un 93,4% corresponde a navegación por smartphones⁷⁰.

El acceso a internet nivel mundial ha aumentado igualmente. A finales del 2017, un 47% de la población mundial tenía acceso a internet, mientras que a junio del 2018, el 55,1%⁷¹. Para diciembre del 2020, el acceso mundial a internet era de un 64.2%⁷².

Esta nueva interconexión ha permitido comunicar y generar datos a gran escala. Gracias a internet, las aplicaciones, las redes sociales, los datos generados por los sensores integrados, ha sido posible crear enormes volúmenes de datos y millones de interacciones en un mundo digital que crece a ritmos acelerados.

⁶⁸ Fuente; Estudios SUBTEL. Online: <https://www.subtel.gob.cl/estudios/internet-y-sociedad-de-la-informacion/>

⁶⁹ SUBTEL. (2018). Informe Anual del Sector Telecomunicaciones 2018. [://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf](https://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf)

⁷⁰ Ibid.

⁷¹ Estadística de internet World stats, la cual concluye la información según el números demográfico declarado por de la United Nations Population Division y la información sobre el uso de Internet proviene de los datos publicados por Nielsen Online, por la International Telecommunications Union y por GfK.

⁷² Siguiendo la estadística de Internet World Stats, son 5,053,900,000 personas. <https://www.internetworldstats.com/stats.htm> (Consultado, abril 2021)

La capacidad e interconectividad masiva que han brindado los dispositivos inteligentes, permite que lo digital cruce cualquier aspecto de la vida. Comunicar, informar, registrar, aprender, procesar es diferente.

Los computadores han hecho lo imposible posible y la forma con la que nos relacionamos con el mundo está cambiando gracias a los dispositivos móviles inteligentes o computadores de bolsillo. En nuestros días, y desde hace unos años ya, es prudente aceptar la reinención del teléfono celular como operador o computador de enorme capacidad. Después de todo, la RAE define “computador” como: “Máquina electrónica capaz de realizar un tratamiento automático de la información y de resolver con gran rapidez problemas matemáticos y lógicos mediante programas informáticos”. Como vemos, podemos afirmar que los computadores en esta época llevaron – al menos en la forma de un Smartphone- a la capacidad de cómputo, el acceso al conocimiento, y a la comunidad global a nivel masivo.

Estos cambios han creado una era donde lo digital es primordial no tan solo para nuestra economía, sino que se ha incorporado en nuestras formas de vida. Son hoy millones los seres humanos los que interactuamos con un objeto inteligente de forma diaria. A octubre 2020⁷³, aproximadamente 5.224.582.000 individuos en el mundo tienen al menos un teléfono móvil activo, los cuales, en su inmensa mayoría, no tienen más de 3 años de antigüedad.

Esta situación evidencia que la humanidad, en un grueso importante, se informa, comunica y trabaja con estos aparatos que median aspectos cruciales de la vida. Por lo mismo, de forma constante, información sobre conductas humanas es registrado y compartido; y en esto, parece estar buena parte de la humanidad.

Evaluando la conectividad, capacidad de cómputo y masividad, ya para el 2012, más de 2.5 quintillones de bytes eran creados cada día⁷⁴, cuando solo accedían a la red 2.8 mil millones de usuarios alrededor del globo⁷⁵.

⁷³Esta cifra es brindada por “GSMA Intelligence”, empresa dedicada al aporte de información sobre los cambios en la industria de la telefonía móvil. En el vínculo se podrá observar una actualización diaria de la cifra. Online <https://www.gsmainelligence.com/data/> [Consultado: octubre 2020]

⁷⁴ Fuente: IBM <https://developer.ibm.com/es/articles/que-es-big-data/> (Consultado, abril 2021)

La digitalización de nuestra vida es un fenómeno común, que ha sido impulsado por una serie de desarrollos tecnológicos que se amplifican y refuerzan entre sí. Similarmente a lo expuesto, Fenwick & Vermeulen (2019)⁷⁶, propone que los desarrollos más importantes para la digitalización como tendencia de esta era han sido: I) El *hardware* digital más barato y pequeño; II) Redes de comunicación global y conectividad masiva (Internet); III) Almacenamiento de datos basado en la nube; IV) Las tecnologías digitales emergentes.

En este contexto, desde la década de 2010, esta época contiene en sí características suficientemente disruptivas en relación con las anteriores revoluciones industriales⁷⁷ como para plantear que nos encontramos en una revolución diferente. En efecto, las potencialidades que han surgido entre los avances disponibles nos hacen presumir que vivimos los albores de la cuarta revolución industrial.

⁷⁵ Fuente: Domo.com En línea: <https://www.domo.com/learn/data-never-sleeps-6> (Consultado, abril 2021)

⁷⁶ Fenwick, Mark & Vermeulen, Erik. (2019). The Lawyer of the Future as “Transaction Engineer”: Digital Technologies and the Disruption of the Legal Profession. DOI: 10.1007/978-981-13-6086-2_10

⁷⁷ Generalmente se clasifican tres revoluciones industriales:

1.- La primera revolución industrial; se identifica con la transformación de muchas sociedades agrarias, en industriales, mecanizadas y urbanas, por el disruptivo desarrollo de la máquina del vapor. Podemos fijar el inicio de esta revolución en Inglaterra, temporalmente en el año 1800, cuando expira la patente de la primera máquina a vapor desarrollada en 1712 por Thomas Newcomen. Esta fase llevó a una fuerte reducción en los costos de transporte y producción, cambiando de forma absoluta el panorama con la aparición de grandes ciudades.

2.- La segunda revolución industrial; se caracteriza por el crecimiento de industrias preexistentes, las cuales se expanden junto a la introducción del acero, el hormigón armado, el petróleo, la electricidad y la producción en serie. Este periodo verá la aparición de maquinarias como el automóvil, el avión, la radio y la televisión. Podemos datar los inicios de la segunda revolución industrial entre los años 1856 y 1870.

3.- La Tercera revolución industrial; es la llamada “Era de la Información” o de la “Sociedad de la información”, se caracteriza por un flujo de trabajo sin precedentes. En esta era aparece el computador personal, la internet, la comunicación satelital y las tecnologías de la información y comunicaciones. La revolución se data generalmente en 1980, siendo sus principales exponentes la URSS, Japón y EE. UU

BREVE INTRODUCCION A LA IDEA DE CUARTA REVOLUCIÓN INDUSTRIAL DE KLAUS SCHWAB

La cuarta revolución industrial es un concepto acuñado por Klaus Schwab⁷⁸, fundador y actualmente⁷⁹ “Executive Chairman” (CEO) en “World Economic Forum”⁸⁰, para referir a una nueva forma de progresión del estado evolutivo de la industria, suficientemente distinto a los anteriores por el nivel de interconectividad y lo enormemente potenciada por sistemas inteligentes.

Schwab (2018) señala que: “la Cuarta Revolución Industrial es una forma de describir un conjunto de inminentes transformaciones en curso en los sistemas que nos rodean [...] impulsadas por la creciente disponibilidad e interacción de las tecnologías emergentes [...] construidas sobre el conocimiento y los sistemas de revoluciones industriales anteriores, en particular, de las capacidades digitales de la tercera revolución industrial.”⁸¹

Dada la naturaleza de la transformación, que se basa en la masividad de la capacidad de cómputo interconectada existente, como señala Schwab, esta revolución destacaría sobre las demás, por ser la más rápida llegar a implementarse a una escala global. Esto, dado que las transformaciones de la ingeniería de datos pueden tener un impacto directo e inmediato.

Hay tres razones que sostienen la convicción de Schwab para afirmar que una cuarta y distinta revolución está en marcha:

“**Velocidad**”: Al contrario que las anteriores revoluciones industriales, esta está evolucionando a un ritmo exponencial, más que lineal. Este es el resultado del mundo polifacético y profundamente interconectado en que vivimos, y del hecho de que la nueva

⁷⁸ Klaus Martin Schwab, es Doctor en Economía por la Universidad de Fribourg; Doctor en Ingeniería por la ETH Zurich (Instituto Federal Suizo de Tecnología); Máster en Administración Pública por la escuela de gobierno John F. Kennedy en la Universidad de Harvard. Igualmente, he recibido más de una docena de Doctorados Honoríficos en diversas Universidades del Mundo.

⁷⁹ A la fecha de abril del año 2021.

⁸⁰ Sitio web de World Economic Forum. Enlace a estructura de liderazgo y de gobierno <https://es.weforum.org/about/leadership-and-governance> -visita el 22 de junio 2020-

⁸¹ Klaus, Davis, N., & Nadella, S. (2018). Shaping the Future of the Fourth Industrial Revolution. (p.19) [Traducción propia]

tecnología engendra, a su vez, tecnología más nueva y poderosa. **‘Amplitud y profundidad’**: Se basa en la revolución digital y combina múltiples tecnologías que están llevando a cambios de paradigma sin precedentes en la economía, los negocios, la sociedad y las personas. No solo está cambiando el «qué» y el «cómo» hacer las cosas, sino el «quiénes somos». **‘Impacto de los sistemas’**: Se trata de la transformación de sistemas complejos entre (y dentro de) los países, las empresas, las industrias y la sociedad en su conjunto.”⁸²

En la idea de Schwab, si bien las tecnologías de la cuarta revolución industrial requieren y se basan en las capacidades y redes digitales creadas por la tercera revolución industrial, cuales a su vez se basan en el desarrollo de la electricidad dado en la segunda revolución, vivimos los albores de una cuarta por el aparecer de capacidades suficientemente distintas.

La capacidad que han demostrado los algoritmos para aprender tiene un potencial transformador que va más allá de lo que ha mostrado la computación digital, cual hemos visto desarrollar desde la década de los sesenta. Por esto, Schwab (2018) afirma que: “En el futuro tendrá poco sentido pensar en algoritmos que aprendan independientemente de los datos no estructurados como meras aplicaciones de la potencia de la computación digital”⁸³.

La capacidad que han demostrado los modelos de *Machine learning* -aprendizaje automático- si bien, emerge de la tercera revolución industrial, es una disrupción que lleva a nuevas fronteras; dotando al presente de las características de una revolución, en particular, por la velocidad en la que se desarrollan nuevas y más poderosas tecnologías, por la profundidad del cambio en la experimentalidad humana, y las repercusiones en los sistemas políticos, económicos y sociales.

El inicio de la nueva revolución industrial ocurre cuando la actual generación de “redes neuronales” comienza a tomar verdaderamente fuerza dentro de la rama de “*Computer Science*”, gracias al exponencial crecimiento de la capacidad de procesamiento que ha

⁸² Schwab, K. (2016). La Cuarta Revolución Industrial (1ra edición). Penguin Random House Grupo Editorial. (Introducción)

⁸³ Cito y parafraseo a Klaus, Davis, N., & Nadella, S. (2018). Shaping the Future of the Fourth Industrial Revolution. (p.37 y 39)

satisfecho la *Ley de Moore*⁸⁴, pues permitió la aplicación de un modelo informático creado en 1943 denominado lógica umbral⁸⁵. Las redes neuronales son el pilar fundamental de los modelos de *Machine learning* que permiten los avances más significativos en el campo de la inteligencia artificial. Es por ello que se puede señalar que, una vez tenido el poder de cómputo para aplicar estos modelos informáticos, se abre la puerta a una nueva revolución y la transformación en las formas de vida humana.

Con esta capacidad revolucionaria, afirma Schwab, “la cuarta revolución industrial dará lugar a ecosistemas de creación de valor que son imposibles de imaginar con una mentalidad atascada en la tercera Revolución Industrial [...] (pues, las tecnologías) se ampliarán exponencialmente, emergerán físicamente y se integrarán en nuestras vidas [...] mucho más rápidamente que las revoluciones anteriores, ya que estas pueden construir y difundirse en las redes digitales de la Tercera Revolución Industrial.”⁸⁶

La conceptualización del exponencial ritmo acelerado que puede vivir la industria como una nueva “revolución industrial”, cobra aún más sentido -siguiendo a Schwab-, si consideramos que, hoy dada la capacidad técnica, existe la posibilidad de incrementar la productividad, calidad y capacidad de la tecnología como nunca en la historia dada la interrelación del avance de la ciencia de los datos junto a elementos físicos, digitales y biológicos⁸⁷.

Como vemos, el progreso tecnológico que implica la idea de la cuarta revolución industrial habla más que de pintorescas técnicas; estos representan cambios radicales en la

⁸⁴ Gordon Moore en 1965 acuñó la Ley de Moore, cual afirma que el número de transistores por unidad de superficie en circuitos integrados se duplicaría cada año, y aunque, posteriormente amplió el periodo a dos años, su ley se ha corroborado empíricamente con la aceleración que ha podido corroborar el mundo desde su afirmación.

⁸⁵ McCulloch, Warren; Walter Pitts (1943). «A Logical Calculus of Ideas Immanent in Nervous Activity». *Bulletin of Mathematical Biophysics* 5 (4): 115-133. doi:10.1007/BF02478259.

⁸⁶ *ibid.* Klaus, Davis, N., & Nadella, S. (2018) (p 39). El entre paréntesis es mío.

⁸⁷ Schwab, en su libro “la cuarta Revolución Industrial” (2016), define como pilares de esta revolución la interrelación de los siguientes elementos físicos, digitales y biológicos: a) Físicos: a.1 vehículos autónomos; a.2 impresión 3D; a.3 robótica avanzada; a.4 nuevos materiales – de composición y formato -. b) Digitales: b.1 El internet de las cosas IOT b.2 blockchain b.3 la potencia de cómputo y el análisis de datos. c) Biológicos: c.1 ingeniería genética c.2 bioimpresión -producir tejidos vivos- c.3 Nuevos métodos de biomonitorio c.4 neurotecnología

forma de vida humana. Es más, la revolución en curso tiene una exponencialidad y alcance nunca visto en la historia. De todas formas, ¿Quién mirando el pasado podría objetar la relevancia del impacto que implicó cada una de las transformaciones que caracterizaron cada revolución industrial en las formas de vida humana y en la subjetividad de los individuos? es fundamental reconocer la gravedad y la influencia transversal de una nueva revolución, y pensar la relación que tenemos frente a la tecnología.

La Cuarta revolución industrial es inevitable y debemos pensar los alcances del poder creado. La revolución que se avecina, sabemos de dónde viene, pero no exactamente a dónde va. Dependerá de las fuerzas que disputen el poder creado.

EXPONER EL FENOMENO Y NUESTRA PROTECCIÓN

El estado de la tecnología ha alcanzado un nivel de masividad, capacidad de cómputo e interconectividad sin precedentes, generando situaciones conflictivas a medida que las tecnologías de tratamiento de datos han mejorado; toda vez que – como veremos- la regulación sobre tratamiento de datos y protección de datos personales se ve sobrepasada y no logra ser una herramienta eficaz ante los riesgos de un tratamiento ilegítimo. Esto entre otras cosas, por las dificultades para percatarse de un tratamiento ilegítimo o la incapacidad del sistema judicial para amparar una vulneración. Como señala Hildebrandt (2016), las vulneraciones “son en su mayoría invisibles, no tenemos manera de impugnarlos. [...] La impugnación de los defectos tecnológicos que regulan nuestras vidas puede ser imposible, porque a menudo son invisibles y porque la mayoría del tiempo no hay jurisdicción ni tribunal.”⁸⁸

En este contexto, la personalización retórica artificial es un poder que surge. Esto, como consecuencia de que nuestra vida ocurra cada vez más mediada por los dispositivos inteligentes, y las experiencias comerciales, informativas y parte de la vida personal, pueda ser registrada y personalizada. En este sentido, Susser, et al. (2019), señalan que hoy, “el entorno en sí se convierte en la interfaz, infundido con tecnologías de sensores, sistemas de identificación [...] (para) inferir las preferencias de una persona a partir de sus comportamientos legibles, registrado por un conjunto de tecnologías invisibles, almacenado

⁸⁸ Hildebrandt, M. (2016). Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. (p.12).

en grandes bases de datos y extraído mediante técnicas matemáticas que permitan la detección de patrones relevantes”⁸⁹.

He aquí nuestro problema. La producción, captación y tratamiento masivo de datos personales, permiten el entrenamiento de algoritmos complejos en constante perfeccionamiento, para la reacción inteligente del ambiente digital con un propósito determinado; como el ejercicio de la retórica.

No por nada el asunto convoca cada vez más preocupación. Tal como afirma Susser et al. (2019), “los estudiosos de la privacidad y la vigilancia se preocupan cada vez más de que los recolectores de datos puedan usar la información que recopilan sobre nuestros comportamientos, preferencias, intereses, ingresos, etc. para manipularnos”⁹⁰. ¿Cómo no despertar preocupación? El cruce entre el avance tecnológico y la naturaleza humana deja a toda la especie envuelta en un capital dilema⁹¹.

Ya buena parte de lo que vemos en el ambiente digital reacciona de acuerdo con el comportamiento que es observado; organizando, modificando, y censurando el contenido de forma automatizada; ya que el ambiente se adecúa para satisfacer objetivos. Esto no es un fenómeno del todo reciente, solo se ha perfeccionado de forma exponencial en los últimos años.

⁸⁹ Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428–460. <https://doi.org/10.1111/j.1468-2230.2010.00806.x> (p.430)

⁹⁰Susser. Et al. (2019). (p.2)

Adjuntamos la nota al pie que acompaña al texto original, a forma de posible hoja de ruta para quien quiera investigar:

“Por ejemplo, Tal Zarsky ofrece una discusión inicial del problema en in “Privacy and Technologies of Identity: A Cross disciplinary conversation” (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006). Frank Pasquale lo señala a lo largo de su libro, “The Black Box Society: The Secret Algorithms That Control Money and Information” (2015). Frederic Zuiderveen Borgesius proporciona un tratamiento útil de las preguntas de manipulación, especialmente en lo que se refiere a la ley europea de privacidad en “Improving Privacy Protection In The Area Of Behavioural Targeting (2015)”. El tratamiento de mayor alcance es la discusión de Ryan Calo sobre manipulación del mercado digital y leyes de protección al consumidor en “digital market manipulation” (2014).”

⁹¹ Este es un guiño a la mentada película de Netflix “Social dilema” (2020), cual a su vez utiliza el término “dilema” en guiño al documental de la PBS “Facebook dilema” (2018), ambos contenidos cuales han popularizado parte de lo que nos inquieta este escrito. No está de más señalar que esta Tesis comenzó a escribirse a finales del 2016.

En este sentido, como señala Hildebrandt. (2016), respecto de la invención de las cookies por Netscape en 1990. “Estas (las *Cookies*) fueron inventadas con el propósito de facilitar transacciones comerciales virtuales entre una tienda virtual y el consumidor. Al final, facilitó el rastreo y búsqueda de los registros que los usuarios de la internet hacían en cada una de sus visitas, permitiendo a los algoritmos que analizaban tal información personalizar los resultados de las búsquedas, las páginas web, las estrategias de precios y noticias. Hoy *Cookies* de hecho regulan nuestro ambiente virtual, creando y señalando formas nuevas de interacción y control; a pesar de sus inmensas implicaciones en la adaptación subliminal del mundo virtual, nunca tuvimos el chance de votar por esto [...] Se utilizan *Cookies* de seguimiento para medir los comportamientos del flujo de clics de sus visitantes, pueden utilizar análisis para medir la influencia de diferentes configuraciones de su plataforma. Esto incluso puede incluir el envío de mensajes falsos a sus usuarios para medir el impacto positivo o feeds negativos.”⁹²

Existen algoritmos que regulan los tipos de discursos que podemos encontrar en la web, algoritmos que deciden qué tipo contenido ver; sea buscando ganancias económicas o ideologías. Existen sesgos generados por privilegiar contenido sobre otros, siempre cuando se adecua el escenario.

Con la capacidad de detección y reacción del ambiente digital, hemos hecho posible la mediación interesada del ambiente en el que se desenvuelve el usuario mediante el perfilamiento y la personalización retórica del contenido en del ambiente digital.

Por ello, como señalan Büchi et al. (2019), “el perfil virtual de una persona física, creado por una ‘empresas con modelos de negocios basados en datos’ (EMNBD), suele ser empleado para determinar los servicios a los que tiene acceso y los productos que puede adquirir, o para incidir en los derechos que le son garantizados, en la información que se le muestra, y en la decisión de ser objeto o no de vigilancia activa”⁹³.

⁹² Hildebrandt, M. (2016). *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Edward Elgar Pub. (p.12)

⁹³ Ospina-Celis y Upegui Mejí. (2020) EMNBD y protección de datos personales en Brasil, Chile, Colombia y México: la experiencia común.

En el mismo sentido, Ospina-Celis y Upegui Mejí. (2020) señalan que, “el perfilamiento se realiza, usualmente, con fines comerciales, como ofrecer publicidad dirigida de acuerdo con los gustos de cada quien. Pero sus usos se pueden diversificar para avanzar distintas agendas ideológicas, políticas, religiosas o comerciales. Las prácticas de perfilamiento pueden causar discriminación —en tanto solo se le ofrece un cierto contenido a solo cierto tipo de personas—, pueden también afectar los derechos de libertad —mediante la inducción a realizar ciertas conductas y a modificar el comportamiento en la web— y pueden tener otros impactos, todavía no suficientemente explorados, sobre el comportamiento de las personas y los derechos humanos.”⁹⁴

Como vemos, con el riesgo creado por el avance tecnológico, procesos artificiales que subyacen a la cotidianidad de millones de usuarios transmutan la realidad actual, y en espacios inéditos de poder, se desafían nuestras instituciones, y aún más, nuestra integridad como seres humanos. En línea con esto, Zuboff (2020), de una forma metafórica expresa, “el titiritero que mueve los hilos del omnipresente aparato digital impone su voluntad a través de este. Este Gran Otro, sensitivo, computacional y conectado, transfiere, convierte, monitoriza, computa y modifica la conducta humana.”⁹⁵

No olvidemos que en el ambiente digital, la comunicación, la socialización, la navegación web, las compras online, la reproducción de contenido audiovisual, el trabajo, el juego, etc. son espacio para la captación de datos personales. Con ello es posible generar un perfil con el cual decidir como personalizar retóricamente el contenido. Siendo así, ya sea mediante el quiebre el sistema -Hack- o por provecho de quienes controlan una plataforma, este es un poder latente. Después de todo, la captación de datos y el quiebre del sistema es siempre una posibilidad, “la tecnología actual de diseño y creación de sistemas informáticos

⁹⁴ Ospina-Celis y Upegui Mejí. (2020) Festín de datos Empresas y datos personales en América Latina. Editorial Dejusticia, ISBN 978-958-5597-31-0 (p.15)

⁹⁵ Zuboff, S. (2020). La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder. Ediciones Paidós. (Capítulo 13 El gran otro y el auge del poder instrumental. p.531)

no ha logrado producir sistemas seguros desde su origen, como ha sido ampliamente documentado en la literatura científica” (Álvarez y Hevia, 2020)⁹⁶.

PRIMERAS EVIDENCIAS EXPERIMENTALES, EL EXPERIMENTO MANIPULATORIO PÚBLICO DE FACEBOOK.

A continuación, destacando uno de los problemas principales de la protección de datos personales, ‘el consentimiento para el tratamiento de datos’; trataremos un famoso experimento que prueba la existencia del poder de inducción que nos preocupa.

En la semana del 11 al 18 de enero de 2012, ocurre una de las primeras pruebas publicadas de la manipulación digital a gran escala. Nos referimos al experimento social psicológico de Facebook llevado a cabo por “*The Core Data Science Team, Facebook*” & “*Departments of Communication and Information Science, Cornell University*”; donde Facebook probó que podía controlar el estado de ánimo de las personas filtrando el contenido que veían de forma automatizada a través de un algoritmo que interpretaba, detectaba y filtraba el contenido emotivo en las palabras utilizadas. En el experimento, Facebook creó un entorno que privilegió cierto contenido sobre otro, con el fin de probar la efectividad de la psicoingeniería del algoritmo que no debía levantar sospecha en los usuarios.

El artículo “*Experimental evidence of massive-scale emotional contagion through social networks*⁹⁷”, publicado el 2014, revela los resultados del experimento social que involucró a 689.003 personas de distintas edades y países que usaban Facebook en inglés. A ellos, por una semana, se les ajustó sus “*News Feed*” -bandeja de noticias- con el objeto de llevar a un grupo de control, de manera imperceptible, a una emotividad “positiva” y otra “negativa”.

⁹⁶Álvarez-Valenzuela, D., & Hevia Angulo, A. (2020). Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile. *Revista Chilena de Derecho y Tecnología*, 9(2), 1. <https://doi.org/10.5354/0719-2584.2020.60658>. Como se citó en referencia a Maurushat, 2013; Kinis, 2018.

⁹⁷ Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24), 8788-8790. <https://doi.org/10.1073/pnas.1320040111>

Esto lo realizó, reduciendo a un grupo el contenido de las publicaciones positivas de sus amigos, y al otro, reduciendo la exposición al contenido emocional negativo.

Aun siendo muy rudimentaria la tecnología utilizada (2012) para interpretar el contenido y exponerlo en momentos precisos, en comparación a la que disponemos hoy; los resultados fueron claros. Cuando terminó la semana de experimentación, los usuarios manipulados tenían más probabilidades de publicar palabras especialmente positivas o negativas⁹⁸. “Las personas expuestas a contenido más positivo tenían publicaciones que eran más positivas, y las expuestas a contenido más negativo tenían publicaciones que eran más negativas.”⁹⁹.

El artículo del estudio concluye: “aunque estos datos proporcionan, a nuestro entender, una de las primeras pruebas experimentales que respaldan las controvertidas afirmaciones de que las emociones pueden extenderse a través de una red, los efectos de las manipulaciones son pequeños [...] No obstante, [...] dada la escala masiva de las redes sociales como Facebook, incluso los pequeños efectos pueden tener grandes consecuencias agregadas”.¹⁰⁰

⁹⁸ Meyer, R. (2014, 28 julio). Everything We Know About Facebook’s Secret Mood-Manipulation Experiment. The Atlantic. <https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/> (consultada 20 de septiembre 2021)

⁹⁹ Conclusión del Profesor Daniel Solove en LinkedIn 30 de junio de 2014. <https://www.linkedin.com/pulse/20140630055215-2259773-the-facebook-psych-experiment-consent-privacy-and-manipulation/> (consulta: 2 de abril de 2021)

¹⁰⁰ Las afirmaciones de este párrafo están contenidas en el estudio en cuestión. Kramer, A. D., Guillory, J. E., & Hancock, J. T. (2014). Op cit. (p. 3). Literal: “Although these data provide, to our knowledge, some of the first experimental evidence to support the controversial claims that emotions can spread throughout a network, the effect sizes from the manipulations are small (as small as $d=0.001$). These Effects nonetheless matter given that the manipulation of the independent variable (presence of emotion in the News Feed) was minimal whereas the dependent variable (people’s emotional expressions) is difficult to influence given the range of daily experiences that influence mood. More importantly, given the massive scale of social networks such as Facebook, even small effects can have large, aggregated consequences”

Tengamos presente que solo se midió el efecto a través de las palabras utilizadas en Facebook, y desconocemos el impacto que ha tenido en los distintos aspectos de las vidas de quienes fueron manipulados.

EL DILEMA DEL CONSENTIMIENTO QUE RIGE LA UTILIZACIÓN DE NUESTROS DATOS

Una vez hecho público el experimento, los cuestionamientos en torno a la legalidad abundaron. Al respecto, *Cornell University*, se desligó de la responsabilidad aduciendo que los resultados fueron entregados por Facebook cuando este ya había realizado el experimento¹²⁰. Por su parte, Facebook esgrimió que la ley estadounidense no tiene una regulación aplicable para este tipo de estudios en humanos¹²¹ cuando es hecho por privados que no reciben dinero federal¹²², e igualmente afirmó, que los usuarios dieron su consentimiento al aceptar

¹²⁰ “Según un comunicado de prensa de la Universidad de Cornell, el profesor de Cornell, Jeffrey Hancock [...] solo tuvo acceso a los resultados, por lo que “la Junta de Revisión Institucional de la Universidad de Cornell concluyó que no estaba involucrado directamente en la investigación humana y que no se requería una revisión por parte del Programa de Protección de la Investigación Humana de Cornell”. Op cit. Meyer, R. (2014, 28 julio).

¹²¹ “La Regla Común federal y la ley de Maryland no fueron diseñadas para abordar la investigación realizada bajo estas circunstancias y ninguna de las autoridades que cita indica lo contrario”. Respuesta de Edward Palmieri, consejero general asociado de privacidad de Facebook. a James Grimmelmann, profesor de derecho de la Universidad de Maryland, quien señala incumplimiento de la normativa, Acceso a la carta de respuesta: <http://james.grimmelmann.net/files/legal/facebook/FacebookResponse.pdf> (consultada 20 de Septiembre 2021) Acceso a la “Regla común federal”: <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html> (consultada 20 de Septiembre 2021)

James Grimmelmann, afirma que: [...] “la denominada “regla común”, regula la investigación sobre personas en los Estados Unidos. Los detalles son complicados, la esencia simple. Si participa en una “investigación con sujetos humanos”, debe tener dos hojas de papel antes de comenzar. Necesita un formulario de consentimiento informado firmado por la persona con la que está experimentando y necesita la aprobación de un IRB (abreviatura de “junta de revisión institucional”).” En línea: <https://medium.com/@JamesGrimmelmann/illegal-unethical-and-mood-altering-8b93af772688>

¹²² Es discutible el alcance normativo a privados, la norma está diseñada para investigaciones hechas con fondos fiscales. “La Ley Nacional de Investigación -la llamada “regla común”- condujo a la creación

la política de uso de datos de la red social, cual incluye el uso de los datos personales para "investigación".

La cláusula a la que se refiere Facebook para validar el consentimiento, se encuentra en la política de datos que cada usuario debe aceptar para estar en la red. Esta, dentro de una larga y ambigua lista, establece que: "la información que recibimos sobre usted [...] puede utilizarse [...] para operaciones internas, incluida la resolución de problemas, análisis de datos, testeo, investigación y mejora del servicios"¹²³. Ante el revuelo y la acusación de ilegalidad, Facebook adujo que al ser el estudio un "testeo de producto", el consentimiento otorgado fue suficiente para obrar dentro de la legalidad.

Aun al 2021¹²⁴, existe una cláusula similar a aquella esgrimida en el año 2014 en los términos y condiciones de la red social más popular de internet¹²⁵. Asunto por lo menos inquietante -para esta red particularmente dinámica, interactiva, intrusiva e incisivamente personalizable-, si consideramos que el modelo de negocios de esta plataforma social gratuita -a los usuarios-, es vender una reacción rentable para los anunciantes. No desconsideremos que, "el modelo de negocio de Facebook gira entorno a la recolección y procesamiento de

de Juntas de Revisión Institucional (45 CFR parte 46) que tienen la responsabilidad de proteger a los seres humanos en cualquier investigación financiada con fondos federales." "El problema más importante es que el "consentimiento informado" tiene un significado legal específico. En 1974, el Congreso aprobó la "Ley Nacional de Investigación" en respuesta a experimentos de investigación en humanos abusivos, como el Experimento de sífilis de Tuskegee (1932-1972) y el Experimento de la prisión de Stanford (1971)". Ph.D. Padfield. (2018, 2 abril). Did Facebook's «Emotional Manipulation» Research Cross an Ethical Line? 1. <https://www.linkedin.com/pulse/did-facebooks-emotional-manipulation-research-cross-jon-padfield-phd/>

¹²³ Original:" the information we receive about you [...] may be used [...] for internal operations, including troubleshooting, data analysis, testing, research and service improvement". (consultada 20 de septiembre 2021)

¹²⁴ https://www.facebook.com/full_data_use_policy (Consulta 2 de abril del 2020). Aún el argumento esgrimido en el 2012 - fecha del experimento- y 2014 - fecha de la publicación del estudio- puede sostenerse de la política de datos que actualmente - febrero 2021 - Facebook establece para con sus usuarios. "Investigación y desarrollo de productos: usamos la información que tenemos para desarrollar, probar y mejorar nuestros Productos (incluso a través de encuestas e investigaciones), así como para probar y solucionar problemas de funciones y productos nuevos."

¹²⁵ Facebook cuenta con: 2.740 millones de usuarios activos; Instagram: 1.221 millones; Tik Tok: 689. Fuente: Informe enero 2021 de "We Are Social" y "Hootsuite" <https://www.slideshare.net/DataReportal/digital-2021-global-overview-report-january-2021-v03> (p.93)

datos personales (e incluso sensibles) para perfilar a sus usuarios y poder vender publicidad personalizada a sus clientes.”¹²⁶

¿Por qué el consentimiento es tan controversial?, pues, en materia de protección de datos personales, el consentimiento sumamente importante. Como señala Daniel Solove¹²⁷ (2013), “el consentimiento legitima casi cualquier tipo de recolección, uso¹²⁸ o divulgación de datos personales”¹²⁹; es “la forma básica de enfrentar la protección de la privacidad, cual se ha mantenido prácticamente inalterada desde la década de 1970”¹³⁰.

El consentimiento es el paradigma de protección de privacidad que rige, prácticamente, en todo el mundo. Otorgando consentimiento, “la mayoría de las formas de recolección, uso o divulgación de datos son aceptables [...] (Por ello) El consentimiento a menudo se convierte en una forma muy cómoda de lograr resultados sin confrontar los importantes valores en juego”¹³¹. Frente a todas las entidades que recolectan y utilizan datos personales, tanto en nuestro derecho, como en la Unión Europea y en EE. UU, el

¹²⁶ Herrera, Paloma y Pablo Viollier. (2020) Rendición de cuentas de Facebook y otros negocios en Chile: la protección de datos personales en la era digital. ISBN: 978-958-5597-32-7 (p.84)

¹²⁷ Daniel J. Solove, es Profesor en la Facultad de Derecho de la Universidad George Washington y el fundador de Teach Privacy, una empresa que brinda capacitación en privacidad y seguridad de datos a empresas, instituciones de salud, universidades y otras organizaciones. - Descripción adecuada, extraída de su LinkedIn. <https://www.linkedin.com/in/danielsolove/> -

¹²⁸ De todas formas, es posible sostener que en nuestro derecho no puede ser establecido en un contrato el consentimiento a ser manipulado a través de un tratamiento de datos. Por una parte, por qué la ley condiciona dicho tratamiento al cumplimiento de tres elementos: 1) el tratamiento debe realizarse de forma concordante con la ley, 2) para finalidades permitidas por el ordenamiento jurídico, y 3) siempre deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que la ley les reconoce (Viollier, 2017; p.20). Siendo así, la manipulación podría entenderse contraria a los elementos que permiten el tratamiento de datos.

Por otro lado, la buena fe objetiva podría impedir la validez de la cláusula aun contra texto expreso. Esto porque el artículo 1546 del código civil impone que: “los contratos deben ejecutarse de buena fe, y por consiguiente obligan no sólo a lo que en ellos se expresa, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por la ley o la costumbre pertenecen a ella”. Por lo tanto, por ir en contra del espíritu general de la legislación, la manipulación a través del tratamiento de datos no puede ser establecida en un contrato. De esta forma, es posible sostener que el consentimiento en materia de protección de datos no es legitimación absoluta en Chile.

¹²⁹ Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. (2013) (p.1880)

¹³⁰ Ibidem. Solove, 2013 (p.1881)

¹³¹ Op cit. Solove, 2013 (p.1903) El entre paréntesis es nuestro.

consentimiento de las personas corrientes es el principal -o único- resguardo de la protección de datos. Sin embargo, muchas veces no es posible generar un real consentimiento en el entorno digital y aun así, el consentimiento legitima prácticas vulneradoras.

El consentimiento es muchas veces ficcional. En este sentido, Pablo Viollier (2020) nos advierte que, “normalmente en estos contratos de adhesión (donde se otorga el consentimiento) hay asimetrías de poder e información, lo que se traduce en que nadie lee los términos y condiciones. No existe una real libertad en consentir sobre el otorgamiento de datos. Es más una pretensión ideológica ilusoria de libertad y autonomía de la voluntad que si uno quiere constatar en la práctica, no se puede ejercer.”¹³² Esto, entre otras cosas, porque “tomaría en promedio 201 horas al año leer todas las cláusulas que los usuarios de internet comúnmente aceptan (Mc Donald y Cranor, 2008); o porque, puede existir una barrera de idioma en los acuerdos; o, muchas veces el nivel de complejidad para entenderles es equivalente al grado de magíster (Beloniell y Becher, 2019)”¹³³.

Para las personas existen dificultades sistémicas en la aceptación del uso de sus datos por terceros. Así mismo, afirma Solve (2014), respecto del consentimiento otorgado por los usuarios del experimento comentado y del paradigma -que llama “autogestión de la privacidad”¹³⁴-. “Es pura ficción que una persona realmente acepte políticas como estas”; (ante una cláusula como la utilizada por Facebook, siquiera) “las personas pueden conocer todos

¹³² ídem. Pablo Viollier. (2020, 26 de marzo) Minuto 39:15.

¹³³ Así mismo, Pablo Viollier. (2020, 26 de marzo) en Clase 5 - Procesamiento de datos personales [Video]. YouTube. <https://www.youtube.com/watch?v=1Q3hWSnE9hw&list=PLUfm9vw9SqXUBEG7kPYD0YMlndEZysZxb&index=2> [Consultado el 10 de julio del 2020] 37:00.

¹³⁴ “Privacy self-management.” “Bajo el paradigma actual, la ley entrega a las personas un conjunto de derechos que les permiten tomar decisiones respecto a cómo gestionar sus datos. Estos derechos consisten básicamente en derechos de notificación, acceso y consentimiento, respecto a la recolección, uso y divulgación de datos personales. El objetivo de este conjunto de derechos es entregar a las personas el control respecto de sus datos personales, para que a través de este control puedan decidir por ellas mismas cómo determinar los costos y los beneficios de la recolección, uso y divulgación de su información. Me referiré a esta aproximación a la regulación de la privacidad como «autogestión de la privacidad».” Op cit. Solove, 2013 (Introducción p.1880)

los posibles usos futuros de sus datos potenciados con otros. No es posible evaluar los riesgos y beneficios”¹³⁵.

En la misma línea, Solove (2013) en “*Privacy self-management and the consent dilemma*”, señala “numerosos obstáculos en la autogestión de la privacidad”. Entre ellos que: “1) la gente no lee las políticas de privacidad; 2) si las leen, no las entienden; 3) si las leen y las entienden, usualmente carecen de los conocimientos y pericia necesarios para tomar una decisión informada; y 4) si las leen, entienden y pueden tomar una decisión informada, su decisión puede verse sesgada por varias dificultades producidas en el proceso de toma de decisiones (por la falsedad del modelo tradicional de agente racional).”¹³⁶

Como afirma Solove, “las personas no pueden manejar adecuadamente su propia privacidad, y el consentimiento no da un control significativo en muchos contextos relacionados con la privacidad¹³⁷”. Sin embargo, como hemos visto, el paradigma imperante presupone al hombre medio como soberano de su información, además de sujeto plenamente consciente y autónomo cuando dispone de sus datos. Claramente, nos encontramos lejos de un mecanismo de protección eficaz ante un abuso en materia de tratamiento de datos.

*

Habiéndonos aproximado a un caso preocupante de manipulación, a la vez que hemos introducido dilemas en “la forma básica de enfrentar la protección de la privacidad” que es “legitimación a casi cualquier tipo de recolección, uso o divulgación de datos personales” ¹³⁸ ; daremos paso a un análisis general breve de la legislación actual en Chile de la protección de datos.

¹³⁵ Daniel Solove en LinkedIn 30 de junio de 2014. <https://www.linkedin.com/pulse/20140630055215-2259773-the-facebook-psych-experiment-consent-privacy-and-manipulation/>

¹³⁶ Op cit. Solove, 2013 (p.1888). Lo paréntesis es nuestro y complementa el sentido dado por el autor en el texto.

¹³⁷ Ibid. Solove, 2013 (p.1894)

¹³⁸Ibid. Solove, 2013 (p.1881 y 1880)

LA SITUACION GENERAL DE LA PROTECCIÓN DE DATOS PERSONALES EN CHILE

Para tener una visión general del estado de la legislatura, sintetizaremos la protección vigente en Chile (2021) para la captación y tratamiento de datos. Esto es sumamente relevante, pues como veremos, permite el perfilamiento necesario para personalizar retóricamente el contenido.

Con este objeto, introduciremos los conceptos necesarios para entender como la ley presume proteger a los individuos, evaluando las herramientas de tutela de la Ley 19.628 para con los derechos ARCO. Al final del capítulo, trataremos el caso de una empresa chilena (InstaGIS), que se dedicaba a la rentabilización del tratamiento de datos para la generación de perfiles.

UN DERECHO EN LA CONSTITUCIÓN DEL 2021

Desde junio del 2018 con la publicación de la Ley 21.096, la protección de datos personales es un derecho fundamental de rango constitucional que se encuentra establecido en el Art. 19 N°4º de la Constitución Política de la República. Este precepto dicta:

“La Constitución asegura a todas las personas: [...] N°4º. El respeto y protección a la vida privada y a la honra de la persona y su familia, y, asimismo, [ahora se agrega] la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.”

Aun con tan importante declaración, lamentablemente, a tres años del vigor de la norma constitucional, no contamos con mayor contenido que nos ayude a identificar el mandato. A

abril del 2020¹³⁹, “no hay nueva literatura disponible desde la entrada en vigor de la reforma” (Álvarez, 2020)¹⁴⁰. Por ello, el principal desarrollo del derecho constitucional en Chile sobre la protección de datos personales, lo encontramos en lo relativo a la Ley 19.628 de 1999.

Esto además es dado porque, si bien se reconoce en la constitución el derecho fundamental a la ‘protección de los datos personales’, en la consagración existe una reserva legal. Esta excluye una regulación supra e infra legal, lo que implica que el contenido debe estar en una ley, ni más ni menos. La constitución manda que “el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley”.

Por lo mismo, en nuestra época, ante la gran capacidad de procesamiento de datos y el reconocimiento de patrones complejos en enormes volúmenes de información que caracteriza la revolución en curso, *hic et nunc*¹⁴¹, en Chile el marco legal que otorga la protección Constitucional se encuentra en “aquella ley cuyo ámbito material de aplicación es el tratamiento de datos de carácter personal en general, cualquiera sea la forma en que dicho tratamiento se lleve a cabo”(Viollier, 2017)¹⁴², es decir, la Ley 19.628 sobre Protección de la Vida Privada (LPVP).

Es cierto que la Constitución asegura la protección de los datos personales en Chile, y esto claramente es un avance significativo; en la práctica importa un principio interpretativo aplicable a todo el ordenamiento jurídico, porque incorpora este derecho dentro de la coherencia general del sistema que prevé la Ley Fundamental. Esto por la aplicación del principio de eficacia horizontal y vertical de los derechos fundamentales¹⁴³.

¹³⁹ Escasa literatura ha emergido en el intertanto, entre ellos, Pablo Contreras, 2020. Mas, nuestro punto sigue en pie, es escasa la elaboración doctrinal y el desarrollo del derecho constitucional a la protección de personales lo encontramos en lo relativo a la Ley 19.628 de 1999.

¹⁴⁰ Álvarez-Valenzuela, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena De Derecho Y Tecnología*, 9(1), 1. doi:10.5354/0719-2584.2020.57777

¹⁴¹ Locución latina que significa literalmente “aquí y ahora”. Se utiliza comúnmente para llamar la atención sobre la necesidad de pensar las cosas desde la realidad.

¹⁴² Viollier, P. & Derechos Digitales. (2017, febrero). El estado de la protección de datos personales en Chile. <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [Consultado: 10 junio 2020]. (p.17)

¹⁴³ El principio de eficacia horizontal de los derechos fundamentales se refiere a la dominancia de estos en las relaciones jurídicas entre los particulares; y el efecto vertical de los derechos fundamentales,

Sin embargo, como quedará en evidencia, el mecanismo determinado por ley para la protección de datos, parece a todas luces no establecer marcos eficaces al desarrollo tecnológico. Como menciona Garrido (2013), “el procedimiento de la ley chilena, no se condice con la realidad tecnológica actual, y más aún carga el peso de la prueba en el afectado”¹⁴⁴.

De todas formas, la eficacia ante un imperativo como el que la Constitución llama no es un asunto simple. La facilidad en la captación masiva, y a sí mismo en la capacidad de sistematización e interpretación de datos, es un desafío global presente y real, más aún cuando pareciera no existir una seguridad total que evite captar y tratar nuestros datos sin nuestro consentimiento, después de todo, “hackear un sistema, es una pelea constante entre detectar vulnerabilidades y parcharlas. (por ello) Más que si un sistema puede ser vulnerado o no, es un asunto de cuántos recursos requiere para ser vulnerado” (Viollier, 2020)¹⁴⁵.

LA LEY DE PROTECCIÓN DE DATOS PERSONALES

Para empezar, y antes de tratar las ideas centrales de la ley, es necesario explicitar que la Ley 19.628 no establece un marco robusto para la protección de los datos personales de los titulares. Hoy existe un consenso entre los expertos, la academia y la sociedad civil en torno a la falta de adecuación de la ley para una efectiva protección de los datos personales¹⁴⁶. Entre otras razones porque: “la ley es una norma que fue redactada con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el

para con las relaciones jurídicas entre el Estado o alguno de sus órganos y de estos con los particulares. (Marshal Barberán, 2010; ISSN 0718-5200)

¹⁴⁴ Garrido Iglesias, R. (2013) El Habeas data y la ley de protección de datos en Chile. Serie Bibliotecología y Gestión de Información N° 83, junio ,2013. ISSN: 0719 - 0832 (p.16)

¹⁴⁵ Pablo Viollier. (2020, 18 abril). 5 razones contra el voto electrónico [Video]. YouTube. <https://www.youtube.com/watch?v=HKjpUXl8HkE&list=PLUfm9vw9SqXUJkSbaiYUjHWf6bNAB8IE8> [Consultado el 10 de julio del 2020] S.0:33.

¹⁴⁶ Como se citó en Herrera, Paloma y Pablo Viollier. (2020) (p.102) a “Comité Evaluación de la Ley 2016” Comité Evaluación de la Ley. Evaluación de la ley 19.628 Protección de la Vida Privada. http://www.evaluaciondelaley.cl/foro_ciudadano/site/artic/20151228/asocfile/20151228124429/informe_final_ley_19628_con_portada.pdf

procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron”(Jijena, 2010);”Obliga a los titulares a recurrir a los tribunales civiles ordinarios de justicia, obligando a las personas comunes y corrientes a contratar un abogado, invertir recursos y esperar un par de años para obtener ojalá una decisión favorable, con tribunales civiles sobrecargados que no manejan la especialidad que requiere la protección de datos personales” (Canales & Viollier, 2019)¹⁴⁷; no determina una autoridad de control que fiscalice con sanciones efectivas las violaciones a nuestra privacidad por parte de privados¹⁴⁸; carece de sanciones efectivas; autoriza uso de datos para *marketing* directo sin consentimiento del titular; no existe un registro de bancos de datos privados; contiene excepciones amplias al consentimiento para el tratamiento de datos; carece de mecanismos procedimentales de resguardo efectivo; no regula el flujo transfronterizo de datos¹⁴⁹; entre otros.

Por otro lado, antes de tratar la ley, debemos tener presente que existen múltiples proyectos para modificar la actual protección de datos. Siguiendo a Álvarez (2016), en el “Congreso Nacional, se han presentado más de setenta y dos iniciativas legislativas (entre

¹⁴⁷ Parte de esta doctrina crítica ha sido recogida desde: <https://www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/>.

¹⁴⁸ A diferencia de lo que ocurre respecto del tratamiento de datos personales por parte de los órganos de la Administración del Estado. En este caso la Ley No. 20.285, sobre acceso a la información pública, encomienda el adecuado cumplimiento de ley sobre de protección de datos de carácter personal al Consejo para la Transparencia.

Sin embargo, el ART 33 M) Ley 20285 al decir “velar por el adecuado cumplimiento de la Ley N°19628 de protección de datos de carácter personal, por parte de la administración del estado”, sólo se otorga al consejo un deber, pues no cuenta con facultades para sancionar. Hoy, el organismo siguiendo una interpretación restrictiva, se ha limitado a oficiar y promocionar el buen uso de datos. No es una verdadera agencia de control. Siguiendo a: (Viollier, 2020) Clase 6 - Observancia de reglas de datos personales. <https://www.youtube.com/watch?v=5xPPPQtYD8k&list=PLUfm9vw9SqXUBEG7kPYD0YMIndEZysZxb&index=3> min (Tiempo: 55:00)

¹⁴⁹ Muchas de estas observaciones críticas de la doctrina han sido extraídas de: Viollier, P. & Derechos Digitales. (2017, febrero). El estado de la protección de datos personales en Chile. <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> [Consultado: 10 junio 2020]. (p.54)

mociones y mensajes)”¹⁵⁰ relativos a la protección de la vida privada de las personas. Entre estos proyectos destaca en particular el Boletín 11.144-07 y 11.092-07 refundidos, aprobado en general por el Senado (2021), que vendría a actualizar en general el contenido de la Ley 19.628. Sin embargo, este proyecto contiene sustancialmente planteamientos técnico-jurídicos relativamente similares a la ley actual (expondremos luego las principales modificaciones).

*

Advertido lo anterior, expondremos la ley vigente partiendo por sus clasificaciones.

¹⁵⁰ Álvarez Valenzuela, d. (2016). Acceso a la información pública y protección de datos personales: ¿puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos? Revista de Derecho (coquimbo), 23(1), 51-79. <https://doi.org/10.4067/s0718-97532016000100003>

Entre estos, los Boletines números 2474-07, 2771-05, 3003-19, 3066-03, 3094-19, 3095-07, 3185-19, 3312-05, 3656-18, 3796-07, 4124-18, 4143-07, 4203-07, 4429-07, 4466-03, 4482-03, 4629-07, 4959-03, 4972-03, 5009-06, 5053-07, 5122-07, 5309-03, 5320-03, 5351-07, 5356-07, 5365-07, 5754-07, 5883-07, 5999-07, 6120-07, 6298-05, 6353-07, 6495-07, 6594-07, 6598-06, 6854-03, 6914-03, 6939-03, 6979-06, 6982-03, 6994-07, 7026-07, 7055-07, 7093-03, 7132-03, 7158-05, 7232-03, 7282-07, 7715-03, 7732-07, 7776-03, 7777-07, 7794-07, 7808-13, 7831-07, 7833-13, 7864-03, 7886-03, 8086-04, 8143-03, 8175-03, 8208-07, 8222-11, 8275-07, 8559-03, 8589-07, 9242-10, 9252-15, 9388-03, 9384-07 y 9308-07. Índice de boletines elaborado por Alvarado, Francisco (2013) “Internet y las fuentes de acceso público a datos personales”.

Podemos sumar hoy los boletines: 12409-03 sobre medidas para incentivar la protección de los derechos de los consumidores; 3828-19 sobre protección de los neuroderechos y la integridad mental, el desarrollo de la investigación y las neurotecnologías; 3827-19 Proyecto que Modifica el artículo 19, número 1°, de la Constitución para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías; 3523-03, que prohíbe comunicar obligaciones financieras durante el período de excepción constitucional; 13452-11, sobre la autorización del tratamiento de datos para el control de pandemia Covid-19.

DATO PERSONAL, PERSONAL SENSIBLE Y ESTADÍSTICO

Dato personal

¿Qué es jurídicamente un dato personal en Chile? por una parte, “un dato es una unidad básica de información” (Cerde, 2012)¹⁵¹ y es personal cuando esta información refiera a una persona. Según la Ley N°19.628 en su artículo 2°:

“se entenderá por: [...] (f) Datos de carácter o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.”

Es decir, un dato personal es cualquier información relativa a una persona natural determinable. Sea que se trate de información numérica, fotográfica, acústica o de cualquier otro tipo que nos lleve a identificar a una persona. Si el dato es asociable a una persona, esa información constituye un dato personal. Por ejemplo, “una patente de auto es un dato personal, pues con esta información podemos referirnos a una persona determinable” (Viollier, 2020)¹⁵². El concepto de dato personal es por tanto amplio, no distingue naturaleza ni soporte.

La naturaleza jurídica del vínculo entre el sujeto identificable y sus datos personales, es un vínculo de titularidad. El titular de los datos personales es la persona natural a la que los datos se refieren, y esta referencia la que otorga el vínculo. “Esta relación de titularidad, en oposición a otras formas de vínculo jurídico como el dominio o la propiedad, implica que el

¹⁵¹ Alberto Cerda Silva, Legislación sobre protección de las personas frente al tratamiento de datos personales. Separata, Centro de Estudios en Derecho Informático, Universidad de Chile 2012. Esta cita la he conseguido de una presentación de Pablo Viollier.

¹⁵²El ejemplo lo ha dado Pablo Viollier. (2020, 24 de marzo). Clase 4 - Introducción a la protección de datos personales [Video]. YouTube. <https://www.youtube.com/watch?v=gxv28qQPCTo&list=PLUfm9vw9SqXUBEG7kPYD0YMIndEZysZxb> [Consultado el 10 de julio del 2020] 23:33.

titular no puede renunciar, ceder o enajenar su capacidad de control sobre los datos relativos a su persona” (Contreras, 2019)¹⁵³.

Datos sensibles

Dentro de los datos personales tenemos una importante subclasificación establecida en el artículo 2 literal g), los datos sensibles. Sin pretensión taxativa, los datos personales sensibles dados por el legislador es lo similar - o tales como -, a lo siguiente; Ley N°19.628, artículo 2°:

“Para los efectos de esta ley se entenderá por: [...] g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.”

En general, esta categoría corresponde a aquellos datos que tienen una relación con la esfera íntima de la persona o cuyo uso podría exponer a discriminación; por ello es denominado sensible.

Datos estadísticos

En la ley existe una categoría de datos que no tienen protección por no referirse a una persona individual determinada o determinable. Fuera de los tipos de datos personales vistos – el personal y el personal sensible-, existe una categoría para aquellos datos sin vínculo de titularidad; los llamados datos estadísticos.

Un dato puede ser estadístico ya bien porque: la información que emite una persona puede no ser un dato personal en origen, aun siendo producida por un individuo; porque no

¹⁵³ Contreras, Pablo. Propiedad de datos personales. Apuntes de derechos. 2019. <https://www.pcontreras.net/blog/propiedad-de-datos-personales>. Como se citó en: Herrera, Paloma y Pablo Viollier. (2020) Rendición de cuentas de Facebook y otros negocios en Chile: la protección de datos personales en la era digital. ISBN: 978-958-5597-32-7 (p.104)

puede ser identificada la información con quien produjo el dato; o, porque un dato personal, producto de un tratamiento de datos¹⁵⁴ llamado disociación, ha sido anonimizado. La Ley describe este tipo de datos de la siguiente manera. Ley N°19.628, artículo 2°:

“e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.”

Frente a la anonimidad de los datos, el tratamiento está permitido, pues no hay un titular de datos al cual asociar la información.

Sin embargo, esta anonimidad, en la práctica, podría ser solo momentánea. Es importante destacar que siendo posible complementar un dato estadístico con distintos datos, al analizar y combinar información, se podría asociar trozos de datos anónimos a una persona determinada. Este es el llamado ‘problema de agregación’, consistente en la potencialidad de la interacción de fragmentos aislados que, al ser tratados, puedan revelar un dato personal de una persona determinada.

Solove (2013) expone el ‘problema de agregación’ de la siguiente manera: “Supongamos que en una oportunidad una persona entrega un dato bastante inofensivo, pensando que no está revelando nada sensible. Más adelante [...] entrega otro dato. Sin pensarlo, esta información puede ser combinada y analizada para revelar hechos bastante sensibles sobre esta persona, la que nunca dio a conocer esta información sensible, ni anticipó que ésta sería descubierta. El problema fue que entregó demasiadas pistas. [...] El análisis de datos, puede deducir bastante información sobre una persona a partir de estas pistas. En otras palabras, pequeños pedacitos de información pueden decir mucho cuando

¹⁵⁴ La ley define tratamiento de datos como: “o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.”

El tratamiento de datos es por tanto lo que se entiende en su sentido amplio, lo similar a trabajar, operar, generar, algo a partir de datos. En esta idea, las Big Data Technologies son tratamientos de datos.

son combinados”¹⁵⁵. Este asunto es problemático, pues el tratamiento de la materia prima, el dato estadístico, es lícito.

DERECHOS ARCO

Habiendo entendido estas categorías, podemos preguntarnos sobre el mecanismo de tutela a los datos protegidos.

Con el objeto de evitar que nuestra información sea procesada de forma indebida y proteger el derecho fundamental a la autodeterminación informativa, es decir, “la facultad que tiene toda persona de disponer respecto a la información personal privada, íntima o sensible” (Nogueira, 1997)¹⁵⁶ o, en otras palabras, tener el control de lo que otros saben de nosotros; la ley 19.628 establece los llamados derechos ARCO sobre los datos personales.

En teoría, los derechos ARCO habilitan a toda persona el derecho a exigir a quien sea responsable del tratamiento de datos personales la información que tenga sobre los datos relativos a su persona, a fin de conocer su procedencia, destinatario y propósito; y rectificar, cancelar o bloquear en caso de ser ilegal en su origen o finalidad.

Estos derechos, en principio, concedidos por la ley sobre protección de la vida privada, son cuatro derechos irrenunciables, gratuitos y que no pueden ser limitados en forma convencional, que puede ejercer el titular de los datos personales. Estos derechos son:

1. El derecho de **acceso**: para conocer y verificar la exactitud y legalidad de los datos;
2. El derecho de **rectificación**: para modificar registros erróneos e inexactos;
3. El derecho de **cancelación**: para solicitar la destrucción de los datos almacenados, cuando su tratamiento carezca de fundamento legal; y,
4. El derecho de **bloqueo**: para solicitar la suspensión cuando la exactitud de los datos no pueda ser establecida.

¹⁵⁵ Op. cit. Solove, 2013. (p.1889)

¹⁵⁶ Nogueira Alcalá, Humberto, Reflexiones sobre el establecimiento constitucional del Hábeas Data, en *Ius et Praxis*, Talca, año 3, N° 1, 1997. [No es una cita literal]. (p.265). En el mismo texto encontramos una cita a Antonio Pérez Luño, en “Los Derechos Humanos en la sociedad tecnológica” (p. 139), quien define la autodeterminación informativa como “el conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables”.

EL CAUCE PROCESAL A LA PROTECCIÓN DE DATOS: HABEAS DATA

La legislación chilena reconoce una herramienta especializada¹⁵⁷ de control del tratamiento de datos para ejercer los derechos ARCO; el “Habeas Data”, la acción legal de rango constitucional contenida en el artículo 16 de la ley 19.628. El mecanismo jurisdiccional consagrado por ley al que refiere actualmente la constitución.

Este recurso busca encausar la protección en manos del individuo, para que tenga la facultad para recurrir a un tribunal civil que corrija y sancione el mal uso de sus datos personales con el ejercicio de los derechos ARCO. Procura proteger el derecho a la autodeterminación informativa, permitiendo conocer y controlar los datos de sus titulares en manos de terceros y, a la vez, cautelar que previamente sea necesario el consentimiento para el tratamiento de datos.

El Habeas Data permite que, ante la denegación o falta de respuesta del responsable de la base datos¹⁵⁹ dentro de dos días hábiles a una solicitud de acceso, rectificación, cancelación y oposición (Derechos ARCO), inclusive cuando esta petición es informal; el titular de los datos personales pueda acudir judicialmente, patrocinado por abogado, ante el juez civil del domicilio del responsable, para solicitar la exhibición de los datos personales. De

¹⁵⁷ El ejercicio de esta acción no obsta a otras vías judiciales indirectas, como el recurso de protección, el de amparo económico y las acciones de indemnización de perjuicios por los daños causados por el tratamiento de datos.

Ciertamente, el recurso de protección es la vía judicial indirecta más utilizada. Sin embargo, este mecanismo requiere demostrar y fundamentar la existencia de una amenaza o vulneración de un derecho fundamental, en lugar de tan solo la denegación o falta de respuesta del responsable dentro de dos días hábiles a la fecha de solicitud de acceso, rectificación, cancelación y oposición, así mismo, no permite exigir indemnización de perjuicio ni multas de beneficio fiscal. En cambio, el recurso de protección no requiere patrocinio de abogado, siendo un procedimiento desformalizado y expedito que permite a la Corte tomar cualquier providencia o medida necesaria para restablecer el imperio del derecho.

¹⁵⁹ Siguiendo la ley, el banco de datos es el conjunto organizado que permite relacionar datos entre sí. Es el responsable del banco de datos “la persona natural o jurídica a quien compete las decisiones relacionadas con el tratamiento de datos controla la base, por tanto, debe hacerse responsable de las decisiones y daños que produzca” (Viollier, 2020)

esta forma, el responsable del banco de datos ante el incumplimiento de la solicitud, deba acceder ante un tribunal en un procedimiento breve y sumario.

Este mecanismo especializado es absolutamente criticable. Como vemos, sin contar con una agencia de protección de datos u autoridad de control que vele por nuestros derechos, para buscar protección ante una eventual vulneración, cae exclusivamente en el individuo patrocinado por abogado la capacidad de proteger sus datos en tribunales.

Como afirma Raúl Arrieta, en el informe del Comité de Evaluación de la Ley del año 2016: “La ley vigente, es obvio que tiene problemas del punto vista que no tiene mecanismos para hacer efectivos los cumplimientos. Hoy día el costo transaccional de reclamar la infracción del derecho es tan alto que la gente no reclama”¹⁶⁰.

Este modelo desmotiva a los titulares de datos, y aun existiendo razones para reclamar los derechos ARCO, como dice Garrido (2013), “hasta hoy en día, (el Habeas Data) no ha tenido una aplicación práctica, masiva y concreta”¹⁶¹. Lo que evita, por lo demás, el eventual efecto disuasivo.

Por otro lado, la sanción judicial pecuniaria tampoco es disuasiva. Luego de un proceso favorable, que exija el respeto al ejercicio de los derechos ARCO, la sanción consiste en multas a beneficio fiscal de dos a diez UTM¹⁶², que podrán ser hasta cincuenta si se afecta información bancaria o comercial, junto a la posibilidad de perseguir indemnización de perjuicios¹⁶³.

Como queda claro, “el monto de las multas no resulta lo suficientemente significativo para tener un carácter disuasivo y una ‘empresas con modelos de negocios basados en datos’

¹⁶⁰ Comité Evaluación de la Ley. Evaluación de la ley 19.628 Protección de la Vida Privada. http://www.evaluaciondelaley.cl/wpcontent/uploads/2019/07/informe_final_ley_19628_con_portada.pdf (p.53)

¹⁶¹ Op. cit. Garrido Iglesias (p.16)

¹⁶² 10 UTM, a la fecha del 13 de julio del 2020, es equivalente a 503.220 pesos chilenos.

¹⁶³ Las sanciones e indemnizaciones de la ley 19.628 ante el ejercicio de la acción Habeas Data están contenidas en el Artículo 16 y 23. El Artículo 16 dispone que se podrá aplicar una multa, que podrá ser de dos a diez UTM, la cual podrá ser hasta cincuenta si afecta información bancaria o comercial; y, Artículo 23 dispone, la posibilidad del titular de perseguir la indemnización del daño patrimonial y moral por el tratamiento indebido de los datos. Esto último, sin perjuicio del art. 173 del Código de Procedimiento Civil que permite reservarse el derecho de discutir el monto indemnizatorio en la ejecución del fallo o en otro juicio diverso.

(EMNBD) del nivel de Google, Amazon, Facebook, Apple y Microsoft (GAFAM) o de una empresa consolidada fácilmente podría incorporar dichas multas como un costo de operación” (Herrera y Viollier, 2020)¹⁶⁴

En otro orden de cosas, por no haber una disuasión real, al ser una cautela *ex post* a la recolección y eventual tratamiento o dispersión, y dado que esto puede ser prácticamente imperceptible, es evidente que esta herramienta especializada de control del tratamiento de datos es inefectiva.

Otro aspecto para tener en cuenta es la dificultad de saber si existe, quién tiene, o donde está el banco de datos con los datos personales. Esto se hace particularmente evidente si consideramos que la captación y tratamiento de datos personales puede ser imperceptible, posible de multiplicar, trasladar y esconder. Al ser el Habeas Data una cautela *ex post* a la recolección y eventual tratamiento o dispersión que debe dirigirse en contra del responsable del banco de datos, se torna virtualmente imposible que el individuo común pueda dirigirse contra todos los eventuales -miles- de responsables, patrocinado de abogado y ante tribunal del domicilio del responsable, para procurar una fiscalización.

HIPÓTESIS DE AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS

Ahora que sabemos qué es lo protegido y cuál es el canal procesal para su protección, debemos saber cuándo es lícito tratar nuestros datos. A continuación, trataremos las hipótesis donde la captación de datos personales es mera y llanamente lícita, y los intereses en juego tras la personalización retórica del contenido, tienen autorización legal para tratar nuestros datos.

Autorización para el tratamiento de datos personales

¹⁶⁴ Op cit. Herrera, Paloma y Pablo Viollier. (2020) (p.120)

La ley 19.628 autoriza en su artículo 4° el tratamiento de datos personales, grosso modo, en tres hipótesis:

1. **Cuando otras disposiciones legales lo autoricen** - así, sean datos necesarios para la determinación u otorgamiento de beneficios de salud -;
2. **Haya autorización (consentimiento) del titular**, cuál debe ser expreso y por escrito; informado, respecto del propósito y la posibilidad de ser compartida esta información; y temporal, en tanto que la autorización puede ser revocada por petición escrita, aunque sin efecto retroactivo.
3. Como excepción a las anteriores restricciones; *“no requiere autorización el tratamiento de datos personales que provengan o **que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.**”*¹⁶⁵

En síntesis, el tratamiento de datos personales es lícito cuando 1) la ley lo autorice, 2) exista consentimiento, o, 3) estos datos estén en una fuente accesible al público y estos datos tengan alguno de los caracteres mencionados.

Esta licitud se da solo sobre el fin para el cual haya sido recolectado, con una importante excepción. Aquel dato que fue captado en una fuente accesible al público, puede ser utilizado para cualquier fin. Como se sigue del artículo 9°:

“Artículo 9°. - Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.”

Autorización para el tratamiento de datos personales sensibles

¹⁶⁵ Transcripción literal del artículo 4°, párrafo quinto de la ley 19.628.

Respecto de los datos sensibles, las causales anteriores no aplican. Estos datos requieren un estándar superior de cuidado, por lo tanto, las hipótesis para su tratamiento son más exigentes. Por ello, a diferencia de los datos personales, aunque estos datos se encuentren en fuentes accesibles al público, el artículo 10 excluye estas excepciones.

El artículo 10 de la ley vigente, permite que los datos sensibles puedan ser tratados solo cuando concurran los siguientes supuestos:

Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

SOBRE LA EXCEPCION AL CONSENTIMIENTO DEL DATO PERSONAL CONTENIDO EN UNA FUENTE DE ACCESO PÚBLICO

La excepción al consentimiento para el tratamiento de datos personales que se obtengan de una fuente accesible al público, puede resultar sumamente problemática. Actualmente, esta es la gran excepción a la protección de datos que permite la captación y tratamiento para la generación de perfiles.

Como se sigue del literal del artículo 2 letra i), los datos que están en fuente de acceso público son aquellos que estén en fuentes como «*los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes*». Para expresarlo en otras palabras, el Consejo para la Transparencia (2016) entiende por información accesible al público aquellos a “los que pueda acceder cualquier persona”¹⁶⁶.

Como vemos, esto implica que todo dato al ser fácticamente accesible, es un dato que

¹⁶⁶ Una Aproximación a la Protección de Datos Personales (PDP). Dirección Jurídica Unidad de Normativa y Regulación, Consejo para la Transparencia. (Ppt) 2016. En línea: https://www.educatransparencia.cl/sites/default/files/pdp_-_introduccion.pdf [Consultado en septiembre, 2020]

se encuentra en una fuente accesible al público. Solo basta que la recopilación sea accesible, como son, por ejemplo, los datos que aceptamos que las aplicaciones de nuestros dispositivos compartan con terceros cuando estos re-comparten o venden.

Ante una interpretación literal del artículo 4° de la Ley, en principio, solo los datos personales pueden ser objeto de tratamiento sin contar con la autorización del titular o consentimiento, en la medida que concurra alguna de las siguientes condiciones (no copulativas) establecidas por el legislador.

Artículo 4°, párrafo quinto de la ley 19.628: “*No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando*”¹⁶⁷:

- (i) los datos sean de carácter económico, financiero, bancario o comercial,
- (ii) se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o
- (iii) sean necesarios para comunicaciones comerciales de respuesta directa o comercializaciones o ventas directas de bienes o servicios.

De todas formas, hay una sección, no del todo minoritaria, que sostiene que por ser un dato proveniente de fuente accesible al público no se requiere consentimiento¹⁶⁸ independiente de las características indicadas.

¹⁶⁷ Artículo 4°, párrafo quinto de la ley 19.628.

¹⁶⁸ Por ejemplo, en “Carey/”, Paulina Silva y Elías Mohor, argumentan: “No es evidente si la fuente accesible al público puede operar como una excepción autónoma (que baste con que un dato se haya obtenido de una fuente accesible al público para que no sea necesario obtener el consentimiento del titular para su tratamiento), o si el dato además debe tener alguna de las características indicadas en el resto del inciso (por ejemplo, que además sea un dato financiero) [...]Sin embargo, el artículo 5 de la LPD (Ley 19.628) exime al responsable de una base de datos accesible al público en general, de deberes que sí se establecen para responsables de otras bases de datos que efectúen procedimientos automatizados de transmisión. Por su lado, el artículo 9 de la misma ley exime a los datos recolectados de una fuente accesible al público, de la obligación de ser tratados estrictamente dentro de la finalidad para la cual se recolectaron. En estos artículos, el legislador no pone calificación a las fuentes de acceso público, lo que podría utilizarse para argumentar que tampoco lo hace en el artículo 4.” Silva, P., & Mohor, E. (2016, 1 marzo). Fuentes accesibles al público y el caso del sitio “datos. 24x7.cl” Hipervinculos. Carey/. <https://www.hipervinculos.cl/fuentes-accesibles-al-publico-caso-del-sitio-datos-24x7-cl-parte-1-planteamiento/> (Consultado: septiembre 2021)

Sin embargo, aun sí nos acotamos al marco de acción que la excepción del artículo 4º literalmente permite, aun así, muchos “consideran que dichas excepciones son de una amplitud tal, que la regla general es para todos los efectos prácticos, la excepción antes que la regla”¹⁶⁹. Aunque ciertamente vendría a limitar el tratamiento de datos personales conseguidos en una fuente accesible al público, la ambigüedad de clasificar un dato como de carácter “económico”, o “comercial”, o para “indicar la pertenencia de un individuo a un grupo” o “para la comercialización de bienes y servicios”, abre enormemente la susceptibilidad de tratar datos personales de fuentes accesibles al público sin consentimiento previo del titular.

Por otro lado, no existe un catálogo que defina que bancos de datos se pueden considerar como acceso público – como ocurre, por ejemplo, en España¹⁷⁰ -. Una fuente pública, podría ser cualquiera. Como menciona Jervis (2005), nuestra situación es, “una hipótesis de aplicación taxativa y alternativa, limitada en cuanto a la información contenida, pero abierta en cuanto a qué tipo de base de datos puede considerarse fuente accesible al público”¹⁷¹. Alvarado (2014), en referencia a lo anterior dice, “este aspecto de la Ley 19.628 es uno de los más criticados, por cuanto la laxitud de la definición permite que cualquier banco de datos pueda considerarse como fuente de acceso público, con las ventajas que ello conlleva para quienes, por ejemplo, hacen negocios en torno al tratamiento de esta información.”¹⁷²

Considerando que el consentimiento es el paradigma para la protección a un adecuado tratamiento, este asunto es de gravedad mayor. Como afirma Anguita (2007), “el régimen de excepciones es suficientemente amplio como para vulnerar el principio del consentimiento”¹⁷³. En el mismo sentido, Viollier (2018), dice: “la prerrogativa contemplada

¹⁶⁹ Como se citó en: Op cit. Viollier, P. & Derechos Digitales, (2017, febrero) (p.21) siguiendo a. el Ciclo de Riesgo, 2014; Jijena, 2010.

¹⁷⁰ Artículo 3 de la Ley Orgánica de Protección de Datos de Carácter Personal.

¹⁷¹ Jervis, Paula (2005). «Categorías de datos reconocidas en la Ley 19.628». Revista Chilena de Derecho Informático, 6: 111-145 (p. 122). Como se citó en: Alvarado Ávalos, F. D. (2014) (p.216)

¹⁷² Alvarado Ávalos, F. D. (2014). Las fuentes de acceso público a datos personales. Revista Chilena de Derecho y Tecnología, 3(2). <https://doi.org/10.5354/0719-2584.2014.33276> (p.216)

¹⁷³ Anguita, Pedro (2007). La protección de datos personales y el derecho a la vida privada. Santiago: Jurídica. (p. 559)

en la misma ley sobre fuentes accesibles al público abre la puerta para que prácticamente todo dato personal que circule en la web sea susceptible de ser utilizado por terceros”¹⁷⁴.

Todo dato eventualmente podría entrar en este supuesto, más si consideramos, como afirma Arieta (2009), “que uno de los defectos sustanciales en esta materia es que radica en el titular del banco de datos la facultad de dejar abierto o no el acceso público al registro, con el consecuente riesgo de fraude a la ley y los derechos del titular de los datos”¹⁷⁵.

INSTAGIS, EMPRESA CHILENA DE TRATAMIENTO DE DATOS PERSONALES

Expuestos los elementos básicos de la protección jurídica ante la captación y tratamiento de datos personales, nos encontramos en condiciones de analizar un caso.

La empresa “InstaGIS”¹⁷⁶, desde 2018 también llamada “Predictable Media”¹⁷⁷, ofrece al mercado, tanto para fines políticos como comerciales, una observación objetiva del comportamiento humano. InstaGIS captura datos, los trata y vende los perfiles. De esta forma, permite focalizar el público y personalizar el contenido de la propaganda o publicidad¹⁷⁸.

¹⁷⁴Viollier, Pablo (2018) en <https://ciperChile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/> [Consultado en septiembre, 2020]

¹⁷⁵ Arrieta, Raúl (2009). Chile y la protección de datos personales: Compromisos internacionales. En Varios autores, Chile y la protección de datos personales: ¿están en crisis nuestros derechos fundamentales? Como se citó en: Alvarado Ávalos, F. D. (2014) (p.219)

¹⁷⁶ Link al sitio de Instagis: <https://www.instagis.com/es/> (consultado: Septiembre, 2021)

¹⁷⁷ Link al sitio de Predictable Media: <https://www.predictablemedia.com/> (consultado: Septiembre, 2021)

¹⁷⁸ “InstaGIS ha desarrollado una plataforma que permite entender de mejor manera las necesidades, expectativas y metas de sus ciudadanos, mediante el procesamiento de información de fuentes de datos de gobierno, municipales y de redes sociales. La consolidación de dichas fuentes, nos permitirá perfilar a cada ciudadano y en base al segmento de la persona, la posibilidad de crear una comunicación segmentada acorde a los intereses de cada persona que vive en la comuna.” “InstaGIS plantea los siguientes objetivos y metas como plan de inversión para aumentar el perfilamiento e interés en ciertas políticas públicas: 3.1- Posicionamiento: Aumentar significativamente el nivel de conocimiento de cada mensaje a comunicar (Awareness). 3.2- Perfilamiento: Aumentar significativamente el número de perfilados en cada tema de interés, para así enfocar en ellos cada

Este servicio lo realiza cruzando la información de diferentes bases de datos de fuentes accesibles al público, como el padrón electoral, el Censo, la Casen, el Registro Social de Hogares, el padrón electoral, y también, vigilando los datos accesibles de redes sociales como Facebook, Twitter e Instagram¹⁷⁹, para perfilar las características y las preferencias de las personas, a fin de vender el perfilamiento realizado.

En el informe de InstaGIS para el Diputado José Manuel Edwards (2016), se manifiesta el mecanismo y propósito del funcionamiento de la empresa: “Estudiando en profundidad a la ciudadanía logramos crear un perfil de registro único para cada ciudadano, que evoluciona en el tiempo dependiendo de sus características demográficas, necesidades, intereses y pasatiempos. Nuestro algoritmo monitorea distintos medios digitales, identificando lo que comentan y los sentimientos de su comunidad con respecto a temas como: salud, educación, seguridad y trabajo. Esta información es combinada con información de grupos etarios, sexo, datos socioeconómicos y otras informaciones recogidas de las bases de datos públicas y las particulares que pueda tener cada municipio, identificando a los usuarios con nombre y cédula de identidad. Estos segmentos se actualizarán constantemente, los cuales representan a las personas de su comunidad ya clasificadas según corresponda. El equipo del parlamentario podrá enviar vía Facebook, Correo electrónico u otros medios de comunicación, mensajes específicos creados por el equipo del Diputado, mediante el uso de

mensaje. 3.3- Relevancia: Maximizar la relevancia de la comunicación a cada habitante, micro segmentando los mensajes para asegurar que sean relacionados a sus dolores e intereses. 3.4- De online a offline: Gracias al trabajo de perfilamiento online, entendiendo dolores e intereses de forma segmentada, y apoyándonos en la plataforma de georreferenciación territorial, poder apoyar la labor en terreno.”

Extraído de “Informe asesoría externa de segmentación y análisis de habitantes del distrito para comunicación de políticas públicas realizado por INSTAGIS SPA. para el Diputado José Manuel Edwards” (2016). En línea: <https://ciperchile.cl/wp-content/uploads/F4573-Informe-Final-38000-Edwards-Jos%C2%AE-Manuel-1.pdf> (Consultado: septiembre 2021)

¹⁷⁹ Siguiendo a CIPER 11/09/2019. En línea: <https://www.ciperchile.cl/2019/09/11/alguien-te-mira-asi-funciona-el-gigante-de-las-campanas-politicas-que-controla-sosafe/> (Consultado: septiembre 2021)

las Bases de Datos creadas y disponibilizadas solo por InstaGIS, para así aumentar su nivel de alcance y asertividad respecto a los intereses de cada lugar”¹⁸⁰

Con la venta de esta clase de servicios a distintos candidatos de “Chile Vamos”¹⁸¹, en las elecciones de 2016 y 2017, InstaGIS recaudó \$274 millones por identificar la adhesión política vía redes sociales, y perfilar a ciudadanos para mostrarles propaganda personalizada, elemento que resultó clave en los triunfos de distintos alcaldes y parlamentarios¹⁸². Hablamos pues, de una empresa influyente.

EL APEGO A LA LEY DE INSTAGIS Y UN BREVE CONTRAARGUMENTO

InstaGIS funda el apego a la legislación vigente, principalmente, en el hecho que la información fue obtenida a través de fuentes accesibles al público¹⁸³. De esta forma, argumentan estar amparados en la excepción contenida en el artículo 4 inciso quinto de la ley 19.628, que señala que terceros no requieren del consentimiento del titular de datos personales para tratar sus datos cuando estos provengan o se hayan recolectado de fuentes accesibles al público.

Planteándonos un ejercicio hipotético del Habeas Data ante InstaGIS; siendo lícita la captación y el tratamiento de datos personales de fuentes accesibles al público, InstaGIS,

¹⁸⁰ “Informe asesoría externa de segmentación y análisis de habitantes del distrito para comunicación de políticas públicas realizado por INSTAGIS SPA. para el Diputado José Manuel Edwards” (2016). En línea: <https://ciperchile.cl/wp-content/uploads/F4573-Informe-Final-38000-Edwards-Jos%C2%AE-Manuel-1.pdf>

¹⁸¹ En el siguiente link, por ejemplo, el contrato entre Instagis y el partido político Renovación Nacional. <https://ciperChile.cl/wp-content/uploads/INSTAGIS-CONTRATO-CON-RN.pdf>

¹⁸² Como se afirma en el reportaje de CIPER “Instagis: el “gran hermano” de las campañas políticas financiado por Corfo “. Disponible: <https://ciperChile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/> [Consultado en Julio 2020]. En él, se puede visualizar el contrato ‘de prestación de servicios para la puesta en marcha y arriendo de servicios de software’ entre, el partido político chileno, Renovación Nacional e Instagis. En línea: <https://ciperChile.cl/wp-content/uploads/INSTAGIS-CONTRATO-CON-RN.pdf>

¹⁸³ InstaGIS respondió algunas consultas de La Tercera: “¿Cuáles son los límites? -Solo trabajar con información pública, a la que puede acceder cualquiera.” <https://www.latercera.com/la-tercera-pm/noticia/instagis-la-empresa-de-datos-que-trabajo-para-pinera-el-limite-es-trabajar-con-informacion-publica/108576/> (en línea: septiembre, 2021)

respecto del titular de datos que solito el ejercicio de los derechos ARCO, posiblemente solo entregará una colección de datos como fotos de perfil de Instagram, los me gusta que se habrían dado en público, el padrón electoral, y otros datos de la “huella digital” en el ciberespacio que se encuentran en fuentes públicas que InstaGIS tenga en su poder, pero no entregará el perfilamiento.

Esto pues, posiblemente¹⁸⁴, InstaGIS argumentaría algo común entre los que viven del negocio de tratamiento de datos; que lo que ellos han hecho al haber tratado nuestros datos no es realmente ante un dato personal, sino un “dato inferido”¹⁸⁵ por la misma empresa. Una especie de “opinión sobre nosotros” que se ha elaborado a partir de información de un conjunto de personas – no solo de quien es perfilado- cual podría no coincidir con la realidad, ya que es solo una probabilidad encontrada por las *Big Data Technologies*. Por lo que este dato inferido, probable, se desentiende de los titulares de los datos personales tratados. En esta visión, el titular de un dato personal es solo titular del dato personal originario, mas no del inferido que no es reclamable.

Ante esta situación, Pablo Contreras (2019) reflexiona: “una de las cuestiones centrales que ha revelado esto, son las deficiencias de nuestra legislación. Porque, precisamente, el perfilamiento de personas, en base a datos personales, aunque sean obtenidos por fuentes públicas, es una de las cuestiones donde están en juego datos sensibles y hoy los ciudadanos no tenemos ninguna forma real de poder oponernos a ese tipo de perfilamiento y tratamiento de datos sensibles.”¹⁸⁶

De todas formas, analizando el caso a la luz de la legislación, es posible argumentar cómo detener a InstaGIS y reclamar la ilegalidad del dato inferido. Esto, gracias a la amplitud

¹⁸⁴ Tristemente, no hay documentos que respalden esta argumentación que sí han sostenido personalmente con Pablo Viollier, quien nos ha comentado esta postura de la empresa. Por nuestra parte, intentamos contactar al CEO de InstaGIS sin resultados, por lo que nos vemos forzados a plantear esto como una hipótesis.

¹⁸⁵ “Los datos inferidos son aquellos obtenidos a partir del procesamiento analítico de un conjunto amplio de datos entre los que se encuentran datos de múltiples personas usuarias y diversas fuentes.” Agencia española de protección de datos. IoT (I): Qué es IoT y cuáles son sus riesgos. (2020, 3 diciembre). AEPD. <https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos> (en línea: septiembre, 2021)

¹⁸⁶ En línea: <https://www.pcontreras.net/blog/october-08th-2019> (consultado: septiembre, 2021)

con la que nuestra legislación entiende que es un dato personal y que es un dato personal sensible. Ya que un “dato inferido”, si es “*relativo a cualquier información concerniente a personas naturales, identificadas o identificables*”¹⁸⁷, no deja de constituir para nuestra legislación un dato caracterizable como dato personal, por lo tanto, no deja de estar protegido por el vínculo de titularidad.

Por otra parte, si dato personal es el que se refiere a una persona determinada y es dato sensible el que tenga las características que la ley describe, el tratamiento de datos personales que derive en un dato sensible debe cumplir con el mismo estándar que establece la ley para el tratamiento de un dato sensible. Siendo así, aunque no fuere necesario contar con el consentimiento del titular para el tratamiento de sus datos personales por este estar en una fuente accesible al público, respecto de los datos personales sensibles debe contar con el consentimiento.

Como sabemos, InstaGIS trata datos para inferir posturas políticas. Así mismo se anuncia en el contrato de ‘prestación de servicios para la puesta en marcha y arriendo de servicios de software’ (2016) entre Renovación Nacional e Instagis: “InstaGIS monitoria distintas Fan Pages públicas de Facebook donde se publican contenidos políticos y donde los usuarios que las siguen realizan interacciones públicas que revelan sus tendencias y preferencias. InstaGIS utiliza estas Interacciones para actualizar la probabilidad de adherencia”¹⁸⁸. Siendo este el caso, el hecho que la empresa genere un perfilamiento probabilístico de una persona natural respecto de sus preferencias políticas o ideológicas, implica que se está tratando un dato personal sensible. De hecho, el artículo 2 letra g), que define que es un dato personal, menciona “las ideologías y opiniones políticas”.

Por lo tanto, la hipótesis de licitud de InstaGIS, que se sostiene en el hecho de que la información fue obtenida a través de fuentes accesibles al público, debiere rechazarse en función de la amplitud con la que nuestra legislación define el concepto de dato personal y dato personal sensible. Pues, independiente si se han conseguido datos desde fuentes

¹⁸⁷ Definición de dato personal contenido en la Ley N°19.628 en su artículo 2° (f).

¹⁸⁸ Punto VII del contrato ‘de prestación de servicios para la puesta en marcha y arriendo de servicios de software’ entre, el partido político chileno, Renovación Nacional e Instagis. En línea: <https://ciperChile.cl/wp-content/uploads/INSTAGIS-CONTRATO-CON-RN.pdf> [Este documento se ha conseguido gracias a CIPER Chile.]

accesibles al público, e independiente si la información que tienen ha sido o no producto de un tratamiento de datos, por referirse el perfilamiento a una persona determinada o determinable y tener connotación de dato sensible, el perfilamiento es ilegal por carecer de consentimiento.

Esto por cuanto los datos personales sensibles tienen un estatuto especial otorgado por la ley, y se establecen causales específicas y taxativas para su tratamiento. De acuerdo con el artículo 10 de la ley 19.628, los datos personales sensibles no pueden ser tratados, salvo cuando: 1) la ley lo autorice, 2) exista consentimiento del titular o 3) sean datos necesarios para la determinación u otorgamiento de beneficios de salud. Por lo que no habría cabida para el tratamiento de los datos sensibles que se refieran a una persona determinable sin su consentimiento.

En efecto, como sostienen Herrera y Viollier (2020): “la legislación define la categoría de dato personal sensible sin distinguir la forma en que estos datos son obtenidos. En este sentido, una interpretación sistemática de la legislación permite concluir que el responsable de base de datos debe cumplir con los requisitos adicionales que la categoría dato personal sensible conlleva, independiente de si el dato es obtenido por medio del consentimiento del titular o por medio de un tratamiento automatizado que permite inferir un dato sensible.[...] En el mismo sentido, los titulares se encuentran habilitados para ejercer su derecho de acceso, rectificación, cancelación u oposición de sus datos personales, incluso si ellos han sido inferidos por el responsable de base de datos mediante mecanismos algorítmicos o automatizados.”¹⁸⁹

¹⁸⁹ Herrera, Paloma y Pablo Viollier. (2020) Op cit. (p.104)

REFORMA A LA LEY DE PROTECCION DE DATOS; EL BOLETÍN 11.144-07 Y 11.092-07 REFUNDIDOS

Dentro de los proyectos de ley en curso para la reforma de la actual protección de datos personales, destaca en particular el boletín aprobado en general por el Senado, el boletín 11.144-07 y 11.092-07 refundidos. Este proyecto modifica casi íntegramente la actual Ley 19.628 sobre protección de la vida privada.

Siendo así, es necesario que consideremos que a la protección actual de datos podrían sumarse algunos aspectos con este proyecto, cual vendría a incorporar a la lógica actual, principalmente lo siguiente:

Son cambios importantes del proyecto:

- La Portabilidad¹⁹⁰ en los Derechos ARCO;
- La creación de una autoridad de control a cargo del Consejo para la transparencia¹⁹¹ y el aumento las multas ante infracciones¹⁹²;
- Nuevas obligaciones a los responsables de datos o controladores: como el deber de reportar medidas de seguridad y reportar brechas a la autoridad y a los titulares;

¹⁹⁰ En palabras de Raúl Arrieta (2019). Portabilidad: Es el derecho del titular de datos a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y a comunicarnos o transferirlos a otro responsable de datos, cuando concurren las siguientes circunstancias: el tratamiento se realice en forma automatizada y el tratamiento está basado en el consentimiento del titular. Raúl Arrieta Cortés. Cortés, R. A. (septiembre, 2019). El nuevo entorno regulatorio de la protección de datos personales en Chile. En línea: <https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-Chile/>

¹⁹¹ Consejo para la transparencia tendrá funciones como, entre otros, supervigilar el cumplimiento, aplicar e interpretar administrativamente la ley, dictar reglamentos e impartir instrucciones de carácter general

¹⁹² El proyecto incorpora un catálogo de infracciones; leves art. 38 bis, graves art. 38 ter y gravísimas art. 38 quáter; e incorpora sus sanciones, en art. 39, como: Leves 1 a 100 UTM, Graves 101-5000 UTM, Gravísimas 5001 – 10.000 UTM.

- La regulación de la transferencia internacional de datos y la cesión de datos;
- La incorporación del interés legítimo como hipótesis de licitud para el tratamiento de datos personales que se encuentran en fuentes accesibles al público y cuyo tratamiento no confronte derechos y libertades fundamentales^{193,194}; y,
- La incorporación, esta vez literal, de la exigencia de consentimiento expreso para el tratamiento de datos sensibles. Este requisito se exceptúa, sin embargo, cuando el tratamiento se basa en un interés legítimo realizado por una persona jurídica de derecho público o privado que no persiga fines de lucro.

El boletín comentado si bien incorpora asuntos importantes, en particular con la creación de una autoridad de control; el desafío al problema que expone esta tesis se mantiene.

¹⁹³ En el Proyecto: “f) el tratamiento que sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que los datos hubiesen sido obtenidos de una fuente de acceso público, y sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales de los titulares de los datos que requieran la protección de datos personales, en particular cuando los titulares sean niños.” [A la fecha de septiembre 2020]

¹⁹⁴ Existe fuerte lobby para aprobar esta nueva excepción al consentimiento que autoriza el tratamiento de datos. Como señala la Gerente de Políticas Públicas de Google, Cono Sur, Eleonora Rabinovich, la postura de Google es que «los intereses legítimos constituyen una base legal tan imprescindible como el consentimiento». Se puede encontrar esta argumentación en Primer informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales, Boletines 11.144-07, 14 de marzo de 2018, (p. 201), disponible en <https://bit.ly/2ZetMaE> [Consultado en agosto 2020]

IDEAS CONCLUSORIAS AL CAPITULO

DIFICULTADES

El desequilibrio entre los miles de interesados en tener nuestros datos y el individuo común no se encuentra en la parte sustantiva de la Ley 19.628, sino quizás como inoficiosa pretensión en la parte orgánica. Pues si bien podríamos pensar que el concepto legal de dato personal contiene en su centro el lugar correcto al procurar tutelar el uso indebido de la información que se refiera a un ser humano en un amplio aspecto; frente a la facilidad que existe para captar y tratar datos, el mecanismo de protección de los datos personales es absolutamente insuficiente.

¿Puede el derecho cautelar *ex ante* el uso de la información que captan nuestros dispositivos inteligentes con todos los intereses económicos y políticos en juego? a fin de cuentas, más allá de que el ordenamiento jurídico actual tenga laxas hipótesis que autorizan el tratamiento de datos sin consentimiento del titular, que defina la carga de la gestión y resguardo de la protección digital en el individuo medio, que dependa de un procedimiento engorroso que requiere de patrocinio de abogado y demanda en el tribunal competente del domicilio del responsable, que sea un procedimiento de protección que opera *ex post* a la vulneración y que sea imposible identificar y dirigirse contra todos los entes que en el mundo capturan y tratan nuestros datos; pareciera que, fácticamente, el ordenamiento no tiene la capacidad de restringir el uso indebido de la tecnología que media, detecta y registra en múltiples niveles el comportamiento humano.

El resguardar el uso de nuestros datos parece una imposibilidad para la capacidad de la ley. Como señalan de forma certera Hildebrandt & Koops (2010)²⁰⁹, “en el núcleo de los mecanismos que nos llevan a creer en las brechas sistémicas de cualquier protección de datos y la ley de privacidad, está el hecho de que la protección legal está incorporada en reglas legales escritas que no pueden adecuadamente hacer frente a la infraestructura tecnológica

²⁰⁹ Hildebrandt, M., & Koops, B. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428-460. doi:10.1111/j.1468-2230.2010.00806.x (p. 443)

proactiva y omnipresente en tiempo real. Estamos tratando con un procesamiento de datos que tiene lugar en una escala enorme, de manera instantánea, ubicua y en una multitud de formas que eluden la observación humana. En esta era, la ley en los libros ha llegado al límite de sus poderes protectores. Como resultado, un enfoque poco sistemático y de parche no será suficiente para abordar las brechas en la protección legal.”²¹⁰ “En un futuro dominado por un ambiente inteligente capaz de adecuarse de manera proactiva y subliminal a las preferencias inferidas de los usuarios, las protecciones basadas en el consentimiento informado o el derecho a no estar sujeto a decisiones automatizadas parecen irremediablemente torpes [...] (por otro lado) ante el común incumplimiento del deber básico de registrarse ante cualquier autoridad antes de realizar operaciones de procesamiento de datos [...] la supervisión del procesamiento de datos es imposible”²¹¹. Así mismo -continúan-, como los procesos de elaboración de perfiles suelen estar cubiertos por disposiciones sobre secretos comerciales o derechos de propiedad intelectual, y debido a que la tecnología puede ser una caja negra incluso para el procesador de datos – el saber que ocurre dentro de una red neuronal-, es inalcanzable una supervisión adecuada del deber de registro.

Por otro lado, Koops (2008), señala que, “el incumplimiento de la ley no siempre ocurre de manera deliberada, muchas veces es solo una falta de conocimiento del derecho”²¹². Sobre todo, porque “las reglas son desconocidas, ambiguas, vagas o demasiado complejas para ser integradas”²¹³

²¹⁰ Original; “At the core of the mechanisms that lead us to believe that the gaps in data protection and privacy law are systemic, is the fact that the existing legal protection is embodied in written legal rules that cannot adequately cope with the real time pervasive and proactive technological infrastructure that may emerge. We are dealing with data processing that takes place on an enormous scale, instantaneously, ubiquitously, and in a multitude of ways that elude human observation. In this era, law in the books has reached the limits of its protective powers. As a result, a piecemeal, band-aid approach will not susceptor address the gaps in legal protection”

²¹¹ Hildebrandt, M., & Koops, B. (2010). Ibid. (p. 442)

²¹² B. J. Koops, ‘How Fragmentation in European law Undermines Consumer Protection: The Case of Location Based Services’ (2008) 33 European Law Review (p.880)

²¹³ Hildebrandt, M., & Koops, B. (2010). Ibid. (p. 440)

SOBRE LA CAPACIDAD DEL PERFILAMIENTO

¿Qué podría hacer InstaGIS, o cualquiera con un perfilamiento? Es prácticamente imposible poder presumir cómo serán utilizados los datos que existen sobre nosotros, sin embargo, el valor puede ser enorme, particularmente, con su uso para fines retóricos.

Como menciona Koops (2008): “Conocer (o inferir) las preferencias, los intereses y los hábitos de una persona, sus amigos y conocidos, la educación y el empleo, la salud física y la situación financiera, coloca al conocedor en condiciones de ejercer una influencia considerable sobre lo conocido; les permite comprender mejor qué motiva a sus objetivos, cuáles son sus debilidades y vulnerabilidades, cuándo son más susceptibles a la influencia y cuál es la forma más eficaz de enmarcar argumentos y apelaciones.”²¹⁴

Como mencionamos anteriormente, no es complejo perfilar un sujeto conociendo parte de su comportamiento. Así lo ha probado el famoso estudio de Kosinski et al. (2013) dilucidando que con las correlaciones entre los “likes” o “me gusta” entre usuarios de Facebook, es posible inferir el género, la orientación sexual, raza, religión, opiniones políticas, estado civil, uso de sustancias, densidad de las redes de amistades, entre otros²¹⁵. Inclusive, el análisis de las correlaciones entre los “likes” puede llegar a ser verdaderamente profundo, y llegar a inferir rasgos psicológicos, por ejemplo, midiendo inteligencia según el “Matrices progresivas de Raven²¹⁶”, o rasgos de personalidad, entre estas por ejemplo en términos de lo medido por el “Fondo Internacional de Elementos de Personalidad” apertura, amabilidad, estabilidad emocional y escrupulosidad²¹⁷. De hecho, estos análisis e inferencias fueron los usados por Cambridge Analytica²¹⁸.

²¹⁴ Susser, Daniel; Roessler, Beate; Nissenbaum, Helen (2019): Technology, autonomy, and manipulation, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 8, Iss. 2, pp. 1-22, <http://dx.doi.org/10.14763/2019.2.1410> (p.2)

²¹⁵ Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences, 110(15), 5802-5805. <https://doi.org/10.1073/pnas.1218772110>

²¹⁶ Fue uno de los estándar utilizado por Kosinski et al para medir la inteligencia.

²¹⁷ Siguiendo a Susser, D., Roessler, B., & Nissenbaum, H. F. (2019) op. cit. (p.10)

²¹⁸ Alexander Nix, Cambridge Analytica - The Power of Big Data and Psychographics. (2016, 27 septiembre). [Video]. YouTube.

Por supuesto que no es tan solo con los "likes" de Facebook que se puede llegar a importantes predicciones. Igualmente se pueden utilizar la datos de información relativa a determinadas búsquedas en línea, reproducciones de música o videos, modo de navegación, horario y frecuencia; y también, con la información del comportamiento de sus contactos, familiares, miembros de su trabajo, personas con su nivel de educación, etc.

Al ser comparados los datos con los de miles de otros sujetos, los algoritmos gracias a las *Big Data Technologies* permiten revelar patrones dentro de perfiles agrupables. De esta forma, es posible generar perfiles psicológicos etiquetados con el que "entrenar" dentro de un conjunto - *cluster* - de datos, y generar estadísticas de probabilidades de comportamiento ante determinados estímulos para tipos de perfil. Estos son los, ya comentados, datos inferidos.

El perfilamiento del dato inferido permite un poder de predicción del comportamiento humano gigantesco. Tanto que puede superar la capacidad predictiva de nuestros amigos o familiares. Esto es lo que concluye otro famoso estudio "*Computer based personality judgments are more accurate than those made by humans*" (Youyou, Kosinski & Stillwell 2015): "Las personalidades de las personas se pueden predecir automáticamente y sin involucrar las habilidades sociocognitivas humanas. [...] demostramos que los juicios de las computadoras sobre la personalidad de las personas basados en sus huellas digitales son más precisos y válidos que los juicios hechos por sus allegados o conocidos (amigos, familia, cónyuge, colegas, etc.)." ²²²"En comparación con la precisión de varios jueces humanos, los modelos informáticos necesitan 10, 70, 150 y 300 Me gusta, respectivamente, para superar a un colega de trabajo promedio, conviviente o amigo, miembro de la familia y cónyuge."²²³ Como resultado, en este estudio han establecido lo siguiente: "i) las predicciones informáticas basadas en una huella digital genérica (me gusta de Facebook) son más precisas que las realizadas por los participantes mediante un cuestionario de personalidad ii) Los modelos

https://www.youtube.com/watch?v=n8Dd5aVXLcC&ab_channel=Concordia [Consultado: marzo 2021]
- Como se cito en: Op cit. Roessler, F. Nissenbaum (2019).

²²² Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040. <https://doi.org/10.1073/pnas.1418680112> (p.1036)

²²³Ibid. Youyou, W., Kosinski, M., & Stillwell, D. (2015). p. 1037

computacionales muestran mayores acuerdos más allá de juicios particulares iii) los juicios de personalidad de las computadoras tienen una mayor acierto al predecir los resultados de la vida, como el uso de sustancias, las actitudes políticas y la salud física”²²⁴.

MIEDOS Y CASOS DE CAPTACION ILÍCITA DE DATOS

Para entender ciertos límites en la soberanía de nuestros derechos digitales, basta mencionar un par de ejemplos. Así el temor de espionaje que llevó a Estados Unidos a “banear”²²⁵ - restringir - a Huawei en el 2019 y a Tik Tok el 2020.

En el revuelo ante Huawei en el 2019, y reflejando la naturaleza del temor, el senador demócrata Mark Warneren declaró: "Las revisiones de software de los productos existentes de Huawei no son suficientes para evitar la posibilidad de que un proveedor presente una actualización maliciosa que permita la vigilancia en el futuro. Cualquier producto chino supuestamente seguro está a una actualización de firmware de ser un producto chino inseguro"²²⁶. A Estados Unidos le queda claro que basta un par de movimientos para filtrar nuestra información.

Por otra parte, respecto de los miedos, mucho más concretas son las revelaciones sobre la red de vigilancia mundial (2013-2015) por parte de Edward Snowden y Cambridge Analytica (2016-2019).

²²⁴ Original: i) computer predictions based on a generic digital footprint (Facebook Likes) are more accurate than those made by the participants' Facebook friends using a personality questionnaire; (ii) computer models show higher interjudge agreement; and (iii) computer personality judgments have higher external validity when predicting life outcomes such as substance use, political attitudes, and physical health.

²²⁵ Banear. Jerga informática para denominar a un tipo de restricción, temporal, parcial o permanente. Con este término es comúnmente conocido este suceso, inclusive en la academia.

²²⁶ El senador demócrata Mark Warneren el medio The Verge. <https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g> [Consultado en Julio 2020]

Edward Snowden, ex agente de Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA), en junio de 2013 filtró documentos que probarían la vigilancia permanente y masiva sobre gran parte de la población mundial; revelando los programas de vigilancia “PRISM” y “XKeyscore”. Snowden, copió y filtró miles de documentos clasificados de alto secreto (*top secret*) mientras trabajaba para Booz Allen Hamilton, uno de los mayores contratistas militares y de inteligencia del gobierno de Estados Unidos. El ex-agente como justificación para filtrar la información alego: “en conciencia, no podía permitir al gobierno de Estados Unidos destruir la privacidad, la libertad en internet y las libertades básicas de la gente de todo el mundo con esta gigantesca máquina de vigilancia que están construyendo en secreto”²²⁷.

Como mostraron los archivos revelados, la red estaba a cargo de la agencia de inteligencia de EE. UU y los miembros del tratado de seguridad UKUSA, conformado por los gobiernos de Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda. Igualmente, en el plan de vigilancia fueron colaboradores los estados de Suiza, Italia, los Países Bajos, España, Suecia, Alemania, Francia, Noruega, entre otros. Estas naciones se valieron de distintos métodos para obtener datos personales de millones de individuos independiente de lo que el derecho nacional y los derechos humanos declaran.

Entre los distintos mecanismos utilizados para captar datos personales, podemos mencionar, la ruptura de la seguridad de los sistemas operativos iOS y Android – para acceder al contenido de teléfonos de forma remota, micrófono, cámara y localización-, la introducción de softwares espías en aplicaciones móviles populares de descarga masiva como Angry Birds o Google Maps, la interceptación de llamadas, registros telefónicos, transacciones

²²⁷ CBS NEWS 12 junio, 2013. En línea: <https://web.archive.org/web/20180918064927/https://www.cbsnews.com/news/man-claiming-to-be-nsa-whistleblower-comes-forward/>

financieras y tráfico de información, entre otros. Nuestro punto es que, simplemente toda la información registrada y de interés fue utilizada sin contención jurídica²²⁸.

Eventualmente, como ha dicho Snowden, “ya existen perfiles informáticos de prácticamente cualquier individuo en el mundo”²²⁹. Como vemos, la garantía a la autodeterminación sobre la vida privada, que incorpora la protección contra la vigilancia y la recopilación de datos, simplemente fue obviada ante los intereses en juego. El derecho poco o nada pudo hacer.

CAMBRIDGE ANALYTICA

En marzo del 2018 Cambridge Analytica comenzó a considerarse un escándalo en materia de protección de datos personales, pero con una arista distinta, este escándalo abiertamente consistía en persuadir a ciudadanos a través del perfilamiento y la personalización del contenido. En particular el cuestionamiento público fue; cómo se logró ejercer influencia en las elecciones presidenciales de EE. UU. de 2016 mediante información personalizada dirigida junto con la dispersión de noticias falsas.

Christopher Wylie, uno de los cofundadores de Cambridge Analytica, quien luego se convertiría en el gran delator, respecto del funcionamiento de Cambridge Analytica dijo: “Explotamos Facebook para recolectar perfiles de millones de personas y crear modelos para explotar lo que sabíamos de ellos y apuntar a sus demonios internos. Esta es la base de la empresa.”²³⁰

²²⁸ Por decir lo menos, el derecho a la vida privada está reconocido como derecho humano en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y, así mismo, en el artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 11 de la Convención Americana sobre Derechos Humanos

²²⁹ “Edward Snowden, after months of NSA revelations, says his mission was accomplished. Disponible:”https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html [Consultado en Abril 2021]

²³⁰ Cambridge Analytica and Facebook: The Scandal So Far, AL JAZEERA (Mar. 28, 2018), <https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html> [<https://perma.cc/PU4C-KNSN>]. Cita extraída de, Susser, D., Roessler, B., & Nissenbaum, H. F. (2019) (p.11)

En el caso en cuestión, Cambridge Analytica empleó una empresa llamada Global Science Research (GSR) para generar repositorios de perfiles de usuarios digitales. A su vez y con negociaciones directas con el Directorio de Cambridge Analytica, GSR tuvo acceso los estudios de Aleksandr Kogan, profesor del Departamento de Psicología de la Universidad de Cambridge.

Christopher Wylie, quien describió el funcionamiento de Cambridge Analytica e hizo posible el escándalo, explica: “Lo que Kogan nos ofreció [...] fueron apps en Facebook que tenían permisos especiales para recolectar data, no tan solo de quienes habían usado la app, si no que podían entrar en toda la red de amistades que estos tenían y captar su data. Cosas como, me gusta, actualización de estados, e incluso en algunos casos mensajes privados. Con esto, solo necesitamos unos cuantos cientos de personas para perfilar a todo Estados Unidos”^{231,232}

Entre las apps que permitían el acceso para general perfiles, destaca uno que Aleksandr Kogan desarrolló el 2014. Un test de personalidad llamado “thisisyourdigitallife”, el cual pago menos de 5 dólares a 270,000 estadounidenses que participaron. Para realizar la encuesta, los participantes tuvieron que iniciar sesión en Facebook, y sin que estos supieran, entregaron acceso a su perfil, ubicación, y sus “Me gusta” de Facebook; e incluso, a segmentos de información de todos sus Amigos de Facebook y con esto, los datos de hasta 87 millones de estadounidenses. Una cuarta parte de todos los usuarios de Facebook de EE. UU.

Con esta información, a través de un tratamiento de datos avanzado, “Cambridge Analytica logró saber cuál debía ser el contenido, tema y tono de un mensaje para cambiar la forma de pensar de los votantes de forma individualizada. [...] (esto con) publicidad personalizada, y noticias falsas que luego se replicaron a través de redes sociales, blogs y medios”²³³.

²³¹ Entrevista de The Guardian a Christopher Wylie. En línea: What is the Cambridge Analytica scandal? (2018, 20 marzo). [Video]. YouTube. https://www.youtube.com/watch?v=Q91nvbJSmS4&ab_channel=TheGuardian [min: 1:10]

²³² Si bien, la investigación Aleksandr Kogan originalmente fue permitida por la política de tratamiento de datos de Facebook al tratarse de una investigación académica, la venta a Cambridge Analytica no estaba permitida.

²³³ Afirmación de BBC. En línea: <https://www.bbc.com/mundo/noticias-43472797>

Debido al escándalo iniciado por Wylie en marzo de 2018, dado que la recolección de datos fue mediante la red social, "Facebook terminó con el suscribiendo un acuerdo con la Comisión Federal de Comercio de Estados Unidos (FTC) comprometiéndose al pago de una multa de 5000 millones de dólares como consecuencia de las diversas irregularidades detectadas en su sistema de privacidad"²³⁴. Sin embargo, dos comisionados de la FTC de los cinco miembros disintieron de la resolución al considerar que la sanción es insuficiente. Al respecto, el comisionado Rohit Chopra, quien voto en contra, expresó: "el acuerdo propuesto hace poco para cambiar el modelo comercial o las prácticas que llevaron a la reincidencia"; y no "impone cambios significativos en la estructura de la compañía ni en los incentivos financieros, que llevaron a estas violaciones"; tampoco "incluye restricciones a la vigilancia masiva o las tácticas de publicidad de la compañía"²³⁵

²³⁴ Como se citó en Herrera, Paloma y Pablo Viollier. (2020) (p.110)

²³⁵ DW. EE.UU. multa a Facebook con US\$5.000 millones por violación de privacidad. El Mostrador. 2019. <https://www.elmostrador.cl/dia/2019/07/24/eeuu-multa-a-facebook-con-5-000-millones-por-violacion-de-privacidad/>

PROBLEMAS CON LA PERSONALIZACION

RETÓRICA ARTIFICIAL

Al no ser limitado el perfilamiento, queda abierta la posibilidad de la personalización retórica del contenido. Como hemos tratado, no hay restricción efectiva en el ordenamiento jurídico.

Habiendo expuesto el contexto tecnológico y la legislación relativa a la protección de datos, en este capítulo trataremos distintas comprensiones del fenómeno y ahondaremos en el uso de la inteligencia artificial para la personalización retórica.

RECAPITULACIÓN

Ya sabemos que el estado de la tecnología es:

- 1- Con los dispositivos inteligentes: masivo, de gran capacidad de cómputo e interconectado. Lo que permite una enorme generación de datos y la mediación de los dispositivos inteligentes del ambiente digital a gran escala.
- 2- Con *Machine learning*: capaz de detectar patrones complejos y reaccionar. Lo que permite, reconocer, imitar y rediseñar soluciones para que algoritmos cumplan determinados objetivos²³⁶.
- 3- Revolucionario: suficientemente disruptivo como para afirmar que vivimos una cuarta revolución industrial, que destaca protagónicamente por el procesamiento de datos y el impacto en las formas de vida humana.

²³⁶ Recordemos que, machine learning implica un aprendizaje que entrena algoritmos en modelos de redes neuronales que pueden utilizar un alto nivel de parámetros y datos. Describimos estas técnicas en el Anexo.

Por otro lado, sabemos que el estado de la protección de los datos personales es:

1- Prioritariamente autogestionada por las personas corrientes mediante:

- i) El consentimiento o aceptación.
- ii) La facultad de recurrir al mecanismo jurisdiccional de tutela al que refiere actualmente la constitución. [La acción Habeas Data para ejercer derechos ARCO.]

2- Ineficiente ante brechas sistémicas frente a la tecnología, pues:

- i) Los dispositivos y softwares son corrompibles.
- ii) El perfilamiento para la personalización no requiere de mucha data.
- iii) La velocidad, escala y forma en la que se tratan los datos eluden fácilmente la fiscalización *ex post*, o la tornan imposible.

LA PERSONALIZACIÓN RETÓRICA ARTIFICIAL.

A lo largo de este trabajo, hemos afirmado que, por el desarrollo masivo e intrusivo de la tecnología y las capacidades del tratamiento de datos, existe el riesgo de la personalización retórica artificial. Fenómeno consistente en la capacidad de teorizar el estímulo adecuado para persuadir en la situación concreta (retórica) a través de la tecnología de procesamiento de datos (artificial) que adecua los estímulos (personalizada).

Como sabemos, la constante captación de data personal junto con la capacidad de detección de patrones en enormes volúmenes de información aumenta exponencialmente. Con esto, ha emergido la capacidad para entrenar al algoritmo que desarrolle una adecuada “toma automatizada de decisiones²³⁷” en torno a pronósticos del comportamiento humano,

²³⁷ Toma automatizada de decisiones o “Automated decision-making” puede ser definido como: “Secuencia de comandos de código de computadora que le dice a una computadora cómo proceder a través de una serie de instrucciones para llegar a un punto final específico”. Lupton, D. (2015). Digital sociology. Routledge, Taylor & Francis Group (p. 49-50). [original] “sequence of computer code

para inducir reacciones mediante una adecuación del escenario de opciones e información en la que navega el 'sujeto'²³⁸. “Ya que con los macrodatos se pueden capacitar sistemas de IA que utilicen redes neuronales y modelos estadísticos, con el fin de predecir algunos acontecimientos y comportamientos” (Herrera y Viollier, 2020)²³⁹

Una vez entrenado el algoritmo que ha detectado como influir en el comportamiento de un individuo, por reconocer en el ciertas tendencias y conocer cómo reaccionan ante determinado estímulo otros individuos con un patrón conductual similar²⁴⁰, se puede personalizar retóricamente un estímulo. Es decir, se logra “aprovechar el acceso a la información sobre los usuarios y su control sobre la experiencia, para inducir a error, coaccionar o perjudicar de cualquier otro modo” (Calo,2017)²⁴¹

De esta forma, tal como señala Wolfie (2017), “las instituciones pueden utilizar la personalización y la persuasión impulsada por datos contra las personas, tanto en el entorno que ellos mismos controlan y como en todo el mundo digital. Basado sobre el acceso a información privada sobre la vida y el comportamiento de las personas, las empresas pueden fácilmente personalizar prácticas manipuladoras, engañosas o incluso coercitivas, utilizando asimetrías de información, debilidades personales o sesgos cognitivos con el fin de confinar o enmarcar las opciones que tiene alguien, o para influir selectivamente en el comportamiento, limitando la agencia personal y política, autonomía y dignidad de las personas. Tales estrategia se utilizan en diversas áreas, como la publicidad conductual, el marketing y las ventas, así como noticias, entretenimiento y campañas políticas.”²⁴²

Como vemos, “las redes actuales de seguimiento y elaboración de perfiles digitales se pueden utilizar claramente para influenciar y manipular a la gente”, y “si bien tales tácticas

commands that tells a computer how to proceed through a series of instructions to arrive at a specified endpoint.”

²³⁸No está de más recordar que, “sujeto” literalmente significa ‘estar sometido’.

²³⁹ Op cit. Herrera, Paloma y Pablo Viollier. (2020) (p.123)

²⁴⁰ Para mayor ahondamiento en como *machine learning* logra esto, ver el acápite de *machine learning* en el anexo.

²⁴¹ Calo, Ryan and Rosenblat, Alex (2017): The Taking Economy: Uber, Information, and Power (March 9, 2017). Columbia Law Review, Vol. 117, 2017; University of Washington School of Law Research Paper No. 2017 08. <https://ssrn.com/abstract=2929643>. Como se citó en Op.cit Christl, Wolfie (2017). (p.31)

²⁴² Op.cit Christl, Wolfie (2017). (p.43)

pueden estar en su infancia ahora, probablemente será aún más eficaz en los próximos años.”²⁴³

EL CORROSIVO PODER

El registro y procesamiento de información para la inducción al comportamiento, es para muchas empresas un asunto de enorme interés. Es más, para muchos, es el modelo de negocios que les sustenta. Sea ya para vender un perfilamiento o, para directamente, prever, inducir o controlar la conducta en base al conocimiento o pronóstico sobre el comportamiento humano.

En este sentido, Ospina-Celis y Upegui Mejí (2020), señalan que, “el valor económico de los datos y las posibilidades que surgen para la industria de su correcta explotación han llevado a que miles de empresas busquen ingresar a dicho mercado [...] estas realizan análisis o recolección de datos, venden productos o servicios que se basan en datos como su fuente principal, y/o los datos son un recurso valioso dentro de su modelo de negocio”²⁴⁴. Por lo mismo, de hecho, “es posible argumentar que el perfilamiento de los usuarios se encuentra en el corazón del modelo de negocios de muchas de los principales gigantes de Internet” (Herrera y Viollier, 2020)²⁴⁵

Compañías como Google y Facebook dependen de la monetización de los perfiles, los que han logrado por registrar detalladamente nuestro comportamiento; y, como contraparte a esta monetización, empresas económicas y políticas, tienen interés en estos datos para inducirnos. Sea con la personalización de sus productos, a fin de hacerlos más atractivos, o con un mensaje, información o margen de opción personalizado, no es difícil ver que a intereses políticos y económicos es un anhelo ostentar la capacidad de segmentar población, entender sus deseos o miedos, y conocer que es lo que estadísticamente los persuade.

²⁴³ Op.cit Christl, Wolfie (2017). (p.43)

²⁴⁴ Ospina-Celis y Upegui Mejí. (2020) Festín de datos Empresas y datos personales en América Latina. Editorial Dejusticia, ISBN 978-958-5597-31-0 (p.6). Citando a (Hartmann, Zaki, Feldman y Neely 2014, 6).

²⁴⁵ Op cit. Herrera, Paloma y Pablo Viollier. (2020) (p.109)

“Por lo general el perfilamiento de los usuarios se da con fines comerciales, como los de ofrecer publicidad dirigida y dar acceso a ciertos bienes o servicios, lo cierto es que esta práctica corporativa no está exenta de riesgos, especialmente de aquellos asociados con la modificación del comportamiento online de las personas” (Marder, Joinson, Shankar y Houghton, 2016)²⁴⁶

En la misma línea anterior, el inversor de una de las referidas compañías “unicornio” más prometedoras a 2020 en Argentina, Martín Migoya, CEO y cofundador de “Globant”, con mucha convicción afirma que los disruptores tecnológicos en el mercado hoy son por un lado “la digitalización” y por otro, la capacidad de “transformación cognitiva”. Afirma: “(El mundo de las empresas) hoy en tecnología está viviendo dos transformaciones masivas al mismo tiempo. La primera es la transformación digital que usted está viviendo con todo el tema de las aplicaciones [...] (Por otro lado) tenemos otro mercado enorme pasando junto a este fenómeno, la transformación cognitiva, que es la llegada de la inteligencia artificial como una herramienta de disrupción para absolutamente todos los negocios que se les ocurran”²⁴⁷.

Como dice Migoya, la “transformación cognitiva” o la “ingeniería social de los datos” es un aspecto que “a toda empresa debiera llamar la atención”. No muy diferente, pero de forma crítica a la consolidación de la empresa que utiliza este poder, Jaron Lanier -famoso informático estadounidense-, refiere que con este fenómeno vivimos la aparición de “*Behavior modification empires*”²⁴⁸.

¿QUÉ TIENE ESTO DE NUEVO?

Posiblemente se preguntarán ¿qué tiene esto de nuevo? siempre se ha querido influir en la comprensión, decisión o comportamiento, del consumidor o ciudadano para aumentar las ventas, apoyo o votos; sea con la ingeniería social o psicológica, la censura o la interesada

²⁴⁶ Ospina-Celis y Upegui Mejí. (2020) EMNBD y protección de datos personales en brasil, chile, colombia y méxico: la experiencia común.

²⁴⁷Experiencia Endeavor Córdoba - 2019 - Martín Migoya - Globant <https://youtu.be/me0K5ghXDeE> (El paréntesis es nuestro)

²⁴⁸ TED. (2018, 3 mayo). How we need to remake the internet | Jaron Lanier. YouTube., online: <https://youtu.be/qQ-PUXPVlos?t=445> [video. 7:25]

enfaticación. Los *Behavior modification empires* ya existían. La influencia psicosocial, como el resultado de un meticuloso estudio del comportamiento y ánimo de los seres humanos, como medio para satisfacer intereses políticos y económicos, no es algo poco frecuente en el sector público o privado desde hace varios años. Los gobiernos desean la obediencia y los privados la venta, el consumo, las ganancias. El poder económico y político ha utilizado la capacidad de generar perspectivas mucho antes de la capacidad de conocer y personalizar de hoy.

De hecho, es la idea contenida en el libro '*Manufacturing Consent*'²⁴⁹ de Noam Chomsky y Edward Herman de 1989. En este libro la idea es clara, los medios informan de forma servil e interesada al público para generar consenso. Es más, Noam afirma que la función primaria de los medios masivos, es movilizar apoyo público a intereses del gobierno y el sector privado²⁵⁰. Para ello, los poderes hacen un 'control de agenda'.

En palabras de Chomsky 'el control de agenda': "lo hacen por todas las maneras posibles; por selección de temas, por distribución de interés, por énfasis, creando falsos problemas, por filtrado de información, mediante delimitar el debate dentro de ciertos límites. Ellos determinan, ellos seleccionan, lo moldean, ellos controlan, restringen, en orden de servir los intereses de los dominantes grupos de élite en la sociedad."²⁵²

De igual forma, la pretensión de generar apoyo, consenso o deseo están presente en la economía y la política. No por nada la publicidad y la propaganda han estado largo tiempo bajo la lupa de la revisión ética del actuar que abiertamente pretende la inducción del comportamiento. Siendo un hecho notorio desde antiguo, como acuso Vance Packard (1957)²⁵³, la industria constantemente ha utilizado el "análisis de motivación" para explotar

²⁴⁹ La traducción literal es "Manufacturación del consentimiento" o "Fabricando consenso", la versión española del libro es 'Los guardianes de la libertad'.

²⁵⁰ Chomsky detecta 5 filtros en el dominio de la discusión pública para generar consenso. 1. La propiedad que instrumentaliza para su beneficio el medio de comunicación. 2. La publicidad, que es el real sustento económico. 3. La complicidad confabulada de la clase dirigente. 4. La marginación, censura y represión a la oposición. 5. El enemigo común.

²⁵² Noam Chomsky - Manufacturing Consent. Extracto del documental "Manufacturing Consent: Noam Chomsky and the Media" (1992). [Video]. YouTube. https://www.youtube.com/watch?v=Rwh1HCb_xnk&ab_channel=Bega (min: 36:48)

²⁵³ Véase en general Packard, V. (1957). *The Hidden Persuaders*.

“fragilidades personales y debilidades de la conciencia”²⁵⁴ al apelar a elementos no racionales y subconscientes para el servicio del *marketing*.

Es más, toda una rama de la psicología emergió y se potencio a propósito de la demanda del mercado para explotar este aspecto. En este campo destaca el trabajo de los psicólogos norteamericanos John Watson -creador del conductismo americano- y Burrhus Skinner, quienes defendieron el uso de la psicología de masas como mecanismo de transformación social²⁵⁵ y, de paso sea, cooperaron activamente con la publicidad y propaganda para probar sus descubrimientos²⁵⁶.

Las ciencias del comportamiento no son un campo nuevo en lo que a *marketing*, propaganda y control mediático respecta. Sin embargo, este escenario es abrumadoramente distinto. Hoy enfrentamos a la ciencia de los datos y del comportamiento aliados. En la historia, el interés sobre la capacidad de influir en nuestro comportamiento siempre ha existido, pero el uso de avanzados medios digitales no. Por ello la preocupación de pensar el fenómeno con otros ojos. Nunca como hoy se ha llevado de forma personalizada, coordinada y masiva, el ejercicio de medios psicológicos para la afectación del comportamiento. Por lo mismo, a este respecto, Sunstein (2016) ha llamado a pensar una nueva “ética de la

²⁵⁴ El autor utiliza los términos ““Hidden weaknesses and frailties”

²⁵⁵ Skinner llamaba a su clase de conductismo, “radical” y propuso el uso extendido de técnicas psicológicas como una forma de ingeniería social. “Skinner pretende explicar, predecir y controlar (provocar y modificar) la conducta de los organismos vivientes (incluyendo al hombre), partiendo del siguiente principio, que con frecuencia es usado en la pedagogía: si reforzamos una conducta, ésta volverá a repetirse, y si no la reforzamos no se aprende. Si esto es verdad, cualquiera que concierta habilidad (tecnología de la conducta) premie o castigue puede hacer que otro haga lo que él quiera mediante el refuerzo o su ausencia”. Luis García Vega. Las principales concepciones psicoantropológicas como referente para la actividad profesional del psicólogo. UNMSM Revista de Investigación en Psicología Año II No. 2

²⁵⁶ Así mismo; “Watson ofreció un curso de psicología aplicada titulado Psicología de la Publicidad, introdujo en varias empresas las técnicas experimentales para el mercadeo de sus productos y, tras su retiro de la vida académica, se vinculó a la agencia de publicidad Walter Thompson, donde desarrolló campañas masivas con los mismos principios de las reacciones emocionales condicionadas. [...] Watson es el precursor de los desarrollos científicos de la psicología del consumidor.” Parrado Corredor, F. (2013). J. B. Watson y la publicidad, los inicios de la psicología del consumidor. Revista Colombiana de Psicología, 22(2), 401-406.

influencia”²⁵⁷, pues ya no tratamos ante el canal tradicional donde la publicidad y la propaganda ya era cuestionable; ahora estamos en un escenario donde el poder de la influencia es mucho más efectivo. El monitoreo de nuestras interacciones, incluso en tiempo real, abrió un campo que levanta aún más cuestionamientos éticos. Comentando las ideas de Sunstein, Susser et al. (2019) dice: “Hay una sensación creciente de que las formas de influir en los consumidores, cuales alguna vez toleramos -quizás a regañadientes-, se han vuelto intolerables.”²⁵⁸

Con la migración del *marketing* al espacio digital, no podíamos esperar que cesase la explotación de nuestras vulnerabilidades, o “fragilidades personales y debilidades de la conciencia”, en términos de Vance Packard. Ha sucedido todo lo contrario. De hecho, el emerger de la relación entre la tecnología de la información y el *marketing* han facilitado el poder sobre la inducción al comportamiento, ya que está amparada en los avances de las ciencias del comportamiento y de los datos -*behavioral science & data science* o *Behavioural Data Science* -.

Similar a lo expuesto, y publicitando sus servicios, “Websfarm” -empresa con sede en Londres de automatización empresarial digital (entre ellos de *marketing*) -, en su sitio web describe la llegada de “*Behavioural Data Science*” al *marketing*: “El uso de datos del comportamiento para comprender las preferencias de los consumidores no es un concepto nuevo para los especialistas en *marketing*. Sin embargo, en el pasado, los investigadores de *marketing* han tenido problemas con la confiabilidad de sus datos; es decir, los datos se limitan a una muestra de encuestados pequeña, hay fallas en el diseño de la encuesta, las técnicas analíticas son incorrectas y mucho más. Los datos de comportamiento (*Behavioural Data Science*), por otro lado, presentan a los especialistas en *marketing* datos precisos y económicos sobre lo que hacen realmente los consumidores. La ciencia de datos del comportamiento, es útil para modelar y predecir mejor el comportamiento, combina técnicas de las ciencias del comportamiento -psicología, sociología, economía, etc.- con una plétora de

²⁵⁷ En general véase: Sunstein, C. R. (2016). *The Ethics of Influence: Government in the Age of Behavioral Science*. Cambridge Studies in Economics, Choice, and Society.

²⁵⁸ Op Cit. Susser, D., Roessler, B., & Nissenbaum, H. F. (2019). (p.6)

enfoques computacionales que van desde las ciencias de la computación, la ingeniería centrada en datos, la estadística y más.”²⁵⁹

Las afirmaciones de esta compañía, que ofrece servicios de *Behavioural Data Science*, no se diferencia mucho de lo que, con temor, señala Wolfie (2017): “el conocimiento generado a partir de grandes conjuntos de datos, conocimientos de la ciencia del comportamiento y de la experimentación permanente con personas reales -producto de un proceso que típicamente ocurre sin el conocimiento de los sujetos -, es capitalizado para el uso de manipuladores y explotadores a través de la personalización del entorno digital”.²⁶⁰

El análisis de datos sobre el comportamiento humano ha cambiado la forma en que el *marketing* opera, y seguirá cambiándolo. Permiéndole ser más persuasivo y eficiente, incluso en términos de inversión. Este aspecto lo podemos ver aumentar en Chile, por ejemplo, en el caso de Falabella y PedidosYa. Como señalan Herrera y Viollier (2020), “en ambos casos la información recolectada gira entorno a sus compras, potenciales compras y hábitos de navegación, con el objetivo de poder ofrecer al usuario ofertas personalizadas para inducirlo a consumir determinados productos.”²⁶¹

Respecto de la evolución del *marketing*, Miyazaki, del departamento de *Marketing & Logistics* de la escuela de negocios de ‘*Florida International University*’, describe “que el poder de cómputo accesible y las soluciones de software se han combinado para mejorar drásticamente el marketing” ²⁶². Miyazaki señala tres grandes ventajas sobre el canal

²⁵⁹ Websfarm Digital Business Automation Company (2021, 12 abril). What’s Behind Behavioural Data Science? En línea: <https://www.websfarm.net/whats-behind-behavioural-data-science/> (consultado en octubre 2021)

²⁶⁰ Christl, Wolfie (2017). How companies use personal data against people. Working paper by cracked LABS. Published. (p.43)

²⁶¹ Op cit. Herrera, Paloma y Pablo Viollier. (2020) (p.92) Los autores también señalan el monitoreo en las respectivas políticas de privacidad de estas compañías. “Así, Falabella señala en forma general la utilización de cookies analíticas “En Falabella usamos cookies y tecnologías similares para personalizar y mejorar tu experiencia de cliente y para mostrarte publicidad online relevante”, mientras que PedidosYa en su apartado de cookies indica con mayor detalle que usan cookies analíticas, de sesión y persistentes al señalar que recopilan “Información acerca de su computadora, y acerca de sus visitas y uso de este sitio web incluyendo su dirección ip, ubicación geográfica, tipo de navegador, fuente de referencia al sitio, duración de las visitas y número de vistas por página”.

²⁶² Anthony Miyazaki - How Digital Is Changing the Future of Marketing / #MarketingMinute 134 (Marketing Strategy). (2020, 14 abril). [Video]. YouTube.

tradicional: En primer lugar, lo digital es flexible y eso permite que campañas se realicen con relativamente poco esfuerzo [...] En segundo lugar, ha ayudado a remodelar las estrategias generales, aclarando necesidades, los deseos del mercado, además de llevarnos a descubrir pasos ocultos en la decisión de compra del cliente [...] y, en tercer lugar, genera la capacidad de micro segmento, que es más eficaz en la entrega del correcto mensaje a las personas adecuadas”

Preguntándose por el futuro del *marketing*, Miyazaki, en el corto plazo reconoce los siguientes cambios: “Se aumentará el conocimiento sobre los consumidores. [...] Todos los dispositivos inteligentes recopilan información sobre el comportamiento del consumidor individual [...] a medida que se tengan los datos de comportamiento, se puede apuntar a audiencias o individuos específicos, con productos relevantes, promociones y los precios relevantes. [...]” Por otro lado, “la ultra micro focalización se convertirá en lo normal. [...] una vez que se tenga suficiente información, el mensaje será dirigido a tus sentimientos particulares, estados de ánimo y comportamientos en el momento exacto [...] en otras palabras en el momento en que te sientes frustrado o alegre o triste o inseguro, se buscara una ventaja sobre tu estado de ánimo.” Además, “el *marketing* se volverá cada vez más automatizado. La inteligencia artificial y *Machine learning* ha permitido crear mensajes e incluso conversaciones personalizadas que no requieren un humano. [...] La toma de decisiones automatizada ya está en uso y la próxima década verá un salto en el uso de estas herramientas.”

LLEGAR A LO ADECUADO PARA PERSUADIR

Como afirma Yeung (2016), no hay verdaderas dificultades en “monitorear y perfeccionar el entorno de elección del individuo a la luz de las tendencias poblacionales identificadas a través del análisis de vigilancia de Big Data”. Esto inclusive, para generar “entornos de elección altamente personalizados en contextos de toma de decisiones, resaltando las

[https://www.youtube.com/watch?v=MjtB32ryJXQ&list=WL&index=11&t=201s&ab_channel=Anthony Miyazaki](https://www.youtube.com/watch?v=MjtB32ryJXQ&list=WL&index=11&t=201s&ab_channel=AnthonyMiyazaki)

vulnerabilidades identificadas a través de la vigilancia digital, en un esfuerzo por influir en nuestras elecciones.”²⁶³

Similarmente, se jacta el exdirector ejecutivo de Cambridge Analytica, Alexander Nix, al describir como personalizar el contenido de forma automatizada y efectiva. “No necesitamos adivinar qué solución creativa puede funcionar o no. Podemos utilizar cientos o miles de puntos de datos individuales sobre nuestras audiencias objetivo para comprender exactamente qué mensajes van a atraer a qué audiencias “[...] “para ello contamos con un instrumento cuantitativo para investigar los rasgos subyacentes que informan la personalidad”²⁶⁴

Cómo y cuándo apelar a lo emotivo o irracional, o a lo que parece ser algo argumentativamente razonable para un determinado perfil con determinadas creencias, gustos e intereses, etc., es asunto de controlar el medio y tener los datos suficientes para entrenar el acertado actuar de una inteligencia artificial a fin de detectar el ánimo y concluir el argumento más persuasivo. En esto, cuanto más información se tenga de las preferencias, hábitos, miedos, deseos, o cualquier otro elemento de la personalidad y psicología, será más simple construir la arquitectura que se adecúe persuasivamente al perfil.

Al respecto Noah Harari²⁶⁵ en Davos²⁶⁶ 2020 afirma: “Con tener suficiente poder de computación y datos, pueden hackear mi cuerpo y mi cerebro [...] Ya saben más sobre mí de lo que sé sobre mí, y pueden hacerlo con todos. [...] puedes conocer mi tipo de personalidad, mis opiniones políticas, mi preferencias sexuales, mis debilidades mentales, mis más profundos miedos y esperanzas. [...] Un sistema que nos entiende mejor de lo que nosotros

²⁶³ Yeung, K. (2016). ‘Hypernudge’: Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118-136. <https://doi.org/10.1080/1369118x.2016.1186713> (P. 122)

²⁶⁴ Alexander Nix, Cambridge Analytica - The Power of Big Data and Psychographics. (2016, 27 septiembre). [Video]. YouTube. https://www.youtube.com/watch?v=n8Dd5aVXLcc&ab_channel=Concordia [Consultado: marzo 2021] – Como se cito en: Op cit. Roessler, F. Nissenbaum (2019).

²⁶⁵ Yuval Harari, es historiador de la Universidad hebrea de Jerusalén, PhD Jesus College in the University of Oxford. Es el conocido autor de los science bestsellers, “Sapiens; de Animales a Dioses” (2014), y “21 lecciones para el siglo 21” (2018), entre otros.

²⁶⁶ Davos es el lugar donde se realiza año a año la exclusiva cumbre del Foro Económico Mundial. En él, se reúnen importantes políticos, empresarios y distintos representantes de organizaciones sociales y culturales para buscar soluciones a problemas globales.

nos entendemos, que puede predecir nuestros sentimientos y decisiones puede, manipular nuestros sentimientos y decisiones, y en última instancia, tomar decisiones por nosotros.”²⁶⁷

Ciertamente, estamos en una situación desafiante. La existencia de un sistema que tenga datos sobre el comportamiento y que busque el medio indicado para persuadir en la situación concreta, monitoreando y perfeccionando el entorno, junto con, “la posibilidad de disponer de un sistema de aprendizaje automático que, en tiempo real, a partir de un flujo de eventos en directo, sea capaz de modificarse para ajustarse a las variaciones de dichos eventos, plantea un reto tan atractivo como complicado”^{268,269}, y no por nada. En lo que a manipulación respecta, es una capacidad que podría transformarlo todo.

LA CAPACIDAD DE TRANSFORMARLO TODO

Con el aparecer de la personalización retórica que permite una nueva escala de influencia a través de lo que señalamos como retórica artificial, algunos autores han teorizado sobre el fenómeno. Entre ellos destaca la psicóloga social y autora del libro ‘La era del capitalismo de vigilancia’, Zuboff.

Zuboff plantea que con esta nueva esfera de influencia ha aparecido un mercado del comportamiento *-behaviour marketplace-* para conocer al individuo y personalizar la producción o el mensaje – microtargeting²⁷⁰-. Con esto, ha emergido lo que ha llamado “capitalismo de la vigilancia”, un sistema político económico y social que requiere la mercantilización de datos personales y su transformación a ser mercancía sujeta a la compraventa con fines de lucro.

²⁶⁷Yuval Noah Harari. (2020, 24 enero). Yuval Noah Harari: How to Survive the 21st Century- Davos 2020. Online: YouTube.

https://www.youtube.com/watch?v=gG6WnMb9Fho&ab_channel=YuvalNoahHarari (minuto 9:40)

²⁶⁸ Tome prestada esta expresión de Jerónimo García y Loygorri Herreros, pero no el sentido con el que fue utilizado, él se refería a otro problema al uso del aprendizaje automático en general, al “desarrollo de sistemas que estén aprendiendo ininterrumpidamente de un flujo (stream) constante de eventos”.

²⁶⁹ Jerónimo García-Loygorri Herreros de Tejada. (2019, 11 abril). BBVA Innovation Labs ; Redes neuronales distribuidas con Tensorflow: Conclusiones- <https://www.bbva.com/es/redes-neuronales-distribuidas-tensorflow-conclusiones/> (Consultado el 6 de abril 2020)

²⁷⁰ Término utilizado comúnmente para referir a mensajes dirigidos altamente personalizados

En sus palabras, el capitalismo de la vigilancia es un “nuevo orden económico que reclama para sí la experiencia humana como materia prima gratuita aprovechable para una serie de prácticas comerciales ocultas de extracción, predicción y ventas” [...] (que) “aspira a imponer un nuevo orden colectivo basado en la certeza absoluta”²⁷¹. En visión de Zuboff, este sistema existe gracias a la posibilidad detectar en tiempo real el estado de ánimo, las preocupaciones, o cualquier otro síntoma que sirva para conocer la reacción posible ante un determinado estímulo. Permitiendo al capitalismo crear orientaciones en base a las predicciones. Zuboff: “Los capitalistas de la vigilancia descubrieron que los datos conductuales más predictivos se obtienen interviniendo en la marcha misma de las cosas para empujar a, persuadir de, afinar y estimular ciertos comportamientos a fin de dirigirlos hacia unos resultados rentables.” [...] “De ese modo, el capitalismo de la vigilancia da a luz a una nueva especie de poder instrumental, que conoce el comportamiento humano y le da forma, orientándolo hacia los fines de otros.”²⁷²

El capitalismo instrumentaliza esta capacidad tecnológica según Zuboff por la necesidad de adecuar la producción a los datos recolectados y, a los sujetos a la producción. Por lo mismo, esta nueva capacidad cruza todo aspecto de la estrategia económica y política contemporánea, siendo el tratamiento de datos un rasgo esencial de los medios de producción para la generación de capital y poder. Como afirma Zuboff, ciertamente, la propaganda y la publicidad han sido el promotor, pero la trascendencia de esta nueva capacidad histórica tiene el un potencial suficiente como para definir la época y las relaciones de producción.

La explotación de las fragilidades personales y debilidades de la conciencia que son reveladas por las ciencia de la computación y del comportamiento, es una herramienta atractiva para el poder. Este es un hecho grave para el libre desarrollo de nuestra conciencia y una gran oportunidad para el mercado.

²⁷¹ Esta definición se encuentra en el libro de la psicóloga social Shoshana Zuboff “La era del capitalismo de vigilancia” en el apartado inicial “definiciones”. El capitalismo de vigilancia es un concepto popularizado el 2014 por la autora.

²⁷² Op cit. Zuboff, S. (2020). La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder. Ediciones Paidós. (p.18)

Como menciona Calo (2013) ²⁷³: “La tendencia es que las empresas no solo aprovechen una comprensión general de las limitaciones cognitivas, si no que descubran, e incluso desencadenen la fragilidad del consumidor inclusive en un nivel individual” [...] lo que, “constituye una forma de persuasión peligrosa para los consumidores o la sociedad”.

Sabemos que el ‘cómo, cuándo y qué’ información es presentada por nuestros dispositivos inteligentes puede tener un efecto significativo en cómo nos sentimos y quiénes somos. Sabemos que toda aquella información que considera en su forma y fondo un tratamiento de datos²⁷⁴ puede ser eficaz en esto. Sabemos que existe un interés en rentabilizar la generación de perfiles y la personalización retórica de la información. Sabemos que este poder despierta un interés más allá que generar anuncios publicitarios dirigidos. Sabemos que este poder tiene la capacidad de moldear la forma con la que entendemos la realidad.

²⁷³ Calo, M. R. (2013). Digital Market Manipulation. SSRN Electronic Journal. doi:10.2139/ssrn.2309703. (p.2)

²⁷⁴ Y, también aquella que es presentada en medios no digitales pero que responden a un análisis que se ha valido de tratamiento de datos. - Labor que, por ejemplo, Instagis cumplía al señalar el espacio publicitario físico más oportuno a sus clientes. -

LA VULNERABILIDAD HUMANA, LA CONCIENCIA ES UN FENOMENO MALEABLE.

Ya en 1992, Bryan Pfaffenberger, denominó “*Networked information Technologies*” aquellas tecnologías que “configuran” a sus usuarios tanto influyendo en su comportamiento como mediando la percepción, ya sea porque predispone el diseño o la información al usuario, a actividades más fáciles o naturales de forma implícita.

Claramente las capacidades tecnológicas hoy han superado el estado donde las “*Networked information Technologies*” fueron pensadas. Definitivamente configurar a los usuarios tanto influyendo el comportamiento como mediando la percepción es más simple, no tan solo porque hay actividades que predisponen de forma implícita, sino especialmente, por poder percibir al usuario y personalizar la interacción para explotar la capacidad de configurar al usuario. Lo tratado por Pfaffenberger, es vigente y más agudo.

El problema de la agencia -el problema de la capacidad que posee un agente para actuar en un mundo-, salta a la vista inmediatamente ante la irrupción del interés y la capacidad técnica que busca predisponer la experiencia humana para influir. Esto pues, captar y reorientar una conducta tanto física como mental es posible dado lo frágil de nuestra condición.

Tenemos distintas aristas vulnerables desde donde ejercer poder y afectar nuestra capacidad de decisión con la personalización del contenido. A continuación, sin desconocer la existencia de otros aspectos vulnerables de la naturaleza humana, intentaremos exponer ciertos aspectos explotables para “configurarnos”.

Para tratar estas vulnerabilidades, tendremos en consideración las tradiciones fundadas por las ideas de Freud, Heidegger y Foucault, y explícitaremos tres aspectos vulnerables que permiten afectar la experimentalidad humana, cuales están íntimamente relacionados entre sí, y con el poder que tratamos.

En los siguientes títulos, trataremos sobre el sesgo cognitivo producto de la imperfección de la racionalidad junto con la dominancia del inconsciente; la gravitación de la tecnología como forma y medio de entender y estar en el mundo; y, la comprensión de realidad mediada por los discursos en el lenguaje.

Sabiendo la naturaleza poco común para los trabajos en derecho en Chile, de en estos términos dar una mirada sobre la vulnerabilidad de la condición humana, es oportuno antes de iniciar hacer manifiesta esta afirmación:

“Actualmente las teorías éticas, políticas, sociales y jurídicas, han abandonado los compartimentos estancos y se interceptan en un productivo espacio de elaboración interdisciplinar (...) no debe sorprender que los juristas se ocupan de la economía o de la literatura o del psicoanálisis o del tiempo. Así entonces el derecho ha de ser repensado, reconstruido desde las paradojas y contradicciones que subyacen a la vida en conjunto en el ciber mundo del s. XXI”. - (Cárcova, 2009) ²⁷⁵

EL SESGO DE LO RACIONAL Y EL INCONSCIENTE

Hay un rasgo permanente en la experimentalidad que puede ser utilizado por la retórica artificial, lo no racional o los espacios ciegos de la razón.

Desde el quiebre que tuvo la ciencia de la modernidad, al consolidar la idea de la existencia y dominancia del inconsciente en la función psíquica²⁷⁶, las ideas torno a la identidad racional, lógica y homogénea, no pudieron sostenerse. El aparato psíquico revelado por Freud era inmensamente endeble y estructurado en una serie de niveles fuera del alcance de la conciencia y de la capacidad de control. Con este giro aparecía evidente una vulnerabilidad. El sujeto opera en el mundo no de forma racional y, tampoco con autodominio. El sujeto vive en una apariencia de libertad. Esta es la idea del sujeto producido fuera del ‘yo’ Freudiano.

²⁷⁵ Cárcova, C. M. (2009): Las Teorías Jurídicas Post Positivistas. (p.125). Como se citó en: Carreño Dueñas, Dalia (2012): "El derecho en la era de la virtualidad. nuevas realidades, nuevo derecho virtual" (p.263)

²⁷⁶ En este mismo sentido Foucault afirma " El psicoanálisis fue ciertamente la práctica y la teoría que replanteó de la manera más fundamental la prioridad conferida al sujeto, que se estableció en el pensamiento occidental a partir de Descartes". Foucault, M., & Lynch, E. La verdad y las formas jurídicas. Ed. Gedisa (1992). (p. 8).

Esta revelación es un giro a la comprensión de mundo en occidente, es una herida inextinguible²⁷⁷, que genera el derrumbe de la teoría económica neoclásica tradicional y así mismo, de todas las ciencias que plantearon al ser humano como el agente racional y autocontrolado.

Con el desarrollo de la psicología, disciplina que procuro buscar estructuras y canales para tratar el padecimiento y entender al ser humano, se revelaron ideas como neurosis – en breve, el conflicto interno entre el consciente (el yo) y el inconsciente (el ello) y su descarga-, o los mecanismos de formación del deseo o el deseo como pulsión²⁷⁸, manifestando una clara área del actuar humano que queda fuera del control. Cual incluso, es maleable a la adecuación de los elementos que tengan la carga psíquica y generen tensión dentro de la estructura del sujeto.

Más allá del psicoanálisis, la dominancia de motores psicológicos complejos fuera de la conciencia, hoy es una afirmación indiscutida en las ciencias económicas y sociales. La conciencia es un fenómeno frágil, fuera de nuestro control. Sabemos plenamente que la voluntad libre es parcial. En este sentido, desde una aproximación distinta -pero complementaria- a Freud, destacan las ideas de Daniel Kahneman y Amos Tversky²⁷⁹.

El concepto *bounded rationality*²⁸⁰ es el concepto consolidado por el artículo que llevaría el premio nobel de Economía del año 2002 a Kahneman. En este artículo, señaló la importancia de la investigación psicológica en la ciencia económica, proponiendo desde sus

²⁷⁷Esta es una alusión a una reflexión de Foucault sobre Freud. Foucault tratando las “revelaciones interpretativas” de la modernidad, comenta a Freud y señala que su planteamiento ha sido un “paso inextinguible de la interpretación moderna”, de lo históricamente imaginable. Siguiendo a esto, parafrasea a Freud. Cita literal: “Freud dice que hay tres grandes heridas narcisistas en la cultura occidental: la herida causada por Copérnico; la que provocó Darwin cuando descubrió que el hombre descendía del mono y la herida hecha por Freud cuando él mismo, a su vez, descubrió que la conciencia reposaba sobre la inconsciencia”. Foucault, M (1981). Nietzsche, Freud, Marx. Anagrama. (p.19)

²⁷⁸ La idea lacaniana de deseo es sumamente interesante, pero no la exploraremos aquí. Solo advertimos que la idea de ‘deseo’ en Lacan, es fundamental para entender la estructura de sujeto que propone. Cabe comentar que la tradición lacaniana del psicoanálisis es una de las más seguidas en el mundo.

²⁷⁹ Quien murió el año 1996 y no recibió el premio nobel.

²⁸⁰Este término fue consolidado por Kahneman Y Taversky, en Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice. Este artículo le haría merecer el Premio Nobel 2002. <https://www.nobelprize.org/uploads/2018/06/kahnemann-lecture.pdf> (última visita agosto 2020).

estudios respecto del juicio humano y la toma de decisiones, un modelo de racionalidad acotada o limitada para superar enteramente la visión del agente racional.

El concepto *bounded rationality*" refiere a que la gente utiliza reconocibles 'atajos' y 'heurísticas'^{281,282} poco fiables ante situaciones de incertidumbre -información incompleta-. Esta idea engloba que la conciencia y el razonamiento es 'limitado', especialmente por la existencia de 'sesgos cognitivos'.

Kahneman plantea que, si fuéramos enteramente racionales, es de suponer que el actuar de todos sería idéntico. Sin embargo, es evidente que no son los elementos objetivos los que ponderamos. No somos seres racionales en nuestras elecciones. Es la imperfección de la racionalidad la que no nos permite ver claramente las opciones. La razón es insuficiente, es limitada por sesgos. Ante situaciones reales, simplemente, los seres humanos no podemos ver claramente las formulaciones alternativas a los problemas, o prever las consecuencias de nuestras decisiones. Existen tendencias constantes que desvían esta capacidad racional. En todos los casos, actuamos sesgadamente.

Kahneman, afirma que no operamos enteramente desde la lógica de los elementos que componen nuestras decisiones. Estas dependen prioritariamente de cómo las opciones son percibidas. Esta característica es llamado efecto marco o "Framing Effect", concepto que dispone que, a grandes rasgos, las personas llegamos a decisiones diferentes, incluso de forma absoluta, según como se nos presente la información.

Kahneman y Tversky, en la década de los 60' y 70' comenzaron a examinar las heurísticas y sesgos humanos; en este periodo de investigación concluyeron que, ante la incertidumbre, las personas usan un número relativamente pequeño de heurísticas no racionales para tomar sus decisiones. Probaron esto demostrando que la información poco relevante para el caso, podía tener una importancia decisiva. Por eso, estos experimentos tuvieron una repercusión transversal significativa tanto en disciplinas como, la psicología, el

²⁸¹ Heurística, grosso modo, son reglas que dominan el juicio o la forma en la que hallar o inventar la decisión. Comparte etimología con eureka.

²⁸² "La heurística se puede describir como "atajos de juicio que generalmente nos llevan a donde necesitamos ir, y rápidamente, pero a costa de desviarnos ocasionalmente del curso" Cita de: Gilovich, Thomas; Savitsky, Kenneth (1996). "Like Goes with Like: The Role of Representativeness in Erroneous and Pseudo-Scientific Beliefs" doi:10.1017/CBO9780511808098.036.

derecho, la economía y las ciencias sociales en general. Hasta la publicación del artículo de 1974 “Juicio bajo incertidumbre: heurística y sesgos²⁸³”, la visión predominante en ramas de la academia que trataron el campo del juicio humano - en particular en la comunidad anglosajona- era que los seres humanos son actores racionales.

En el artículo “Judgment under Uncertainty: Heuristics and Biases”, de Amos Tversky y Daniel Kahneman, se exponen tres comunes heurísticas que como humanidad compartimos. “*Representativeness*” o, representatividad, “*availability heuristic*” o, heurística de disponibilidad y “*anchoring effects*” o, efecto anclaje.

De forma simple, podemos describir a estos sesgos cognitivos como:

- 1) *Representativeness heuristic*: refiere a la tendencia a sobrestimar las similitudes para predecir. Si algo nuevo se ajusta a una categoría existente, probablemente se perciba de esa forma. Esto revela la tendencia a agrupar lo similar para entenderlo, dotando de valor a lo que quizás no lo tiene, solo por el hecho de tener una similitud reconocida.
- 2) *Availability heuristic*: refiere a la preponderancia en las evaluación o decisión, de lo fácilmente recordable. Sea porque la información es más reciente, o se expuso de forma llamativa, o se hizo de forma reiterada.
- 3) *The anchoring effects*: “es un sesgo cognitivo que describe la tendencia humana común a depender demasiado de la primera información ofrecida (el “ancla”). Las personas usan la pieza inicial de la información para hacer juicios posteriores.”²⁸⁵

Las investigaciones de Kahneman y Tversky no se detuvieron ahí. Con los años continuaron con su labor por establecer y esclarecer en la comunidad académica el dominio de elementos no racionales en el comportamiento humano, exponiendo, en definitiva, lo limitado de la razón. Esto ciertamente porque era demostrable, y peligrosamente replicable.

²⁸³ Tversky & Kahneman. (1974) Judgment under Uncertainty: Heuristics and Biases, Science. New Series, Vol. 185, No. 4157 (Sep. 27, 1974), pp. 1124-1131 En línea en: <https://www.jstor.org/stable/1738360?seq=1> (Consultado, abril 2021)

²⁸⁵ Staff, P. (2020, 21 mayo). The Anchoring Effect and How it Can Impact Your Negotiation. PON - Program on Negotiation at Harvard Law School. Daily Blog: “El efecto ancla y cómo puede afectar su negociación”.

Dado que la humanidad comparte sesgos y entendimientos similares²⁸⁶, en cuanto podemos reconocer estos y sus consecuencias, podemos replicarlos de forma intencionada²⁸⁷. De esta forma, una inteligencia artificial -o humana- que percibe externamente nuestra conducta podría encontrar el medio indicado para persuadir, utilizando las vulnerabilidades de nuestro aparato psíquico, como, por ejemplo, las expresadas por Kahneman y Tversky.

Esto es problemático, pues son reconocibles y replicables asuntos que son fuente de sesgo. Por esto es que “los diseñadores utilizan su conocimiento sobre el comportamiento humano (por ejemplo, psicología) y los deseos de los usuarios finales para implementar funciones engañosas que no son lo mejor para el usuario” (Gray et al, 2018). De esta forma, se utilizan distintos métodos para desorientar visualmente a los consumidores, así como también la utilización de lenguaje confuso, opciones ocultas o falsas urgencias²⁸⁸

Siendo posible mediante la experiencia detectar asuntos que generan perspectivas y predecir reacciones, con la capacidad que han demostrado las *Big Data Technologies*, podemos alterar el proceso de juicio y de toma de decisiones de forma más efectiva y precisa.

Ciertamente, utilizar los sesgos de la razón o valerse de la neurosis particular de un sujeto, no es necesariamente engañar; es principalmente ordenar y exaltar de tal forma que lleve a una conclusión o disposición deseada. Pero, dado que es realmente frágil nuestro entendimiento, y no actuamos de forma plenamente racional, explotar el gran ámbito fuera de nuestro control que nos puede producir una determinada percepción, y cambiar nuestro curso de acción, o patrón de comportamiento, nos deja en una situación de vulnerabilidad.

²⁸⁶ Sobre entendimientos similares, célebremente concluye de manera dialéctica, Sócrates en el Dialogo de Platón. Gorgias 481d: “Sócrates: si los hombres no experimentaran las mismas sensaciones, unos de un modo, otros de otro, sino que cada uno de nosotros experimentara sensaciones propias sin relación con las de los demás, no sería fácil hacer conocer a otro lo que uno mismo experimenta”

²⁸⁷ He seguido para la elaboración de esta conclusión, que une las ideas de Daniel Kahneman con la posibilidad de manipular a: Online Manipulation: Hidden Influences in a Digital World 2019 Georgetown law technology review. Daniel Susser, Beate Roessler, Helen F. Nissenbaum. 10.2139/ssrn.3306006 SSRN Electronic Journal. (p.22)

²⁸⁸ SERNAC (2021). Informe de Resultados de Levantamiento de Dark Patterns en Comercio Electrónico (V: 1.2) (p.3)

No podemos desconsiderar el hecho de que la tecnología en sí misma es un agente que afecta la forma con la que entendemos y nos relacionamos con la realidad. La tecnología nos revela el mundo, y en tanto que es así, con las capacidades de hoy, se puede inducir una determinada perspectiva. Al mismo tiempo, dado que con la tecnología nos relacionamos cotidianamente incluso desde lo más íntimo, en una dialéctica, muchas veces sin defensas o cuestionamientos, nos encontramos en una situación de vulnerabilidad.

En esto, la reacción inteligente en tiempo real tiene un efecto mucho más significativo en el devenir del fenómeno de la conciencia. En este sentido es importante tener presente las consideraciones filosóficas de mundo de Martin Heidegger. En la misma línea de “Ser y Tiempo” -libro que pone en jaque la oposición cartesiana sujeto/objeto²⁸⁹ -, Heidegger, en el ensayo “La cuestión de la tecnología”, exclama la necesidad de pensar la relación dialéctica constante que tiene la materialidad y el sujeto, que inscribe al Ser en el mundo, dando énfasis a la relación del sujeto / tecnología.

En esta reflexión advirtió que la tecnología es, en último término, un instrumento que nunca es neutral a la forma en la que entendemos el mundo, es más, lo moldea. Nos dispone a ser de una determinada manera al revelarnos el mundo a través de él, a la vez que nos disponemos a ser con ella para operar. Por esto, toda tecnología influye de una forma tal, que escapa del control de nuestra comprensión. Heidegger exclama, mirando este problema, que la forma de influir la tecnología en su amplio aspecto, es el peligro más grande para la

²⁸⁹ Heidegger en el libro ‘Ser y Tiempo’ da un salto en la concepción de la filosofía contemporánea, llamando a tener como prioridad la necesidad pensar la cuestión del Ser en el tiempo, inserto en la realidad presente que transcurre y no separado de él. Con ello, Heidegger, transformo radicalmente la noción del «yo» que dominaba en ciertas tradiciones clave de la filosofía moderna, que dejó el problema del Ser y la influencia de la temporalidad en un plano secundario. En su sistema, “la cotidianidad es uno de los conceptos metódicos más importantes, pues determina el punto de partida de la analítica existencial”.

He seguido “El «yo» en ser y tiempo de Martin Heidegger” (2020), la Tesis para optar al grado de Licenciado en Filosofía UC de mi querido amigo, Vicente Jiménez Gimpel. (p.39)

experimentalidad²⁹⁰. La tecnología es un medio para relacionarnos, entender y exponernos de una forma condicionada en el mundo. Heidegger trata esta idea, en una síntesis, en la siguiente cita: "La tecnología, por lo tanto, no es un mero medio. La tecnología es una forma de revelar. Si prestamos atención a esto, entonces otro campo la esencia de la tecnología se abrirá a nosotros²⁹¹".

No en un sentido muy distinto, Verbeek (2005)²⁹² dice: "los artefactos también median las formas en que le damos sentido al mundo, organizando nuestras percepciones y proporcionando heurísticas". Klaus Schwab, similarmente afirma, y advirtiendo de lo que puede ser la cuarta revolución industrial que, "después de todo, las tecnologías están ligadas a cómo sabemos las cosas, cómo tomamos decisiones y cómo pensamos acerca de nosotros mismos y de los demás. La tecnología está conectada con nuestras identidades, visiones del mundo y futuros potenciales"²⁹³, más aún cuando estas "participan en todos los aspectos de la vida humana, median nuestras interacciones, facilitan nuestras economías, impactan nuestros cuerpos y el medio ambiente, y procesan la información de la que dependen las instituciones y los ciudadanos individuales."²⁹⁴. Por ello, "Las tecnologías y las sociedades se moldean mutuamente de manera reflexiva: somos el producto de nuestras tecnologías tanto como ellos son productos que creamos. [...] Finalmente, "las tecnologías son soluciones y productos desarrollados a través de procesos sociales que ya reflejan prioridades y valores arraigados"²⁹⁵ y "dan forma a las perspectivas sociales y nuestros valores. (Por ello) Requieren nuestra atención precisamente porque construimos nuestras economías, sociedades y visiones del mundo a través de ellos. Dan forma a cómo interpretamos el

²⁹⁰ Los tres puntos han sido destacados del ensayo en cuestión como los principales, siguiendo, o acordando con, el recomendado canal de difusión filosófica 'Epoch Philosophy' en: "Martin Heidegger: the Question Concerning Technology. (2020, 4 agosto). [Video]. YouTube. https://www.youtube.com/watch?v=gaVmEN-vGWk&ab_channel=EpochPhilosophy."

²⁹¹ Heidegger, M. (1954). *The Question Concerning Technology, and Other Essays* (1977 ed.). GARLAND PUBLISHING, INC. New York & London. (p.12)

²⁹²Citas extraídas de, Cap. 4 *The Networked Self in the Modulated Society*, Julie E. Cohen. Been, W. D., Arora, P., & Hildebrandt, M. (2015). *Crossroads in new media, identity, and law: The shape of diversity to come*. Palgrave Macmillan. (p. 68)

²⁹³Op cit. Schwab, Klaus, Davis, N., & Nadella, S. (2018). (p. 55)

²⁹⁴ Ibid. (p. 61)

²⁹⁵ Ibid. (p.73)

mundo, cómo vemos a los demás a nuestro alrededor y las posibilidades que vemos para nuestro futuro.”²⁹⁶

Tener presente entonces lo susceptible, vulnerable, que somos al relacionarnos con la tecnología en lo cotidiano, que nos dispone, tanto por ser medio y forma, a la revelación del mundo, es imprescindible para evaluar el potencial que tiene para inducir el comportamiento.

EL LENGUAJE Y EL CONTROL DE LA EPISTEME

La personalización retórica del contenido puede darle forma a la perspectiva al instrumentalizar el lenguaje, ya que el lenguaje puede ser capturado para evitar los cambios o fomentarlos. En términos de Foucault, es posible la instrumentalización de la episteme.

No es un asunto nuevo la idea de deconstruir y re-focalizar discursos, o la episteme, de forma interesada y paulatina para generar cambios magmáticos en la sociedad como estrategia ideológica. Pero explotar esta arista mediante la inteligencia artificial y la personalización del contenido, podría ser una realidad pronta -o actual-, y es un problema mayor al que somos vulnerables²⁹⁷. Perfectamente podríamos ver la idea de ‘control de agenda’ de Chomsky en una versión digital, donde una inteligencia artificial haga personalmente una “selección de temas, por énfasis, creando falsos problemas, por filtrado de información o por delimitación del debate dentro de ciertos límites, seleccionando, moldeando, controlando, restringiendo”²⁹⁸, en orden de servir a ciertos intereses.

²⁹⁶ Ibid. (p.318)

²⁹⁷ En un sentido similar, Håvard Rustad Markussen, de Universidad Sueca de Defensa, al describir el problema de la alteración del contenido, afirma: “Los discursos que rodean la focalización del mercado, o de cualquier aspecto, producen al sujeto a través y al mismo tiempo que reproducen significantes simbólicos de significado.” Esta conclusión la desarrolla tratando el caso de Cambridge Analytica desde una mirada Lacaniana. Håvard Rustad Markussen, The Political Subject of Surveillance Capitalism. (2020, 18 diciembre). [Video]. YouTube. https://www.youtube.com/watch?v=GImo8ajDyZE&list=WL&index=27&ab_channel=TheEndsofAutonomy [min 6:00]

²⁹⁸ Noam Chomsky - Manufacturing Consent. Extracto del documental "Manufacturing Consent: Noam Chomsky and the Media" (1992). Adaptado.

Ante la retórica artificial, es imprescindible considerar la vulnerabilidad humana a la personalización de las relaciones semánticas en el lenguaje. Una alteración del lenguaje puede interferir profundamente en la delicada construcción del entendimiento. No llegar a cierta información, no captar cierta relación, o lo contrario, promover cierta relación de ideas y hacer desaparecer otras, es una nueva capacidad de la tecnología que tiene alto impacto en los seres humanos, porque el lenguaje es un espacio vivo de poder.

El dilema del lenguaje es un asunto que ha marcado drásticamente la discusión en las ciencias sociales desde finales del siglo XIX, pues es una estructura que existe más allá del individuo y lo delimita a una red de significados que permite lo pensable. Las ciencias sociales han afirmado este aspecto rotundamente; el sujeto no está dado definitivamente en la historia, se constituye en el interior de la sociedad y es fundado y fundador, siendo el lenguaje, las narraciones o los relatos los que condicionan las posibilidades materiales e históricas del sujeto. Por esto, el lenguaje, como estructura que contiene discursos, paradigmas o relaciones semánticas de comprensión de mundo, ha sido descrito largamente - en particular por los postestructuralistas- como poder. Pues no representa la realidad en sí, sino una interpretación constructora de la realidad. El lenguaje construye realidad. Aun no siendo más que convenciones sociales, representa un espacio de disputa de poder ante el cual somos vulnerables, pues el lenguaje delimita y posibilita la comprensión e interrelación de las ideas.

Es apropiado plantear la interesante idea de quien evidenció el poder de crear entendimientos a través del lenguaje para generar canales de poder. Me refiero Michelle Foucault. Foucault en su libro "Las palabras y las cosas: una arqueología de las ciencias humanas" (1966), excava, o explora, la historia de las ideas, a la vez que afirma, cómo se revela del uso del lenguaje ciertas 'condiciones subyacentes de verdad' que constituyen el orden social, evidenciando que estos entendimiento han variado con el tiempo.

Con este estudio, consolida la idea de discurso como un conjunto de reglas, no solo semánticas, si no, que requieren de sistemas entrelazados de discursos validados para otorgar sentido. Estas reglas susceptibles de pequeñas variaciones, definen y posibilitan, lo que puede decirse para la verdad de una época, o conjunto de personas. Las condiciones subyacentes de verdad, la estructura de poder, es el entendido de lo que socialmente, de forma implícita, se ha sido convenido como cierto o aceptable. Foucault establece esta idea

bajo el concepto, reconstruido, de 'episteme'. El marco de saber acorde a determinada 'verdad' impuesta desde un poder en cada época y cultura.

Lo que se toma como cierto para una determinada época, la episteme, permite una forma propia de conocer el mundo. Lo que para Foucault produce al sujeto, las instituciones, las practicas, saberes y los nuevos discursos. Estos, aun siendo producto de una episteme cambiante -y por tanto ficticia y moldeable-, es estructura que en un momento histórico reprime y reproduce la estructura que la sostiene; incitando, induciendo, inhibiendo, facilitando, dificultando, limitando, haciendo probable o improbable, obligando o impidiendo, las formas en que el sujeto entiende la realidad. Por todo esto, Foucault habla derechamente que el sujeto es producido por estas relaciones de poder que generan la estructura.²⁹⁹

Tomar el control de esta cuestión ciertamente, se ha intentado y con relativo éxito, antes de la capacidad tecnológica que es capaz de reconocer y adaptar -incluso dentro de nichos de entendimiento específico- las relaciones discursivas³⁰⁰.

Tanto el hecho de vivir dentro de un conjunto de prácticas y saberes discursivos que nos moldean, como el ser posible incidir en la modificación de estos, es un aspecto que nos vuelve vulnerables ante una retórica artificial que entienda el entramado discursivo que envuelve un determinado sujeto y lo utilice para conducir desde, o para modificar hacia, un interés particular.

²⁹⁹ Algunas de estas ideas de este párrafo las he desarrollado siguiendo a: Diaz Felix en; Foucault, Sujeto y Verdad. (2019, 3 diciembre). [Video]. YouTube. https://www.youtube.com/watch?v=zTLX9s1VBA4&t=554s&ab_channel=ResumenesEntelekia

³⁰⁰ Para denotar esto, son propicias las reflexiones de I. Errejón, C. Mouffe, en el texto "Construir pueblo. Hegemonía y radicalización de la democracia" (2015), donde tratan sobre a especificidad de la postura de Mouffe en el famoso texto "Hegemonía y estrategia socialista" (1985), al unir el posestructuralismo con la idea de hegemonía cultural de Gramsci: "Evidentemente, con respecto a Lukács nosotros teníamos la ventaja, estábamos en un período en el cual el postestructuralismo ya se estaba desarrollando. Era el momento en que las obras de autores como Foucault, Lacan o Derrida eran importantes. Nos dimos cuenta de que había, en ese tipo de discurso, unas herramientas teóricas que nos permitían poner en cuestión la concepción esencialista y elaborar una noción de lo social como espacio discursivo, producto de articulaciones política contingentes, que no tienen nada de necesario y podrán siempre haber sido de otra forma" [...] pareciera haber una lógica propia de la política como actividad de construcción de sentido, donde se articulan los discursos de poder." [...] La clave es el cambio cultural subterráneo, magmático, por el cual el clima del momento cambia [...] Estas modificaciones en el sentido común de época son las que permiten imaginar la construcción de una intervención política excepcional." (p.11)

*

Ya podemos ver que, como citamos en la introducción, “dado que todos estamos envueltos en esta situación, la premisa de partida debe ser que todo el mundo es vulnerable (“vulnerabilidad generalizada”), pues no solo afecta a grupos o personas particularmente vulnerables” (Skatova et al., 2019)³⁰¹ ; ya que, “a través de la personalización basados en datos, las empresas y otras instituciones pueden utilizar fácilmente las asimetrías de información para explotar las debilidades personales con eficiencia calculada para generar persuasión personalizada, pudiendo influir eficazmente en el comportamiento a gran escala.” (Wolfie, 2017)³⁰².

Habiendo tratado de forma no taxativa sobre las vulnerabilidades humanas que nos hacen susceptibles a una modificación interesada a través de la personalización retórica artificial. Trataremos a continuación sobre la disciplina de la retórica a fin de proponer una forma de conceptualizar y entender el problema.

³⁰¹ Ibid. (p2)

³⁰²Ibid. Wolfie (2017) (p.4)

EL PODER DE LA PERSUACIÓN Y LA UTILIDAD DE ENTENDER EL PROBLEMA COMO RETÓRICA

El problema que tratamos ha sido abordado de diversas formas, sin embargo, la idea de retórica brinda claridad sobre qué es lo que sostiene este nuevo poder “socio-técnico”.

Existe emergente literatura donde se proponen nociones para tratar los sistemas que utilizan la informática para influir en nuestros comportamientos; hay los que tratan lo macro y profundo en juego, como la noción económico político de “capitalismo de vigilancia” (Zuboff³⁰⁴) o como la nueva relación de la especie/tecnología en “dataísmo” (Harari³⁰⁵), que, aun siendo valiosos aportes, son muy amplios; hay también otros conceptos que no abarcan lo suficiente, como “online manipulation” (Susser et. al³⁰⁶) que explícitamente excluye influencias como la coerción y la persuasión (Susser et al., 2019, p.3) o como “hyper-nudging” (Yeung³⁰⁷) que se centran en la idea de “Nudge³⁰⁸” (Sustein) y métricas del comportamiento en el espacio digital.

La retórica en cambio, es el abierto pero acotado aspecto de todo lo que busque influir para inducir el comportamiento (físico, psíquico, social), y pertenece a una tradición intelectual de discusión activa enfrascada en el fenómeno que tiene, a lo menos, 2300 años

³⁰⁴En particular, Zuboff, S. (2020). La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder. Ediciones Paidós.

³⁰⁵ En particular, desarrollado en, Harari, N. Y. (2015). Homo deus: Breve historia del mañana. Penguin Random House Grupo Editorial.

³⁰⁶ En particular en, Susser, D., Roessler, B., & Nissenbaum, H. F. (2018). Online Manipulation: Hidden Influences in a Digital World. SSRN Electronic Journal, 1. <https://doi.org/10.2139/ssrn.3306006>

³⁰⁷ En particular, Yeung, K. (2016). ‘Hyper nudge’: Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118-136. doi:10.1080/1369118x.2016.11867

³⁰⁸ “Nudge”- empujón- “es cualquier pequeño rasgo en el ambiente que atrae nuestra atención e influencia el comportamiento en la decisión que tomamos”. “Nudging” - empujar- se realiza a través de lo que se denomina “choice architecture”- arquitectura decidida-, que refiere a la idea de quien diseña la experiencia de a quien se quiere influenciar. El concepto dado en el inicio fue extraído de: Richard Thaler - Nudge: An Overview - <https://www.youtube.com/watch?v=xoA8N6nJMRs> (consultado: 09 de abril del 2020).

El concepto de se popularizó en el 2008 gracias al libro “Nudge: Improving Decisions About Health, Wealth, and Happiness”, escrito por el economista conductual Richard Thaler y el jurista Cass Sunstein.

(Ars Rhetorica, Aristóteles IV a.C.). La complementariedad de esta disciplina con lo que es posible hacer mediante el perfilamiento y la personalización del contenido digital, dan una clara idea del problema final que debe tratarse con urgencia en el derecho, y a sí mismo, transversalmente en la sociedad; la capacidad de inducir el comportamiento a través del tratamiento de datos, lo que hemos llamado personalización retórica artificial.

¿Qué es la retórica? tal como Aristóteles afirma; “la retórica es la facultad de teorizar lo que es adecuado en cada caso para convencer”³⁰⁹. No ha sido pretencioso invocar a nuestro querido filósofo. Ríos de tinta se han vertido para entender qué es la retórica desde hace más de 2000 años. Por lo mismo, además de llevar al lector medio a aceptar la conclusión por autoridad como bien fundada, esta es precisa y útil. Espanta prejuicios y preconcepciones en una idea simple que se ha mantenido como la principal en la materia en occidente. Mantengamos esto, en definitiva, la retórica es la disciplina que busca los medios para la persuasión en sentido lato. Es una disciplina que estudia y sistematiza el uso persuasivo del lenguaje en su amplio aspecto, que trata, cómo encontrar el medio adecuado para generar la construcción de la perspectiva que invite o instruya a observar de cierto modo cualquier materia.

La retórica es teorización, o búsqueda, del medio indicado para persuadir en la situación concreta. Este es el objeto de *Machine learning* cuando su fin es encontrar como inducir un patrón de conducta asociado a un perfil de usuario. Buscar y encontrar que curso de acción seguir para tener un resultado preciso, modificar un patrón con la personalización del contenido. El objeto es el mismo, tanto para la retórica humana, como para la retórica artificial. La diferencia está en que esta teorización no la realiza la inteligencia humana, si no una inteligencia artificial, que se vale de un tratamiento de datos para teorizar, en un plan probabilístico, el medio adecuado para persuadir.

Si bien es algo nuevo en la historia, tiene por objeto lo que la retórica tiene encomendado desde antiguo. Ambos, tanto la retórica humana como artificial, tienen por fin

³⁰⁹ Aristóteles, Retórica. Editorial Gredos, Madrid. - 1. Definición y estructura lógica de la retórica. 2.1 Definición de retórica y generalidad de su aplicación. (p. 173) Contexto: la retórica: “no pertenece a ningún género definido, sino que le sucede como a la dialéctica; y, asimismo, su tarea no consiste en persuadir, sino en reconocer los métodos de convicción más pertinentes para cada caso, tal como ocurre en todas las otras artes”.

encontrar lo adecuado para inducir en el caso concreto. Por consiguiente, la búsqueda del estímulo acertado a través del perfilamiento y la personalización digital del contenido, es un ejercicio retórico.

De todas formas, el ejercicio es distinto. La búsqueda del medio y la persuasión que utiliza las *Big Data Technologies* se puede realizar de forma tal, que, en último término, aun siendo retórica, no es lo que los oradores, o cualquier otra afectación persuasiva humana realizada en tiempos pasados pudo hacer. Esto, no por tener un propósito distinto, buscar el medio, sino, por la efectividad científica del análisis de datos que permite una estrategia nueva y más poderosa para convencer.

Ahondando sobre lo que se ha dicho de la retórica en general. Podemos comentar que a su respecto Platón, en diversas ocasiones³¹³, expresaba que este arte podría ser moralmente malo, meramente manipulación, seducción, engaño o mentira, o una especie de droga que controlaba los estados emocionales y las creencias de las personas³¹⁴. Así también lo entendió Kant: “El arte oratorio, en cuanto arte de servirse de la debilidad humana para los propios fines -sean supuesta o realmente buenos- no merece ninguna estima”³¹⁵. Y es que, es claro, el lenguaje no es una estructura neutra de razones, “en todo intercambio comunicativo hay una estructura de poder”³¹⁶ que puede ser percibida y utilizada, para traspasar la fina frontera entre influir con información que permita valorar libremente y, ser inducido utilizando la debilidad humana. Este asunto afecta transversalmente a la sociedad y por ello, Platón -con razón- condenaba y temía como habilidad que puede corromper la república³¹⁷.

³¹³ En particular, en Diálogos, Gorgias. En específico, podemos señalar el párrafo 459a, donde básicamente, rechaza la demagogia retórica categorizándola de habilidad táctica para seducir e influir en un auditorio ignorante sin buscar la verdad del filósofo.

³¹⁴ Sin embargo, en Fedro, Platón acepta que pudiera haber un ‘arte’ de la retórica que complemente la filosofía dialéctica. No del todo distintivo a Aristóteles, quien acepta con fe en la tendencia del humano a encontrar la verdad, que los discursos deben complementarse con la capacidad retórica. Aristóteles sabe que la retórica es una herramienta útil que puede estudiarse y utilizarse para que la verdad conocida.

³¹⁵ Kant, I. (1781); *Critica de la razón pura*, II, cap. II, seg. III. Cita extraída de: Cattani, Adelino en *Filósofos y oradores. filosofía en la retórica, retórica en la filosofía*. Revista ‘RÉTOR’ de la Asociación Argentina de Retórica de la Facultad de Derecho UBA, 1 (2), p. 119-130, 2011.

³¹⁶ Cita a Valenzuela Cori en clases, 2016.

³¹⁷ Por esto, famosamente en su obra la República, expulsa a los poetas por utilizar las palabras para cautivar los sentidos en lugar de buscar la verdad.

El desprecio a la retórica es razonable. Claro, es un poder tal que desde antiguo se sabe incluso más poderosa que la fuerza física, que de lograr su cometido, es actividad donde no hay resistencia. Se adecúa la intención ajena de forma tal que, al integrarse como perspectiva, parece libertad. Así Odiseo, en la obra de Filoctetes de Sófocles, cuando intenta convencer al hijo de Aquiles, Neoptólemo³¹⁹, a utilizar la retórica como un arma sin importar actuar con engaño³²⁰, pues en el caso, la fuerza física no era suficiente para doblegar al enemigo. Argumenta Odiseo: “también yo cuando era joven tenía una lengua ociosa y una mano activa; pero ahora, puesto a prueba, veo a la lengua y no a los actos dirigiéndolo todo para los mortales”.³²¹ Similarmente, afirma el famoso -quizás el más famoso- sofista³²² Gorgias, en “Elogio a Helena”³²³³²⁴: “la palabra es un poderoso soberano que con un pequeñísimo e invisible cuerpo lleva a cabo las obras más divinas. Pues es capaz de detener el miedo, apartar la tristeza, infundir la alegría y aumentar la compasión.”³²⁵

³¹⁹ Neoptólemo pensaba que el uso de la palabra, de la seducción del alma, es una maquinación reprochable, vergonzosa, indigna. Sin embargo, en el diálogo, Odiseo le obliga a ponderar entre lo provechoso y lo vergonzoso.

³²⁰ Esto a fin de: “seducir el alma de Filoctetes con tus palabras” debiendo “ser fiel a tu cuna no solo con el cuerpo”.

³²¹ Filoctetes, Sófocles

³²² El término sofista, del griego “Sophia” –Sabiduría –, era el nombre que recibía quien enseñara sabiduría, pero derivó con el tiempo al nombre de quienes supieran cautivar con palabras, y particularmente para su propia utilidad. Terminando en ser una idea similar a lo que entendemos hoy por charlatán.

³²³ Gorgias lo afirma al plantear una defensa para Helena de Troya ante las acusaciones de traición; argumentando que de haber sido convencida por la palabra debe ser exenta de culpa, pues la palabra puede enajenar la voluntad.

³²⁴ Cuando debe defender a Helena ante el pueblo que reclama condena por la traición, al haber sido considerada como la culpable de la guerra de Troya; Gorgias argumenta la inocencia de Helena ser capturada por la retórica, o la palabra; el pequeño sobreaño.

³²⁵ Contexto de literal de la cita en Elogio a Helena de Gorgias: “Yo quiero, dando un cierto razonamiento a mi discurso, suprimir la acusación que recae sobre esta mujer de la que se oyen males, y dejar en evidencia a aquellos que mienten al reprocharla, y, además, mostrando la verdad quiero detener la ignorancia.” [...] (seguido de diversos argumentos, agrega finalmente) “Y si fue en cambio la palabra quien la persuadió y engaño su alma, tampoco en este caso es difícil hacer su defensa y liberarla de la acusación de la siguiente manera: La palabra es un poderoso soberano que con un pequeñísimo e invisible cuerpo lleva a cabo las obras más divinas” [parágrafo 8]

No por nada el fenómeno de la persuasión fue temido. El estudio de Aristóteles justamente es a propósito de ver que la incipiente democracia griega, era captada por la agilidad de la palabra de los oradores sofistas cuando se deliberaban importantes decisiones en asamblea. El mismo poder al cual Odiseo llama a actuar, por ser la vía más “provechosa”, incluso mediante las “malas artes” y “tretas”, para seducir al alma y dirigir a los mortales; complicó a filósofos y políticos.

Esto último porque la retórica es creadora de los sentidos que pueden llevar a acciones. Ahí, una de las cualidades más importantes de la humanidad, pero de la cual se desprende un riesgo fundamental. Los humanos podemos convencernos los unos a los otros para significar el entorno que habitamos y con esto, interpretarlo dentro de una narrativa, individual y común. Siendo desde esta comprensión generada de la realidad que actuamos como actuamos. “El hombre no es solamente un productor de historias, sino, antes que nada, el producto de ellas”³²⁶. Es por ello que justamente, “es de la actividad de inventar relatos que desarrollamos una visión de futuro y, por tanto, abrimos un horizonte que nos va a impulsar a emprender acciones”³²⁷. La creación de sentido, o perspectiva, moldea el actuar. En este sentido, Isócrates (s.V-IV a.C.) afirmó que, es “debido a que en nosotros ha sido implantado el poder de persuadir [...], no solo hemos dejado atrás la vida de las bestias salvajes, sino que nos hemos unido y hemos fundado ciudades, hemos hecho leyes he inventado las artes [...] no hay institución concebida por el hombre a la que el poder del lenguaje no haya ayudado a establecer”³²⁸.

El perfilamiento y la personalización del contenido tiene todos los elementos para hacer de la retórica, en su versión artificial, un asunto de enorme poder para la inducción al comportamiento que moldee las instituciones y formas de vida humana. Como advirtió Cicerón, quien dominara la retórica; “podrá lograr mediante el uso de la palabra sus propósitos quien conozca a fondo la naturaleza humana, y las causas mediante las que los

³²⁶ Rafael Echeverría tratando el pensamiento de Heidegger, *Ontología del lenguaje* - J. C. Sáez Editor, 2003- (p.246)

³²⁷ Rafael Echeverría, *Ontología del lenguaje* - J. C. Sáez Editor, 2003- (p. 247)

³²⁸ Isócrates (s.V-IV a.C.). *Discursos*, Antidosis. Parágrafo 254

espíritus se excitan o se amansan”³²⁹. Dada la enorme producción de datos personales y la continua capacidad para detectar patrones complejos, para reconocer tendencias y asociaciones, y a la vez, aprender de estos; la capacidad para que algoritmos encuentren el medio indicado para persuadir por conocer “las causas mediante las que los espíritus se excitan o se amansan”, es un problema mayor. El uso de *Big Data Technologies* permite detectar nuestras vulnerabilidades, las causas que generan las emociones y nuestros sesgos, concluyendo la reacción previsible que modifique nuestro comportamiento. Junto con esto, el ambiente digital es un medio perfecto para el ejercicio de la personalización retórica. Las plataformas digitales son lo suficientemente intrusivas, interactivas y dinámicas para adaptarse a lo que perciben para explotar nuestras vulnerabilidades individuales con un diseño inteligente.

El escenario parece aún más abrumador que aquel que llevó a tanto cuestionamiento en la incipiente democracia griega. Después de todo, la retórica sin cambiar el objeto de su disciplina, puede ser ejercida por una inteligencia artificial y a gran escala. Esta vez no será en asamblea, o en el diario de noticias, o con el afiche en la calle. El ambiente digital es completamente artificial, y en él se puede acomodar intencionalmente y de forma automatizada lo que resulte adecuado en cada caso para convencer de forma imperceptible y constante

¿Por qué es relevante jurídicamente destacar la retórica en un problema de protección de datos?

El debate en derecho en torno a la protección de datos personales suele mirar en menos o derechamente desconocer la capacidad de persuasión y/o afectación del entendimiento, lo que sí ha sido largamente tratado por la tradición que se ocupó por la retórica, y a sí mismo, por quienes se preocuparon en las humanidades de la persuasión en general o de la creación de discursos. Por lo mismo, para exaltar lo que está en juego ante el derecho, planteamos

³²⁹ Cicerón, *Sobre el Orador*, Editorial Gredos, Madrid. [52]. (p.110) [he modificado la oración mas no su contenido. La idea de Cicerón está en negativo y la he pasado a positivo. El afirma “no podrá lograr [...] quien no conozca “]

como acertado hablar de retórica, y propiamente, artificial. Vinculando así, el tratamiento de datos que perfila y personaliza el contenido, directamente con la búsqueda del medio indicado para persuadir en la situación concreta, es decir, la retórica.

El énfasis del término retórica sitúa y refiere el problema descrito evocando lo vulnerable de nuestra comprensión a la persuasión de terceros. Esto es útil no tan solo para tomar el peso de lo que está en juego, sino también para re focalizar el valor tutelado, ya no tan solo como privacidad³³⁰, si no como dignidad, en tanto que lo importante es la integridad psíquica ante el tratamiento de datos que tenga por fin hallar el medio indicado para persuadir. La preocupación radicaría principalmente en las amenazas que se derivan de la forma en que se procesan los datos y no de la tenencia de los datos en sí mismos.

El énfasis en la retórica y el valor dignidad, puede crear todo un mundo de soluciones que vayan más allá de la protección de los datos personales relativos a la privacidad, como la protección al consentimiento como fuente de autorización para tratar datos personales y los derechos ARCO³³¹. En su lugar, el derecho acudiría directamente a regular y tutelar la afectación del tratamiento de datos, persiguiendo y prohibiendo lo que supere un límite de influencia tolerable en la personalización del contenido.

Si bien los valores privacidad y dignidad están estrechamente relacionados, en tanto que la privacidad puede ser una condición previa de la dignidad o la autonomía; como largamente se ha discutido, la privacidad muchas veces es la antesala a la libertad en tanto que en lo privado pareciera no poder ser uno constreñido u obligado a tomar una decisión - por lo mismo, ésta es la justificación del voto secreto-; aquí, lo que nos resulta más problemático, es la vulnerable naturaleza de la conciencia humana que exige un nuevo paradigma para la efectiva protección ante el ambiente digital que percibe constantemente lo

³³⁰ La protección de datos personales en Chile esta Constitucionalmente establecida en el Artículo 19 N°4. Este artículo consagra tres garantías, la protección de la honra, la vida privada y la protección de los datos personales. Todos buscan proteger la privacidad de la persona natural, el individuo de la especie humana. La protección de los datos personales, y la regulación del tratamiento de datos, de esta forma, consta como un asunto ligado al derecho fundamental a la "Privacidad". He seguido para este punto a Lorena Donoso en "Desafíos tecnológicos en la nueva Constitución" 19 de noviembre 2020. Online <https://youtu.be/jNWzI55e0II> [Min 31:10]

³³¹Los Derechos ARCO son aquellos derechos que puede ejercer el titular de los datos, consisten en: Acceso a conocer; Rectificar lo erróneo; Cancelar o destruir los datos ilegales; Oponer, bloquear cuando es inexacto.

privado. Después de todo, la privacidad debe transar a un sistema de gestión de la información por parte de terceros necesariamente, por el hecho de producirse y administrarse la data personal inmediatamente por un tercero. Por lo mismo la privacidad es burlable o difícil de fiscalizar.

La protección a la privacidad de los datos y la protección ante la personalización persuasiva o retórica, no son excluyentes. Se complementan en muchos sentidos, evidentemente. Sin dejar de lado las herramientas que nos han dejado las políticas de protección y tratamiento de datos, la incorporación del valor dignidad o integridad para tratar el problema, cambia el centro desde la protección de los datos del titular, a la afectación del tratamiento de datos y en especial, la que es producida por la personalización del contenido. El concepto personalización retórica artificial, tutelado por el valor dignidad, deja así por centro explícito la tutela a la vulnerabilidad humana ante la personalización.

A forma de humilde propuesta, junto con esto, deben existir normas expresas sobre lo que a personalización del contenido respecta. A mi juicio, debe haber ley expresa que regule la afectación por tratamiento de datos. Se debe regular la venta de perfiles, permitiendo aquella que en venta pública incorpore la protección y los valores del derecho, generando un canal ético al interés tras las potencialidades de este nuevo poder; así mismo, se debe perseguir y disuadir el mercado negro de perfiles. Se deben dictar leyes que traten la prohibición y persecución activa de la retórica artificial, consolidando un sistema de responsabilidad sancionatorio, tanto para personas jurídicas como naturales. Estas han sido solo unas ideas iniciales, no son más que sugerencias para estimular el pensamiento legislativo.

Finalmente, lo importante es que, el derecho debe evitar en el mayor grado posible, aquella personalización que tenga por fin inducir el comportamiento de forma abusiva, es decir, que explote más allá de un límite razonable³³² nuestras vulnerabilidades.

*

³³² Se deberá pensar una nueva 'ética de la influencia', como lo ha planteado Sunstein.

CONCLUSIÓN

En lo principal, este texto buscó evidenciar de forma didáctica el problema de la personalización retórica artificial, explicitando que, las transformaciones tecnológicas, la falta de restricción efectiva, y el interés por esta nueva capacidad; permiten explotar nuestras vulnerabilidades biopsicosociales, dejando en juego una delicada parte de la experimentalidad humana junto con sus repercusiones en la esfera política y social, sin una protección efectiva.

En este sentido, tratamos sobre lo que permite, o no limita, la modificación interesada del comportamiento humano por medios digitales. Esto lo hemos desarrollado:

- 1) Contextualizando los elementos que permiten la capacidad de perfilar y personalizar el contenido. Es decir, el uso de las *Big Data Technologies* y los dispositivos inteligentes, en una nueva era caracterizable como cuarta revolución industrial.
- 2) Constatando la incapacidad del ordenamiento jurídico para hacer frente al poder de la personalización retórica artificial, exponiendo, entre otras cosas, la lógica de la protección vigente y los problemas relativos a; generar un real consentimiento; tener un engorroso medio de tutela judicial poco efectivo; y la existencia de brechas sistémicas del derecho con la tecnología.
- 3) Evidenciando la existencia de intereses en el ejercicio de este poder, que se han manifestado antes y se manifiestan hoy, junto con, reflexiones al respecto.
- 4) Analizando la posibilidad de inducir el comportamiento mediante la explotación de nuestras vulnerabilidades
- 5) Exponiendo que, la búsqueda del medio adecuado al caso para persuadir con el uso de las nuevas tecnologías, es un peligroso nuevo tipo de retórica.

Es claro que el desarrollo y existencia de los dispositivos inteligentes nos beneficia en múltiples sentidos. Por lo mismo, es difícil no aplaudir que el grueso de la población pueda acceder a estos y con ello al conocimiento en internet o la intercomunicación posible.

Masividad, poder de cómputo y conectividad pueden ser algo valioso, indiscutiblemente. Sin embargo, no todo es beneficio. Esta época trae desafíos importantes. El registro masivo del comportamiento humano, junto con el tratamiento masivo de datos personales, sumado a una inteligente capacidad para poder disponer de forma sutil y coordinada distintos estímulos en el ambiente artificial en el que se desenvuelve la experiencia del usuario, es un campo perfecto para ejercicio de la persuasión.

Tenemos que entender lo amenazante de la personalización retórica artificial y lo desprotegido que estamos ante este poder. Por ello, la gran problematización que presento esta tesis fue la capacidad existente que surge a propósito de las *Big Data Technologies* que no encuentra una eficaz restricción por parte del derecho.

Esta ineficaz protección es dada, en general por:

- 1) Las brechas sistémicas de cualquier protección de datos y leyes de privacidad escrita, que no pueden hacer frente a la infraestructura tecnológica de procesamiento de datos que tiene lugar en una escala enorme, de manera instantánea, proactiva, ubicua y en una multitud de formas que eluden la observación humana.
- 2) Por ser imposible la supervisión del procesamiento de datos; cuando falta el registro ante una autoridad antes de realizar operaciones de procesamiento de datos; y cuando la tecnología puede ser una caja negra incluso para el procesador de datos.

Por otro lado, en Chile, es asunto patente prioritariamente, porque:

- 1) El ordenamiento jurídico actual tiene laxas hipótesis que autorizan el tratamiento de datos sin consentimiento del titular, en particular a lo que respecta las fuentes accesibles al público, lo que abre la susceptibilidad a que todo el contenido en internet pueda ser tratado;
- 2) Define la carga de la gestión y resguardo de la protección digital en el individuo medio, ante la inexistencia de una autoridad de control, dependiendo la gestión prioritariamente en el consentimiento que por lo general es ficticio – y legitima casi cualquier tipo de recolección, uso o divulgación de datos personales-, y su resguardo, en una tutela judicial ineficaz;
- 3) La tutela judicial depende de procedimiento engorroso, que opera ex post a la vulneración, no tiene efectos disuasivos y requiere de patrocinio de abogado y demanda en el tribunal competente del domicilio del responsable, cuando es

prácticamente imposible identificar y dirigirse contra todos los entes que en el mundo capturan y tratan nuestros datos.

La personalización retórica artificial, la identificamos como un nuevo poder en la historia, advirtiéndole que está en constante perfeccionamiento y existen enormes intereses detrás. A la vez, categorizamos derechamente el poder que surge del perfilamiento y la personalización, como retórica. Afirmando que es un concepto útil para dimensionar el problema, por un lado, por la larga tradición que se ha ocupado del asunto, y, por otra parte, dado que pone en el centro del problema la integridad de experimentalidad humana.

*

NOTA FINAL

El derecho debe actuar, y estar a la altura de las circunstancias. Debe gobernar y regular estas tecnologías apropiadamente y mitigar los daños. De no hacerlo, fracasaría como herramienta social y disciplina. Habría perdido los ideales y valores de los fines últimos de su propósito. Si aceptamos que el derecho es una herramienta que se aproxima a la realidad social para “procurar controlarla, dirigirla y hacer efectivos en ella determinados planes, modelos económicos, sociales y políticos”³³⁹, debe reaccionar ante la capacidad del poder de cómputo y la masividad de los aparatos que median interacciones humanas, pues esta tiene repercusiones concretas en el poder social. La capacidad técnica que nos preocupa no es neutral, y podría tener un impacto masivo de serias consecuencias.

La cuarta revolución industrial implica para los juristas una responsabilidad compleja. Ante los desafíos del progreso y el poder, tenemos el deber de resguardar la vigencia de los valores del ordenamiento ideando los mecanismos necesarios. En esto, no podemos permitir que un poder latente tome por asalto a una generación y a la humanidad

³³⁹ Estos elementos de la naturaleza de derecho fueron extraídos del libro de Pompeu Casanovas, “Manual de Filosofía y Teoría del Derecho”, capítulo “Tecnología, Inteligencia Artificial y Web Semántica”, (2013).

para siempre. El poder que deriva de la recolección y tratamiento de datos con el objeto de adecuar intencionadamente debe ser regulado, restringido y perseguido.

En esta labor el derecho no puede ser ajeno a las restantes ciencias sociales de las que se nutre. Por esto, este ensayo procuro dialogar desde distintas ciencias los alcances de esta revolución; pues estamos ante un terreno nuevo y vertiginoso. Este asunto no es exclusivo de disciplina alguna, y por lo mismo, debe ser tratado de forma rizomática³⁴⁰, incorporando no tan solo los valores y principios propios del derecho, sino también una perspectiva sobre la capacidad tecnológica, la vulnerabilidad de la condición humana y distintos razonamientos de las más variadas disciplinas, como la psicología, la sociología, la ingeniería y la filosofía.

Pero en esto, el derecho tiene un rol protagónico, pues el derecho es conductor en el poder. Parafraseando a Bodenheimer, el derecho “debe ser aquel punto medio entre anarquía y despotismo, deber crear restricciones al ejercicio arbitrario del poder.”³⁴¹

FIN

³⁴⁰ El Rizoma es un concepto trabajado por Gilles Deleuze que presenta una idea de pensamiento opuesto al arbóreo, o de un solo tronco. La “idea de rizomática” se asemeja al conjunto que hacen ciertos arbustos que comparten su raíz -rizoma- sobre un sistema nodal.

³⁴¹ Bodenheimer (1942) Op cit. (p.28)

ANEXO

IDEAS INTRODUCTORIAS A LOS DISRUPTORES TECNOLOGICOS

Como consecuencia de que nuestra vida ocurra cada vez más mediada por la tecnología, y las experiencias comerciales, informativas y gran parte de la esfera íntima de la vida personal, puedan ser registradas y personalizadas; la capacidad de manipulación en línea³⁴² parece un poder latente. ¿Pero qué permite que los datos generen algo que induzca el comportamiento?

A continuación, expondremos de forma simple y breve qué es la Inteligencia Artificial, *Machine learning*, Redes Neuronales y *Big Data*, con el objeto de que el lector tenga una visión general de los conceptos que componen los elementos disruptivos en el ámbito tecnológico que permiten la adecuación inteligente del contenido a partir de los datos que existen sobre nosotros, permitiendo lo que llamamos retórica artificial.

Este título solo expone una noción³⁴³ de las tecnologías disruptivas. No es absolutamente necesario entender este aspecto a cabalidad para ver que el problema que tratamos es grave, sin embargo, es una aproximación a la tecnología que la permite, cual dará claridades a conceptos comúnmente utilizados cuando se trata el tema.

³⁴² “La manipulación en línea es el uso de la tecnología de la información para influir de forma intencionada y encubierta en los toma de decisiones, apuntando y explotando sus vulnerabilidades en la toma de decisiones.” Susser, D; R, Beate; Nissenbaum, H. F. (2019): Technology, autonomy, and manipulation, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 8, Iss. 2, pp. 1-22, <http://dx.doi.org/10.14763/2019.2.1410> (p.1)

³⁴³ Advertimos desde ya que en lo relativo a Machine Learning y redes neuronales, solo veremos lo esencial para tener una visión general de como interactúa el sistema con la información de entrada y salida. Solo nos interesa que exista una idea de la interacción de este sistema con su entorno, es decir saber qué hace y no el cómo lo hace.

Respecto del aprendizaje automático (Machine Learning), no veremos más allá de la forma que tiene para generar de la experiencia o datos, un aprendizaje. De las redes neuronales trataremos solo un tanto más que su arquitectura.

BIG DATA

Big Data, o macrodatos³⁴⁴, refiere justamente a una enorme cantidad de datos, tal, que supere la capacidad de un software convencional para administrarlos y procesarlos. También, es el análisis posible y el conjunto total de datos generados por cualquier procesador que almacene información; sea la base de datos de los ganadores de un Club de Ajedrez en Somalia, o lo que se desprenda de cada película vista en Netflix, como las preferencias, las pausas, el volumen, horario, programas corriendo en paralelo, etc.

Podemos entender que todo registro informático es parte de la enorme, gigantemente enorme, cantidad de información contenida en la idea de “*Big Data*”. Se trata del conjunto de datos y el posible conocimiento que la interrelación de estos puede generar.

El nacimiento del término “*Big Data*” es generalmente atribuido a John Mashey, Ph. D en computer science, que en la década de los noventa usó el término para referirse a “aquella data tan grande y compleja que las herramientas que poseemos para recolectar e interpretar no son suficientes”.

Una definición formal reciente fue dada por la académica de la Universidad de Roma, Andrea De Mauro, en el 2016, con la publicación científica “formal definition of *Big Data* based on its essential features”, que procuro dar definición al popular concepto de la forma siguiente: “información caracterizada por un alto volumen, velocidad y variedad que requieren tecnología y métodos analíticos específicos para su transformación en valor”³⁴⁵. Por otro lado, Crawford & Schultz, definen Big Data como un “término generalizado e impreciso que se refiere al uso de grandes conjuntos de datos en la ciencia de datos y el análisis predictivo”³⁴⁶.

³⁴⁴Este término ha sido usado para referirse a Big Data en español. Así mismo, por el Parlamento Europeo 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html (En línea, abril 2021)

³⁴⁵ De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, 65(3), 122-135. <https://doi.org/10.1108/lr-06-2015-0061>

³⁴⁶ Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014)

El salto de las concepciones dentro de la idea nacida hace más de veinticinco años, es variada y ciertamente imprecisa. Y es que, dado el cambio en la capacidad de procesamiento y de las técnicas de integración de datos, lo que se planteó como algo enorme y complejo, imposible de decodificar, hoy ya podemos, al menos en grandes cantidades, analizar. De todas formas, el carácter de ser algo que requiere de poderosas tecnologías y avanzados algoritmos para entregar valor persiste. Seguramente, a medida que aumente la capacidad de cómputo e interés en descubrir patrones, distintas ideas dadas para el concepto de *Big Data* queden obsoletas. Lo central parece ser una enorme cantidad de información, y la idea de potenciales revelaciones en estos enormes volúmenes de datos.

A medida que nuestra capacidad para procesar datos aumenta, la capacidad para producirlos se acelera, aumentando la potencialidad de las revelaciones y el tamaño de la *Big Data*. Hemos creado un mundo interconectado donde millones de individuos generan información sobre todo lo que sea registrable. Como comentamos, ya para el año 2012, se había creado un tráfico de 2.5 quintillones de bytes por día según IBM³⁴⁷.

Sumado a esto, en las grandes de las urbes del mundo, todo un ecosistema de “Smart objects” emerge, coleccionando datos para comunicarse y armonizarse con el usuario. La llamada Internet de las cosas³⁴⁸ (IoT por su sigla en inglés, *Internet of Things*) estará presente en nuestro refrigerador, automóvil, puerta, reloj, parlantes, o en cualquier cosa que le sea insertable el barato, fácil y conveniente acceso a internet, que posibilite, una mayor inteligencia sobre estas cosas. La *Big Data* no deja de crecer.

La *Big Data* entendida como una fuente desde la que extraer y analizar información, requiere ciertas aristas en la Data para aumentar el poder de la información que derive del análisis. Comúnmente se dice que la capacidad de la *Big Data* para identificar tendencias y patrones dependerá de las llamadas “3Vs” de Análisis. También, *Big Data* puede ser

³⁴⁷ Siguiendo a IBM <https://developer.ibm.com/es/articles/que-es-big-data/>

³⁴⁸ “El concepto de Internet de los objetos, o de las cosas, se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red”. Fuente: Dictamen 8/2014 del Grupo de Trabajo del Artículo 29, ahora Comité Europeo de Protección de Datos

definido³⁴⁹ como el proceso de análisis y la relación de estas características. Las 3Vs son: Volumen – la cantidad de datos-; Velocidad – rapidez en la que se genera, almacena y procesa los datos -; Variedad – el tipo de datos accesible, sus fuentes y formatos (e.g. video, documentos, etc.) -.

LAS BIG DATA TECHNOLOGIES

Para dar utilidad a la *Big Data*, están Las *Big Data Technologies*. Estas son todas aquellas herramientas útiles para analizar, procesar e integrar información en grandes volúmenes de datos. Comprende una gran variedad de técnicas, tales como, la minería de datos, la aplicación de redes neuronales sobre grandes conjuntos de datos, la automatización de sistemas que administran datos, entre otros que, resumidamente, buscan analizar grandes volúmenes de datos con el objeto de reconocer patrones, tendencias y asociaciones relacionadas con el comportamiento humano, la naturaleza y la información en general. Siendo así, tanto la detección de patrones como la toma de decisiones sobre grandes volúmenes de información son áreas técnicas que se engloban dentro de las llamadas *Big Data Technologies*, las cuales han sido potenciadas enormemente por el desarrollo de los algoritmos de “*Machine learning*”.

¿Qué hacer con esos datos?, es un “terreno abierto a la imaginación “que permite la “estadística del todo”³⁵⁰ donde se pueden encontrar correlaciones sin conocer previamente la causa. El análisis de los datos permite la detección de patrones y con ello, la predictibilidad para el apoyo de toma de decisiones.

³⁴⁹ Así mismo se define en “Oussous, A., Benjelloun, F.-Z., Ait Lahcen, A., & Belfkih, S. (2018). Big Data technologies: A survey. *Journal of King Saud University - Computer and Information Sciences*, 30(4), 431-448. <https://doi.org/10.1016/j.jksuci.2017.06.001>” citando a su vez a Furht and Villanustre, 2016

³⁵⁰ Hueso, L. C. (2016). Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales ISSN 1989-7022, citando a Martínez (2014,3) a partir del clásico Mayer Schönberg.

LA INTELIGENCIA ARTIFICIAL

Sobre la inteligencia artificial la ciencia ficción ha tratado bastante; igualmente, la preocupación que teoriza sobre las consecuencias de una inteligencia no humana dentro de las ciencias o la ingeniería aplicada no ha sido poca. Stephen Hawking dijo *“El desarrollo de la inteligencia artificial completa podría significar el fin de la raza humana”*³⁵¹. Elon Musk por otro lado advierte, *“Al menos cuando hay un dictador malvado, ese humano va a morir. Pero para una IA, no habrá muerte, vivirá para siempre. Y entonces tendrías un dictador inmortal del que nunca podríamos escapar.”*³⁵² La investigación y el progreso en Inteligencia Artificial siempre se han entrelazado, y no sin razón, con la ciencia ficción y un profundo temor; como afirma el psicólogo Chileno Roberto Mussa, *“el asunto bordea una conciencia mítica que despierta relatos que se asemejan a Prometeo, el Golem o Frankenstein”*³⁵³. Es difícil no fascinarse o temer a lo que se propone emular la inteligencia humana. El dilema sobre el desarrollo en curso y lo que pasará cuando la IA pueda leer, adaptarse y enseñarse a sí mismo millones de veces más rápido que nosotros, como ha dicho Musk³⁵⁴, es una preocupación latente cuyo riesgo debiera despertar más temor que la eventualidad de una guerra nuclear.

Pero ¿qué es la Inteligencia Artificial?, *AI* o *Artificial Intelligence*, es una disciplina científica propia de la Informática -*Computer Science*-; cual, como disciplina, es una colección de conceptos y métodos para resolver problemas, que busca que objetos puedan manifestar un funcionamiento similar al pensamiento humano, siendo esta similitud o imitación igualmente llamada, inteligencia artificial. La inteligencia artificial es la inteligencia manifestada por un objeto y a la vez, es la disciplina que lo ha hecho posible.

³⁵¹ Stephen Hawking en entrevista para BBC 2014 <https://www.bbc.com/news/technology-30290540> Original: *“The development of full artificial intelligence could spell the end of the human race”*.

³⁵² Elon Musk en el Documental *“Do You Trust This Computer?”, 2018*. Original: *“At least when there's an evil dictator, that human is going to die. But for an AI, there will be no death — it would live forever. And then you would have an immortal dictator from which we could never escape.”* 1:55 min.

³⁵³ Sobre esta fascinación mítica; Musa Giuliano, R. (2020). *Echoes of myth and magic in the language of Artificial Intelligence*. *AI & SOCIETY*, 35(4), Springer-Verlag London Ltd., 1009-1024. <https://doi.org/10.1007/s00146-020-00966-4>

³⁵⁴ 1:55 *ibid*.

En general, se suele hacer la diferencia entre dos clases de Inteligencia Artificial, fuerte -*general AI, strong AI o Broad AI*- y blanda -*Soft AI o Narrow AI*-. *La IA Fuerte – Strong IA*- es aquella capaz de manejar una amplia gama de tareas en lugar de una particular, aproximándose a la sensibilidad o la conciencia. Es aquella a la que tememos por poder tomar el control y que actualmente no ha sido desarrollada. *La IA Débil – Narrow AI* – por el contrario, es aquella que se especifica en una tarea determinada o limitada.³⁵⁵ Esta última inteligencia es con la que contamos hoy. Lo más similar a una IA Fuerte hoy (2021) es IBM Watson y GPT-3 de OpenAI.

MACHINE LEARNING

Machine learning o Aprendizaje Automático, es la rama de la Inteligencia Artificial y de la informática que busca dotar a las máquinas de capacidad de aprendizaje, generalizando el conocimiento a partir de un conjunto de experiencias. La esencia de *Machine learning* son los algoritmos que dan a los computadores la capacidad de aprender de los datos para luego hacer predicciones y decisiones³⁵⁶. *Machine learning* puede ser considerado como una tecnología de las *Big Data Technologies* cuando se le utiliza para detectar patrones en enormes volúmenes de información.

Podemos definir *Machine learning* (o aprendizaje automático) como “el conjunto de sistemas que mejoran su rendimiento en una tarea determinada con más y más experiencia o datos³⁵⁷”. Siguiendo “The *Machine learning* Dictionary” (University of New South Wales): “se dice que el aprendizaje automático ocurre en un programa que puede modificar algún

³⁵⁵ Los conceptos han sido extraídos de; DeepAI. (2020, 25 junio). Narrow AI. <https://deepai.org/machine-learning-glossary-and-terms/narrow-ai>

³⁵⁶ Machine Learning & Artificial Intelligence: Crash Course Computer Science #34. (2017, 1 noviembre). [Video]. YouTube. https://www.youtube.com/watch?v=z-EtmaFJieY&ab_channel=CrashCourse

³⁵⁷ Concepto dado en el Curso 2020 “elementsofai.com/” de la Universidad de Helsinki “Helsingin yliopisto”.

aspecto de sí mismo, a menudo denominado su estado, de modo que, en una ejecución posterior con la misma entrada, se produce una salida diferente”³⁵⁸.

Tres paradigmas de aprendizaje en *Machine learning*. Hay tres mecanismos en los que la información es transformada en aprendizaje en *Machine learning*. Estos son los llamados paradigmas de aprendizaje, o formas de aprendizaje. Con estos, sean solos o combinados, es posible convertir datos, o experiencia, en aprendizaje para que un programa pueda hacer sus propios juicios basados experiencias previas de tareas similares.

Los tres paradigmas de aprendizaje son: el aprendizaje supervisado - *supervised learning*-, que aprende por ejemplos; el autoaprendizaje sin supervisión - *unsupervised self learning*- que aprende por detectar patrones y agruparlos; y, el aprendizaje reforzado - *Reinforcement Learning*- que aprende de cómo se deben tomar acciones en un entorno para maximizar la recompensa³⁵⁹. Con un poco más de detalle, podemos decir que:

1. *Supervised learning* es “un tipo de aprendizaje automático que requiere ejemplos y etiquetas -que se manifieste que es y que no es-, para que el algoritmo compare su salidas con las salidas correctas, de modo que pueda identificar cuál es su error y modificarse en consecuencia”³⁶⁰. El aprendizaje se basa en descubrir la relación existente entre las variables de entrada y sus salidas deseadas. El objetivo entonces es utilizar los patrones descubiertos para cada etiqueta, con el objetivo de posteriormente obtener predicciones correctas sobre ejemplos nunca vistos por el modelo. Las salidas pueden ser las etiquetas- valores discretos- o valores reales. Por ejemplo; una salida con valores reales, puede ser aquel a cuya entrada se le da una foto de la calle y, por salida se espera el ángulo del manubrio para girar, 0° a 360°.

³⁵⁸ Este Diccionario sigue los conceptos comprendidos en el compilado COMP9414 de la University of New South Wales, Sydney.
<https://web.archive.org/web/20180826151959/http://www.cse.unsw.edu.au/~billw/mldict.html#activfn>

³⁵⁹ Extraído de Wikipedia citando a: Hu, J.; Niu, H.; Carrasco, J.; Lennox, B; Arvin, F. (2020). Transacciones IEEE sobre tecnología vehicular. 69 (12): 14413-14423.

³⁶⁰ Definición proveniente de “The Machine Learning Dictionary” de la Universidad de New South Wales, Sydney.
<https://web.archive.org/web/20180826151959/http://www.cse.unsw.edu.au/~billw/mldict.html#neurals>

Las salidas de etiquetas, es aquel que ya comúnmente se utiliza para reconocer objetos³⁶¹, sea de imágenes, sonidos o cualquier información, como inclusive, los sentimientos en un texto³⁶².

2. *Unsupervised self learning* o aprendizaje no supervisado, es el paradigma que consigue producir conocimientos únicamente de los datos que se proporcionan como entrada, sin necesidad, en ningún momento, de explicar en el sistema qué resultado es el correcto³⁶³; el sistema recibe datos de entrada, y se le ordena descubra patrones de similitud, regularidades, para generar agrupaciones entre los datos entregados. Esta es la técnica más utilizada para la agrupación de información en categorías que no están previamente definidas. Por ejemplo, es este el paradigma aplicado para encontrar contenido con temáticas similares, o agrupar perfiles de usuarios con rasgos parecidos entre sí, o que puedan reaccionar de forma similar a cierto contenido presentado.

3. *Reinforcement Learning* o Aprendizaje Reforzado, es un tipo de técnica de aprendizaje automático, inspirado en la psicología conductista, que permite a un algoritmo aprender en un entorno interactivo mediante prueba y error. Retroalimentándose de sus propias acciones y experiencias, a través de premios y castigos, logra encontrar un modelo de acción adecuado, fin que maximice la recompensa acumulativa total del agente³⁶⁴. Este modelo comúnmente

³⁶¹ Como ejemplo, puede utilizar de forma gratuita 'LOBE', una aplicación simple que permite el reconocimiento de imágenes -como el estar o no usando mascarilla- a través de etiquetas e imágenes utilizando este paradigma de aprendizaje. Aquí el video oficial promocional: <https://youtu.be/Mdcw3Sb98DA> ; Aquí el sitio oficial: <https://www.lobe.ai> [En línea, ambos consultados en marzo 2021]

³⁶² Así mismo, es posible clasificar los rasgos de personalidad, por ejemplo, siguiendo el "modelo de los 5 grandes" definidos por en "Fondo Internacional de Elementos de Personalidad" en grados de: apertura, amabilidad, estabilidad emocional y escrupulosidad. Esta clasificación fue la utilizada por Cambridge Analytica.

³⁶³ Fuente: ¿Qué es el Aprendizaje Supervisado y No Supervisado? | DotCSV. (2017, 16 octubre). [Video]. YouTube. https://www.youtube.com/watch?v=oT3arRRB2Cw&ab_channel=DotCSV

³⁶⁴ Esta información, que ha sido adecuada, proviene de: Bhatt, Shweta. [Data Scientist | Google Developer] (2019, 19 abril). Reinforcement Learning 101 - Towards Data Science. Medium. <https://towardsdatascience.com/reinforcement-learning-101-e24b50e1d292> (Consultado: abril 2020)

utilizado para entrenar una inteligencia en videojuegos; luego de varias partidas iniciando en movimientos aleatorios, lograra captar que combinaciones hacer para no perder.

REDES NEURONALES

Las redes neuronales son un tipo de algoritmo de *Machine learning* que se caracteriza por utilizar perceptrones, las denominados neuronas, para la optimización de parámetros mediante la técnica '*backpropagation*'. Tanto el paradigma de aprendizaje supervisado, no supervisado y reforzado, se pueden utilizar para entrenar redes neuronales.

El nombre neurona es dado por la similitud con nuestras neuronas, células que procesan y transmiten mensajes mediante señales eléctricas y químicas, que toman una o más entradas, las procesan, y emiten una nueva señal dentro de una enorme interconectada red. En lugar de ser señales como las nuestras, las neuronas artificiales, reciben valores de entrada y proyectan uno de salida dentro de una organización en capas, formando una red conectada por enlaces³⁶⁵. Las redes neuronales son entonces una serie de arquitecturas basadas en neuronas y un algoritmo de optimización que entre ellas genera enlaces. Estos enlaces son conocidos como parámetros, y pueden ser muchos, por ejemplo, la Inteligencia Artificial GPT-3 (2020) tiene 175 billones de parámetros.

La secuencia de conexiones entre neuronas genera capas, estas son la columna de neuronas que reciben información procesada por la capa anterior. Dada la complejidad del proceso, desconocemos exactamente porque una neurona proyecta un valor o ajusta el peso entre las capas, la técnica '*backpropagation*' las modula; por ello, la primera capa es denominada capa de entrada, las intermedias ocultas y la final, de salida. A grandes rasgos, utilizando los paradigmas comentados, podemos decir que las primeras capas detectan conceptos o información concreta, y luego las capas posteriores utilizan lo aprendido previamente para concluir conceptos más abstractos³⁶⁶. Como, por ejemplo, "en una primera

³⁶⁵ Parte de la formulación de lo que es machine learning lo he extraído de: ¿Qué es el Machine Learning? ¿Y Deep Learning? Un mapa conceptual | DotCSV. (2017, 1 noviembre). [Video]. YouTube. https://www.youtube.com/watch?v=KytW151dpqU&t=104s&ab_channel=DotCSV (En línea, consultado, abril 2021)

³⁶⁶

capa podrían detectarse trazos curvos, y con esta información podrían detectarse ruedas en una capa posterior, concluyendo finalmente que podría tratarse de un auto”³⁶⁷.

DEEP LEARNING

No hay límites en la cantidad de capas, esta dependerá en la capacidad de cómputo que se disponga. De aquí proviene el término aprendizaje profundo o *Deep Learning*. Esta profundidad se refiere a la complejidad del modelo matemático utilizado que ha sido resultado del proceso de muchas capas y parámetros.

Un modelo de *Deep Learning*, tendrá más capacidad de detección de patrones si tiene más parámetros y capas de neuronas. Entre mayor sea la capacidad de los sistemas lógicos - cantidad neuronas y conexiones-, posible con los mayor cantidad de transistores, la capacidad de hacer funcionar un modelo matemático de *Machine learning* aumenta, “permitiendo que encuentre lógicas más avanzadas, pueda modularizar su aprendizaje, o pueda almacenar información en los estados internos”³⁶⁸. Por lo mismo, una de las razones de porque estos algoritmos empezaron a tomar más relevancia en la actualidad, es debido a que el gran número de capas requiere de una capacidad de cómputo que solo recientemente ha sido alcanzado, lo que ha permitido a los investigadores aumentar esta complejidad para alcanzar niveles que aparecen no solo cuantitativamente distintos, sino también cualitativamente diferentes a los modelos utilizados anteriormente, llegando a poder descifrar patrones sumamente complejos. Esta capacidad puede proyectar patrones, y generar, por ejemplo, una partitura inexistente similar a la que hubiera hecho Bach, o generar

³⁶⁷ El ejemplo me lo ha dado mi amigo ‘Esteban Reyes de Jong’, ingeniero civil eléctrico que trabaja con redes neuronales. Aprovecho de decir que, gracias a Esteban y ‘Tomas Palomo Koscina’, licenciados de la escuela de ingeniería de la Universidad de Chile, he podido entender y corroborar esta información. Agradezco profundamente el poder haber discutido latamente el asunto de esta Tesis con ellos.

³⁶⁸ Esta frase es una cita de la misma fuente que inspira todo este párrafo sobre capacidad de cómputo y machine learning. Este párrafo esta especialmente guiado por: Csv, D. (2020, 6 diciembre). ¿La Ley de HUANG es la nueva Ley de Moore? | Data Coffee #14. www.youtube.com/watch?v=Jlboxj182bhg&ab_channel=DotCSV

objetos inexistentes a partir de descripciones de texto³⁶⁹, o mantener una discusión en tiempo real, como lo ha hecho IBM Debater, inteligencia que logra la “redacción y presentación de discursos basados en datos [...], y pronunciarlo de manera persuasiva” mediante “el desarrollo de técnicas de aprendizaje automático para extraer de corpus masivos, afirmaciones y pruebas y utilizarlos para generar argumentos relevantes para un tema controvertido.”³⁷⁰

³⁶⁹ Recomiendo para ver en primera persona la capacidad de generación de imagen por descripción de texto conocer a DALL-E, una inteligencia artificial que utiliza redes neuronales con 12 billones de parámetros. Con entrar al siguiente link podrá ‘jugar’ con unas de las capacidades liberadas al público de GPT-3: <https://openai.com/blog/dall-e/> [En línea: abril 2021]. Descripción oficial: “Hemos entrenado una red neuronal llamada DALL · E que crea imágenes a partir de leyendas de texto para una amplia gama de conceptos que se pueden expresar en lenguaje natural.”

³⁷⁰ How Project Debater work. (2021). IBM Research AI. <https://www.research.ibm.com/artificial-intelligence/project-debater/how-it-works/>

Bibliografía

Altraide, D. (2019). *New Thinking: From Einstein to artificial intelligence, the science and technology that transformed our world*. Mango Media.

Alvarado Ávalos, F. D. (2014). Las fuentes de acceso público a datos personales. *Revista Chilena de Derecho y Tecnología*, 3(2). <https://doi.org/10.5354/0719-2584.2014.33276>

Álvarez Valenzuela, Daniel. Acceso a la información Pública y Protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *Revista de Derecho*. Universidad Católica del Norte. Año 2013 N°1.

Anguita, Pedro (2007). *La protección de datos personales y el derecho a la vida privada*. Santiago: Jurídica. (p. 559)

Aristóteles. (s. IV a. C). *Retórica*. Editorial Gredos, Madrid

Bodenheimer, E. (1942). *Teoría Del Derecho*. Fondo de Cultura Económica.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. <https://doi.org/10.1080/00913367.2017.1339368>

Calo, M. R. (2013). Digital Market Manipulation. *SSRN Electronic Journal*. Published. <https://doi.org/10.2139/ssrn.2309703>

Carreño Dueñas (2012): "El derecho en la era de la virtualidad. nuevas realidades, nuevo derecho virtual"

Comité Evaluación de la Ley. Evaluación de la ley 19.628 Protección de la Vida Privada. http://www.evaluaciondelaley.cl/wpcontent/uploads/2019/07/informe_final_ley_19628_con_portada.pdf

Gilovich, Thomas; Savitsky, Kenneth (1996). "Like Goes with Like: The Role of Representativeness in Erroneous and Pseudo-Scientific Beliefs" doi:10.1017/CBO9780511808098.036.

Chomsky, N. & Herman, E. S. (1988). *Manufacturing Consent: The Political Economy of the Mass Media* (Reprint ed. 2002). Pantheon Books.

Cicerón, *Sobre el Orador*. (106-43 a.C.) Editorial Gredos, Madrid

Comité Evaluación de la Ley. Evaluación de la ley 19.628 Protección de la Vida Privada. http://www.evaluaciondelaley.cl/wpcontent/uploads/2019/07/informe_final_ley_19628_con_portada.pdf

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, 65(3), 122-135. <https://doi.org/10.1108/lr-06-2015-0061>

- Echeverría, R. (2003) *Ontología del lenguaje*. J. C. Sáez Editor.
- Errejón, I. Mouffe, C. (2015). *Construir pueblo: Hegemonía y radicalización de la democracia* (1.a ed.). Icaria editorial.
- Favaretto, M., de Clercq, E., & Elger, B. S. (2019). *Big Data* and discrimination: perils, promises and solutions. A systematic review. *Journal of Big Data*, 6(1). <https://doi.org/10.1186/s40537-019-0177-4>
- Fenwick, Mark & Vermeulen, Erik. (2019). The Lawyer of the Future as “Transaction Engineer”: Digital *Technologies* and the Disruption of the Legal Profession. DOI: 10.1007/978-981-13-6086-2_10
- Flanagan, M. Howe, D. Nissenbaum, H. (2005). *Values in Design: Theory and Practice*
- Foucault, M., & Frost, E. C. (1966). *Las palabras y las cosas: Una arqueología de las ciencias humanas*. Siglo XXI Editores.
- Garrido Iglesias, R. El Habeas data y la ley de protección de datos en Chile. Serie Bibliotecología y Gestión de Información N° 83, junio ,2013. ISSN: 0719 – 0832
- Georgias. (s.V). *Elogio a Helena*
- Han, B.-C. (2014). *Psicopolítica: Neoliberalismo y nuevas técnicas de poder* (Pensamiento Herder) (1.a ed.). Herder Editorial.
- Herrera., Viollier. (2020) *Rendición de cuentas de facebook y otros negocios en chile: la protección de datos personales en la era digital*. ISBN: 978-958-5597-32-7
- Hildebrandt, M., & Gutwirth, S. (Eds.). (2008). *Profiling the European Citizen*. Profiling the European Citizen. Published. <https://doi.org/10.1007/978-1-4020-6914-7>
- Hildebrandt, M., & Koops, B.-J. (2010). The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, 73(3), 428–460. <https://doi.org/10.1111/j.1468-2230.2010.00806.x>
- Hildebrandt, M. (2015). *Crossroads in New Media, Identity and Law: The Shape of Diversity to Come* Palgrave MacMillan.
- Hildebrandt, M. (2016). *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Edward Elgar Pub.
- Hildebrandt, M. (2020). *Law for Computer Scientists and Other Folk* (Illustrated ed.). Oxford University Press, USA.
- Hueso, L. C. (2016). *Big Data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales* ISSN 1989-7022
- Isócrates (s.V-IV a.C.). *Discursos, Antidosis*.
- Jijena, Renato. (2020). *Contenido y alcances del derecho fundamental a la protección de datos personales en la constitución de 1980*. Tesina de Magister.

Jiménez, Vicente. (2020). El «yo» en ser y tiempo de Martin Heidegger. Tesis para optar al grado de Licenciado en Filosofía UC

Kahneman, D. (2002). Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice. *American Psychologist*, 58(9), 697–720. <https://doi.org/10.1037/0003-066x.58.9.697>

Kate Crawford & Jason Schultz. (2014) Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. Rev. 93

Kant, I. (1873). *Principios Metafísicos del Derecho*.

Kant, I. (1781). *Critica de la Razón Pura*.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15), 5802-5805. <https://doi.org/10.1073/pnas.1218772110>

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111(24), 8788-8790. <https://doi.org/10.1073/pnas.1320040111>

Lanzing, M. "Strongly Recommended" Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking *Technologies*. *Philos. Technol.* 32, 549–568 (2019). <https://doi.org/10.1007/s13347-018-0316-4>

Leiser, M., & Murray, A. (2016). The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital *Technologies*. *Oxford Handbooks Online*. Published. <https://doi.org/10.1093/oxfordhb/9780199680832.013.28>

Lupton, D. (2015). *Digital sociology*. Routledge, Taylor & Francis Group

Montbrun, Alberto. (2010). Notas para una revisión crítica del concepto de "poder". *Polis* (Santiago), 9(25), 367-389. <https://dx.doi.org/10.4067/S0718-65682010000100022>

Musa Giuliano, R. (2020). Echoes of myth and magic in the language of Artificial Intelligence. *AI & SOCIETY*, 35(4), Springer-Verlag London Ltd., 1009-1024. <https://doi.org/10.1007/s00146-020-00966-4>

Nogueira Alcalá, Humberto, Reflexiones sobre el establecimiento constitucional del Hábeas Data, en *Ius et Praxis*, Talca, año 3, N° 1, 1997.

Ospina-Celis y Upegui Mejí. (2020) *Festín de datos Empresas y datos personales en América Latina*. (Introducción) Editorial Dejusticia, ISBN 978-958-5597-31-0

Ospina-Celis y Upegui Mejí. (2020) *EMNBD y protección de datos personales en Brasil, Chile, Colombia y México: la experiencia común*.

Plantón. (s.V). *Diálogos*. Gorgias

Schwab, K. (2016). *La cuarta revolución industrial*. Debate.

- Schwab, K., & Davis, N. (2018). *Shaping the Fourth Industrial Revolution*. CITIC Press Corporation.
- Seaver, N. (2019). Captivating algorithms: Recommender systems as traps. *Journal of Material Culture*, 24(4), 421–436. <https://doi.org/10.1177/1359183518820366>
- SERNAC (2021). Informe de Resultados de Levantamiento de Dark Patterns en Comercio Electrónico (V: 1.2) https://www.sernac.cl/portal/617/articles-62983_archivo_01.pdf
- Skatova, A.; Lorenz-Spreen, P.; Lewandowsky, S.; Leiser, M.R.; Herzog, S. (2019) Response to the Centre for Data Ethics and Innovation: [call for a] review of online targeting. <https://hdl.handle.net/1887/83089>
- Sófocles (s.V) Filoctetes.
- Solove, Daniel J. (2013) Privacy Self-Management and the Consent Dilemma, 126 *Harv. L. Rev.*
- Susser, D., Roessler, B., & Nissenbaum, H. F. (2018). Online Manipulation: Hidden Influences in a Digital World. *SSRN Electronic Journal*, 1. <https://doi.org/10.2139/ssrn.3306006>
- Susser, D; R, Beate; Nissenbaum, H. F. (2019): Technology, autonomy, and manipulation, *Internet Policy Review*, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 8, Iss. 2, pp. 1-22, <http://dx.doi.org/10.14763/2019.2.1410>
- Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Illustrated ed.). Yale University Press.
- Tversky., Kahneman. (1974) Judgment under Uncertainty: Heuristics and Biase., *Science*. New Series, Vol. 185, No. 4157 (Sep. 27, 1974), pp. 1124-1131 <https://www.jstor.org/stable/1738360?seq=1>
- Viollier, P. & Derechos Digitales, (2017, febrero). El estado de la protección de datos personales en Chile. <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>
- Valenzuela Cori, R. (2009). *Retórica: un ensayo sobre tres dimensiones de la argumentación*
- Weber, Max, *economía y Sociedad. Esbozo de sociología comprensiva* (1922). Ed. FCE, México, 2008
- Wolfie C, (2017). How companies use personal data against people. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. Working paper by cracked LABS.
- Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036-1040. <https://doi.org/10.1073/pnas.1418680112>
- Yeung, K. (2016). 'Hypernudge': *Big Data* as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–136. <https://doi.org/10.1080/1369118x.2016.1186713>
- Zarsky, T. (2015). The Trouble with Algorithmic Decisions. *Science, Technology, & Human Values*, 41(1), 118–132. <https://doi.org/10.1177/0162243915605575>

Zuboff, S. (2020). La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder. Ediciones Paidós.

Bibliografía no académica

NO AUDIOVISUAL

Agencia española de protección de datos. IoT (I): Qué es IoT y cuáles son sus riesgos. (2020). AEPD. <https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos>

Angie Hobbes. In our time - rhetoric - BBC Sounds. (2004) <https://www.bbc.co.uk/sounds/play/p004y263>

Álvarez, Daniel (2021) “El Estado es un muy buen recolector de datos personales de los pobres”. The Clinic. <https://www.theclinic.cl/2021/10/29/daniel-alvarez-experto-en-derechos-digitales-y-privacidad-de-datos-el-estado-es-un-muy-buen-recolector-de-datos-personales-de-los-pobres/>

Arrieta (2019). El nuevo entorno regulatorio de la protección de datos personales en Chile. En línea: <https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-Chile/>

Bio-bio. (2019) So Safe niega traspaso de datos personales: los controla empresa que asesora campañas electorales. <https://www.biobiochile.cl/noticias/nacional/chile/2019/09/13/so-safe-niega-traspaso-de-datos-personales-los-controla-empresa-que-asesora-campanas-electorales.shtml>

Cambridge Analytica and Facebook: The Scandal So Far, AL JAZEERA (2018), <https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html> [<https://perma.cc/PU4C-KNSN>].

CBS NEWS (2013). Man claiming to be NSA whistleblower comes forward <https://web.archive.org/web/20180918064927/https://www.cbsnews.com/news/man-claiming-to-be-nsa-whistleblower-comes-forward/>

CIPER (2018) Instagis: el “gran hermano” de las campañas políticas financiado por Corfo en <https://ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/>

CIPER (2019). Alguien te mira: así funciona el gigante de las campañas políticas que controla Sosafe <https://www.ciperchile.cl/2019/09/11/alguien-te-mira-asi-funciona-el-gigante-de-las-campanas-politicas-que-controla-sosafe/>

Contrato entre Instagis y el partido político Renovación Nacional. (2017) <https://ciperChile.cl/wp-content/uploads/INSTAGIS-CONTRATO-CON-RN.pdf>

Contreras, Pablo. (2019) <https://www.pcontreras.net/blog/october-08th-2019>

Daniel Solove. LinkedIn. Facebook's Psych Experiment: Consent, Privacy, and Manipulation. (30 de junio de 2014). <https://www.linkedin.com/pulse/20140630055215-2259773-the-facebook-psych-experiment-consent-privacy-and-manipulation/>

Dictamen 8/2014 del Grupo de Trabajo del Artículo 29. Comité Europeo de Protección de Datos.

Informe Domo.com 6. (2017) <https://www.domo.com/learn/data-never-sleeps-6>

El Mostrador. DW. EE.UU. multa a Facebook con US\$5.000 millones por violación de privacidad. El Mostrador. (2019). <https://www.elmostrador.cl/dia/2019/07/24/eeuu-multa-a-facebook-con-5-000-millones-por-violacion-de-privacidad>

FACEBOOK POLICY (2021) https://www.facebook.com/full_data_use_policy

IBM Research AI. How Project Debater work. (2021). <https://www.research.ibm.com/artificial-intelligence/project-debater/how-it-works/>
<https://www.latercera.com/la-tercera-pm/noticia/instagis-la-empresa-de-datos-que-trabajo-para-pinera-el-limite-es-trabajar-con-informacion-publica/108576/>

IBM ¿Qué es Big Data? (2012) <https://developer.ibm.com/es/articles/que-es-big-data/>

Informe asesoría externa de segmentación y análisis de habitantes del distrito para comunicación de políticas públicas realizado por INSTAGIS SPA. para el Diputado José Manuel Edwards” (2016). En línea: <https://ciperchile.cl/wp-content/uploads/F4573-Informe-Final-38000-Edwards-Jos%C2%AE-Manuel-1.pdf>

Internet World Stats <https://www.internetworldstats.com/stats.htm>

Jerónimo García-Loygorri Herreros de Tejada. (2019). BBVA Innovation Labs ; Redes neuronales distribuidas con Tensorflow: Conclusiones- <https://www.bbva.com/es/redes-neuronales-distribuidas-tensorflow-conclusiones/>

Jon Padfield, PhD. LinkedIn. Did Facebook's «Emotional Manipulation» Research Cross an Ethical Line? (2018) <https://www.linkedin.com/pulse/did-facebooks-emotional-manipulation-research-cross-jon-padfield-phd/>

La Tercera: “¿Cuáles son los límites? -Solo trabajar con información pública, a la que puede acceder cualquiera.(2018) <https://www.latercera.com/la-tercera-pm/noticia/instagis-la-empresa-de-datos-que-trabajo-para-pinera-el-limite-es-trabajar-con-informacion-publica/108576/>

Madeleine K. Albright, Chairman National Democratic Institute, at #DisinfoWeek (2017). <https://medium.com/dfrlab/we-need-21st-century-responses-6b7eed6750a4>

Mark Warneren The Verge. Is huawei a security threat? seven experts weigh in. (2019) <https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g>

Meyer, R. (2014, 28 julio). Everything We Know About Facebook's Secret Mood-Manipulation Experiment. The Atlantic. <https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/>

Reinforcement Learning 101 - Towards Data Science. Medium. (2018)
<https://towardsdatascience.com/reinforcement-learning-101-e24b50e1d292>

Sam Machkovech, Facebook Helped Advertisers Target Teens Who Feel "Worthless," ARS TECHNICA (2015)
<https://arstechnica.com/informationtechnology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/>

Silva, P., & Mohor, E. (2016, 1 marzo). Fuentes accesibles al público y el caso del sitio "datos. 24x7.cl" Hipervinculos. Carey/.
<https://www.hipervinculos.cl/fuentes-accesibles-al-publico-caso-del-sitio-datos-24x7-cl-parte-1-planteamiento/>

Staff, P. (2019). The Anchoring Effect and How it Can Impact Your Negotiation. PON - Program on Negotiation at Harvard Law School. <https://www.pon.harvard.edu/daily/negotiation-skills-daily/the-drawbacks-of-goals/>

SUBTEL. (2017) <https://www.subtel.gob.cl/estudios/internet-y-sociedad-de-la-informacion/>

SUBTEL. (2018). Informe Anual del Sector Telecomunicaciones 2018. ://www.subtel.gob.cl/wp-content/uploads/2019/04/PPT_Series_DICIEMBRE_2018_V2.pdf

Universidad de Helsinki "Helsingin yliopisto" (2020). elementsofai.com/

University of New South Wales, Sydney.
<https://web.archive.org/web/20180826151959/http://www.cse.unsw.edu.au/~billw/mldict.html#activfn>

AUDIOVISUAL

¿La Ley de HUANG es la nueva Ley de Moore? | Data Coffee #14. (2020, 6 diciembre) [Video]. YouTube.
www.youtube.com/watch?v=Jlbxj182bhg&ab_channel=DotCSV

¿Qué es el Aprendizaje Supervisado y No Supervisado? | DotCSV. (2017, 16 octubre). [Video]. YouTube.
https://www.youtube.com/watch?v=oT3arRRB2Cw&ab_channel=DotCSV

¿Qué es el Machine Learning? ¿Y Deep Learning? Un mapa conceptual | DotCSV. (2017, 1 noviembre). [Video]. YouTube. https://www.youtube.com/watch?v=KytW151dpqU&t=104s&ab_channel=DotCSV

Alexander Nix, Cambridge Analytica - The Power of Big Data and Psychographics. (2016, 27 septiembre). [Video]. YouTube.
https://www.youtube.com/watch?v=n8Dd5aVXLCc&ab_channel=Concordia

Anthony Miyazaki - How Digital Is Changing the Future of Marketing / #MarketingMinute 134 (Marketing Strategy). (2020, 14 abril). [Video]. YouTube.
https://www.youtube.com/watch?v=MjtB32ryjXQ&list=WL&index=11&t=201s&ab_channel=AnthonyMiyazaki

Christopher Wylie: What is the Cambridge Analytica scandal? (2018). [Video]. YouTube. https://www.youtube.com/watch?v=Q91nvbJSmS4&ab_channel=TheGuardian

Diaz, Felix. Foucault, Sujeto y Verdad. (2019, 3 diciembre). [Video]. YouTube. https://www.youtube.com/watch?v=zTLX9s1VBA4&t=554s&ab_channel=ResumenesEntelekia

Håvard Rustad Markussen, The Political Subject of Surveillance Capitalism. (2020, 18 diciembre). [Video]. YouTube. https://www.youtube.com/watch?v=GImo8ajDyZE&list=WL&index=27&ab_channel=TheEndsofAutonomy

Machine Learning & Artificial Intelligence: Crash Course Computer Science #34. (2017, 1 noviembre). [Video]. YouTube. https://www.youtube.com/watch?v=z-EtmaFJieY&ab_channel=CrashCourse

Martin Heidegger: the Question Concerning Technology. (2020, 4 agosto). [Video]. YouTube. https://www.youtube.com/watch?v=gaVmEN-vGWk&ab_channel=EpochPhilosophy.

Martín Migoya. Experiencia Endeavor Córdoba (2019) - Globant [Video]. YouTube. <https://youtu.be/me0K5ghXDeE>

Chomsky - Manufacturing Consent. Extracto del documental "Manufacturing Consent: Noam Chomsky and the Media" (1992). [Video]. YouTube. https://www.youtube.com/watch?v=Rwh1HCb_xnk&ab_channel=Bega

Richard Thaler - Nudge: An Overview (2011) [Video]. YouTube. <https://www.youtube.com/watch?v=xoA8N6nJMRs>

Shoshana Zuboff: We Need Rights to Protect Us from Big Data Surveillance | Amanpour and Company. (2021) YouTube. [Video]. https://www.youtube.com/watch?v=D8qAGQQbZd0&ab_channel=AmanpourandCompany

Rt. Revd. Dr. Steven Croft. The Ethics of Artificial Intelligence | Stories of Impact. (2020, 13 julio). [Video]. YouTube. <https://www.youtube.com/watch?v=06oa2kQxvRs&t=323s>

The Social Dilemma. (2020) Netflix

Viollier. (2020, 24 de marzo). Clase 4 - Introducción a la protección de datos personales [Video]. YouTube. <https://www.youtube.com/watch?v=gxv28qQPCTo&list=PLUfm9vw9SqXUBEG7kPYD0YMIndeZysZxb>

Viollier. (2020, 18 abril). 5 razones contra el voto electrónico [Video]. YouTube. <https://www.youtube.com/watch?v=HKjpUXl8HkE&list=PLUfm9vw9SqXUJkSbaiYUjHWf6bNAB8IE8>

Viollier. (2020) Clase 6 - Observancia de reglas de datos personales. [Video]. YouTube. <https://www.youtube.com/watch?v=5xPPPQtYD8k&list=PLUfm9vw9SqXUBEG7kPYD0YMIndeZysZxb&index=3> min

Yuval Noah Harari. (2020, 24 enero). Yuval Noah Harari: How to Survive the 21st Century- Davos 2020 [Video]. YouTube. https://www.youtube.com/watch?v=gG6WnMb9Fho&ab_channel=YuvalNoahHarari

