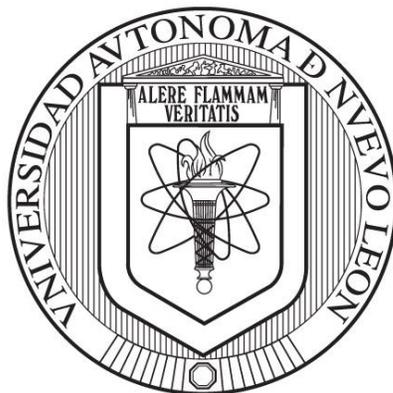


UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE FILOSOFÍA Y LETRAS
LICENCIATURA EN FILOSOFÍA Y HUMANIDADES



LOS PRINCIPIOS DEL PODER DEL CONOCIMIENTO DE LOS DATOS PRIVADOS
EN LA ERA DIGITAL Y SUS INFLUENCIAS DE COMPORTAMIENTO EN LO
PÚBLICO

TESIS

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FILOSOFÍA Y
HUMANIDADES

PRESENTA

ELADIO DE JESÚS TOVAR ORTIZ

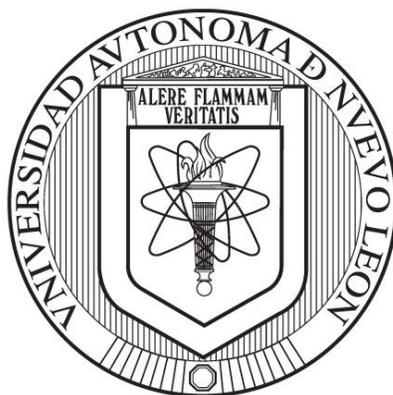
ASESOR

DR. JOSÉ LUIS CISNEROS ARELLANO

SAN NICOLÁS DE LOS GARZA, N.L.

FEBRERO 2023

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE FILOSOFÍA Y LETRAS
LICENCIATURA EN FILOSOFÍA Y HUMANIDADES



LOS PRINCIPIOS DEL PODER DEL CONOCIMIENTO DE LOS DATOS PRIVADOS
EN LA ERA DIGITAL Y SUS INFLUENCIAS DE COMPORTAMIENTO EN LO
PÚBLICO

TESIS

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FILOSOFÍA Y
HUMANIDADES

PRESENTA

ELADIO DE JESÚS TOVAR ORTIZ

ASESOR

DR. JOSÉ LUIS CISNEROS ARELLANO

SAN NICOLÁS DE LOS GARZA, N.L.

FEBRERO 2023

A mi familia, mi cimiento y motivación

A mis padres, lluvia que alimenta y calma el alma

A Liz, mi aliento inagotable, mi refugio

A la filosofía, la herramienta bella

Resumen

El objeto de este trabajo es realizar un análisis explicativo acerca de los principios del funcionamiento de la estructura del poder tecnológico en la Era digital basado en el conocimiento de los datos personales y privados de las personas. En un primer momento realizaremos una revisión del concepto de privacidad desde sus perspectivas filosófica, descriptiva y normativa, así como su trascendencia en el sistema democrático liberal y su íntima relación con la idea de libertad y persona. Después, analizaremos el momento histórico de la transición informática analógica-digital y lo que representó para la reconfiguración del valor de los datos personales y su uso en la Era digital. Señalaremos lo que hace que un dato sea personal, para luego explicar cómo los datos personales han sido usados por empresas tecnológicas y organismos particulares para beneficiarse económica y políticamente mediante el uso de la inteligencia artificial capaz de inferir rasgos de personalidad, predecir el comportamiento humano y manipular las decisiones políticas de la sociedad. Mostraremos los impactos que el uso de este tipo de tecnología tiene en la salud mental, y particularmente la relación compleja que surge entre los conceptos de orden y control que engendran poder y las necesidades psicológicas innatas, la cual guarda los fundamentos de la tecnología basada en el conocimiento de datos personales y el desarrollo humano. Por último, nos aventuraremos a dar un concepto que engloba nuestro análisis en una disyunción inclusiva que se desarrolla en una nueva y distinta forma de poder: el Doble Poder. Concepción metafísica que fundamenta las causas del funcionamiento de este poder tecnológico y responde al nulo accionar político frente a los peligros que representa este tipo de poder para la salud mental y el desarrollo de las democracias del mundo.¹

Índice

Resumen	II
Introducción	V
Capítulo I. ¿Qué es la Privacidad?	1
1.1 Privacidad e intimidad.....	2
1.2 La experiencia de Privacidad en la antigüedad occidental.....	4
1.3 La finalidad de la política	6
1.4 Persona, Privacidad y Democracia	8
1.5 Antecedentes de la Privacidad como Derecho.....	18
1.5.1 Kant y Locke en Privacidad.....	20
1.5.2 Derechos de la Personalidad y el valor social de la Privacidad.....	21
1.6 Características de los Derechos Humanos y su relevancia en el Derecho a la Privacidad	26
1.7 El Derecho a la Privacidad en la Declaraciones de Derechos Humanos	27
1.8 Las tres generaciones de derechos de Karel Vasak y la idea de Privacidad... ..	28
Capítulo II. Los datos en la Era digital.....	36
2.1 El Big Data	40
2.2 Los datos personales	44
2.2.1 Modelo analítico para usos morales e identificación de datos personales. .	48
2.3 El uso de los datos personales en la Era digital	50
2.4 Malentendidos de la privacidad en la Era digital.....	57
Capítulo III. Impactos de la Era digital en lo público	65
3.1 Inferencias de datos sensibles	66
3.2 Predicción de comportamiento (Análisis Predictivo)	70
3.2.1 El caso Cambridge Analytica	76
3.2.2 Conocimiento y Poder	85

3.3 Manipulación política.....	88
3.4 Impactos a la salud mental	95
Capítulo IV. Doble Poder	103
Conclusión	116
Referencias bibliográficas.....	119
Anexos	132

Introducción

El origen de la filosofía está en el *thaumadzein*,
en el maravillarse y ser embargado por el asombro de modo duradero,
lo cual constituye el negocio del filósofo.
Hannah Arendt, *La condición humana* (2015)

El objetivo de esta investigación es mostrar el funcionamiento de la estructura de poder tecnológica basada en el uso de datos personales y la violación del derecho a la privacidad, a la vez que se realiza un análisis explicativo de las herramientas y dispositivos fundamentales creados y utilizados para la obtención de este poder. Nuestro punto de partida está en la creencia de la existencia de un mecanismo de poder tal, que genera una casi demencia colectiva respecto a la violación de la privacidad. Por tanto, nuestra pregunta primordial busca conocer cuáles son los elementos esenciales que posibilitan el desarrollo del poder tecnológico basado en el conocimiento de los datos personales y privados, a la vez que damos ciertos presupuestos para comprender el valor de la privacidad en una sociedad democrática y establecemos los funcionamientos de la extracción, acumulación y uso de los datos personales que violan la privacidad de las personas.

En el primer capítulo trataremos de definir el concepto de privacidad, delimitando su diferencia y señalando su relación con el concepto de intimidad. También, realizamos una breve revisión histórica de las concepciones de privacidad en la libertad de los antiguos y la de los modernos, mientras trazamos las delimitaciones entre la esfera pública y la esfera privada. De la misma manera, precisamos el valor y la importancia de la privacidad en el ser persona y la vida democrática liberal. Y por último, veremos la fundamentación de la privacidad como derecho humano y su evolución gradual hasta nuestros días en la clasificación de las tres generaciones de derechos de Karel Vasak.

En el segundo capítulo, señalamos las nociones normativas y legales de la definición de datos personales, así como su fundamentación filosófica a través de un método analítico para usos morales e identificación de datos personales. Después, nos adentraremos a conocer el funcionamiento y el inicio histórico del uso de los datos personales y la violación del derecho a la privacidad, por parte de las empresas tecnológicas y gobiernos. Y para finalizar, analizaremos algunos malentendidos de la privacidad en la práctica cotidiana.

Para el tercer capítulo, damos a conocer el funcionamiento de la inferencia de datos sensibles, la predicción del comportamiento humano y la manipulación de decisiones políticas y económicas mediante el uso de inteligencia artificial, a la vez que las señalamos como cualidades nuevas y distintas de este tipo de poder, generadas a partir del uso de datos personales en la Era digital. Del mismo modo, reconocemos que este tipo de dispositivos de poder, provocan impactos peligrosos en las sociedades democráticas y la salud mental de las personas.

En nuestro capítulo conclusivo, damos a conocer que este nuevo poder tecnológico desarrollado por las Big Tech está fundamentado en la relación compleja de dos elementos esenciales que posibilitan el desarrollo humano. Reconocemos que a pesar de los peligros, este poder tecnológico es posible y sigue desarrollándose. Por último, presentamos una propuesta para nombrar a este tipo de poder, mientras damos a conocer a través de un movimiento hegeliano las concepciones metafísicas de nuestro análisis investigativo, es decir, los elementos esenciales que posibilitan el desarrollo de este poder bajo un modelo analítico.

Capítulo I. ¿Qué es la Privacidad?

El lugar del individuo es la sociedad,
pero el lugar de la persona es un íntimo espacio.
María Zambrano, *Persona y Democracia* (1956)

Durante algunos años del siglo XX en diversas latitudes del mundo se gestaron y florecieron regímenes dictatoriales y totalitarios. La negación de la pluralidad y libertades individuales entre sus ciudadanos fue su bandera. Fueron esos regímenes los que han llevado más lejos su desprecio por la libertad de las personas y la invasión de su privacidad.¹ Fue esto mismo – en conjunto con diversos factores – lo que en su final vendría a ser su enfermedad y desembocara en su hundimiento. La pluralidad de ideas, emociones y acciones de cualquier persona reclama una salida a un régimen que lo controla todo. Existe algo que hace que el ciudadano del mundo se diferencie de los demás, cierta individualidad demarcada por un límite entre el afuera y el adentro. En otras palabras, la existencia de una libertad en la mente y para sí mismo denota un *adentro* en el que nadie puede entrar, a menos que el propio individuo de entrada. Este adentro es entendido por Jean-Jacques Rousseau como la intimidad del corazón. Una intimidad libre de la insoportable perversión del corazón humano por parte de la sociedad y su intrusión a las zonas más íntimas del hombre.² Sin embargo, para el régimen dictatorial es fundamental cerrar los espacios a la pluralidad y ejercer un amplio dominio del sujeto desde el poder. Formarlo a su manera e intereses.³ Penetrar en lo

¹ Manuel Toscano, “Sobre El Concepto de Privacidad: La Relación Entre Privacidad e Intimidad,” *Isegoria*, no. 57 (2017): 533–52, <https://doi.org/10.3989/isegoria.2017.057.06>.

² Hannah Arendt, *La Condición Humana*, 1a ed. (Buenos Aires: Paidós, 2003), 49–50.

³ Michel Foucault, *Microfísica Del Poder* (Buenos Aires: Siglo Veintiuno, 2019).

más íntimo de la persona. Entrar en cada aspecto de su vida: su pasado, presente y futuras enfermedades, miedos, pérdidas, caídas, traumas, fantasías.⁴ Es innegable la existencia de ese espacio intangible que guarda lo más íntimo de cada persona. Y es este mismo espacio intangible el que cobró valor para las sociedades liberales y democráticas. En un primer momento, trataremos de definir qué es lo que queremos decir con privacidad, su diferencia con la intimidad, a la vez que demarcamos su límite y relación con lo público, para después profundizar en la garantía del derecho a la privacidad como fundamento de las libertades individuales.

1.1 Privacidad e intimidad

La privacidad muchas veces es confundida con la intimidad. Se cree erróneamente que lo privado es lo íntimo y que solo lo íntimo puede contar como privado.^{II} La intimidad será entendida como «la esfera de confianza y confidencialidad que se crea entre las relaciones cercanas»,⁵ aunque también es entendida como una especie de escenario que carece de proyección exterior; esto es, nuestros deseos, sentimientos, pensamientos, intenciones de nuestros actos. Las cuales se apoyan en un yo imaginario en relación con el yo imaginarios de los otros. El escenario íntimo tiene la propiedad de ser observable solo para el sujeto.⁶ Así pues, podríamos decir que la intimidad guarda dos sentidos en su significado, uno en relación con alguien más, “un confidente” y otro capaz de advertir una realidad propia del sujeto y que solo él conoce, pero que puede ser conocida por alguien más

⁴ Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (London: Bantam Press, 2020), 45.

⁵ Carissa Véliz, “Más Sobre Privacidad. Respuesta a Los Comentarios Sobre ‘Privacidad Es Poder,’” *EUNOMÍA. Revista En Cultura de La Legalidad*, no. 21 (2021): 432, <https://doi.org/10.20318/eunomia.2021.6366>.

⁶ Carlos Castilla del Pino, “Teoría de La Intimidad,” *Revista de Occidente* 182–183 (1996): 19.

a partir de la exteriorización. La intimidad es el lugar donde suceden las relaciones sexuales, las charlas en un estado de desnudez del alma, los pensamientos libres de juicio exterior, los sueños extraños que no se dicen por pena, los secretos que se llevarán a la tumba. Es el espacio de libertad por excelencia. Ahí donde uno es libre y se muestra sin filtros. Y a pesar de que esto esté fuertemente ligado a la privacidad, existen diferencias que hacen que se distingan una de la otra.

Ahora bien, para dar una definición descriptiva a lo que nos referimos con privacidad diremos que es «la llave que abre los aspectos más íntimos y personales de uno mismo, aquellos que expresan ser más lo que eres».⁷ «...Es la que protege los aspectos más íntimos y personales de los individuos, los que los singularizan, y también los que los hacen más vulnerables».⁸ «Es un espacio (físico y metafórico) lejos de los demás que nos protege de las presiones de estar con otras personas y de los abusos de poder».⁹ También es entendida por Roger Clarke como un interés individual en mantener un espacio personal, libre de interferencias de otras personas y organizaciones.¹⁰ Así pues, por un lado la privacidad protege, controla y crea un espacio seguro con respecto a terceras personas, mientras que por otro lado la intimidad es el espacio donde se puede encontrar la confidencialidad y lo inobservable por principio (pensamientos, deseos, intenciones) por otros sujetos, más no incognoscible. En suma, la privacidad es necesaria para tener intimidad.¹¹ La privacidad tiene un sentido identitario para la persona, todo lo íntimo – decía Pessoa – es ridículo.

⁷ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 45.

⁸ Carissa Véliz, “La Privacidad Como Instrumento de Resistencia Colectiva,” *Anuario Internacional CIDOB 2021*, 2021, 22.

⁹ Véliz, “Más Sobre Privacidad. Respuesta a Los Comentarios Sobre ‘Privacidad Es Poder,’” 432.

¹⁰ Roger Clarke, “Internet Privacy Concerns Confirm the Case for Intervention,” *Communications of the ACM* 42, no. 2 (1999): 60, <https://dl.acm.org/doi/pdf/10.1145/293411.293475>.

¹¹ Véliz, “Más Sobre Privacidad. Respuesta a Los Comentarios Sobre ‘Privacidad Es Poder,’” 432.

1.2 La experiencia de Privacidad en la antigüedad occidental

Sin embargo, esta concepción de privacidad no siempre fue así. Como la gran mayoría de las cosas, su comprensión e importancia ha ido cambiando a través de la historia. Y dado que cada sociedad establece un equilibrio distintivo entre la esfera privada y el orden público, basado en la filosofía política de la sociedad,¹² habrá que echar mano de los procesos políticos e históricos, de tal manera, que se pueda hacer una revisión de lo que le da sentido y sustento a nuestra idea de privacidad. La esfera privada, en el caso de la antigüedad y específicamente en las sociedades de Roma y Grecia, se perdía en la colectividad, o bien en la libertad colectiva como lo llama Constant. Esta libertad consistía:

...En ejercer colectiva pero directamente muchas partes de la soberanía entera; en deliberar en la plaza pública sobre la guerra y la paz; en concluir con los extranjeros tratados de alianza; en votar las leyes (...) pero, al mismo tiempo que era todo esto lo que los antiguos llamaban libertad, ellos admitían como compatible con esta libertad colectiva la sujeción completa del individuo a la autoridad de la multitud reunida. (...) Aun en las relaciones domésticas más ocultas también intervenía la autoridad (...) las leyes regulaban las costumbres; y, como éstas tienen conexión con todo, nada había que aquéllas no pretendiesen arreglar.¹³

Como vemos, la distinción entre la vida pública que tiene lugar en el ágora, el foro o la plaza pública, a la vista de todos, y el ámbito doméstico (*oikos*) donde transcurre la vida familiar es conocido desde antiguo.¹⁴ Esto es, la esfera pública y la esfera privada. Dos grandes formas de vivir el desarrollo de ser humano. Es primordial resaltar la fuerza que cobraba el colectivo frente al individuo, si es que siquiera podemos considerar la existencia

¹² Alan F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59, no. 2 (2003): 431–53, www.forstbuch.de.

¹³ Benjamin Constant, "De La Libertad de Los Antiguos Comparada Con La de Los Modernos," in *Del Espíritu de Conquista* (Madrid: Tecnos, 1989), 68.

¹⁴ Toscano, "Sobre El Concepto de Privacidad: La Relación Entre Privacidad e Intimidad."

del individuo, dada su opacidad frente al entramado político y colectivo. El ejemplo claro de esto reside en que todas las acciones privadas estaban sometidas a una severa vigilancia:

...nada se concedía a la independencia individual ni bajo el concepto de opiniones, ni del de industria (...) En las cosas que nos parecen más útiles, la autoridad del cuerpo social se interponía, y mortificaba la voluntad de los particulares. De tal forma que concebir los derechos individuales en ese tiempo era imposible. Los antiguos, como dice Condorcet, no tenían noción alguna de los derechos individuales. Los hombres no eran, sino máquinas, cuyos resortes y ruedas regulaba y dirigía la ley. Por decirlo así, el individuo estaba de alguna manera perdido en la nación, y el ciudadano en la ciudad.¹⁵

Para que sucediera un cambio en la forma en como era comprendida y desarrollada la libertad existieron diversos factores, uno de ellos fue el comercio. Esta actividad fue el medio para obtener aquello que se deseaba sin la necesidad de la guerra. Con él, los intereses particulares fueron aumentando y con ellos la necesidad de protegerlos. Poco a poco el individuo fue obteniendo mayor prevalencia frente al colectivo, dada su aspiración a la independencia individual y la satisfacción de los deseos sin la intervención de la autoridad. En Atenas, por ejemplo, que era de las repúblicas griegas la más comerciante, se concedía mayor libertad individual que en Roma o Esparta. El desarrollo de la libertad fue girando de lo público a lo privado; de la libertad en la participación activa en y por el bien público, a la libertad de la satisfacción individual de los deseos. Así pues, lo que en la antigüedad era entendido como libertad, en la modernidad su concepción está más cerca de ser casi lo contrario. La libertad de los modernos es comprendida de la siguiente manera:

...el derecho de no estar sometido sino a las leyes, no poder ser detenido, ni preso, ni muerto, ni maltratado de manera alguna por el efecto de la voluntad arbitraria de uno o de muchos individuos: es el derecho de decir su opinión, de escoger su industria, (...) de ir y venir a cualquier parte sin necesidad de obtener permiso, ni de dar cuenta a nadie de sus

¹⁵ Constant, "De La Libertad de Los Antiguos Comparada Con La de Los Modernos," 68–69.

motivos o sus pasos: es el derecho de reunirse con otros individuos, (...) es en fin, para todos el derecho de influir o en la administración del gobierno, o en el nombramiento de algunos o de todos los funcionarios.¹⁶

La libertad de los modernos dota al individuo de garantías propias para desarrollarse y cumplir con sus intereses privados. Ha de comprenderse como «el goce pacífico y la independencia privada».¹⁷ Se marca la delimitación, así como la protección de una esfera privada, a la que el ciudadano puede retirarse para perseguir libremente sus proyectos y relaciones personales, es una de las dimensiones fundamentales del constitucionalismo liberal por cuanto sirve a su propósito fundamental: la limitación del poder político a fin de salvaguardar los derechos y libertades individuales.¹⁸

Podemos reconocer ahora los cambios que existieron en las concepciones de libertad y en la delimitación entre la esfera pública y la esfera privada, cuyo proceso histórico llevaría a una protección de esta última de la primera. El surgimiento de los derechos individuales nace a partir de la necesidad del cuidado, protección y garantía de libertades del ciudadano en sus intereses, relaciones y vida doméstica. Tanto la delimitación de lo público y lo privado como la libertad fueron determinadas por la política, una actividad específicamente humana y por lo cual parece primordial señalar su fin y sentido, así como lo que hacía que se distinguiera de otro tipo de convivencia humana.

1.3 La finalidad de la política

La palabra *politikon* – adjetivo que Aristóteles le asignaba a la organización de la *polis* –, el cual hacía referencia a la particularidad humana de vivir en la llamada ciudad-

¹⁶ Constant, 67.

¹⁷ Constant, 75.

¹⁸ Toscano, “Sobre El Concepto de Privacidad: La Relación Entre Privacidad e Intimidad.”

estado y que la organización de ésta representa la suprema forma humana de convivencia; es, por lo tanto, humana en un sentido específico, igualmente alejado de lo divino, que puede mantenerse por sí solo en plena libertad y autonomía, y de lo animal, en que la convivencia – sí se da – es una forma de vida marcada por la necesidad. La política surgió debido al hecho elemental y prepolítico de la necesidad biológica, que hace que los hombres se necesiten los unos a los otros en la ardua tarea de mantenerse con vida. Por lo tanto, según Aristóteles, la política no es en absoluto una obviedad ni se encuentra dondequiera que los hombres convivan, puesto que lo que distinguía la convivencia de los griegos de otras formas de convivencia humana era la libertad. Ser libre y vivir en una *polis* eran en cierto sentido uno y lo mismo. Para estar en el espacio de la *polis* el hombre debía estar libre de las obligaciones necesarias para vivir, que era el sentido propio del *scholê* griego o el *otium* romano, el ocio como le decimos hoy. El fin de lo político era la liberación prepolítica para la libertad en la *polis* y su sentido era que los hombres se relacionaran entre ellos en libertad, más allá de la violencia, la coacción y el dominio, iguales con iguales, que mandaran y obedecieran solo en momentos necesarios – en la guerra – y, si no, que regularan todos sus asuntos hablando y persuadiéndose entre sí.¹⁹ Cuando la libertad es condición inamovible de la *polis*, la política cobra su sentido primordial. El animal político no surge así como así, esto solo sucede en los supuestos de libertad e igualdad, ambos dan la posibilidad de palabra y persuasión en la convivencia en el ágora.

La misión y el fin de la política es asegurar la vida en el sentido más amplio. Es ella quien hace posible al individuo perseguir en paz y tranquilidad sus fines no importunándole.²⁰ Más la política así entendida puede actuar dentro de un abanico de posibilidades muy amplio,

¹⁹ Hannah Arendt, *La Promesa de La Política* (Ciudad de México: Paidós, 2005), 120, 151–54.

²⁰ Arendt, 151.

en el cual podemos presenciar un comportamiento amable y de cuidado por todos los individuos o bien, la imposición bajo el uso de la fuerza del gobierno justificándose en asegurar la vida para unos cuantos. Para que la política cobre un sentido eficaz y óptimo la relación con y entre los individuos ha de ser distinta, sobre todo habrá de delimitar conceptos e ideas aplicables en la sociedad que lleven al funcionamiento del cuidado de los intereses personales y el bienestar del pueblo. Para ello, más que solo hablar del sentido y fin de la política habremos de hablar de democracia, sociedad en la cual no solo es permitido, sino exigido, el ser persona.²¹

1.4 Persona, Privacidad y Democracia

Para Zambrano y para los fines de este trabajo, el término persona hace referencia a la condición ya conocida en tal sociedad política que ya hemos mencionado, el individuo. Más para que éste tome el carácter propio de la vida democrática y no solo como un individuo insertado en la masa política, ha de estar dotado de conciencia. Cabe decir por tanto, que la persona es algo más que el individuo: «es el individuo dotado de conciencia, que se sabe a sí mismo y que se entiende a sí mismo como valor supremo, como última finalidad terrestre (...) como futuro a descubrir».²² A partir de ésta concepción de persona la democracia tiene sentido, no desde la de individuo en la que la política solo centra sus esfuerzos en el cuidado de la vida, en la democracia a parte de éste se observan muchos más. En otras palabras, esta condición de persona nos abre nuevas posibilidades a diversos cuidados, a diversos derechos. Derechos que no tienen relevancia necesaria en la vida de la polis, sino que cobran sentido en la vida propia de la persona. Uno de ellos y que aquí nos interesa, es el derecho a la

²¹ María Zambrano, *Persona y Democracia* (España: Alianza, 2019), 183.

²² Zambrano, 143.

privacidad, que como hemos visto, su relevancia en la antigüedad era casi nula, sin embargo, bajo los presupuestos de la democracia cobra valor y sobre todo es base fundamental para su desarrollo casi o igual que el presupuesto de persona. Empecemos pues, por entender la relación existente entre el ser persona y privacidad.

La persona se encuentra en la historia, la cual no se fundamenta en el origen, en la causalidad. La historia no es un asunto lógico. Es ella misma sistema, según lo muestra Ortega y Gasset. Tal sistema se constituye en la forma de una razón narrativa, donde hay visión y descubrimiento.²³ La persona es la última finalidad terrestre que se descubre en el futuro. La conciencia de sí aparece en la *polis*, aquí donde se hace cuestión del hombre, pues en ella la dimensión propiamente humana estaba en juego. Este mismo descubrimiento de la conciencia en la historia acarrea en sí el quehacer político – el cambio de actitud que Sócrates sugiere a cada uno de los que a él se acercan –, el ejercicio de su ciudadanía. Es en la *polis* donde por vez primera el hombre trataba con el hombre como tal, la convivencia se establecía en virtud de la simple condición humana. Esta condición da libertad e igualdad desde la conciencia.²⁴ De tal manera podemos decir que, en el recorrido del individuo en la historia, su máximo es ser persona como protagonista. Aunado a los conceptos de persona, igualdad y libertad como ejercicio de la propia conciencia, se encuentra una salida a la vida propia del hombre. Al hombre se le concede una especie de vacación para darse a conocer: una salida por donde asomarse a tener un nombre, un tiempo para buscarse, y una pausa para reconocerse y reconocer, para identificarse. Ortega señala la diferencia entre el hombre y el animal en la condición que el hombre tiene de ensimismarse, de entrar en su lugar propio, dónde retirarse de la atención al contorno. Es un detener este «tener que estar viviendo» para

²³ Zambrano, 143.

²⁴ Zambrano, 154–55.

entrar en sí, en ese lugar donde su soledad le aguarda, en donde vive de otro modo.²⁵ Ser hombre es ser persona, y ser persona es soledad. Una soledad dentro de la convivencia. Y allá en ese fondo de la soledad en que vive cada hombre se mira y se ve; luego se piensa. El lugar del individuo es la sociedad, pero el lugar de la persona es un íntimo espacio, y en el reside un absoluto: soledad y libertad. Y es en la soledad donde nace la elección y la responsabilidad de la elección.²⁶ Este adentro nos colma la conciencia en la historia dado su fundamento para el desarrollo de la libertad y el discurrir, propios de lo humano. Por ahora podemos decir que este adentro nos condiciona personas y nos dirige hacer vida.

Frente a esta concepción podemos adoptar como principio la sentencia del Apolo delfico: «conócete a ti mismo». Del cual Sócrates concluyó: «Es mejor estar en desacuerdo con el mundo entero, que siendo uno solo, estar en desacuerdo conmigo mismo».²⁷ Al final solo mediante el conocimiento de lo que me parece a mí, puedo de algún modo entender la verdad, es decir a través de la *doxa*; la verdad de la propia opinión se ha de revelar a uno mismo y a los demás. Sin embargo, esta verdad es limitada en su equivocidad y por lo tanto el acceso a la verdad por parte de los hombres también lo es. Pero esto no quiere decir que no pertenezca a la verdad, lo es en su adhesión invariable. El no contradecirse a sí mismo es el criterio por el cual el hombre puede comunicar verazmente su *doxa*. Esta no contradicción nace del diálogo que surge entre el pensamiento y uno mismo y es el imperativo de todo proceso dialéctico griego. Se es un «*dos-en-uno*»²⁸ cuando se piensa; o como dice Aristóteles: «*otro sí mismo*».²⁹ Esto quiere decir que la facultad de discurso con los otros y el hecho de

²⁵ Zambrano, 163–64.

²⁶ Zambrano, 171–72.

²⁷ Platón, *Diálogos II. Gorgias, Menéxeno, Eutidemo, Menón, Crátilo*, Td. Calonge, *Biblioteca Clásica Gredos* (Madrid: Editorial Gredos, 1987), 482 c.

²⁸ Arendt, *La Promesa de La Política*, 57.

²⁹ Aristóteles, *Ética Nicomáquea Ética Eudemia* (Madrid: Gredos, 1985), 1166 a 10–15.

la pluralidad humana intrínseca, en tanto su diferencia y equivocidad, se corresponden el uno con la otra, puesto que al hablar conmigo mismo, vivo junto a mí mismo. Por tal motivo, el principio de no contradicción surge como regla fundamental del pensamiento. La posibilidad de contradecirse a sí mismo existe, – pues se es dos-en-uno – y siendo así, se huye de la contradicción por el miedo a la división. Es esta pluralidad inherente que acompaña permanentemente a todo ser humano en el diálogo entre los dos del dos-en-uno. Ahora bien, la compañía genera que el diálogo interno se detenga y arroja al ser humano al examen del diálogo con los demás. El uno mismo que sabe estar consigo mismo, podrá saber estar con el otro. Pero para que ello suceda, es decir, aparecer en el espacio público-político, es imprescindible que predomine la realidad de persona con conciencia pensante de lo que se es y sus capacidades. Esa es la relevancia política en el pensamiento de Sócrates: la condición necesaria para el buen funcionamiento de la *polis* es la soledad – el espacio privado de diálogo consigo mismo – el cual da mayor garantía que las reglas de comportamiento forzadas por las leyes y el miedo al castigo.³⁰

Por otro lado, visto desde una perspectiva psicológica y antropológica, existen cualidades inherentes al hombre que deben ser satisfechas. La cualidad más importante es la tendencia a crecer y a realizar las potencialidades que el hombre ha desarrollado en el curso de la historia, por ejemplo, el pensamiento creador y crítico, la facultad de tener experiencias emocionales y sensibles diferenciadas. Esta tendencia al crecimiento origina impulsos específicos, como el deseo de libertad y el odio a la opresión, dado que la libertad constituye la condición fundamental de todo crecimiento. Análogamente, el deseo de la libertad puede ser reprimido y desaparecido así de la conciencia del individuo, pero no por ello dejará de

³⁰ Arendt, *La Promesa de La Política*.

existir como potencialidad, revelando su existencia por medio de aquel odio consciente o inconsciente que siempre acompaña a tal represión.³¹

El origen de la libertad positiva consiste en la actividad espontánea de la personalidad total integrada, es decir el ejercicio de la propia y libre voluntad en una aceptación total de la personalidad sin reprimir partes esenciales del yo.³² Ésta se encuentra en el deseo que proviene de ese íntimo espacio que surge a través de la conciencia de persona dentro de la historia. Este íntimo espacio se equipara al concepto de soledad, en tanto se reconocen sus cualidades de utilidad en la convivencia. No es, por tanto, una soledad asocial o ahistórica, es en cambio el espacio donde reside la cualidad de decisión, en otras palabras la cualidad de voluntad. Dado que esto cobra mayor relevancia en la relación que se tiene con los otros en la toma de decisiones y la responsabilidad que esto conlleva, hemos de dirigir nuestra mirada al sistema político que permite y da mayor potencialidad para el desarrollo de dichas cualidades humanas; nos referimos al sistema del régimen liberal democrático.

La democracia se refiere a un sistema de gobierno en el que el soberano es el pueblo, aspira a que los iguales sociales se gobiernen a sí mismos y logren un orden social realmente justo, sin dictadores ni gobernantes autocráticos.³³ Sabemos que actualmente nuestras democracias están fracturadas y en crisis, también hemos comprobado que tal vez no es el mejor sistema de gobierno que quisiéramos, sobre todo por la desconfianza generalizada en los servidores públicos cuando se dan casos de corrupción o malversación de los recursos públicos, o cuando no nos sentimos representados en las elecciones de nuestra localidad. Existe – por si fuera poco – actualmente, entre la clase política de las grandes potencias

³¹ Erich Fromm, *El Miedo a La Libertad*, 6a ed. (México: Paidós, 2012), 291.

³² Fromm, *El Miedo a La Libertad*.

³³ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 82.

mundiales cierta tendencia a la equivalencia moral entre la democracia y la autocracia, ejemplo de esto fue lo expresado por Donald Trump en una entrevista con Joe Scarborough en 2015: «Él gobierna su país y al menos es un líder – declaraba hablando de Putin – a diferencia de lo que tenemos en este país... Creo que nuestro país también comete muchos asesinatos».³⁴ Esto refleja un asentimiento con la política autocrática de Rusia y se da permisividad para actuar en conformidad con esta nación, es un “De acuerdo, Rusia es corrupta, pero todos los demás también lo son”. Este argumento socava la convicción, la esperanza y la creencia de que los estadounidenses – o cualquiera – puede estar a la altura de lo que dice su Constitución. Esta creencia de que en el fondo la democracia no es distinta de la autocracia es un argumento familiar utilizado por los autocráticos. Ya en 1986, Jeane Kirkpatrick – académica, intelectual y embajadora de Reagan en la ONU – escribió sobre el peligro que entrañaba tanto para los Estados Unidos, como para sus aliados la retórica de la equivalencia moral que en aquel momento provenía de la Unión Soviética: «Para destruir una sociedad, primero hay que deslegitimar sus instituciones fundamentales».³⁵ Si uno cree que las instituciones de un país no son diferentes de sus opuestos, entonces no hay razón alguna para defenderlas.³⁶

La democracia es en definitiva asechada por todo aquel con aluviones fascistoides o autoritarios. En un reportaje de la unidad de inteligencia del The Economist se describió 2019 como «un año de retrocesos democráticos», con la puntuación media mundial de la democracia en su punto más bajo desde 2006, cuando se elaboró por primera vez el Índice

³⁴ Donald J. Trump, entrevista con Joe Scarborough, Morning Joe, MSNBC, 18 de diciembre de 2015. <https://www.washingtonpost.com/news/the-fix/wp/2015/12/18/donald-trump-gladto-beendorsed-by-russias-top-journalist-murderer%3E/>

³⁵ Jeane Kirkpatrick, «The Myth of Moral Equivalence», Imprimis, enero de 1986.

³⁶ Anne Applebaum, *El Ocaso de La Democracia* (México: Penguin Random House, 2021), 150–52.

de Democracia.³⁷ Sin embargo, y a pesar de todo esto, la democracia sigue siendo el sistema que más se adecúa a proteger los derechos fundamentales de todos.³⁸ Las democracias – dice Karl Popper – son la mejor manera de deshacerse de los malos gobiernos sin derramamiento de sangre, y de aplicar las reformas sin violencia.³⁹ Orwell sostenía que el mejor activo de la democracia es «la sensación comparativa de seguridad» de la que pueden disfrutar sus ciudadanos. Estar seguro de que nadie te castigará si no has infringido la ley, y saber que "la ley está por encima del Estado".⁴⁰ Por otro lado, Zambrano reconoce en la democracia un síntoma de enfermedad en ella misma, pues sucede como si ésta fuera en contra de sí misma. Esto sucede cuando entre minorías se encargan de dirigir a la masa, una masa que hace invisible al pueblo, donde habitan personas. Tal síntoma es la situación negativa de la democracia misma:

...el momento en que la democracia aparece negándose a sí misma y sin embargo... extrañadamente, es democracia. Sin embargo, esto no viene a ser otra cosa más que su propia afirmación. Se afirma en su propia negación. En su deformación, su tergiversación, en su caricatura y en su andar a tientas. Esta negación aparente hace pensar su fracaso e imposibilidad, pero es solo que se confunde en la afirmación.⁴¹

La democracia dota a la persona de libertad para el desarrollo de sus capacidades, bajo los presupuestos de la protección y el cuidado del poder de ejercer su capacidad de elección. A partir de este fundamento la democracia se vuelve necesaria para el desarrollo de nuestras capacidades humanas. Sin embargo, para que esta protección se vuelva efectiva son necesarios los esfuerzos del liberalismo para que el cumplimiento de los derechos de todos

³⁷ The Economist Intelligence Unit, "Democracy Index 2019. A Year of Democratic Seatbacks and Popular Protest" (London, 2019).

³⁸ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 83.

³⁹ Karl R. Popper, *The Open Society and Its Enemies: The Spell of Plato*, 4th ed., vol. I (London: Routledge & Kegan Paul, 1962), <https://doi.org/10.5840/thought1952272108>.

⁴⁰ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 84.

⁴¹ Zambrano, *Persona y Democracia*, 212–13.

esté garantizado. Si la democracia no es liberal se puede caer en lo que John Stuart Mill llama «la tiranía de la mayoría». Esto quiere decir que una mayoría puede llegar a ser tan opresiva con una minoría como un autócrata. De esta forma el liberalismo busca siempre y esforzadamente permitir la mayor libertad a los ciudadanos a la vez que garantiza el respeto de los derechos de todos.⁴² El liberalismo impone sólo los límites necesarios para que cada ciudadano persiga su ideal de buena vida sin interferir con los demás. En conclusión, las democracias liberales nos permiten autogobernarnos, como individuos y como sociedades.⁴³

En tal equilibrio entre derechos y libertad que promueve el liberalismo, se corre el riesgo de caer en la tentación de dejar que los reclamos que vienen de la entraña – al no estar cubiertas las necesidades primordiales y básicas – adquieran un papel fundamental en la toma de decisiones para la elección de uno o varios representantes que prometan la solución de tales problemas o el final para los llamados “opresores”. De tal suerte que puede suceder un desequilibrio que cobra valor para algunos, pero somete a otros. La democracia se ve en caída y los regímenes fascistas pueden tomar su lugar, tal como sucedió con el nazismo o el chavismo. El descuido del liberalismo trae en consecuencia la destrucción de la democracia. Para entender cómo funciona esa destrucción de la democracia el filósofo británico Jonathan Wolff ha argumentado que el primer paso de la destrucción fascista de la democracia es priorizar la voluntad de la mayoría sobre los derechos de las minorías. El segundo paso es cuestionar e impugnar los medios a través de los cuales la voluntad de la mayoría se expresa, socavando de esta manera el voto.⁴⁴ Ese fue el camino trazado por Hitler, ir destruyendo los medios de poder de las personas mediante un cuestionamiento de su efectividad e incluso

⁴² John Stuart Mill, *Sobre La Libertad* (Madrid: Alianza, 1993).

⁴³ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 84–85.

⁴⁴ Jonathan Wolff, “The Lure of Fascism,” *Aeon*, 2020, <https://doi.org/10.4324/9780203007259-32>.

burlándose de ellos, como lo hizo en el discurso que dio para los industriales de Dusseldorf en 1932:

Por lo tanto, es natural que cuando las inteligencias capaces de una nación, que son siempre minoritarias, son consideradas sólo como del mismo valor que todas las demás, entonces el genio, la capacidad, el valor de la personalidad son lentamente sometidos a la mayoría y este proceso es entonces falsamente llamado el gobierno del pueblo. Porque esto no es el gobierno del pueblo, sino en realidad el gobierno de la estupidez, de la mediocridad, de la tibieza, de la cobardía, de la debilidad y de la insuficiencia (...) Así, la democracia conduce en la práctica a la destrucción de los verdaderos valores de un pueblo. Y esto también sirve para explicar cómo es que los pueblos con un gran pasado desde el momento en que se entregan al dominio ilimitado y democrático de las masas (...). Y así, en estas condiciones, un pueblo perderá gradualmente su importancia no sólo en las esferas cultural y económica, sino en su totalidad; en un tiempo comparativamente corto ya no mantendrá su antiguo valor en el marco de los demás pueblos del mundo.⁴⁵

De esta manera se puede decir que la democracia liberal limita el gobierno de la mayoría para garantizar la protección de los derechos de la minoría. En ella se atiende a sus instituciones encargadas de salvaguardar a los ciudadanos del poder del gobernante. Proteger y enriquecer a las instituciones de las democracias liberales es una protección para el pueblo de los abusos de poder.⁴⁶ El proceso para alcanzar una sociedad democrática liberal donde se protejan a las minorías y se limite el poder, luce a veces lejano de la realidad. Se podrá decir que nunca se vivirá fielmente en una sociedad con un establecimiento tal que proteja los derechos para todos y que no dé espacio para que la mayoría gobierne sobre la minoría. Sin embargo, olvidar los objetivos que como sociedad democrática liberal hemos de resguardar, nos encamina a otro tipo de gobierno que no es democrático.

⁴⁵ Adolf Hitler, "Adolf Hitler Speech of January 27, 1932," 2022.

⁴⁶ Wolff, "The Lure of Fascism."

Frente a este sistema de gobierno la política emerge de la pluralidad de cada persona y es en el espacio público donde cada uno se encuentra entre nosotros y puede experimentar libertad. «Si ese espacio entre nosotros se derrumba, y si la política se convierte sólo en un medio para conseguir un fin (sea cual sea el fin que se pretenda), entonces no estamos lejos del totalitarismo».⁴⁷ Y ante esto, Hannah Arendt nos invita a desvincularnos de la ilusión de que la forma más eficaz de hacer que la sociedad sea buena es hacer que cada uno de sus miembros sea una persona buena.⁴⁸

En resumen, podemos decir que si ser persona es ser soledad, – dos-en-uno – es decir, es tener un adentro dentro de la convivencia, y es en este yo-conmigo-mismo donde nace la elección y de ahí más delante la responsabilidad de lo elegido en la historia, tal parece que el ambiente donde se da la posibilidad de desarrollar tales capacidades inherentes al ser persona es en una democracia liberal «el régimen de la unidad en la multiplicidad, del reconocimiento, por tanto, de todas las diversidades, de todas las diferencias de situación».⁴⁹ Es aquí donde el *adentro* de la persona así pensado por Ortega y después por Zambrano necesita de un vestido que lo cubra, de una protección que resguarde la realidad imprescindible de la pluralidad humana inserta en cada ser humano de donde surge el diálogo y la ética. Tal protección es la privacidad, aquella pensada por Véliz como la llave que puede abrir los aspectos más íntimos, aquellos que configuran a la persona y la hacen ser lo que es, pero que a la vez protege de las presiones de otras personas y de los abusos de poder. Es ese espacio personal, – dice Clarke – libre de interferencias de otras personas y organizaciones.

⁴⁷ Luciano Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, ed. Luciano Floridi (Oxford, UK: Springer Open, 2015), https://doi.org/10.1007/978-3-319-04093-6_21.

⁴⁸ Hannah Arendt, *Entre El Pasado y El Futuro. Ocho Ejercicios Sobre La Reflexión Política* (Barcelona: Península, 1996).

⁴⁹ Zambrano, *Persona y Democracia*, 221.

Tal protección se llevará a cabo a partir de su fundamento en el derecho a la privacidad, del cual poco se habla o se ignora su relevancia, pero guarda una fuerte relación para la efectiva realización del Estado de Derecho.

1.5 Antecedentes de la Privacidad como Derecho

Para hablar del derecho a la privacidad primero habremos de hablar acerca del proceso histórico y político de los derechos, y en particular del que nos compete aquí, pues visto de este modo podremos ampliar nuestra perspectiva acerca de la realidad actual en vistas a conocer el fundamento, que como sociedad nos será útil para futuros avances en tales derechos. Ciertamente es que el valor de la privacidad ha ido cambiando, este camino se hace evidente en la poca relevancia que tenía en la antigüedad y que en nuestros tiempos más cercanos sus implicaciones directas en el buen funcionamiento de una sociedad democrática hayan tomado un papel fundamental en la realización y desarrollo propios de cada ser humano. De la misma forma, el camino en la formulación de la privacidad como un derecho fundamental humano ha atravesado distintos momentos que lo han ido formando a través de etapas históricas, políticas, sociales y tecnológicas. La primera vez que apareció un registro de la defensa de la privacidad en términos legales fue en 1890 en el *Harvard Law Review* en el artículo “The Right to Privacy” de los juristas Samuel Warren y Louis Brandeis. Ellos defendían el derecho a no ser molestado o ser dejado en paz (*the right to be alone*), en él se lee lo siguiente:

Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y para garantizar al individuo lo que el juez Cooley denomina *el derecho a no ser molestado*. Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer

realidad la profecía que reza: «lo que susurre en la intimidad, será proclamado a los cuatro vientos».⁵⁰

En él también reconocen el carácter contingente del *common law*:

El *common law* [sic] en su *eterna juventud*,^{III} evoluciona para dar cabida a las demandas de la sociedad (...) hoy en día, el derecho a la vida significa el derecho a disfrutar de la vida, el derecho a no ser molestado; el derecho a ser libre garantiza el ejercicio de un amplio haz de derechos subjetivos; y el término «propiedad» abarca, en su significado actual, todo tipo de derechos de dominio, tanto tangibles como intangibles.⁵¹

Para Warren y Brandeis es justo que el individuo tenga el control sobre la información propia, y particularmente sobre las fotografías instantáneas, el invento reciente del momento. El reclamo ahí expuesto se esfuerza por reivindicar la propiedad privada en tanto control y acceso único por parte de quien lo posee. Y es así como la privacidad es vista en un primer momento, como parte de la propiedad y bajo el control y escrutinio propios. Sin embargo, aunque en la legalidad y en los social el término de privacidad había sido poco explorado, este artículo fue el antecedente para futuros debates y análisis que contribuyeron a una mejora en su formación. A partir de este precedente, la privacidad fue entendida como un derecho a la no injerencia de terceros en la vida privada o íntima, a menos que existiera un consentimiento para que ello sucediera.

Esto llega a vislumbrar lo dicho por Mill respecto a la libertad individual; su objetivo era «trazar los límites del control social, tal control solo puede ser justificado para prevenir el daño a otros, y asegurarle así plena independencia en lo que respecta a su propio cuerpo y mente».⁵² Aunque Mill nunca menciona privacidad o vida privada en su texto sobre la libertad, sí habla de «*la esfera de la conducta*» del individuo en la que la sociedad no guarda

⁵⁰ Samuel Warren and Louis Brandeis, *El Derecho a La Intimidad*, ed. Benigno Pendás and Pilar Baselga, 1ª ed. (Madrid: Civitas, 1995), 25.

⁵¹ Warren and Brandeis, 21–22.

⁵² Mill, *Sobre La Libertad*, 65.

ningún interés y en el que no debería entrometerse, pues abarca «*esa parte de la vida de una persona que le afecta solo a ella*». A esta misma imagen la define como «*la región apropiada de la libertad humana*»,⁵³ dentro de la que puede perseguir sin interferencias su concepción de vida buena, es decir el ideal de autonomía individual y el libre desarrollo de la personalidad.⁵⁴ Por otro lado existe una postura diferente respecto a la privacidad, entendida no solo como el control sobre la información o libertad frente al Estado^{IV} sino como defensa de la propia dignidad humana. Podríamos decir de hecho, que así fue su evolución gradual e histórica, lo cual se explica a continuación.

1.5.1 Kant y Locke en Privacidad

El pensamiento liberal de base lockeana influyó fuertemente en la resolución de las declaraciones de derechos posrevolucionarias burguesas de Occidente como defensa a las libertades individuales dada la idea de que la libertad individual constituye por naturaleza la esencia de todo ser humano.⁵⁵ Sin embargo, la postura kantiana abre la posibilidad de pensar la fundamentación de la esencialidad humana desde otro lugar. Para Kant,

todo hombre tiene legítimo derecho al respeto de sus semejantes y también él está obligado a lo mismo, recíprocamente, con respecto a cada uno de ellos, puesto que la humanidad misma es una dignidad; porque el hombre no puede ser utilizado como medio por ningún hombre (ni por otros, ni siquiera por sí mismo), sino siempre como fin, y en esto reside precisamente su dignidad (la personalidad), en virtud de la cual se eleva sobre todos los demás seres del mundo que no son hombres y sí pueden utilizarse propiedad.⁵⁶

⁵³ Mill, 68. El énfasis en itálicas es nuestro.

⁵⁴ Toscano, “Sobre El Concepto de Privacidad: La Relación Entre Privacidad e Intimidad,” 537.

⁵⁵ John Locke, *Segundo Tratado Sobre El Gobierno Civil* (Madrid: Alianza, 2004).

⁵⁶ Immanuel Kant, *La Metafísica de Las Costumbres*, 4ta. (Madrid: Tecnos, 2008), 335.

Esta dignidad no proviene de la naturaleza humana, sino por el ejercicio práctico de la razón. Para Locke el objetivo del derecho es asegurar el desarrollo libre de cada individuo. Para Kant este desarrollo habría de cumplir las condiciones que racionalmente requería la categoría de ser humano, tales condiciones exigían el compromiso de todos en la concepción del concepto que lo cambió todo: dignidad humana. Las aspiraciones de Kant van más allá que las de Locke, al tener la mira puesta en el desarrollo de un mundo cosmopolita en paz. Locke es filósofo de la subjetividad. Kant en cambio, de la intersubjetividad.⁵⁷

1.5.2 Derechos de la Personalidad y el valor social de la Privacidad

Para Pérez Luño el principio legitimador de los denominados «*derechos de la personalidad*» es el de la dignidad del hombre, la cual implica la dimensión moral de la personalidad, que tiene por fundamento la propia libertad y autonomía de la persona, entre ellos están el derecho al honor, a la propia imagen y a la intimidad personal y familiar.⁵⁸ La jurisprudencia de algunos estados europeos tomó en cuenta estos derechos, tal como el derecho a la privacidad que fue tenido en cuenta como derecho a la dignidad y no asociado a la propiedad personal, como lo fue y lo ha sido tomado por parte de la jurisprudencia estadounidense.⁵⁹

A partir de la obra del jurista e historiador Carl Friedrich von Savigny se ve la influencia kantiana en la escuela del derecho. Él rezaba a favor del derecho positivo autónomo basado en la determinación de cada pueblo, es decir, su propuesta se alejaba de los

⁵⁷ Alberto Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento” (Tesis Doctoral, Universidad Complutense de Madrid, 2015), 415–17, <https://doi.org/10.14201/14771>.

⁵⁸ Antonio Enrique Pérez Luño et al., *Historia de Los Derechos Fundamentales Tomo II: Siglo XVIII. Vol. II: La Filosofía de Los Derechos Humanos*. (Madrid: Dykinson, 2001).

⁵⁹ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento,” 418.

derechos innatos por considerarlos inexistentes. Desde este momento se distinguieron los derechos patrimoniales y los derechos de la personalidad. La protección de estos últimos va más allá del control que uno pudiera ejercer sobre los propios actos y posesiones.⁶⁰ El derecho a la privacidad, que está dentro de los derechos de la personalidad, forma parte de un conjunto de predisposiciones que velan por la dignidad humana. Bajo esta perspectiva la responsabilidad del cuidado de la privacidad nos compete a todos y no solo a quién sea propietario de cierta información. Esto quiere decir que la privacidad es colectiva en tanto que su pérdida nos afecta a todos. La pérdida de privacidad sin justificación ética o legal – incluso frente a ciertos casos en los que la legalidad la avala – es en última instancia perder dignidad y perder dignidad nos aleja de la colectividad humana; aquella que nos permite el reconocimiento de nuestros derechos humanos y nos da autonomía y libertad.

Por tanto, pensar que la privacidad solo es ejercer el control sobre la propiedad y sus formas de uso es equivocada. Si bien es cierto que al ejercer la privacidad se ejerce el control sobre lo propio, es también cierto que se ejerce un derecho colectivo. En otras palabras, si el interés primordial es velar por el cumplimiento y respeto por el derecho a la privacidad de todos, el control por lo propio vendrá por añadidura y no al revés. Esta diferencia de perspectivas de la privacidad tiene sus influencias en las jurisprudencias europea y estadounidense, tanto que el papel de víctima tiene una marcada diferencia y es contraria. Alberto Sánchez nos lo explica a continuación:

En el caso europeo, primando la defensa de la dignidad humana, culparían a aquél que hiciese público aquello que nunca debió publicarse; por el contrario, en el caso americano, haciendo un énfasis mucho mayor en la defensa de la libertad de cada individuo, me culparían a mí, que debía haber tenido más cuidado si no quería que mi

⁶⁰ Pérez Luño et al., *Historia de Los Derechos Fundamentales Tomo II: Siglo XVIII. Vol. II: La Filosofía de Los Derechos Humanos*.

secreto fuese públicamente conocido. Así pues, podemos afirmar que, mientras que el concepto de privacidad americano posee un carácter meramente individual –siendo responsabilidad de cada uno prestar atención a aquello que expone en público–, en Europa, por el contrario, ha adquirido un carácter más social –donde no sólo es cada individuo, sino que somos todos en conjunto quienes debemos velar por el cumplimiento generalizado de determinada noción de dignidad–.⁶¹

En adición, podemos ver que desde la perspectiva de Dewey el valor de la protección de los derechos individuales surge de su contribución a la sociedad. Los derechos individuales son protecciones de la sociedad frente a su propio *intrusismo*. La sociedad deja espacio para el individuo debido a los beneficios sociales que este espacio proporciona. Por lo tanto, Dewey sostiene que los derechos deben valorarse en función de «la contribución que hacen al bienestar de la comunidad».⁶² De lo contrario, en cualquier tipo de cálculo utilitario, los derechos individuales no serían lo suficientemente valiosos como para superar la mayoría de los intereses sociales, y sería imposible justificar los derechos individuales. Por ello, Dewey argumentó que debemos insistir en una «base y una justificación sociales» para las libertades civiles. Tanto para Daniel Solove como para Dewey, el valor de la protección del individuo es social, pues parte de lo que hace que una sociedad sea un buen lugar en el que vivir es la medida en la que permite a las personas liberarse del intrusismo de los demás. Una sociedad sin protección de la privacidad sería asfixiante, y no sería un lugar en el que la mayoría querría vivir.⁶³ De la misma manera Robert Post ha argumentado que la privacidad no es simplemente un conjunto de restricciones a las reglas y normas de la

⁶¹ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento,” 419.

⁶² John Dewey, *Liberalism and Social Action* (New York: G.P. Putnam’s Sons, 1935).

⁶³ Daniel J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *The Individual and Privacy: Volume I*, 2016, 745–72, <https://digital.sandiego.edu/cgi/viewcontent.cgi?article=2790&context=sdlr>.

sociedad. Por el contrario, la intimidación constituye un intento de la sociedad de promover reglas de comportamiento, decoro y civismo.⁶⁴

La sociedad protege la intimidad como medio para imponer un tipo de orden en la comunidad. La privacidad, por tanto, no es la defensa del individuo contra los intereses de la sociedad, sino la protección del individuo basada en las propias normas y valores de la sociedad. La privacidad no es simplemente una forma de liberar a los individuos del control social, ya que ella misma es una forma de control social que surge de las normas de una sociedad. No es una restricción externa a la sociedad, sino que es, de hecho, una dimensión interna de la sociedad. Por lo tanto, la privacidad tiene un valor social. Incluso cuando protege al individuo, lo hace por el bien de la sociedad.⁶⁵ De esta manera, la privacidad por la que se ha de velar es aquella que tenga como prioridad el cuidado colectivo de lo privado – como lo son los datos personales – alentando a la ciudadanía a crear redes que la protejan. Por tal motivo, es fundamental pensar en el contenido que protege la privacidad, lo cual, entre otras cosas, se convierte en el móvil de tal protección.

Pensemos por un momento en aquello que cada persona reserva en su privacidad. Podría ser una conversación, cartas, fotografías, su sexualidad, su cuenta bancaria, sus enfermedades, contraseñas, sus próximos proyectos o inclusive un tipo de producto que le gusta usar pero no le gustaría que alguien más se entere. Nuestra privacidad en definitiva es muy amplia dada la diversidad de estratos de la vida en las que puede estar y por tanto, – como algunos lo piensan^V – indefinible. Sin embargo, existe algo que una todas estas actividades u objetos humanos reduciendo su amplitud y buscando que su accesibilidad sea

⁶⁴ Robert C. Post, “The Social Foundations of Privacy: Community and Self in the Common Law Tort,” *California Law Review* 77, no. 5 (1989): 957–1010, <https://doi.org/10.4159/9780674276994-004>.

⁶⁵ Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.”

efectiva. En nuestros días – de tecnología algorítmica, inteligencia artificial e Internet de las cosas –, y desde hace tiempo, hay “algo” que es entendido como dato, cuyo significado proviene de la raíz latina «*datum*», es decir, «lo que se da», y se refiere a «la información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho».⁶⁶ En otras palabras, el dato es el extracto expedito de información de nuestras actividades u objetos creados o no. Esto quiere decir que tanto las conversaciones, cartas, fotografías, sexualidad, cuentas bancarias, enfermedades y contraseñas, entre otras cosas, guardan en sí mismas información. Todas estas actividades o formas de ser en el mundo de cada ser humano pueden ser traducidas a datos.⁶⁷ Esto es, información y registro acerca de casi toda nuestra persona.⁶⁸ En definitiva, la fuente de información que da a conocer la vida de las personas está en los datos y por lo tanto, necesitan protección. Hemos de comprender con claridad que la protección de la privacidad tiene su sentido en la protección del contenido de ésta, pues es al final lo que reclama protección.

Este descubrimiento de conocimiento mediante información y registros de datos es de uso reciente, pues fue a través de las tecnologías de la información que su uso se masificó. Por tanto, el derecho – en su permanente cambio – que es continuamente exigido conforme a su tiempo, ha buscado las formas de protección adecuadas para la privacidad desde la realidad del uso de datos, como lo veremos más adelante. Por ahora parece necesario rescatar ciertas características de los derechos que nos ayudarán a tener una mejor comprensión del derecho a la privacidad en su versión más reciente.

⁶⁶ Real Academia Española, “Diccionario de La Lengua Española,” 23, [versión 23.5 en línea], 2022, <https://dle.rae.es>.

⁶⁷ Byung-Chul Han, *No-Cosas* (Ciudad de México: Penguin Random House, 2021).

⁶⁸ Han.

1.6 Características de los Derechos Humanos y su relevancia en el Derecho a la Privacidad

Las características principales de los derechos humanos las podemos resumir en dos: su universalidad y su indivisibilidad-interdependencia. La primera de ellas quiere decir que pertenecen a todos y cada uno de los miembros de la comunidad humana. La segunda condición nos habla de su cualidad de indivisibilidad, por lo que cada uno de los derechos considerados humanos forman una unidad. De la misma forma su interdependencia dado que en la práctica el disfrute de unos derechos depende de la previa satisfacción de otros⁶⁹, como bien lo señalan Warren y Brandeis al hablar acerca del derecho fundamental a la vida y sus implicaciones actuales durante ese momento; en este caso las implicaciones de no ser molestado tienen relación con los derechos a la libertad de pensamiento y expresión, de la misma forma que con las demás libertades individuales. Y es así, que ahora el derecho a la privacidad permite otros derechos como el de libre expresión o libertad de interferencias.

Hemos de señalar la habitual confusión que existe entre la privacidad y el derecho a la privacidad con otros conceptos de las capacidades humanas, y estas a su vez hacen ver a los derechos fundamentales sin limitaciones entre sí. Concretamente esto sucede al pensar que el derecho a la privacidad se pierde entre los conceptos de libertad, no injerencia, soledad, intimidad o control, por tal motivo es necesario recordar la intersubjetividad-interdependencia y universalidad que existe entre los derechos. Es decir, ni el derecho a la libertad, a la no injerencia, a la intimidad y al control, se confunden al estar al lado del derecho a la privacidad, sino que nos ayudan a entender tal derecho en diferentes momentos históricos y facetas de cada persona. Ni siquiera pensar en la soledad como posibilitadora de

⁶⁹ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento.”

la privacidad reduce el amplio espectro que ésta abarca. En otras palabras, estos conceptos en la realidad práctica son posibilitadores del derecho a la privacidad, más nunca suplen tal derecho ni mucho menos lo confunden.⁷⁰ Pasemos ahora a realizar una breve revisión del derecho a la privacidad en las declaraciones de los derechos humanos de reciente elaboración y así conocer la realidad del derecho en este ámbito.

1.7 El Derecho a la Privacidad en la Declaraciones de Derechos Humanos

La relevancia del derecho a la privacidad cobra sentido dadas las consecuencias de su violación. Sin privacidad se pierde la libertad, la autonomía y sobre todo la dignidad. Por tal motivo la vida democrática de nuestro tiempo no debe prescindir de él. Tal ideal se ve reflejado después de los acontecimientos tan desastrosos para la humanidad en la Segunda Guerra Mundial – como lo fue el Holocausto Judío en el cual la pérdida de la privacidad fue clave para su ejecución.^{VI} El valor de este derecho está instaurado en el primer antecedente histórico de su protección en el artículo 12 de la Declaración de los Derechos Humanos adoptada y proclamada por la Asamblea General de la Organización de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948, que expone lo siguiente: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.»⁷¹

⁷⁰ Cfr. Tavani, H. (2007). Philosophical Theories of Privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1–22. <http://www.jstor.org/stable/24439672>

⁷¹ Asamblea General de las ONU, “Declaración Universal de Derechos Humanos,” 1948, <https://doi.org/10.1017/S0031819117000274>.

Después en 1978, en el artículo 11 del llamado Pacto de San José⁷², dedicado a la Protección de la Honra y de la Dignidad, se declara lo siguiente:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.⁷³

Estas declaraciones de una relativa reciente ejecución nos han guiado en el camino para diversas normativas y jurisprudencias nacionales, correspondientes a territorios bien establecidos que gozan de soberanía y que a través de sumarse a estos organismos se comprometen a hacer cumplir tales derechos. Si bien, estas declaraciones de derechos humanos han cobrado mayor relevancia dado el fortalecimiento de los organismos internacionales no provienen solo del siglo pasado, sino que tienen sus antecedentes mucho tiempo atrás, como nos lo explica Karel Vasak con su idea de las tres generaciones de derechos, en las cuales aparece la idea de privacidad así como su constante lucha por defenderla.

1.8 Las tres generaciones de derechos de Karel Vasak y la idea de Privacidad

A finales de los años 70 del siglo pasado, Karel Vasak quien era el Director de la División de los Derechos Humanos y de la Paz de la UNESCO, realizó una clasificación por

⁷² Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos San José, Costa Rica 7 al 22 de noviembre de 1969. Adoptada en San José, Costa Rica el 22 de noviembre de 1969 Entrada en Vigor: 18 de julio de 1978, conforme al Artículo 74.2 de la Convención.

⁷³ Organización de Estados Americanos [OEA], “Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica,” *Tratados Multilaterales Interamericanos*, no. 9460 (1978): 24, http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf.

generación de los derechos humanos, esta distinción se realizaba en función de cuándo, cómo y para qué surgieron en nuestra historia.⁷⁴ Estas generaciones tenían como base de su origen cierta revolución o cambio de paradigma que exigía una determinada forma de atender a los derechos humanos.⁷⁵

Alberto Sánchez nos dice que la primera generación de derechos surgió como contrapartida a un orden mundial con fundamento divino que privilegiaba teóricamente la libertad de unos sobre el servilismo de otros, los cuales englobarían los derechos civiles y políticos a través de la Carta de Derechos inglesa de 1688, la Declaración de Derechos del Buen Pueblo de Virginia estadounidense de 1776, y la Declaración de los Derechos del Hombre y del Ciudadano francesa de 1789.⁷⁶ Peces Barba comenta que estas tres declaraciones, fruto de una ideología liberal que defendía la menor intervención posible del Estado en el desarrollo privado de la vida de cada individuo, propugnaban fundamentalmente derechos relacionados con la libertad.⁷⁷

Dichos derechos pueden ser divididos en dos categorías interdependientes: derecho a la libertad individual y derecho a la protección de dicha libertad individual. De tal manera que cualquier intromisión injustificada a la vida privada era un delito y pasaba a ser castigada por la ley. Esta fue la primera vez que el espacio privado estaba protegido por la ley. Tal idea de derecho puede ser asociada con la definición expuesta por Warren y Brandeis como “*the right to be alone*” esto es, *el derecho a no ser molestado*; y ésta a su vez tiene

⁷⁴ Karel Vasak, “A 30-Year Struggle. The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights,” *The UNESCO Courier* (París: UNESCO, 1977), 29;32.

⁷⁵ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento,” 368–69.

⁷⁶ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento.”

⁷⁷ Gregorio Peces-Barba Martínez, *Derecho Positivo de Los Derechos Humanos* (México: Debate, 1987).

correspondencia con la idea de libertad negativa. Una libertad entendida – así por Robert Alexy – como la falta de impedimentos externos a la hora de llevar una vida digna.⁷⁸

La segunda generación – nos dice Alberto Sánchez – se le conoce como la generación de la igualdad puesto que llevaría en su estandarte a los derechos sociales, económicos y culturales. La génesis de tales derechos está en las revoluciones obreras y el pensamiento humanista y socialista de finales del siglo XIX. Tales derechos nos fueron reconocidos hasta la mitad del siglo pasado por medio de la Declaración Universal de los Derechos Humanos. A parte de recoger derechos con injerencia en la vida política y social del individuo se agregaron aquellos con implicaciones en la vida biológica y social. Estos derechos son la reacción frente a las desigualdades en la distribución de la riqueza dado que esto permitía una mayor libertad a unos que a otros. Además la igualdad jurídica daba un cambio de paradigma para el papel del Estado frente a los derechos, esto es que se le impone como exigencia que intervenga cuando sea necesario con el fin de proteger la dignidad de todas y todos. Huye de su papel de enemigo de los derechos para convertirse en un aliado, árbitro y defensor.⁷⁹ Se ve marcada su participación – dice Amartya Kumar Sen – como un posibilitador de las capacidades humanas y su continuo desarrollo. Ahora ya no se trata solo de garantizar el libre desarrollo de los ciudadanos siempre y cuando éstos dispongan por sí mismos de los medios que los lleven a su efectivo disfrute, ahora se trata de que todos puedan lograrlo independientemente de los medios de que dispongan.⁸⁰

⁷⁸ Robert Alexy, *Teoría de Los Derechos Fundamentales* (Madrid: Centro de Estudios Constitucionales, 1993).

⁷⁹ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento.”

⁸⁰ Amartya Sen, “Human Rights and Capabilities,” *Journal of Human Development* 6, no. 2 (2005): 151–66, <https://doi.org/10.1080/14649880500120491>.

Herman Tavani y James Moor introdujeron en los años noventa la teoría de la privacidad de acceso restringido/control limitado^{VII} (RALC, por sus siglas en inglés) en ella conciben que un individuo tiene privacidad «en una situación con respecto a otros [si] en esa situación el individuo... está protegido de la intrusión, la interferencia y el acceso a la información por parte de otros.»⁸¹ Tal definición se parece mucho a la dada por Warren y Brandeis, sin embargo en esta misma teoría, aparte de dar una definición del concepto de privacidad, se habla de privacidad normativa cuya definición está en términos de protección contra la intrusión y el acceso a la información por parte de otros en una situación determinada. Se tiene privacidad normativa en una situación en la que se está protegido por normas, políticas o leyes explícitas que se han establecido para proteger a los individuos en esa situación.⁸² Podemos decir que esta definición de privacidad normativa guarda relación con la segunda generación de derechos, dado el interés por crear mecanismos de defensa política y jurídica para la protección de la privacidad.

Por último, la tercera generación tiene que ver con los derechos colectivos y de la humanidad. Esta generación tiene su inicio en los movimientos ecologistas de 1960 frente a los efectos globalistas cada vez con mayor impacto. Entre los derechos que defendían se encuentran el derecho a un medio ambiente limpio y sano, este se recoge en la Declaración de Río sobre Medio Ambiente y Desarrollo en 1992. Otros de ellos es el derecho a la autodeterminación de los pueblos, el derecho a una cultura de paz, los derechos relacionados con el progreso de la biotecnología genética, el derecho a la protección de los datos personales^{VIII} o el derecho al patrimonio común de la humanidad.⁸³ Justo dentro de esta

⁸¹ Herman Tavani, "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy," *Metaphilosophy* 38, no. 1 (2007): 1–22, <http://www.jstor.org/stable/24439672>.

⁸² Tavani.

⁸³ Sánchez Rojo, "Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento," 379.

generación están las Directrices para la Regulación de los Archivos de Datos Personales Informatizados adoptadas mediante la resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990. En ella se leen los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados dado el avance de las nuevas tecnologías de la información que hacían posible almacenar una mayor cantidad de datos, así como acceder a ellos de un modo más sencillo y rápido.⁸⁴

Dentro de estas directrices destacan las siguientes:

Principio de legalidad y lealtad: La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

Principio de especificación de la finalidad: La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que:

a) Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados;

b) Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados;

c) El período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

Principio de no discriminación: Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6 (Facultad para hacer excepciones: justificados por la seguridad nacional, el orden público, la salud pública o la moralidad) no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual,

⁸⁴ Asamblea General de las Naciones Unidas, “Directrices Para La Regulación de Los Archivos de Los Datos Personales Informatizados,” 1990.

opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

Principio de seguridad: Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

Supervisión y sanciones: El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados.⁸⁵

Tanto gobiernos como empresas privadas tenían la posibilidad de almacenar y manejar fácilmente información personal de individuos particulares, lo cual entraba en conflicto con el derecho humano a la privacidad si no era regulado.⁸⁶ Esta no regulación facilita la pérdida de privacidad como derecho fundamental. Y en tanto derecho, universal – colectivo –, intersubjetivo y clave para el cumplimiento de otros derechos. Esta idea de privacidad como derecho colectivo, además del inicio de la regulación para su protección en el uso de datos personales, guarda relación con la definición que ya hemos visto dada por Carissa Véliz.

A través de este breve recorrido podemos colegir, una vez más, que nuestra idea de privacidad ha sufrido diversos cambios, tanto en su sentido descriptivo como normativo, en sus aplicaciones, así como en su comprensión a partir de los distintos aspectos de la vida

⁸⁵ Organización de las Naciones Unidas.

⁸⁶ Sánchez Rojo, “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento,” 379.

humana. Sin duda estos cambios seguirán existiendo y serán – en su mayoría – en beneficio de nuestra sociedad. También, hemos visto que la comprensión de la idea de privacidad está unida a los contextos políticos, sociales, económicos y tecnológicos de cada tiempo. En la época de Warren y Brandeis las necesidades de respuesta ante las intromisiones a la vida privada por las fotografías instantáneas eran distintas a las que se pueden encontrar durante la época de la Guerra Fría y anterior a ella en el desarrollo de dispositivos tecnológicos capaces de escuchar a través de las paredes, como lo son también ahora en la era de Internet, de la inteligencia artificial, del Deep Learning y el Big Data, cuyas capacidades sobrepasan por mucho las simples potencialidades de violación a la privacidad de una fotografía en el siglo XIX. Los tiempos cambian, las necesidades con ello y nuestras capacidades de respuesta han de estar a la altura de nuestras circunstancias.

Por tanto, la idea de privacidad en el siglo XXI – en la Era digital – es distinta a partir de las necesidades en las que se encuentra. La Era digital da su paso inicial con la creación del Internet en la época de 1960, como un desarrollo tecnológico militar de Estados Unidos.⁸⁷ Su uso y democratización poco a poco se fue expandiendo hasta nuestros días en los que poco más de 4.9 mil millones de personas en 2021 son usuarias de Internet es decir, 63 por ciento de la población mundial están dentro de esta red de información.⁸⁸ Sin embargo, hemos de comprender que las potencialidades de esta tecnología se encuentran y nacen en el uso, distribución y – su reciente – comercialización de información. El término información se traduce frecuentemente en el ámbito digital como datos. Datos que van desde letras y

⁸⁷ “A Brief History of the Internet,” Online Library Learning Center, accessed September 18, 2022, https://doi.org/10.1007/978-3-642-13247-6_1.

⁸⁸ ITU, *2021 Measuring Digital Development: Facts and Figures*, ITU Publications (Geneva: International Telecommunication Union, 2021), [https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU Facts and Figures 2019 - Embargoed 5 November 1200 CET.pdf%0Ahttps://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx](https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU_Facts_and_Figures_2019_-_Embargoed_5_November_1200_CET.pdf%0Ahttps://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx).

números sin más hasta información precisa de comportamiento en seres humanos – esta variable es importante y será abordada más adelante –. Existe todo tipo de datos que aunados a una inteligencia artificial con una buena base algorítmica son capaces de crear resoluciones en muy corto tiempo, que para la capacidad humana sería simplemente imposible.⁸⁹ Sin duda, pudiéramos dar un preámbulo mucho más amplio para la comprensión de lo que representa esta época en nuestra sociedad y los cambios tan radicales que ha traído, sin embargo hacerlo sería pecar de olvido y obiedad de la propia realidad de hoy que nos sumerge en su mundo tecnológico y de inteligencia artificial. No se trata de evidenciar lo evidente, puesto que no es la empresa de este trabajo. Lo que se busca es extraer de lo evidente sus implicaciones y cuestionarlas. De esta manera, pensemos en las implicaciones que tienen el uso de los datos en la Era digital y la forma en cómo se relaciona con la idea de privacidad.

⁸⁹ Yuval Noah Harari, *Homo Deus. Breve Historia Del Mañana*, 10ma. (México: Penguin Random House, 2018).

Capítulo II. Los datos en la Era digital

*You are a source of power.*⁹⁰
Carissa Véliz, *Privacy is Power* (2020)

Durante el año 2021 el London Speaker Bureau^{IX} entrevistó a diferentes autores, entre ellos se encontraba Carissa Véliz^X. En esta entrevista se le cuestionó si consideraba que los datos eran el nuevo petróleo, a lo que ella respondió lo siguiente:

Esta analogía es interesante, es el nuevo petróleo en el sentido de que las personas lo quieren, gran parte de la economía depende de él y es muy valioso. Así que hay algunas similitudes, pero curiosamente, algunas de las similitudes son también negativas. El petróleo es famoso por haber creado mucha contaminación y, aunque nos ha ayudado a avanzar en nuestra economía, ha tenido un precio muy alto y ahora está bastante claro que es insostenible y que el futuro son las energías limpias y no el petróleo (...) Y de la misma manera los datos personales o las empresas que dependen de la explotación de los datos personales son una especie de modelo obsoleto, en el sentido de que tienen una fecha de caducidad (...) pero son tan peligrosos que son insostenibles, así que en ese sentido la analogía funciona.⁹¹

Esta insostenibilidad reside en el peligro que representa a la sociedad y a la salud mental del individuo. El peligro emerge de los datos. Más no de los datos de orden público, sino de aquellos que impactan a la esfera pública y privada. Estos son los datos personales y privados. Los datos personales en la Era digital se han convertido en moneda de cambio para gran parte de las actividades que hoy se realizan. Así es como funcionan y son rentables corporaciones como Google, Facebook, Amazon, Apple, Microsoft, entre muchas otras. Usan los datos personales y privados, tales como: la ubicación de usuario, comunicaciones, búsquedas de Internet, información biométrica, relaciones sociales, compras y entre muchos

⁹⁰ Énfasis de la autora.

⁹¹ Carissa Véliz, "London Speaker Bureau. Interview Series," 2021, <https://londonspeakerbureau.com/interview-carissa-veliz/>.

otros, para luego venderlos a terceras partes y así lograr su rentabilidad.⁹² Por ahora tratemos de definir qué son los datos y qué es lo que los hace personales y privados, así como su relación con la llegada de Internet.

En este sentido, puede afirmarse que *los datos son un registro o rastro de información de forma analógica o digital*. Los esfuerzos se enfocan en su recopilación, acumulación y preservación por un largo periodo de tiempo. En su libro “Big Data, la revolución de los datos masivos”, Mayer-Schönberger y Cukier piensan a los humanos a través de la historia como seres que analizan datos:

...los seres humanos llevan milenios analizando datos. La escritura nació en la antigua Mesopotamia porque los burócratas querían un instrumento eficiente para registrar la información y seguirle la pista. Desde tiempos bíblicos, los gobiernos han efectuado censos para recopilar enormes conjuntos de datos sobre sus ciudadanos, e igualmente durante doscientos años los analistas de seguros han hecho grandes acopios de datos acerca de los riesgos que esperan entender; o, por lo menos, evitar.⁹³

A través del formato analógico la recopilación y el análisis de datos resultaba enormemente costosa y consumía mucho tiempo. Sin embargo, el avance hacia la gestión más eficiente de los datos llegó con el advenimiento de la digitalización: hacer que la información analógica fuese legible por los ordenadores, lo que también la vuelve más fácil y barata de almacenar y procesar. La recopilación y el análisis de información, que en otros tiempos exigía años, podía ahora hacerse en días, o incluso menos.⁹⁴ Tal digitalización no se entiende sin la llegada de Internet y su interconectividad global que proclamaba libertad de conocimiento y un nuevo camino abierto para la mejora potencial de la condición humana,

⁹² Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 1.

⁹³ Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. La Revolución de Los Datos Masivos*, 2013.

⁹⁴ Mayer-Schönberger and Cukier.

incluyendo libertad, justicia, igualdad y paz mundial.⁹⁵ Inclusive existía una certeza augurada por ciertos tecno optimistas, que esta revolución inevitable nivelaría la sociedad, derrocaría a las élites y daría paso a una especie de libre utopía global.⁹⁶ Pero esto a su vez inició la transición de una sociedad basada en la propiedad a una basada en la información, creando nuevas estructuras de poder que disponen del potencial suficiente para oprimir y explotar a aquéllos que carezcan de las capacidades necesarias para el acceso a la información y a las herramientas comunicacionales.⁹⁷

La llegada de la Era digital trajo consigo cambios enormes, ha sido una revolución en todos los sentidos. Tal concepto existe desde los años sesenta, y su puesta en marcha ha sido progresiva hasta nuestros días.⁹⁸ Esta Era representa una transición de lo analógico a lo digital, es decir, ha sido un proceso social derivado del despliegue y la adopción de las TIC (Tecnologías de la Información y Comunicación).⁹⁹ Un claro ejemplo de esto nos lo da Martin Hilbert, de la Annenberg School de Comunicación y Periodismo de la Universidad del Sur de California, con su estudio publicado en la revista Science. Hilbert se esfuerza por contabilizar todo lo producido, almacenado y comunicado, lo cual comprendía libros, cuadros, correos electrónicos, fotografías, música y vídeo (analógico y digital), así como videojuegos, llamadas telefónicas, navegadores de vehículos y cartas enviadas por correo postal. Según su cómputo, en el año 2000 una cuarta parte de la información almacenada en el mundo era digital, el resto estaba en papel, película, discos LP de vinilo, cintas de cassette

⁹⁵ John Perry Barlow, “Declaration of Human Rights in Cyberspace” (Davos, Switzerland: Electronic Frontier Foundation, 1996), <https://www.eff.org/cyberspace-independence>.

⁹⁶ Eli Pariser, *El Filtro Burbuja: Cómo La Red Decide Lo Que Leemos y Lo Que Pensamos*, Td. Mercedes Vaquero (Barcelona: Penguin Random House, 2017).

⁹⁷ Robert Gelman, “Draft Proposal: Declaration of Human Rights in Cyberspace” (The digital Be-In, 1997), <https://www.be-in.com/10/rightsdec.html>.

⁹⁸ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

⁹⁹ Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, 43.

y similares. En cambio para el 2007 tan solo el siete por ciento de los datos totales eran analógicos, el resto eran ya digitales.¹⁰⁰ Además de esto las cifras de datos totales que estimó en el mismo año llegaron a los 300 exabytes y para 2013 se estimaba que la cantidad total de información almacenada en el mundo fuera de alrededor de 1200 exabytes, de los que menos del dos por ciento seguía siendo analógica.¹⁰¹

Alguien que ha dado testimonio histórico del proceso del traslado de la información de lo analógico a lo digital es Edward Snowden^{XI} en su libro *Vigilancia Permanente*. Snowden – como mayormente se le conoce – vivió este cambio a muy temprana edad. Como él mismo menciona, su generación fue la última sin digitalizar, es decir, fue la última generación en crecer con formatos analógicos como diarios escritos a mano, Polaroids o cintas VHS. Este proceso – de la llegada de Internet así como su desarrollo – lo narra de la siguiente manera:

Yo nací en 1983, cuando se acabó el mundo en el que la gente ponía la hora por sí sola. Ese año, el Ministerio de Defensa de Estados Unidos partió por la mitad su sistema interno de ordenadores interconectados; de ahí surgió una red llamada MILNET, que era la que iba a usar el personal de defensa, y otra red para el gran público, a la que llamaron internet. Antes de que acabase el año, existían normas nuevas que definían los límites de dicho espacio virtual; eso dio lugar al DNS (Domain Name System o sistema de nombre de dominio) que seguimos utilizando todavía hoy. Y a los códigos de países asignados al resto del mundo: .uk, .de, .fr, .cn, .ru, etcétera (...) tendrían que pasar otros seis años hasta que se inventara la World Wide Web (...) internet no es una sola entidad (...) La realidad técnica es que todos los días nacen redes nuevas en el cúmulo global de redes de comunicaciones interconectadas (...) la red de redes universal que conecta la mayoría de los ordenadores del mundo entre sí mediante una serie de los protocolos compartidos.¹⁰²

¹⁰⁰ Martin Hilbert and Priscila López, “The World’s Technological Capacity to Store, Communicate, and Compute Information,” *Science* 332, no. 6025 (2011): 60–65, <https://doi.org/10.1126/science.1200970>.

¹⁰¹ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

¹⁰² Edward Snowden, *Permanent Record* (New York: Metropolitan Books, 2019), 27.

Con la llegada de las TIC y esta red de uso público llamada Internet, aunada a la gran cantidad de datos digitalizados y almacenados surgió una nueva forma de comunicarse, trabajar, investigar, en pocas palabras ha sido un cambio que ha transformado la vida cotidiana de las personas que tienen acceso a ello.

2.1 El Big Data

Los datos masivos, o el Big Data como se le conoce en la ciencia de los datos, «designa el tratamiento de grandes volúmenes de datos mediante algoritmos matemáticos con el fin de establecer correlaciones entre ellos, predecir tendencias y tomar decisiones».¹⁰³ Esta era del Big Data trastoca en definitiva la forma en que se había vivido e interactuado con el mundo. Esto significa también, un cambio de paradigma epistemológico, es decir, ahora la sociedad tendrá que desprenderse de su obsesión por la causalidad a cambio de meras correlaciones: «ya no sabremos por qué, sino sólo qué».¹⁰⁴ Con ello también inicia la fundamentación que sostiene que «el universo consiste en flujos de datos, y que el valor de cualquier fenómeno o entidad está determinado por su contribución al procesamiento de datos»,¹⁰⁵ ha esta creencia que busca expandir las leyes matemáticas de lo electrónico a lo bioquímico, así como la resolución en una teoría única global que unifique todas las disciplinas científicas utilizando los mismos conceptos y herramientas del flujo de datos, se le ha denominado dataísmo.¹⁰⁶ Esto contraría las prácticas establecidas durante siglos y choca con nuestra comprensión más elemental acerca de cómo tomar decisiones y aprehender la

¹⁰³ M. R. Llácer, M. Casado, and L. Buisan, “Document Sobre Bioètica i Big Data de Salut: Explotació i Comercialització de Les Dades Dels Usuaris de La Sanitat Pública” (Barcelona: Publicacions i Edicions de la Universitat de Barcelona, 2015), 33.

¹⁰⁴ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

¹⁰⁵ Noah Harari, *Homo Deus. Breve Historia Del Mañana*, 400.

¹⁰⁶ Noah Harari, *Homo Deus. Breve Historia Del Mañana*.

realidad. Esta nueva realidad que nos aviene sienta su fundamento en la gran cantidad de datos disponibles para su uso, de ahí que el procesamiento a gran escala traiga consigo nuevas percepciones y cree nuevas formas de valor, transformando los mercados, las organizaciones, las relaciones entre los ciudadanos y gobiernos, etc.¹⁰⁷

Existen otros autores que al hablar de Big Data se refieren a los «grandes volúmenes de datos que son muy variados y veloces, al punto de que resulta muy complicado capturarlos y procesarlos con métodos tradicionales».¹⁰⁸ Dentro de esta definición se encuentran cinco características peculiares que nos ayudan a designar con mayor claridad el Big Data. Para ello es utilizado el termino 5V, haciendo referencia a las cinco características seguido de la inicial de los conceptos utilizados, como se puede apreciar en la siguiente tabla.

Tabla 1

Las 5V del Big Data

Concepto	Definición
Volumen	El almacenamiento de la cantidad masiva de datos que pueden ser recolectados de múltiples fuentes como páginas web, redes sociales, IoT (Internet of Things), etc.
Velocidad	Los datos se generan en tiempo real gracias a las interacciones con las fuentes mencionadas, por lo que deben ser procesados con la misma velocidad.

¹⁰⁷ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

¹⁰⁸ Anthony Manota, “Big Data: Qué Es y Para Qué Sirve,” 2021, <https://platzi.com/blog/big-data/>.

Variedad	Todo tipo de datos ya sea estructurados o no estructurados. Podrían ser tablas, texto, imágenes, videos, audio, bases de datos, etc.
Veracidad	Es la calidad y confiabilidad de los datos. Al llegar de diversas fuentes, se vuelve complejo realizar su limpieza para evitar usar valores incorrectos.
Valor	Los datos deben poder proporcionar un valor o beneficio a la empresa que los está usando. ¹⁰⁹

En esta misma tónica hemos de decir que los datos guardan un valor en sí mismos, cuyo impacto se ve reflejado en diferentes ámbitos de la vida humana. Sin duda este valor tiene su principal fuente en el volumen de datos, puesto que el tamaño cuantitativo de datos hace que se realice también un cambio cualitativamente. Es decir, a mayor cantidad de datos acerca de algo, su conocimiento mejora, con ello su control y el anhelo de exactitud se ve medianamente relajado. Por ejemplo, en nanotecnología se dice que cuando se alcanza el nivel molecular, las propiedades físicas pueden alterarse. Con ello, se pueden dar metales más flexibles y cerámicas expandibles. Conocer esas nuevas características supone que se pueden inventar materiales que hagan cosas antes imposibles. Es por eso, que cuando aumentamos la escala de los datos con los que trabajamos, podemos hacer cosas nuevas que no eran posibles cuando sólo trabajábamos con cantidades más pequeñas.¹¹⁰ En este caso el

¹⁰⁹ Manota.

¹¹⁰ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

valor de los datos radica en su aplicación en la realidad física en la cual nos movemos y existimos. Existen otros casos en los cuales el tipo de valor es social, económico, científico, humanitario u otro. Inclusive pueden verse reunidos distintos tipos de valores dependiendo el ámbito donde se desempeñe el uso de determinados datos.

En definitiva los datos ya no se contemplan como algo estático o rancio, cuya utilidad desaparece en cuanto se alcanzaba el objetivo para el que habían sido recopilados. Por el contrario, los datos se convirtieron en una materia prima del negocio, en un factor vital, capaz de crear una nueva forma de valor económico. En la práctica, con la perspectiva adecuada, los datos pueden reutilizarse inteligentemente para convertirse en un manantial de innovación y servicios nuevos. Son ellos los que pueden revelar secretos a quienes tengan la humildad, el deseo y las herramientas para escuchar.¹¹¹

Hasta ahora parece que la llegada de la Era digital nos ha traído una transformación llena de beneficios y cambios a favor de la humanidad. Se muestra tan evidente que el desarrollo computacional y el almacenamiento de datos masivos guarda tanto valor en sí mismo que es vital para el desarrollo de la vida en el siglo XXI. Actualmente existe un crecimiento enorme de dispositivos, sensores, robots y aplicaciones móviles, y son estas mismas tecnologías emergentes las que nos llevan a pensar en una nueva fase de los datos, una fase en la que la unión entre los *bits* y otras formas de realidad es tan profunda que cambia radicalmente la condición humana.¹¹²

Pero detengámonos un momento, analicemos cómo se desarrollan estas tecnologías, pensemos en sus fundamentos y el material que utilizan, tratemos de desmenuzar la fuente primera de donde nace su potencial. Algunos dirán que su fortaleza está cimentada en el

¹¹¹ Mayer-Schönberger and Cukier.

¹¹² Mayer-Schönberger and Cukier.

desarrollo algorítmico o bien, en las capacidades técnicas de la maquinaria de la red de redes que genera una interconectividad nunca antes vista. Sin embargo, la fuente primordial para el desarrollo de las tecnologías antes creadas y ahora en constante desarrollo, está en los datos, pero sobre todo en los datos personales. Como bien nos dice Yasmina Soto: «la verdadera revolución no estriba en las máquinas que calculan los datos, sino en los datos mismos y en cómo los usamos y usaremos en el futuro».¹¹³ Precisamente, esa es la razón por la cual las computadoras producen datos como un producto, para ello se utilizan tecnologías digitales que crean un rastro de datos y estos, a su vez, son extraídos de las actividades humanas realizadas cotidianamente por las grandes corporaciones tecnológicas: datos acerca de lo que se ha hecho, cuándo y dónde. Al inicio de la Era digital estos datos no eran usados comercialmente, solo eran utilizados como retroalimentación para mejorar el sistema para los usuarios,¹¹⁴ hasta la llegada de diferentes empresas tecnológicas y en particular Google. Pero antes de conocer las formas de extracción de datos personales por parte de las grandes corporaciones tecnológicas, dejemos en claro lo que queremos decir con el concepto de datos personales.

2.2 Los datos personales

Para el Instituto Federal de Acceso a la Información Pública en su compendio de lecturas y legislación acerca de la protección de datos personales, estos

se refieren a toda aquella *información relativa al individuo que lo identifica o lo hace identificable*. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional. Además de ello, los datos

¹¹³ Yasmina Soto, “Datos Masivos Con Privacidad y No Contra Privacidad,” *Revista de Bioética y Derecho* 0, no. 40 (2017): 113, <https://doi.org/10.1344/rbd2017.40.19165>.

¹¹⁴ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 28.

personales también describen *aspectos más sensibles o delicados* sobre tal individuo, como es el caso de su *forma de pensar, estado de salud, sus características físicas, ideología o vida sexual*, entre otros. Los datos personales son necesarios para que un individuo pueda interactuar con otros o con una o más organizaciones sin que sea confundido con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes.¹¹⁵

O en otras palabras, como lo definen^{XII} la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO)¹¹⁶, o bien la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),¹¹⁷ el concepto de dato personal se refiere a «*cualquier información concerniente a una persona física identificada o identificable*».¹¹⁸

Al hablar de datos personales se ha de tener en cuenta aquello que lo hace ser una información con carácter personal, es decir, eso que lo diferencia de otro tipo de información. En principio la información personal será aquella que indique la identificación de una persona directamente, y sin necesidad de averiguación posterior. «En consecuencia, para que una información se considere dato personal, deben existir dos elementos: la información y la persona a la que concierne dicha información.»¹¹⁹

Además, al hablar de datos personales habremos de señalar dos categorías especiales. La primera involucra información sensible es decir, los datos que guardan identidades específicas y que cuyo conocimiento y tratamiento abierto – o no – podría llevar importantes

¹¹⁵ IFAI, *Protección de Datos Personales. Compendio de Lecturas y Legislación*, 1a. (México: Tiro Corto Editores, 2010).

¹¹⁶ Cámara de Diputados del Congreso de la Unión, “Ley General de Protección de Datos Personales En Posesión de Sujetos Obligados,” Pub. L. No. 26-01–2017, Diario Oficial de la Federación 52 (2017).

¹¹⁷ Cámara de Diputados del Congreso de la Unión, “Ley Federal de Protección de Datos Personales En Posesión de Los Particulares,” Pub. L. No. 05-07–2010, 18 (2010).

¹¹⁸ Isabel Davara Fernández de Marcos, *Diccionario de Protección de Datos Personales. Conceptos Fundamentales* (Ciudad de México: Instituto Nacional de Transparencia, Acceso a al Información y Protección de Datos Personales, 2019), 211.

¹¹⁹ Davara Fernández de Marcos, 215.

riesgos para los derechos y las libertades fundamentales; estos son los datos personales sensibles.¹²⁰ Los Estándares de Protección de Datos para los Estados Iberoamericanos los definen de la siguiente manera:

aquellos que se refieran a la *esfera íntima de su titular*, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como *origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos* dirigidos a identificar de manera unívoca a una persona física.¹²¹

La segunda de ellas hace referencia a la información física o corpórea de las personas, estos son los datos biométricos, como bien lo mencionan los Estándares de Protección de Datos para los Estados Iberoamericanos dentro de su definición de datos sensibles, pero que por su particularidad y características especiales es necesaria su definición y con ello cierta distinción con otras categorías de datos. El Reglamento General de Protección de Datos^{XIII} los define como^{XIV}: «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las *características físicas, fisiológicas o conductuales de una persona física* que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos». ¹²² Ejemplos de estos datos pueden ser los siguientes: «las huellas dactilares, los modelos retinales, la estructura facial y las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera

¹²⁰ Comisión Europea, “Reglamento General de Protección de Datos,” Diario Oficial de la Unión Europea § (2016), <https://doi.org/10.2307/j.ctv17hm980.4>.

¹²¹ Red Iberoamericana de protección de datos, “Estándares De Protección De Datos Personales Para Los Estados Iberoamericanos,” no. 1 (2017): 8, https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.

¹²² Comisión Europea, Reglamento General de Protección de Datos.

particular de caminar o de hablar, etcétera)».¹²³ Los datos biométricos guardan en sí una diferencia muy marcada en contraste con otro tipo de datos personales, dada su identificación única, de tal manera que hablar de datos biométricos es hablar de información exacta y precisa de las personas. Pues son «rasgos físicos, biológicos de comportamiento de un individuo que lo identifican como único del resto de la población.»¹²⁴

Mediante este significado de datos personales que dan estas declaraciones de regulación en el ámbito de la información, la normativa se rige y dirige las jurisprudencias donde tiene aplicación. Estas normativas, aunque de recién ejecución, han sido útiles para una constante mejora en la regulación de la información. Sin embargo, en algunas ocasiones, el enfoque no ha sabido dirigir como debería ser el tratado de la información. Durante mucho tiempo ha sido el propio titular el responsable del cuidado y el control de su información, apelando a un control – y enfoque – individualista, el mismo de la declaración de Warren y Brandeis en 1890: *the right to be alone*. Salome Viljoen ha rechazado el individualismo a nivel conceptual y afirma que los daños del capitalismo informacional son sociales. Para ello se requieren sistemas democráticos de responsabilidad sobre la extracción y el procesamiento de datos.¹²⁵ Sin duda este enfoque ha ido cambiando a uno de tintes mucho más colectivos, dado que las violaciones a la protección de los datos tienen un impacto con relevancia más social que individual, y de los cuales hablaremos más adelante. Sin embargo, para que este cambio sea evidente, es necesario una reformulación en el análisis de los datos personales. Es decir, los datos personales necesitan un análisis más profundo que nos ayude a

¹²³ Grupo de Trabajo del Artículo 29, “Dictamen 4/2007 Sobre El Concepto de Datos Personales,” 2007, 9, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

¹²⁴ INAI, “Resolución Del Procedimiento de Verificación 3S.07.02-039/2017,” 2017, https://inicio.inai.org.mx/pdf/resoluciones/2017/03S_02-039.pdf.

¹²⁵ Salome Viljoen, “A Relational Theory of Data Governance,” *Yale Law Journal* 131, no. 2 (2021): 573–654.

distinguirlos de otro tipo de datos y reconocer el vínculo que guarda con otros conceptos, tales como el de control y propiedad. Es por eso, que un análisis filosófico sería el ideal para poner las cosas en claro.

2.2.1 Modelo analítico para usos morales e identificación de datos personales.

Valgámonos del concepto filosófico de *separability* o separabilidad, usado por Montagnani y Verstraete en su texto *What Makes Data Personal?*, el cual suele servir para distinguir a las personas de las cosas. Esta distinción nos ayuda, para que en términos de propiedad, se conceda el derecho de control sobre las cosas, a la vez que se niega el derecho de control sobre las personas. Un ejemplo de esto es el que realiza G. W. F. Hegel, quien afirma que solo las cosas que son externas a la persona son adecuadas para reclamar la propiedad. En este sentido, las cosas son separables cuando pueden existir separadas de una persona.¹²⁶ Otros como Immanuel Kant y Margaret Jane Radin, apelan a la separación física para determinar las condiciones de separabilidad. Las partes del cuerpo, o cualquier cosa conectada físicamente a la persona, son inseparables y no deben ser tratadas como propiedad.¹²⁷ En este caso, la ilegalidad del tráfico de órganos humanos puede ser un claro ejemplo. Sin embargo, la separación física reduce a la persona a sus límites físicos, olvidando que algunas cosas que son fundamentales para la persona no están conectadas físicamente, y aun así pueden conservar otras conexiones, como lo son las relaciones del contenido de los datos, los cuales vinculan a una persona con los mismos, dado que la describen y pueden

¹²⁶ G. W. F. Hegel, *Filosofía Del Derecho*, 5a. (Buenos Aires: Claridad, 1968).

¹²⁷ Margaret Jane Radin, "Property and Personhood," *Stanford Law Review* 34, no. 5 (1982): 957–1015, <http://www.jstor.org/stable/1228541>.

persistir después de una transferencia de información. Regresemos al ejemplo de los órganos humanos, pero ahora en su uso con los trasplantes que se realizan de manera legal.

Aunque un órgano pueda ser transferido y pasar a ser de otra persona, sigue habiendo usos potenciales que están relacionados con el donante debido al vínculo genético que persiste. Está claro que utilizar un órgano donado para realizar funciones corporales rutinarias no implica al donante. Sin embargo, la extracción del material genético que queda en el órgano para averiguar el potencial del donante para ciertas enfermedades y comercializar productos médicos basados en esta información sigue estando conectada con el donante, aunque el órgano se transfiera físicamente.¹²⁸

De esta manera podemos distinguir dos caminos en los que la idea de separabilidad nos permite tener claridad. Por un lado el de conexión, que nos muestra la vinculación que existe entre la persona y aquello que puede ser nombrado inseparable, a la vez que determina la disposición de propiedad de una persona hacia una cosa. Y por el otro el de uso, el cual nos indica precisamente el uso que se da a esa conexión de inseparabilidad existente, es decir el control de uso. En el caso de los datos personales, nos señalan en primer lugar que existe una conexión entre ellos y la persona, puesto que la descripción de estos da a conocer a la persona; existe por tanto una conexión de inseparabilidad. En segundo lugar, al existir tal conexión, las personas deben conservar los derechos de control sobre el uso de sus datos personales, de otra manera se puede hacer uso de esta conexión para intereses particulares que pueden afectar a la persona que describen tales datos. Sin embargo pudieran existir – y de hecho existen – usos de tinte colectivos y democráticos que no afectan a la persona en su autonomía y dignidad.¹²⁹ Esta idea de separabilidad expuesta por Montagnani y Verstraete nos ofrece una analítica para identificar cuándo los usos de los datos personales implican

¹²⁸ Maria Lilla Montagnani and Mark Verstraete, “What Makes Data Personal?,” *UC Davis Law Review* 56, no. 3 (2022): 33–34, <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13958/10070>.

¹²⁹ Montagnani and Verstraete, 34–35.

afectaciones, o bien cuándo los intereses personales siguen la dignidad y autonomía de la persona.

Desde el punto de vista normativo, este enfoque ofrece a la ley de privacidad de la información una base más rigurosa en la filosofía moral, ya que los usos inseparables (o los usos que están conectados con la persona) implican preocupaciones kantianas sobre el tratamiento de una persona como una cosa y el uso de una persona como medio para un fin. Como resultado, la separabilidad proporciona un análisis rico para diferenciar entre los usos de la información que utilizan la conexión personal inherente a la información (y son inseparables) y los usos que no lo hacen y, por tanto, no son necesariamente moralmente inadmisibles.¹³⁰

Ahora que ya sabemos qué son los datos personales con sus categorías más importantes, así como un modelo analítico que nos ayude a identificarlos, pasemos a ver la manera cómo estos datos son utilizados y tratados por las grandes corporaciones tecnológicas.

2.3 El uso de los datos personales en la Era digital

Para conocer el método de extracción, uso y almacenamiento de datos personales en la Era digital hemos de empezar por entender los inicios y desarrollo de una de las empresas con mayor poder económico en el mundo: Google. Este buscador en Internet se valúa a fecha del 31 de diciembre de 2021 en 257,637 billones de dólares¹³¹ y cuenta con 156,500¹³² empleados alrededor del mundo, pero en sus inicios fue muy distinto. Apenas alcanzaba los

¹³⁰ Montagnani and Verstraete, 32.

¹³¹ Alphabet Inc., “United States Securities and Exchange Commission. Form 10-K. Annual Report.” (Washington D.C., 2021), 61, https://abc.xyz/investor/static/pdf/20220202_alphabet_10K.pdf?cache=fc81690.

¹³² Alphabet Inc., 9.

3,000 empleados para finales del 2004¹³³ y en el año 2000 estaba valuado en 19,108 dólares.¹³⁴ Veamos el inicio de esta empresa tecnológica y tratemos de comprender cómo fue que en un lapso muy corto de tiempo superó en valor económico a otras empresas que tienen ya más de un siglo en su haber.

Todo empezó cuando en el verano de 1995 el graduado de ingeniería de la Universidad de Michigan Larry Page se encontró al estudiante de informática de la Universidad de Stanford Sergey Brin, en un tour por el campus en la misma universidad.¹³⁵ En 1996 desarrollaron juntos el algoritmo^{xv} PageRank, el cual se convertiría en el núcleo de Google. Este algoritmo realizaba una tarea compleja para su época; consistía en contar el número y la calidad de los enlaces a una página para evaluar el grado de autoridad de ese sitio web, con lo cual después realizaba una clasificación de los resultados de búsqueda. De esta forma, Page Rank asume que el sitio web con mayor importancia es el que recibe más enlaces de otros sitios web que cuentan con mayor autoridad. Por ejemplo, el algoritmo de Page y Brin da más visibilidad a los periódicos que a los blogs desconocidos. Este algoritmo fue inspirado por el funcionamiento de las citas académicas, en el cual se desarrolla la importancia de un artículo de investigación dependiendo las veces que ha sido citado por otros autores. Es decir, mientras más citado sea un artículo de investigación mayor visibilidad se le da y su reconocimiento de autoridad aumenta. En este sentido, PageRank estableció un orden que hizo a un lado el ruido sin sentido de Internet, de tal manera que las consultas de

¹³³ Google Inc., “United States Securities and Exchange Commission. Form 10-K. Annual Report.” (Washington D.C., 2005), 14, <https://www.sec.gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm>.

¹³⁴ Google Inc., 22.

¹³⁵ Samuel Gibbs and Alex Hern, “Google at 20: How Two ‘obnoxious’ Students Changed the Internet,” *The Guardian*, 2018, <https://www.theguardian.com/technology/2018/sep/24/google-at-20-larry-page-sergey-brin-internet>.

búsqueda fueran mucho más informativas y valiosas.¹³⁶ Fue así que Google fue creciendo por su uso en el ámbito académico dada su efectividad y la confianza que daba a sus usuarios al dar a conocer a través de su postura que en su motor de búsqueda no se incluiría publicidad de anunciantes, como sus mismos creadores lo declararon en un artículo publicado en la revista *Computer Networks and ISDN Systems* en 1998:

Además de un enorme crecimiento, la Web también se ha vuelto cada vez más comercial con el tiempo. En 1993, el 1,5% de los servidores web estaban en dominios .com. Esta cifra aumentó a más del 60% en 1997. Al mismo tiempo, los motores de búsqueda han pasado del ámbito académico al comercial. Hasta ahora, la mayor parte del desarrollo de los motores de búsqueda se ha llevado a cabo en empresas con poca publicación de detalles técnicos. Esto hace que la tecnología de los motores de búsqueda siga siendo en gran medida un arte negro y esté orientada a la publicidad. Con Google, tenemos el firme objetivo de impulsar un mayor desarrollo y comprensión en el ámbito académico.¹³⁷

Sin embargo, su postura al respecto duro muy poco, dado que en los próximos años la apuesta fue por el desarrollo de una ingeniería en un sistema de anuncios. En el cual se pensaba que tanto Google, los anunciantes y los usuarios estarían contentos, pues al final todos salían ganando. Esto sucedió a raíz de diversos problemas financieros por los que pasó la compañía, aunque esto significara la contradicción de la postura de Brin y Page en los años anteriores. El cambio trascendental sucedió con el descubrimiento realizado por Amit Patel de las memorias caché de datos fortuitos que guardaba Google. Esto es, el registro de señales estructuradas que iba dejando cada persona de sus acciones en línea. A partir de este registro, Patel inició a construir historias a detalle sobre cada persona con sus ideas, sentimientos y

¹³⁶ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 28–29.

¹³⁷ Sergey Brin and Larry Page, “The Anatomy of a Large-Scale Hypertextual Web Search Engine,” *Computer Networks and ISDN Systems* 30, no. 1–7 (1998): 109, [http://dx.doi.org/10.1016/S0169-7552\(98\)00110-X](http://dx.doi.org/10.1016/S0169-7552(98)00110-X)
http://apps.webofknowledge.com/full_record.do?product=UA&search_mode=GeneralSearch&qid=6&SID=X1pOWPMuSmOv1SlwJ6f&page=1&doc=2.

temas de interés.¹³⁸ «Patel llegó a la conclusión de que esos datos proporcionaban en realidad una especie de “sensor amplio del comportamiento humano”»¹³⁹ junto con este descubrimiento se creó un equipo que enfocaría sus esfuerzos en el desarrollo de un sistema capaz de generar crecimiento económico para la compañía. A este grupo de seis personas se le llamó AdWords. Mientras que por su parte «Google orientaría su propia memoria caché de datos sobre comportamientos, así como su potencia y sus conocimientos informáticos, hacia un solo objetivo y una única tarea: emparejar anuncios con búsquedas».¹⁴⁰

En el sistema AdWords los anuncios que consiguen que más personas hagan clic en ellos tienen prioridad, con lo cual se pretende garantizar que los anuncios sean útiles para los usuarios. Los anunciantes pagan por cada clic y el funcionamiento de cobro se desarrolla de la siguiente manera: los anunciantes presentan una oferta de cuánto están dispuestos a pagar por cada vez que un usuario haga *clic* en su anuncio, luego el anunciante que gana la puja debe pagar un céntimo más que el que quedó en segundo lugar. Al cobrar por clic^{XVI}, Google permite a los anunciantes pagar por los anuncios sólo cuando funcionan. Ciertamente, es una innovación que hace ganar tanto a la plataforma como a sus anunciantes. Otra gran innovación que realizó Google fue que redujo el precio de los anuncios más efectivos, alentando a la creación de mejores anuncios.¹⁴¹ (Actualmente, los procedimientos en los anuncios son diversos, el que más sobresale es el Real Time Bidding por su alta utilidad y triangulación de datos^{XVII}). Para que el funcionamiento de este sistema sea efectivo es

¹³⁸ Jennifer Lee, “Postcards From Planet Google,” *The New York Times*, 2002, <https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciid.onion/2002/11/28/technology/postcards-from-planet-google.html>.

¹³⁹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019), 76.

¹⁴⁰ Zuboff, 83.

¹⁴¹ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 30.

necesario cierto indicador que guíe a los anunciantes cómo mejorar en la creación de anuncios más llamativos y relevantes para el usuario, y así conseguir un mayor número de clics. Pues si su anuncio llega a ser pobre visual o auditivamente se verá en desventaja con sus competidores en la lucha de nuevos clientes, y sus ganancias disminuirían por el poco impacto generado. Para que esto no suceda, Google encontró una solución: la información personal generada en las búsquedas de sus usuarios, quienes con una alta probabilidad pueden ser los clientes ideales que los anunciantes están buscando. Con ello, los anuncios ya no estarán ligados a las palabras claves usadas en una consulta de búsqueda, sino que irán «dirigidos» a cada individuo en particular,¹⁴² usando diversos recursos como el Data Mining^{XVIII} (Minería de Datos). De esta manera, Google inició la venta de datos personales a otras empresas que estaban buscando nuevos clientes, sin que estas gastaran altas cantidades de dinero en publicidad, y lo mejor de todo – para los anunciantes – era que esta publicidad tenía un alto nivel de efectividad comparándolo con otras formas de marketing.^{XIX}

La creación de una nueva patente por parte de Google dio la confirmación de lo que se venía haciendo. En 2003, se presentó la patente «Generating User Information for Use in Targeted Advertising» [«Generación de información de usuario para su uso en publicidad dirigida»] con ella, se hacía una “lectura de la mente” de los usuarios. El objetivo era que recibieran anuncios correspondientes a sus intereses; intereses que se deducirían a través de los rastros colaterales de comportamiento dejados en línea. Mediante los datos de comportamiento se deduce ampliamente y con una alta probabilidad lo que un individuo concreto está pensando, sintiendo y haciendo en un momento y lugar concretos. Ahora, el poder de trasladar un mensaje particular a una persona en concreto, justo en el momento en

¹⁴² Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 83.

que más probabilidades se tiene de influir realmente en su comportamiento es una realidad. Una nueva realidad con una economía política y universo moral propio.¹⁴³ «Google pasó a crear y cazar datos de los usuarios con el objetivo expreso de utilizarlos para orientar la publicidad».¹⁴⁴ Después de esto, compró la compañía de anuncios DoubleClick en 2007, la cual usaba “cookies”^{XX} para acceder a los datos personales de los usuarios, incluyendo el historial de búsqueda, antes de que el propio usuario diera clic en el anuncio; y con ello empezó a usar anuncios en pantalla como lo son los banners gráficos. Existen fuentes similares de seguimiento en línea, como por ejemplo, las balizas web (o web beacon)^{XXI}, «la mayoría de las cuales están vinculadas a "cookies" que pueden utilizarse en todos los sitios web, y cuyo acceso puede venderse a los compradores interesados».¹⁴⁵ Con esto y demás sistemas y dispositivos^{XXII} capaces de extraer la mayor cantidad de datos posibles, Google continúa en constante crecimiento.

Lamentablemente, la víctima de este sistema gigantesco de uso de datos personales ha sido la privacidad – nuestra privacidad – de las personas que ingresan a la plataforma en búsqueda de información; información que no está alejada de la vida humana. No está en un mundo lejano, perdido de la realidad, sin relación alguna con el desarrollo de la vida personal de sus usuarios. Toda la información que se ingresa al realizar una simple búsqueda en Internet habla acerca del usuario, (que para los intereses de este trabajo, habla acerca de la vida de una persona^{XXIII}); sus intereses, gustos, aficiones, miedos, enfermedades, etc.^{XXIV} Habla acerca de aquello a lo que todo individuo, por curiosidad o necesidad desea saber, sin que por ello consienta entregar sus datos personales que correspondan al ámbito privado. Es

¹⁴³ Zuboff, 87.

¹⁴⁴ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 32.

¹⁴⁵ Jim Isaak and Mina J. Hanna, “User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,” *Computer* 51, no. 8 (2018): 58, <https://doi.org/10.1109/MC.2018.3191268>.

por eso, que a las empresas tecnológicas les viene muy bien la idea – o mito, dicen algunos – de la autogestión de la privacidad. Esta sucede cuando se alude al control en la decisión de estar de acuerdo en los términos y condiciones de los servicios, plataformas o redes sociales, pues se hace referencia a la autogestión del análisis que se hace por parte de cada persona en la toma de decisión.^{XXV} Sin embargo, esta responsabilidad individualista trae consigo problemáticas cognitivas y estructurales^{XXVI}. Pues, como plantea Solove

La autogestión de la privacidad se basa en el consentimiento: trata de ser neutral respecto al fondo —si determinadas formas de recopilar, usar o divulgar datos personales son buenas o malas— y se centra en si la gente autoriza determinadas prácticas respecto de su privacidad. El consentimiento legitima casi cualquier tipo de colección, uso o divulgación de datos personales.

Con una gran cantidad de datos extraídos de las búsquedas cotidianas en Internet, es posible construir una imagen precisa de la mente, tanto colectivamente como individualmente – de la forma que Google ya lo ha hecho.¹⁴⁶ Pues,

además de palabras claves, cada búsqueda en Google produce una estela de datos colaterales, como el número y la pauta de términos de búsqueda, la manera de expresar cada búsqueda, su ortografía, su puntuación, el tiempo que duraba, las pautas de cliqueo y la ubicación.¹⁴⁷

Un ejemplo del procesamiento y almacenamiento de datos es Live Query. Una pantalla que Google mostró en el 2002 para dar a conocer la información extraída de las búsquedas realizadas alrededor del mundo. «Era como estar viendo la consciencia colectiva del mundo» expresó la reportera del The New York Times Jennifer Lee.¹⁴⁸ Para el 2013 Google procesaba más de 24 petabytes de datos al día, «un volumen que representa miles de

¹⁴⁶ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 31.

¹⁴⁷ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 75.

¹⁴⁸ Lee, “Postcards From Planet Google.”

veces la totalidad del material impreso que guarda la Biblioteca del Congreso de Estados Unidos ». ¹⁴⁹

De esta manera – extrayendo, almacenando, analizando y obteniendo valor de los datos personales –, Google ha tenido un crecimiento económico exponencial en un lapso muy corto de tiempo ¹⁵⁰(1998–). Siguiendo estos mismos pasos, empresas como Facebook ^{XXVII} (actualmente, Meta ^{XXVIII}), Apple ^{XXIX}, Microsoft ^{XXX} y Amazon ^{XXXI} han convertido la industria tecnológica en la industria de los datos. En otras palabras, estas empresas se han convertido millonarias y con un poder político mayor a los de muchos países, gracias a los datos personales de todos aquellos que utilizamos sus productos y servicios.

2.4 Malentendidos de la privacidad en la Era digital

Hasta este punto, pudiera parecernos que no existe una problemática tan grave por el hecho de que nuestros datos sean utilizados por estas empresas. Algunos pudieran pensar – por ingenuo que parezca – que si éstas son capaces de almacenar tales y tantos datos, es porque tienen las herramientas de seguridad suficientes para protegerlos y por lo tanto, no debe de existir preocupación alguna. Sin embargo, lamentablemente, los protocolos de seguridad de estas empresas se han visto en problemas en ciertas ocasiones al ser hackeados ^{XXXII} con la finalidad habitual de robar los datos – personales – almacenados ^{XXXIII}. Inclusive existen empresas dedicadas exclusivamente al comercio de datos conocidas como ‘Data Brokers’ ^{XXXIV} las cuales ceden a diario miles de millones de datos personales que

¹⁴⁹ Mayer-Schönberger and Cukier, *Big Data. La Revolución de Los Datos Masivos*.

¹⁵⁰ Alphabet Inc., “United States Securities and Exchange Comission. Form 10-K. Annual Report.”

recorren el mundo en apenas unos segundos obteniendo a cambio grandes beneficios¹⁵¹. Como es el ejemplo de la empresa española TapTap^{xxxv}. Tal empresa utiliza una plataforma llamada Sonata, en ella se divide el mundo en celdas de 500 metros de lado y se cruzan con datos de todo tipo, tanto personales como de fuentes públicas. En estos datos se encuentran el gasto medio de las tarjetas de crédito en una área determinada y los productos en los que se realiza tal pago, el tipo de viviendas que hay, los comentarios en redes sociales en esa zona y en ese momento, los rangos de edad de las personas que pasan por allí, su lugar de nacimiento, qué sistema operativo usan sus móviles, cuál es su estado de ánimo, entre otros.¹⁵² La extracción de esta cantidad de datos es posible gracias a la forma de configuración y funcionamiento de los mismos teléfonos móviles, como lo es el de la ubicación en tiempo real. Pues, por decirlo de alguna manera, está en el corazón del dispositivo dar a conocer la conexión a Internet que se tiene a las operadoras de telefonía. Ejemplos del uso de Sonata en el mercado los dan los responsables de esta tecnología:

Está la del fabricante de cereales para el desayuno que solo se mostraba a personas cercanas a un Mercadona a determinada hora, porque era en esa cadena de supermercados dónde había lanzado una oferta. Está el productor de coches que quería impactar en hombres interesados en deporte en las cercanías de gimnasios. O la marca de refrescos que segmentó su publicidad para que la vieran personas de 25 a 35 años pero solo en zonas en las que hubiera un determinado ratio de bares por calle, o que se encontraran a 10 minutos de ellas, contando con el tráfico de ese momento.¹⁵³

¹⁵¹ Javier Goizueta, “El RGPD Pone En Jaque El Gran Negocio Del Siglo XXI,” *El Confidencial*, September 13, 2018, https://blogs.elconfidencial.com/espana/tribuna/2018-09-13/datos-rgpd-gran-negocio-sigloxxi_1614624/.

¹⁵² Carlos Del Castillo, “Así Trabaja Una Empresa Española Que Compra y Vende Datos Personales Para Hacer Publicidad: ‘Recogemos Toda La Información Posible,’” *Diario.Es*, October 21, 2019, https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_1_1297691.html.

¹⁵³ Del Castillo.

En una situación similar las Big Tech comparten datos personales entre ellas y otras empresas a cambio de diversos beneficios. Como por ejemplo, Facebook, que da acceso a los datos personales de sus usuarios a otras compañías a cambio de que estas le den un trato preferencial en sus plataformas. Es así como, «le da a Netflix y a Spotify la capacidad de leer los mensajes privados de sus usuarios, de la misma manera que le da a Amazon el acceso a los nombres e información de contacto de los usuarios a través de sus amigos».¹⁵⁴ Parte de esta “colaboración” entre compañías son los datos que alimentan la herramienta de sugerencias de amigos en Facebook “Personas que quizás conozcas”.¹⁵⁵

La realidad en la compra y venta de datos es muy habitual entre las grandes empresas, así como el traspaso de información a cambio de ciertos privilegios; sin olvidar las ya mencionadas data brokers. Un ejemplo de ello es lo barato que es la compra de información bancaria de una persona; los números de cuenta pueden ser comprados por 50 centavos de dólar y el reporte completo bancario desde 95 centavos de dólar.¹⁵⁶ O bien, la compra de perfiles de citas online; en donde el presupuesto para conseguir casi 5 millones de ellos llega apenas los 150 dólares. Precisamente esta compra fue la realizada a USDate, una empresa estadounidense que comercia con perfiles de citas de todo el mundo, en mayo de 2017 por la empresa Tactical Tech y la artista Joana Moll. El lote de perfiles de citas incluía fotos (casi 5 millones de ellas), nombres de usuario, direcciones de correo electrónico, nacionalidad, género, edad e información personal detallada sobre todas las personas que habían creado los perfiles, su orientación sexual, intereses, profesión, características físicas minuciosas y rasgos de personalidad. La compra de estos datos puso al descubierto una vasta red de

¹⁵⁴ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 130.

¹⁵⁵ Véliz, 130.

¹⁵⁶ Elizabeth Dworskin, “FTC: Data Brokers Can Buy Your Bank Account Number for 50 Cents,” *The Wall Street Journal*, 2014, <https://www.wsj.com/articles/BL-DGB-39567>.

empresas que están sacando provecho de esta información sin el consentimiento de los usuarios.¹⁵⁷ «Que los datos personales sean a la vez tan valiosos y tan baratos de conseguir es la peor combinación posible para la privacidad».¹⁵⁸ En definitiva, que los datos almacenados estén en los servidores de estas empresas no quiere decir que estén resguardados y seguros. Es por lo tanto, necesario una mejora en las medidas de ciberseguridad dentro de estas empresas, a la par que las regulaciones nacionales e internacionales enfoquen sus esfuerzos por la protección y seguridad de las bases de datos.

Por otro lado, también parece importante mencionar una idea muy habitual en el colectivo social y que comúnmente se hace uso de ella para evadir la privacidad de las personas: «*No tengo[tienes] nada que ocultar y por eso no tengo[tienes] nada que temer*». Han existido diferentes momentos en los que se ha utilizado este argumento. En ocasiones ha sido usado por personas que han sido culpadas sin motivo alguno, y quienes para hacer valer su inocencia disponen de este argumento. En otras ocasiones se ha utilizado como eslogan de campaña para un programa del gobierno del Reino Unido que declaraba: «Si no tienes nada que ocultar, no tienes nada que temer». Inclusive en Estados Unidos, una persona anónima del Departamento de Justicia comentó: «Si [los funcionarios del gobierno] necesitan leer mis correos electrónicos... que así sea. No tengo nada que ocultar».¹⁵⁹ Después de los ataques terroristas del 11-S en Estados Unidos el gobierno creó todo un novedoso sistema de vigilancia que pretendía descubrir y detener a terroristas que estuvieran planeando un ataque.¹⁶⁰ Con dicho argumento abrieron camino a diferentes formas de espionaje en masa.

¹⁵⁷ Joana Moll, “The Dating Brokers: An Autopsy of Online Love,” Tactical Tech, 2018, <https://datadating.tacticaltech.org/viz>.

¹⁵⁸ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 128.

¹⁵⁹ Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” 748.

¹⁶⁰ United States Government, “The USA PATRIOT Act : Preserving Life and Liberty,” *USA Department of Justice*, 2001, http://www.justice.gov/archive/11/what_is_the_patriot_act.pdf.

El The New York Times reveló que, tras los atentados la Administración Bush autorizó en secreto a la Agencia de Seguridad Nacional (NSA, National Security Agency) realizar escuchas telefónicas sin orden judicial de las llamadas de los ciudadanos estadounidenses.¹⁶¹ Después en 2002, los medios de comunicación revelaron que el Departamento de Defensa estaba construyendo un proyecto de extracción de datos, denominado «Conciencia Total de la Información» (TIA, «Total Information Awareness»), bajo la dirección del almirante John Poindexter.¹⁶² Curiosamente, mucha gente cree que no hay amenaza para la privacidad cuando es el gobierno quien se dedica a la vigilancia, y si se diera el caso que el gobierno descubriera una actividad ilegal, no existe justificación para reclamar tal privacidad. Pareciera que este argumento no se refiere a toda la información personal, sino sólo a ese subconjunto de información personal que probablemente esté involucrada en la vigilancia gubernamental. Pero ¿cómo saber que solo ese subconjunto de datos personales es el que las agencias de vigilancia a través de los historiales de búsqueda están extrayendo y almacenando? No se tiene la certeza que así sea. Por otro lado, también parece permear la idea de utilizar la privacidad como moneda de cambio. Es decir, en este caso la posible pérdida de privacidad se ve como un intercambio por una posible ganancia de seguridad.¹⁶³ Pero lamentablemente, en el caso de la llamada «mass surveillance» o vigilancia masiva desarrollada por los Estados Unidos a través del President's Surveillance Program^{xxxvi} (PSP)¹⁶⁴ no ha ayudado a prevenir el terrorismo. El argumento principal en el combate contra

¹⁶¹ James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring," *The New York Times*, 2005, <https://doi.org/10.4324/9781315549293-15>.

¹⁶² John Markoff, "THREATS AND RESPONSES: INTELLIGENCE; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans," *The New York Times*, 2002, <http://www.nytimes.com/2002/11/09/politics/09COMP.html>.

¹⁶³ Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy."

¹⁶⁴ Snowden, *Permanent Record*.

el terrorismo radica en que el aumento de los datos de las personas ayudará a prevenir los malos acontecimientos, como lo son los actos terroristas. Sin embargo, esto es solo una idea intuitiva. No existe evidencia contundente que sugiera que este argumento es cierto y que haya sido comprobado.¹⁶⁵ De hecho, no se pudo encontrar un solo caso en el que la vigilancia masiva por medio de las escuchas telefónicas haya detenido algún ataque.¹⁶⁶ De la misma manera, el programa STELLARWIND^{XXXVII}, creado exclusivamente para el programa de vigilancia a través de los teléfonos y la acumulación de los correos electrónicos no contribuyó significativamente en la identificación de terroristas.¹⁶⁷ Actualmente, el método de vigilancia masiva se hace cada vez más cotidiano para algunos países como China – un país de régimen comunista – a raíz de los acontecimientos suscitados por la pandemia de COVID-19. «China está intentando establecer nuevas normas en materia de derechos digitales, privacidad y recopilación de datos, suprimiendo al mismo tiempo la disidencia en el país y promoviendo los objetivos geoestratégicos del PCC».¹⁶⁸ Este tipo de “soluciones tecnológicas” para contener la pandemia han sido utilizados por otros países democráticos y parece seguir teniendo alta aceptación, aunque diversas organizaciones ya hayan expresado una postura de desacuerdo al respecto.¹⁶⁹

Así que, volviendo a nuestro argumento principal, si una persona se dedica exclusivamente a actividades legales, no tiene nada de qué preocuparse. Pero realmente lo

¹⁶⁵ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 38.

¹⁶⁶ Michael Isikoff, “NSA Program Stopped No Terror Attacks, Says White House Panel Member,” *NBC News*, 2013, <http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588>.

¹⁶⁷ Charlie Savage, “Declassified Report Shows Doubts About Value of N.S.A.’s Warrantless Spying,” *The New York Times*, 2015.

¹⁶⁸ Lydia Khalil, “Digital Authoritarianism , China and COVID,” *Lowy Institute for International Policy*, 2020.

¹⁶⁹ “Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights,” *Human Rights Watch*, 2020, <https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight>.

que sale a relucir con el uso del argumento de ‘nada que ocultar’ es la falta de una concepción de la privacidad y de su valor. No existe, por lo tanto una evaluación del valor de la privacidad y las pérdidas que trae consigo su violación.¹⁷⁰ Pues lo que está en juego es que el ocultamiento es tomado como sinónimo de negación al escrutinio social, o de esconder actos ilegales. Pero en la realidad, no se oculta solo aquello que pueda traer problemas con las relaciones más cercanas a una persona, como un amigo o la misma familia. Se oculta todo aquello que haga sentir vulnerable a la persona, como lo pueden ser los miedos y fobias más penetrantes, así como también aquello que da seguridad económica y de vivienda, como lo es la información financiera bancaria o las llaves del hogar.¹⁷¹ En cambio, el ocultamiento, sí que es sinónimo de privacidad e intimidad, como bien lo afirma Edward Snowden:

Puedes optar por cederla [la privacidad] por conveniencia, o alegando el pretexto tan extendido de que la privacidad solo la exigen quienes tienen algo que esconder. No obstante, afirmar que no necesitas o no quieres privacidad porque no tienes nada que esconder es dar por hecho que nadie debería, o podría, tener que esconder nada (...) De este modo, se da por sentado que nadie, ni tú mismo, podría oponerse a desvelar ante nadie información sobre sus creencias religiosas, afiliaciones políticas y actividad sexual, con la misma despreocupación con la que se desvelan gustos cinematográficos y musicales o preferencias lectoras. En última instancia, decir que no te importa la privacidad porque no tienes nada que esconder no es diferente a afirmar que no te importa la libertad de expresión porque no tienes nada que decir; o que no te importa la libertad de prensa porque no te gusta leer; o que no te importa la libertad de religión porque no crees en Dios; o que no te importa la libertad de reunión pacífica porque eres agorafóbico perezoso y antisocial. El hecho de que esta o aquella libertad no tenga importancia para ti ahora mismo no quiere decir que la tenga o que no la vaya a tener mañana.¹⁷²

¹⁷⁰ Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.”

¹⁷¹ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 47–49.

¹⁷² Snowden, *Permanent Record*, 208–9.

Existen diversas variaciones del argumento de ‘nada que ocultar’ aplicable a diversos estratos del desarrollo personal o gubernamental, como puede ser la relación de pareja, amigos o familia, así como en los estados con ideales democráticos pero con prácticas más bien autoritarias, como ya lo vimos en la extracción y acumulación de datos por parte de gobiernos. Al final no existe una respuesta concluyente que nos permita refutar de una vez y permanentemente este argumento. Valdría la pena realizar más tarde un esfuerzo y llevar a cabo un análisis de separabilidad, que nos ayude a distinguir entre los valores implicados; entre el ocultamiento y la exposición señalando sus funcionalidades, así como la evaluación de los usos futuros de los datos personales.

Capítulo III. Impactos de la Era digital en lo público

La tecnología, al haber provisto la unidad del mundo,
puede destruirla con la misma facilidad,
y los medios de la comunicación global
fueron diseñados al mismo tiempo
que los medios de la posible destrucción global.
Hannah Arendt, *Hombres en Tiempos Oscuros* (1990)

En definitiva y como ya lo vimos, la cantidad exorbitante de datos genera un cambio cualitativo en el conocimiento de las cosas:

Asistimos a una transición hacia la datificación y la monetización que comporta extraer un nuevo valor de los datos y rentabilizarlos, tanto desde el interés privado como el público, o una combinación de ambos. Es una tendencia inserta en una floreciente industria basada en el conocimiento adquirido a través de la reutilización de los datos y su explotación.¹⁷³

Pero sobre todo, y para dejarlo en claro, debemos de tener en cuenta que todo lo que se hace en un smartphone o dispositivo con conexión a Internet, «cada transacción financiera que realizamos, cada viaje, cada receta y prueba médica, cada acción que realizamos en Internet o en las aplicaciones es rastreada»,¹⁷⁴ la gran parte de esta información está disponible para su compra en el mercado de datos, para ser usada por empresas con capacidades en inteligencia artificial y aprendizaje automático con el objetivo de la identificación de patrones o rasgos que indiquen alguna manera de hacer mejorar el negocio, su único objetivo es maximizar el valor de la empresa.¹⁷⁵

¹⁷³ Llácer, Casado, and Buisan, “Document Sobre Bioètica i Big Data de Salut: Explotació i Comercialització de Les Dades Dels Usuaris de La Sanitat Pública,” 33.

¹⁷⁴ Roger McNamee, “Facebook Will Not Fix Itself,” *Time*, 2021, <https://time.com/6104863/facebook-regulation-roger-mcnamee/>.

¹⁷⁵ McNamee.

Es por eso, que cuando la cantidad de datos al respecto de algo aumenta, su propio conocimiento también. Así que no es de sorprender que los datos personales recopilados por las Big Tech^{xxxviii} y los gobiernos cobren valor después de un análisis y procesamiento propio de la información y que den como resultado un nuevo conocimiento de las personas. Una de estas formas de conocimiento distinto que a su vez se convierten en nuevas cualidades, son las inferencias de preferencias, gustos o enfermedades de las personas.

3.1 Inferencias de datos sensibles

Los rastros digitales que se van dejando en las interacciones con las tecnologías son tratados como muestras de comportamiento, que luego son usados para hacer inferencias acerca de ello.¹⁷⁶ Estos rastros se convierten en indicadores de nuevos datos; no conocidos hasta ese momento. Las inferencias, como se sabe, son deducciones o conclusiones de otra cosa, las cuales derivan en un juicio de otros.¹⁷⁷ Como cuando se infiere las preferencias sexuales de una persona al escucharla hablar o ver su vestimenta, aunque probablemente podamos tener una conclusión equivocada. Para evitar el error necesitaríamos más datos que nos indiquen sus preferencias sin tener un conocimiento explícito. Sin embargo, cuando se trata de inferencias ordinarias, como una resolución matemática o la respuesta a un saludo, su conclusión es en las más de las veces correcta, sin la necesidad de ningún otro dato. Para dejarlo más en claro, esta figura lógica tan conocida nos da una imagen precisa: «El silogismo es una enunciación, en la que, una vez sentadas ciertas proposiciones, se concluye

¹⁷⁶ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

¹⁷⁷ Aristóteles, *Tratados de Lógica (Organon)*, 12a ed. (México, D. F.: Porrúa, 2008).

necesariamente en otra proposición diferente, solo por el hecho de haber sido aquellas sentadas». ¹⁷⁸

Es de esta forma, y a través de un modelo de razonamiento tan antiguo, que en la Era digital se llegan a diversas inferencias a través de los rastros que las personas van dejando en su recorrido por sitios web o mediante el uso de dispositivos tecnológicos, como son los Smartphones, los wearables y todo aquel dispositivo dentro de la categoría “Internet of Things”^{xxxix}. Algunos de estos rastros son entendidos como metadatos, los cuales, no son más que, datos acerca de datos. Por ejemplo, una llamada telefónica guarda ciertos metadatos, como la fecha y la hora de la llamada, la duración, el número desde el que se ha llamado, el número al que se ha llamado y las ubicaciones de ambos. También son entendidos como datos de actividad, pues revelan los lugares donde ha estado una persona y el tiempo que ha estado en ellos, a través de la ubicación de su teléfono celular. En otras palabras, los metadatos son la sustancia de la comunicación, es la esencia misma del contenido. ¹⁷⁹ Estos rastros de datos son producidos automáticamente sin tener un control acerca de ellos.

Toda esa información personal es la materia prima usada en la Era digital para la generación de inferencias que concluyan en datos personales sensibles. De esta manera lo hace Facebook con el botón ‘Me gusta’, e infiere los siguientes datos: patrones de comportamiento, preferencias sexuales, religión, afiliaciones políticas, capacidad intelectual,

¹⁷⁸ Aristóteles, 94.

¹⁷⁹ Snowden, *Permanent Record*.

edad y género.¹⁸⁰ De la misma manera que las expresiones faciales o las publicaciones en Twitter poden ser usadas para descubrir depresión.¹⁸¹

Estas inferencias son hechas basadas en algoritmos previamente establecidos por científicos de los datos.^{XL} Aunque trabajan automáticamente, no fueron creados por sí mismos. Es decir, los algoritmos son una representación mental humana y por lo tanto el error, sesgo o ecuanimidad son traspasados a él. Es por eso, que algunas inferencias, basadas en la probabilística de los algoritmos, pueden estar equivocadas, parecido al ejemplo del que hablamos algunos párrafos atrás acerca de las preferencias sexuales, solo que la gran diferencia radica en que la primera se realiza de una persona a otra con pocos datos, mientras que la hecha por los algoritmos es usada a escala y su resolución es hecha con una cantidad masiva de datos. Estas inferencias, aunque equivocadas, no son desechadas, al contrario, son usadas con tal de sacar el máximo provecho económico para las empresas¹⁸² o gobiernos con propósitos particulares. Pero ¿qué problema puede existir si una persona es “clasificada” o “etiquetada” erróneamente por un sistema que usa algoritmos? Existen en diferentes formas y pueden ser desastrosos, como lo muestra el caso «toeslagenaffaire» en Holanda.

En 2019 se reveló que las autoridades fiscales holandesas habían utilizado un algoritmo de aprendizaje automático para crear perfiles de riesgo, esto como un esfuerzo por detectar personas que cometían fraude con las prestaciones del cuidado de los niños. De esta manera, las autoridades fiscales sancionaron a familias hasta con 100 mil euros, por una mera sospecha de fraude basada en los indicadores del sistema algorítmico. Dadas las altas cifras

¹⁸⁰ Michal Kosinski, David Stillwell, and Thore Graepel, “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior,” *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (2013): 5802–5, <https://doi.org/10.1073/pnas.1218772110>.

¹⁸¹ Christopher Burr and Nello Cristianini, *Can Machines Read Our Minds?, Minds and Machines*, vol. 29 (Springer Netherlands, 2019), <https://doi.org/10.1007/s11023-019-09497-4>.

¹⁸² Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

económicas de las sanciones, miles de familias fueron orilladas a la pobreza, inclusive algunas víctimas llegaron a suicidarse y más de mil niños fueron llevados a orfanatos.¹⁸³ El director de la autoridad neerlandesa de protección de la privacidad, Aleid Wolfsen, se pronunció en un comunicado al respecto: «Durante más de 6 años, las personas fueron a menudo etiquetadas erróneamente como defraudadores, con consecuencias nefastas. Algunos no recibieron un acuerdo de pago o no pudieron acogerse a la reestructuración de la deuda».¹⁸⁴ En el mundo de la Era digital, los errores de las inferencias hechas por algoritmos pueden provocar pobreza e incluso la muerte.

Por otro lado, en los casos en los que las inferencias hechas por un sistema algorítmico son acertadas e inclusive funcionales para ciertos propósitos, – como lo puede ser en un diagnóstico médico – los beneficios y el aprovechamiento de ello puede lograr su objetivo económico o social. Sin embargo, cabría hacer un análisis ético y cuestionar los procesos y el material utilizado para llegar a tales resoluciones; probablemente encontremos intrusiones no consentidas a la vida privada de las personas. Adicionalmente, cabe decir que esta práctica inferencial no es nueva en la Era digital, pues el modelo de razonamiento lleva siglos formando parte de la lógica humana. Donde se encuentra el cambio, en primer lugar, puede ser detallado en la recopilación y el análisis de las actividades humanas mediadas por las plataformas en línea.¹⁸⁵ Por ejemplo, en los estudios de las ciencias sociales la experimentación era tratada a pequeña escala con cuestionarios u observaciones de laboratorio; en cambio ahora, son estudios a gran escala, en «los que los investigadores

¹⁸³ Melissa Heikkilä, “Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms,” *Politico*, 2022, <https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/amp/>.

¹⁸⁴ Heikkilä.

¹⁸⁵ Burr and Cristianini, *Can Machines Read Our Minds?*

observan el comportamiento de miles o millones de individuos y buscan regularidades estadísticas y principios subyacentes». ¹⁸⁶ Esto sucede – como ya se ha mencionado – gracias a las huellas digitales (rastros de actividad y comportamiento en línea, esto es, los datos y metadatos) que son permanentemente dejadas a lo largo de nuestras interacciones con los dispositivos con conexión a Internet, para que después sean utilizados como muestras de comportamiento y así inferir información psicológica sobre cada persona. ¹⁸⁷ Esto quiere decir – en definitiva –, que la cantidad de datos, el proceso automatizado y las resoluciones a escala puestas en marcha en la vida real, marcan el inicio de un sistema nuevo y con cualidades propias que pueden ser desplegadas en diferentes ámbitos. Dejando con ello en claro, que en su novedad, el poder también se renueva. Por estos motivos, y los mencionados en los diversos ejemplos, la práctica inferencial basada en algoritmos es fruto del cambio de paradigma del Big Data y la Era digital.

3.2 Predicción de comportamiento (Análisis Predictivo)

Pensar en la idea de predicción trae consigo diferentes variantes en su acercamiento. Una de ellas es la concebida desde antaño por lo mágico o misterioso, un espacio que atiende a la necesidad primitiva del hombre por conocer su destino y lo que va irremediamente a pasar en su vida. Predecir algo, es anunciar con seguridad que un acontecimiento sucederá en el futuro ¹⁸⁸ sin ningún impedimento. Esta necesidad de la persona por conocer el futuro, y particularmente el suyo, atiende a esa cualidad antropológica por conocer lo no conocido y

¹⁸⁶ Renaud Lambiotte and Michal Kosinski, “Tracking the Digital Footprints of Personality,” *Proceedings of the IEEE* 102, no. 12 (2014): 1–6, <https://doi.org/10.1109/JPROC.2014.2359054>.

¹⁸⁷ Burr and Cristianini, *Can Machines Read Our Minds?*

¹⁸⁸ Real Academia Española, “Diccionario de La Lengua Española.”

solventar así la caótica inseguridad del porvenir.¹⁸⁹ Otro acercamiento es el que se hace a través de la lectura de los signos de los tiempos, esto es, la interpretación de los signos materiales, meteorológicos y astronómicos que suceden en la historia. Pues son mediante ciertos acontecimientos, que se puede predecir o pronosticar los cambios de clima, estación, y con ello, los tiempos de siembra para la futura alimentación de la comunidad. El descubrimiento de esta capacidad de predicción quedó fundada en la teoría de Newton, en ella el asombro de sus contemporáneos se hizo presente, al saber que la predicción de las posiciones de los planetas con gran antelación, cumplía con los sueños de profetizar el futuro distante y sobre todo, que esto no traspasaba los límites de la capacidad humana.¹⁹⁰ Con este breve preámbulo, podemos darnos cuenta de que la predicción es una actividad realizada desde ya hace mucho tiempo, tal vez más de lo que podamos concebir; actualmente no es la excepción.

La predicción se ha vuelto tan necesaria como cotidiana en la vida de las personas en el siglo XXI, para ello basta ver los pronósticos del clima que se dan hasta por diez días a través de las aplicaciones móviles de los celulares y su utilidad tan relevante para la planificación en diferentes ámbitos de la vida, o bien los pronósticos financieros surgidos desde la teoría económica. Pero ¿qué se necesita para hacer una predicción? Primero habremos de definir el tipo de predicción que aquí nos interesa, a saber, la predicción social o de comportamiento y no la predicción astronómica o física. En otras palabras, la predicción sociológica y de comportamiento nos interesa porque cobra valor dentro del aparato complejo de los sistemas del Big Data en la Era digital.

¹⁸⁹ Arendt, *La Condición Humana*.

¹⁹⁰ Karl R. Popper, *La Miseria Del Historicismo*, 3a ed. (Madrid: Alianza, 2014).

Hagamos también una distinción entre dos tipos de predicciones (y respondamos en parte, a nuestra pregunta anterior): aquellas hechas por la ciencia, como la física o la astronomía, y las predicciones hechas desde y por las ciencias sociales, como lo es la sociología. Las primeras de ellas son guiadas por un método específico. En él, las leyes naturales cobran un valor fundamental, pues dotan al conocimiento con antelación de las condiciones y variables necesarias y suficientes para que suceda cierto acontecimiento. Las segundas, las de las ciencias sociales, son guiadas por un método distinto al científico, puesto que sus fundamentos para dar predicciones son tendencias, repeticiones o modelos que a lo largo de la historia se han ido dando y que guardan cierta relación de paralelismo con aquellos que están sucediendo en el presente, o bien con lo que puede suceder en el futuro.¹⁹¹

Para Popper las predicciones sociales son imposibles, puesto que la sociedad en su conjunto y especificidad no se entiende como una analogía física a la manera de los cuerpos que se rigen por leyes naturales, acá solo existe unicidad en tanto se desarrolla a lo largo de la historia (no se controla). Es decir, bajo las leyes naturales las condiciones suficientes para que un acontecimiento sea en el futuro existen, puesto que estas leyes están basadas en la permanencia constante de la naturaleza, y por tanto controlable, y se puede cuantificar o matematizar, como lo es la ecuación de la ley de la gravedad universal^{XLI}, la cual afirma la imposibilidad de alguna cosa; digamos vagamente, de la no-gravedad. Sin embargo, en las ciencias sociales, no existen leyes universales dado que no hay permanencia constante y las “fuerzas” o “movimientos” sociales son impredecibles, en tanto no se pueden controlar y cuantificar. Existen tendencias, que no son leyes, pero que nos pueden ayudar a relacionar acontecimientos parecidos, más no idénticos. Cada acontecimiento social representa la

¹⁹¹ Popper.

novedad y lo único. Es nuevo dada la unión de diversas fuerzas humanas, que por su cualidad de acción, crean y se renuevan constantemente. Y es único, porque nunca antes de ese acontecimiento había existido uno igual, y nunca después volverá a suceder de la misma manera. Por lo tanto, todo aquello que se pueda decir de un acontecimiento histórico no es más que una proposición histórica singular y específica. Es por eso, que no podemos basar predicciones en la existencia de tendencias.¹⁹²

Sin embargo, y distinto a lo pronunciado por Popper, uno de los fundamentos más importantes de la Era digital, es la cuantificación de cualquier registro humano (dato) y con ello el control sobre las cosas cuantificadas, para luego hacer una predicción. Como sabemos, una de esas “cosas” cuantificadas son – somos – los seres humanos y que después abarca a la sociedad en su totalidad. Tal vez, de una manera casi inconsciente el método para estudiar la sociedad en su conjunto y especificidad por parte de la ciencia de los datos ha seguido un camino inductivo, es decir, se extrae lo particular (los datos personales), para después encontrar lo universal (tendencias políticas, económicas o sociales) que hace que la sociedad sea de una manera u otra.

Ante esto, cabe preguntarnos ¿Qué pasa si lo que era concebido en el pasado como “incuantificable” se convierte en cuantificable? La primera cualidad de lo cuantificable es, que para el conocimiento humano es controlable, tratable, manipulable. No lo cuantificable en sí mismo, sino el acto que se ejerce sobre lo cuantificable para ser tratado dentro de sus posibilidades. Es decir, conocer la temperatura del sol no hace que pueda controlar su temperatura, pero si concebir que el tratamiento de ese conocimiento puede ayudarme a saber que la existencia de la vida humana es imposible a cierta distancia del sol. O bien, saber que

¹⁹² Popper.

las personas religiosas que tienen una alta probabilidad a tendencias ideológicas de tinte nacionalista puedan votar con una alta probabilidad por el candidato republicano o nacionalista, o llevémoslo más allá; saber que las personas que les gusta Mozart o El Señor de los Anillos tienen un alto coeficiente intelectual; y bajo, aquellos que les gusta Jason Aldean o la marca de motocicletas Harley Davidson, nos ayudará a predecir a qué tipo de población dirigir cierta campaña de publicidad en tiempo real, según vayan cambiando los datos, con el fin de obtener mayores ingresos.¹⁹³

Por medio de un estudio, se llegó a la resolución de que la forma en cómo se usa el teléfono celular puede predecir puntuaciones de un examen de habilidades cognitivas, como la memoria y la concentración. Esto se hace usando ciertos rasgos, como la rapidez para escribir en el teléfono y los errores que se cometen, así como la prontitud para desplazarse en la lista de los contactos telefónicos.¹⁹⁴ En estos ejemplos cabe hacer una distinción, el primero de ellos está fundamentado en leyes universales naturales de la física, los siguientes en modelos cuantificables del comportamiento de las personas, y estos a su vez en datos personales (gustos, fobias, religión, movimientos etc.) que hablan de ciertos atributos de la personalidad.

Si bien es cierto, la persona en su cualidad permanente crea; pues está dotada de la acción, cualidad intrínseca del ser humano para sentar un «nuevo comienzo» – es el empezar de nuevo único del ser persona – y del cual nace la libertad.¹⁹⁵ Esto no quiere decir que los modelos de comportamiento ya establecidos por las personas a lo largo de su historia, no se

¹⁹³ Kosinski, Stillwell, and Graepel, “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior.”

¹⁹⁴ Rachel Metz, “The Smartphone App That Can Tell You’re Depressed before You Know It Yourself,” MIT Technology Review, 2018, <https://www.technologyreview.com/s/612266/the-smartphone-app-that-can-tell-youre-depressed-before-you-know-it-yourself/>.

¹⁹⁵ Arendt, *La Promesa de La Política*.

puedan cuantificar. En otras palabras, la novedad intrínseca de la acción del ser persona, no evita ni protege la determinación de los modelos de comportamiento del pasado que definen a una persona. Desde hace ya tiempo y ahora con mayor seguridad, se sabe que las preferencias definen a una persona. Es por eso, que los atributos personales, como son el «género, edad, religión, orientación sexual y tipo de personalidad están relacionados con [la] elección de productos, conceptos y actividades».¹⁹⁶ Y ese es el motivo principal por el cual, las empresas están tan dispuestas a recopilar información personal sobre sus consumidores. Como ya lo habíamos mencionado: «La publicidad es mucho más eficaz cuando se dirige a grupos de personas que tienen más probabilidades de estar interesadas en un producto».¹⁹⁷

Para que ello suceda, el paso de lo analógico a lo digital, de lo cualitativo a lo cuantitativo es imprescindible, es decir, de la narración de fenómenos que pasan en la realidad a registros de información detallada con posibilidades estadísticas y matemáticas. A principios de 2010 se captó la evidencia de este traspaso de poblaciones enteras en el sitio web más popular de aquel tiempo.

Una página de Facebook contiene datos sobre conductas «naturales» en el entorno del hogar, sin las huellas dactilares de un investigador. Se rastrea cada desplazamiento de pantalla, cada movimiento, cada «me gusta». Todo está ahí: matices, intereses, desagradados. Y todo se puede cuantificar. Eso significa que los datos de Facebook han conseguido cada vez una mayor validez ecológica, en el sentido de que no los provocan las preguntas de los investigadores, que inevitablemente inyectan cierto sesgo. En otras palabras, se pueden mantener muchos de los beneficios de la observación pasiva cualitativa que se emplea en antropología o sociología. Además, como muchas interacciones sociales y culturales que ahora quedan capturadas en los datos digitales,

¹⁹⁶ John Bohannon, “Facebook Preferences Predict Personality Traits,” *Science Now*, 2013, 1, <https://doi.org/10.1126/article.26288>.

¹⁹⁷ Bohannon.

podemos añadirles los beneficios de la generalización que se consigue en la investigación cuantitativa.¹⁹⁸

La posibilidad de la predicción en la sociedad está fundamentada en los registros de modelos del comportamiento humano (datos y metadatos) y su forma habitual de desarrollarse en el mundo. Esto quiere decir, que ha existido y existe, un proceso tecnológico de lo cualitativo a lo cuantitativo; del desarrollo de la vida humana en el mundo digital o no (Online u Offline¹⁹⁹), en el cual, a pesar de que la imposibilidad de la exactitud de las predicciones se hace presente, dada su base probabilística, existe su uso verificado en la realidad. Esto es, el proceso por contener la vida humana en datos a llevado a la experimentación y comprobación de un método estadístico y de probabilidad de predicción. Podemos afirmar, por lo tanto y a diferencia de Popper que, las predicciones sociales existen, a partir de su puesta en marcha en el mundo real por las Big Tech y la comprobación de la eficacia de su uso para fines políticos y económicos. Veamos pues, algunos acontecimientos históricos en donde las predicciones hechas por Inteligencia Artificial (IA)^{XLII} a partir de los datos privados y personales de los usuarios de diversas plataformas tecnológicas, han comprobado su funcionamiento e impacto en la sociedad.

3.2.1 El caso Cambridge Analytica

Analicemos el caso de la empresa de análisis de datos Cambridge Analytica (CA) que trabajó con el equipo electoral de Donald Trump y la campaña ganadora del Brexit. Esta empresa «recopiló millones de perfiles de Facebook de votantes estadounidenses, en una de las mayores filtraciones de datos del gigante tecnológico, y los utilizó para construir un

¹⁹⁸ Christopher Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar* (Barcelona: Roca Editorial, 2020), 85.

¹⁹⁹ Floridi, *The Onlife Manifesto. Being Human in a Hyperconnected Era*.

potente programa informático para predecir e influir en las elecciones en las urnas».²⁰⁰ Era propiedad del multimillonario Rober Mercer, dirigida por Steve Bannon, principal asesor de Trump y el Director General era Alexander Nix. La información obtenida en 2014 – sin autorización alguna – fue usada para crear un sistema de IA con la capacidad para elaborar perfiles de personalidad con la finalidad de dirigir anuncios políticos personalizados (micro-targeting).²⁰¹ Christopher Wylie nos lo explica a continuación:

Por medio de él, [micro-targeting o microsegmentación] unos algoritmos de aprendizaje automático asimilaban grandes cantidades de datos acerca de votantes y dividían al electorado en estrechos segmentos; de ese modo, podían predecir qué «votantes individuales» eran a los que más fácil se podía persuadir o aquellos a los que podían hacer entrar en acción en unas elecciones.²⁰²

Wylie es un experto canadiense en análisis de datos que trabajó en CA en el desarrollo del sistema de IA de esta empresa.²⁰³ En 2018 decide denunciar los hechos ocurridos en relación con el uso del «arma psicológica de destrucción masiva»²⁰⁴ utilizada en países como Trinidad y Tobago con la campaña política Do So!, Nigeria, Letonia, así como otras regiones del Caribe, para luego llevarla a las campañas políticas del referéndum en Gran Bretaña en 2014 y las elecciones de Estados Unidos de 2016.²⁰⁵ Wylie ha sostenido en su libro *Mindf*ck: Cambridge Analytica and the Plot to Break America* que Facebook es una amenaza para la

²⁰⁰ Carole Cadwalladr and Emma Graham-Harrison, “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach,” *The Guardian*, 2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

²⁰¹ Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*.

²⁰² Wylie, 20.

²⁰³ Cadwalladr and Graham-Harrison, “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.”

²⁰⁴ Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*, 16.

²⁰⁵ Fleur Jongepier and Michael Klenk, *The Philosophy of Online Manipulation, The Philosophy of Online Manipulation* (New York: Routledge, 2022), <https://doi.org/10.4324/9781003205425>.

seguridad nacional de los Estados Unidos, pues la concentración de poder de la que disfruta este gigante tecnológico es un peligro para la democracia estadounidense.

La forma de proceder para la extracción y recopilación de datos siguió diferentes matices, pero el primer paso definitivo fue el realizado por el académico Aleksandr Kogan a través de su empresa Global Science Research (GSR) en colaboración con CA. Kogan creó la aplicación *thisisyourdigitallife*, y por medio de su empresa, se pagó a 270,000 usuarios de Facebook (de 1 a 2 dólares a cada uno²⁰⁶) con el objetivo de realizar una prueba psicométrica, en la cual cada persona accedía a que se recopilaran sus datos personales para uso académico.²⁰⁷ Después de ello, la aplicación descargaba todos los datos de aquellas personas que eran usuarios de Facebook con el objetivo de encontrar una correlación; por ejemplo, entre los rasgos de personalidad y los “Likes”.²⁰⁸ Aparte de esto, la aplicación recopiló la información de los amigos de Facebook de los participantes en la prueba, sin su conocimiento y autorización. Con lo cual, los datos se multiplicaron de tal manera que Kogan logró elaborar entre 50 y 87 millones de perfiles psicológicos de usuarios de Facebook²⁰⁹, y a pesar de que no se tenía la prueba psicométrica de los sujetos de los datos que no habían hecho la prueba, se apelaba al uso de los “Likes” en Facebook, para luego realizar suposiciones basadas en los estudios hechos con los datos de las personas que si habían hecho la prueba.

Ya dado el primer paso, los científicos de los datos determinaron a las personas en una categoría específica de personalidad. Para ello, se valieron de un análisis factorial en el

²⁰⁶ Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*.

²⁰⁷ Matthew Weaver, “Facebook Scandal: I Am Being Used as Scapegoat – Academic Who Mined Data,” *The Guardian*, 2018, <https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica>.

²⁰⁸ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

²⁰⁹ Cadwalladr and Graham-Harrison, “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach”; Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

que existían cinco factores principales (Big Five Personality Traits²¹⁰ u OCEAN^{XLIII}) con los cuales creaban perfiles de personalidad:

1. *Apertura* (Openness): hace referencia a qué tan abierto se está a nuevas experiencias, ósea a la tendencia de la persona a ser curiosa en el plano intelectual, y creativa y abierta a sensaciones.
2. *Responsabilidad o Consciencia* (Conscientiousness): se refiere a las preferencias respecto a lo planeado o espontáneo y a la tendencia a manifestar autodisciplina, organización y disposición a ejecutar tareas.
3. *Extraversión* (Extraversion): la tendencia de una persona a ser expansiva y enérgica y a encontrar estimulante la compañía de otras.
4. *Afabilidad* (Agreeableness): la calidez, la compasión y la disposición a cooperar; se determina la medida de la sociabilidad de la persona.
5. *Neuroticismo o Inestabilidad emocional* (Neuroticism): clasifica la propensión a experimentar emociones negativas como el enojo o el miedo.²¹¹

Después de haber realizado esta clasificación se aplicaba el algoritmo predictivo al perfil de personalidad para calcular de una escala de 0 a 100 por ciento, qué tan común era que la persona votara o por ejemplo, qué tan probable era que participara en un problema político.²¹² Es justo en este momento, en que la predicción sociológica basada en la probabilidad se hace realidad y se deja atrás las predicciones basadas en tendencias históricas,

²¹⁰ John Bohannon, “Your Computer Knows You Better than Your Friends Do,” *Science*, 2015, 10–12, <https://doi.org/10.1126/science.aaa6329>.

²¹¹ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*; Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Bohannon, “Your Computer Knows You Better than Your Friends Do”; Alexander Nix, “The Power of Big Data and Psychographics” (Concordia Summit, 2018), <https://archive.org/details/CambridgeAnalyticaThePowerOfBigDataAndPsychographics>.

²¹² Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

ahora los modelos de personalidad definen a una persona generándole así una determinación futura. Para Nix está claro que la forma de ver el mundo esta influenciada por los datos demográficos, geográficos y económicos de una persona, pero sobre todo que la personalidad impulsa el comportamiento, y este a su vez influye en las preferencias políticas y de voto. Esto quiere decir, que la comunicación conductual o de comportamiento tiene mayor poder de persuasión. Por ejemplo, para las personas que tenían una personalidad con porcentajes altos en *Responsabilidad o Consciencia y Neuroticismo* el mensaje con mayor efectividad que usaba CA para mostrar apoyo a la segunda enmienda debía apelar a lo racional y basada en el miedo y la emoción, mientras que para el segmento de personas con un alto nivel de *Afabilidad*, el mensaje debía dirigirse apelando a las tradiciones y a la familia incluyendo el proceso de enseñanza de padre a hijo en el uso de armas.²¹³ CA sabía que tomar este tipo de valores hacía la comunicación altamente efectiva y persuasiva.

Luego del paso anterior, Brittany Kaiser menciona en su libro *Targeted: My Inside story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*, que CA analizaba el espacio online donde podría encontrar a la persona real a la cual le había hecho una predicción; podría ser la TV, YouTube, o las redes sociales. Todo esto con la finalidad de mostrar el contenido dirigido a la persona específicamente diseñado basado en el estudio y posterior análisis de la personalidad, es decir el análisis de comportamiento basado en datos personales y privados como, gustos, familia, amigos, trabajo, lugar de vivienda, etc., para luego comprobar la eficacia de sus predicciones y seguir

²¹³ Nix, “The Power of Big Data and Psycographics.”

perfeccionándolas.²¹⁴ El análisis de datos determina el tipo de audiencia al cual dirigir anuncios que apelen a sus valores, personalidades y futuros comportamientos.²¹⁵

Además de esto, CA inició una búsqueda por las vulnerabilidades de la mente de las personas con la finalidad de identificar aquellas con más propensión a ser influenciadas. Para ello, utilizaron la personalidad del *Neuroticismo* y escogieron a las personas que encajaban con los rasgos de personalidad de la «dark triad» (Tríada oscura): Narcisismo, Maquiavelismo (interés propio desproporcionado) y Psicopatía. El objetivo de esto era dirigir a este tipo de personalidades contenido que provocara ira, enojo, odio o que los hiciera sentir atacados. Para ello, se valieron de páginas de blogs, fake pages (páginas web falsas) o bots^{XLIV} que replicaban comentarios incendiarios, irrelevantes u ofensivos en redes sociales.²¹⁶ Y es precisamente este tipo de información y notas falsas, las que apelan a emociones o sentimientos fuertes, como lo son el miedo, desprecio, asco o amenaza; pues según el psicólogo William Brady y el investigador de la Universidad de Nueva York Jay Van Bavel, se calcula que existe un veinte por ciento más de reacciones a las fake news que a las noticias convencionales, a la vez que se difunden seis veces más rápido que una noticia real. A partir de este tipo de emociones, es que se hacen valer los grupos radicales de ultraderecha, racistas, terroristas o de extrema izquierda para ganar adeptos.²¹⁷ Lo cierto es, que las predicciones hechas con tecnología algorítmica dan profecías desde las – permítamele llamarle de esta forma – “leyes del comportamiento humano” con lo cual se extrae cierto

²¹⁴ Brittany Kaiser, *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy* (London: HarperCollins, 2019).

²¹⁵ Nix, “The Power of Big Data and Psycographics.”

²¹⁶ Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*.

²¹⁷ Sonia Ruspini and Thierry Chaminade, “Manipulación y El Poder de Las Emociones,” *DW Documental*, 2022, <https://www.youtube.com/watch?v=RRxJ7U0-G90>.

valor mediante la minería de datos²¹⁸ y tienen influencia en lo público cambiando el mundo real.

Para el Director General de CA la puesta en marcha de este sistema se resumía en tres factores presupuestados por el Big Data.^{XLV} El primero son los factores demográficos y geográficos; estos son, la edad, género, origen étnico, religión, educación, estado socioeconómico y geográfico. El segundo son los factores psicográficos y psicológicos que se refieren a los datos de consumo, actitudinales, estilo de vida, compras, confianza respecto a la economía, así como los datos respecto a compromiso y opiniones políticas. Y el tercero son los factores de personalidad o datos de comportamiento, que son los datos de las resoluciones de personalidad mediante el método OCEAN y las formas de persuasión basadas en la reciprocidad, escasez, autoridad, miedo y la prueba social. Al final lo que se busca encontrar es el móvil que dirige la forma particular de ver el mundo de cada persona: «Si quisiéramos profundizar más, podríamos resolver los datos a nivel individual, donde tenemos cerca de cuatro o cinco mil puntos de datos sobre cada adulto de los Estados Unidos».²¹⁹

A través de este sistema de datos masivos, Nix vislumbra un futuro cada vez más cercano a la comunicación o publicidad dirigida, sintiéndose emocionado por el hecho, de que tal vez sus nietos no se toparán más con la publicidad general, en la que se espera que todas las personas vean la misma publicidad y se sientan atraídas por ella. Ahora la comunicación y publicidad que es recibida a través de diferentes medios es dirigida, no solo

²¹⁸ Edwin León Pluas et al., “Minería de Datos En El Análisis de Tendencias Políticas En Redes Sociales,” *Ciencia Digital* 3, no. 3.4. (2019): 91–103, <https://doi.org/10.33262/cienciadigital.v3i3.4..837>; Henry Fernando Vallejo Ballesteros, Edelmira Guevara Iñiguez, and Segundo Rafael Medina Velasco, “Minería de Datos,” *Recimundo* 2 (2018): 339–49, <https://doi.org/10.26820/recimundo/2.esp.2018.339-349>.

²¹⁹ Nix, “The Power of Big Data and Psycographics.”

con los productos y servicios que más interesan, sino – sobre todo – que es matizada en orden a la manera en cómo cada persona ve el mundo.²²⁰ Esto es lo que Zuboff interpreta como personalización:

La personalización es, una vez más, el eufemismo que abandera a esta generación de productos predictivos manufacturados con la materia prima del yo personal. Estas innovaciones amplían la lógica de otras rondas de desposesión anteriores: se ha ido pasando así del rastreo web al rastreo de la realidad, primero; y al rastreo de la vida, después, para llegar finalmente al *rastreo del yo*.²²¹

Baste decir que las campañas políticas – tanto la campaña presidencial de Trump como la campaña Vote Leave que apoyaba el Brexit – que contrataron el sistema de IA con algoritmos predictivos de Cambridge Analytica tuvieron buenos resultados para su causa. Por si fuera poco, no solo se corrobora el uso de tecnología capaz de inferir y predecir computacionalmente el comportamiento, personalidad y preferencias de las personas, sino que todo este aparato predictivo sociológico se experimenta en el mundo real con la puesta en marcha de los acontecimientos ya mencionados.^{XLVI}

Ciertamente, se puede predecir y crear las condiciones para generar cambios políticos y económicos específicos en el futuro próximo y que no suelen presentarse como singularidades inesperadas; sin embargo, en el caso específico del conocimiento científico aún «no es posible predecir por métodos racionales o científicos, el crecimiento futuro de nuestros conocimientos científicos», y por lo tanto, «no podemos predecir el curso futuro de la historia humana».²²² Con ello la tesis del historicismo que respalda la idea del desarrollo histórico que a su vez a abanderado los movimientos políticos con tintes fascistoides o

²²⁰ Nix.

²²¹ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

²²² Popper, *La Miseria Del Historicismo*, 14.

nacionalistas, cae por su propio peso, y cabría preguntarnos si mediante el camino iniciado por los sistemas de IA la posibilidad de fundamentar al historicismo se abre nuevamente. Esto es, la creación de nuevos relatos que creen un conjunto de opiniones o saberes acerca de la historia humana sin tener en cuenta un orden metafísico.²²³

Por otro lado, cabe decir que las consecuencias para la vida colectiva y política de las sociedades democráticas han sido desastrosas. Carissa Véliz destaca particularmente dos elementos peligrosos. El primero de ellos, destaca, es la diferencia tan dramática en el tipo de contenidos que se muestran a la población, pues son adaptados y diseñados específicamente a la personalidad de cada individuo. Las campañas políticas son personalizadas. Por tal motivo, la experiencia de comunidad es destruida y la generación de diálogo y discusión pública se va perdiendo sin saber exactamente por qué.²²⁴ Es decir, la plaza pública – el ágora –, el fundamento de toda democracia es reemplazada por la realidad online – creada por científicos de datos y alejada del mundo real – y las redes.²²⁵

El segundo elemento es lo peligroso que puede llegar a ser una campaña que no aparenta ser una campaña política. Es decir, a través de la creación de usuarios que no se identifican como creadores de contenido de campaña política sino como usuarios ordinarios, y que comparten artículos de noticias que aparecen sin referencia alguna a cierta campaña, pero que en el fondo toman partido mediante esa noticia. Es crear las condiciones mediáticas de una campaña política sin que un claro representante tome la batuta, con lo que ocasiona que la decisión del electorado sea sesgada y sin ningún debate serio que le ayude a profundizar más su postura. Bajo este mismo tenor cabe hablar de lo atractivo que puede ser

²²³ Jean-François Lyotard, *La Condición Postmoderna*, (Buenos Aires: Cátedra, 1987).

²²⁴ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

²²⁵ Wylie, *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*.

Facebook como objeto de estudio social; ya que generalmente existe cierta naturalidad y transparencia en las actividades de las personas con la plataforma. Con ello, lo que se trata de decir es que los perfiles de Facebook no son autorretratos idealizados, más bien reflejan la personalidad real del usuario, y es la actuación cotidiana de las personas lo que hace que los datos ahí recopilados hablen efectivamente de su vida real.²²⁶ Facebook ha sido un experto en difundir noticias falsas y generar polarización en la sociedad, es así que ha influido en las elecciones de Trump, Bolsonaro y el referéndum para la separación del Reino Unido de la Unión Europea. Con el uso del método del dirigente nazi Gobbels: «una mentira repetida mil veces se convierte en una verdad» es que nuestros gobiernos y democracias han perdido un espacio de comunidad verdadera que propicie el diálogo.²²⁷

3.2.2 Conocimiento y Poder

Otro elemento que podemos agregar – y el de mayor importancia en este trabajo – es la asimetría tan pronunciada de conocimiento y poder entre las empresas poseedoras de datos y los sujetos de los datos, pues resulta ser un agregado esencial para la efectividad de los medios de modificación de comportamiento, y es por ello por lo que su relevancia es determinada por el peligro que puede y ha generado para las sociedades. Para Wylie, es claro que a través del modelo de análisis de personalidad y la predicción política generada por algoritmos, la que él llama la «guerra de la información», trae consigo una grave problemática:

²²⁶ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*; Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

²²⁷ Alexandra Argüelles and Brenda Battaglia, *Violencia Digital En México: El Estado vs La Sociedad Civil* (México: Malpaís, 2021).

Creo que es peor que acosar, pues la gente no sabe necesariamente lo que se le está haciendo. Al menos, el acoso es respetuoso con la capacidad del acosado para reaccionar y actuar, porque este sabe de qué está siendo objeto, [...] pero si tú no respetas la capacidad de acción de las personas, todo lo que hagas a partir de ese punto ya no puede incidir en beneficio de una democracia. En esencia, la guerra de la información no es nada propicia a la democracia.²²⁸

En el caso de Cambridge Analytica, como en otros paralelos a éste, el poder está fundamentado en los datos personales. Es decir, el poder de los gigantes tecnológicos emerge de los datos de las personas, que a su vez son extraídos de la privacidad, ese espacio donde cualquier tipo de intervención altera nuestra capacidad de decisión en libertad y autonomía.²²⁹ Ahora los gobiernos, partidos, corporaciones y demás organismos con poder de los datos tienen los mecanismos —en forma de redes y algoritmos— para que una noticia, o mejor aún, una noticia falsa, llegue personalizada a cada grupo o persona y se repita ampliamente.²³⁰ Con la irrupción de esta tecnología «los ordenadores sobrepasan a los humanos en juicios de personalidad; algo que presenta unas oportunidades y desafíos significativos en las áreas de la evaluación psicológica, el marketing y la privacidad».²³¹ La incapacidad de la acción política de la sociedad al no saber lo que se está o estaba haciendo con el uso de sus datos personales, o peor aún, el desconocimiento total o parcial de la recopilación de datos personales, demuestra lo peligroso que puede llegar a ser este sistema para las democracias liberales. No cabe la menor duda que lo que en el pasado «tradicionalmente se evaluaba

²²⁸ Carole Cadwalladr, “‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower,” *The Guardian*, 2018, <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.

²²⁹ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

²³⁰ Argüelles and Battaglia, *Violencia Digital En México: El Estado vs La Sociedad Civil*.

²³¹ Bohannon, “Your Computer Knows You Better than Your Friends Do.”

laboriosamente de forma individual puede deducirse automáticamente para millones de personas sin que se den cuenta [...] lo cual es sorprendente y a la vez da un poco de miedo».²³²

Cabría preguntarnos si hemos llegado al momento histórico en el que la sociología, psicología, antropología y otras ramas que estudian al ser humano han tenido el éxito suficiente para proporcionarnos una «presciencia» (conocimiento de las cosas futuras) política con validez científica. Probablemente nuestra respuesta sea afirmativa, y por tal motivo es que cobra un gran valor para los políticos, y no justamente para aquellos con sentido democrático del destino histórico.²³³

El desenlace de este caso termina con el cierre de esta empresa, tras los cuestionamientos éticos y legales sobre sus prácticas comerciales y políticas²³⁴, a la vez que dejaba mal posicionado a Facebook luego de que la Oficina del Comisionado de Información (ICO por sus siglas en inglés) en Gran Bretaña le impuso una multa de 500,000 libras por su papel en el escándalo de los datos de Cambridge Analytica.²³⁵ Este caso aquí analizado no es esporádico o único, en el mundo existen otras empresas como Cambridge Analytica que siguen expandiéndose. Esto lo comprueba un estudio realizado por TacticalTech en 2018, en el cual se identificaron 329 organizaciones alrededor del mundo trabajando con partidos políticos a través de campañas basadas en datos personales.²³⁶ De la misma manera que las grandes empresas tecnológicas por sí mismas siguen utilizando los anuncios personalizados

²³² Bohannon, “Facebook Preferences Predict Personality Traits.”

²³³ Popper, *La Miseria Del Historicismo*.

²³⁴ Andrew Prokop, “Cambridge Analytica Shutting down: The Firm’s Many Scandals, Explained,” *Vox*, 2018, <https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller>.

²³⁵ BBC, “Facebook Fined £500,000 for Cambridge Analytica Scandal,” *BBC*, 2018, https://www.bbc.com/news/technology-45976300?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-data-scandal&link_location=live-reporting-story.

²³⁶ Amber Macintyre, “Who’s Working for Your Vote?,” *Tactical Tech*, 2018, <https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote/>.

para sacar el mayor provecho económico de ellos. A este mecanismo de extracción, recopilación y uso de datos para su uso comercial o político algunos autores le llaman economía de los datos y otros capitalismo de la vigilancia.²³⁷ El peligro sigue latente y nuestras democracias no apuntan precisamente a un buen destino.

En resumen, podemos dejar en claro que las capacidades de predicción de un sistema algorítmico de Inteligencia Artificial basadas en perfiles de personalidad mediante el uso de los datos personales recopilados en tiempo real hacen posible la violación del derecho a la privacidad con el único objetivo de dirigir anuncios comerciales o políticos personalizados,²³⁸ es un producto de la Era Digital y el Big Data, una nueva y distinta forma de poder nunca antes vista en la historia de la humanidad. A parte de esta capacidad de predicción, existe una cualidad que crea nuevos horizontes históricos, cambiando o distorsionando la realidad. Esta es la capacidad de manipulación, de la cual hemos dado ciertos atisbos, pero cabe detenernos en la comprensión del rol que juega en este entramado social y digital.

3.3 Manipulación política

Primeramente hagamos una distinción entre dos conceptos: manipulación e influencia. Pues parece que pueden tomarse como sinónimos o ideas que se dirigen a lo mismo, para ello vayamos al significado propio del verbo.

²³⁷ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*; Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

²³⁸ Jongepier and Klenk, *Philos. Online Manip.*

Manipular: «Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc. con distorsión de la verdad y la justicia, y al servicio de intereses particulares».²³⁹

Influir: «Dicho de una persona o de una cosa: Ejercer predominio, o fuerza moral».²⁴⁰

Páginas anteriores tomamos como ejemplo el sol para reconocer la cualidad primera de lo cuantificable. En él dábamos a comprender que el conocimiento cuantificable de una cosa nos da cierto control sobre ella, es decir, el acto que se da sobre lo cuantificable para ser tratado dentro de sus posibilidades. La manipulación en este caso es tomada como acto seguido al control, puesto que al tener el conocimiento cuantificable del sol, se abre la posibilidad para manipular o intervenir ese conocimiento a conveniencia. Es aquí donde se encuentra el punto crucial de diferencia con la influencia. Influir es mostrar “fuerza” sobre algo sin más, es saber que dicho predominio está predispuesto por condiciones *a priori* al conocimiento de algo o alguien. Por el contrario, la manipulación necesita del conocimiento de algo o alguien para dar paso a la acción, es decir, necesita condiciones *a posteriori* al conocimiento para crear nuevas condiciones que le abran paso a creaciones y experiencias significativas. Por ejemplo, el agente J puede ser influenciado en decisiones políticas o económicas por P, con quien guarda una relación de hijo, o por A, quien es su jefe directo en la empresa donde labora, pero difícilmente será influenciado por K, quien atiende los abarrotes en la esquina de su casa. Por otro lado, para que J pueda ser manipulado en sus decisiones políticas o económicas, bastaría que tanto P, A o K, conocieran algún rasgo particular o tipo de comportamiento habitual respecto a sus decisiones políticas o económicas, para que mediante el uso de este conocimiento hicieran cambiar de opinión o

²³⁹ Real Academia Española, “Diccionario de La Lengua Española.”

²⁴⁰ Real Academia Española.

decisión a J a conveniencia. Influir y manipular no son lo mismo, aunque en la práctica puedan confundirse con mucha facilidad. En el caso de las empresas tecnológicas podemos decir, que a través de su poderío tecnológico influyen en la compra y usos de sus productos y servicios, para luego manipular mediante el uso de contenido emocional a sus usuarios bajo sus intereses. Esta condición permite, incluso, que se susciten actos de corrupción, en el sentido de una relación de desequilibrio en donde un elemento se encuentra en condiciones de dominio o preponderancia respecto al otro.²⁴¹ Es «el desequilibrio que altera inmoral e ilegalmente la política y la economía de un contexto, con el objetivo de [imposición o dominación de] una de las partes que componen la relación entre un particular (o conjunto de particulares) y un sistema».²⁴²

Ahora bien, en este apartado nos interesa la manipulación, en particular la que se lleva a cabo en la política. Podemos decir que este tipo de accionar político es muy antiguo. Ya desde los tiempos de la conquista territorial se tenía como mote el: *Divide et impera*; “Divide y vencerás” o conquistarás (de dudoso origen, atribuida al dictador y emperador romano Julio César²⁴³). Haciendo referencia a que la manipulación para crear peleas o discusiones en las comunidades que se querían conquistar daba como resultado la división de esta, con lo cual era mucho más sencillo vencer al adversario lleno de confusión, odio y miedo. Y es de la misma manera que este mote sigue haciéndose presente en las prácticas de las Big Tech. Como ya lo vimos, existen mecanismos de IA mediante los cuales se generan noticias y

²⁴¹ José Luis Cisneros Arellano, “La Asesoría y La Consultoría Filosófica Frente a La Corrupción,” in *Humanidades Inter y Transdisciplinarias En Contextos de Incertidumbre: Nuevas Ideas, Nuevos Enfoques, Nuevos Temas.*, ed. Ludivina Cantú Ortiz (Monterrey: Facultad de Filosofía y Letras, UANL, 2021), 865–90.

²⁴² Cisneros Arellano, 877–78.

²⁴³ Juan Perea, “Divide y Vencerás, Una Estrategia Política Generalizada,” *El Confidencial*, December 2, 2014, https://www.elconfidencial.com/alma-corazon-vida/2011-09-30/divide-y-venceras-una-estrategia-politica-generalizada_522447/.

anuncios con ideales, gustos o preferencias personalizadas, sin que por ello signifique que están dentro del mundo real y existen realmente.

Esto quiere decir, que la personalización de las noticias y anuncios usadas en las plataformas, crean una especie de cámara de eco en la que resuena únicamente la personalización propia. De tal manera, que la determinación de la persona que se va creando, fundamentada en lo propio, genera un condicionamiento en la información que se va alimentando permanentemente en tiempo real, para la única y exclusiva satisfacción de la persona, y así obtener su atención por más tiempo, traducándose en mayores ganancias para la plataforma.²⁴⁴ Por tal motivo, la información que se recibe es segmentada, a partir de las intenciones o conveniencia de quienes tengan en su poder la capacidad de decisión. Es por eso, que las intenciones por crear un diálogo abierto, respetuoso y equitativo en estos tiempos se vuelve casi imposible, pues no existe una realidad común, cada persona se ve alimentada con información diversa, contraria o falsa. En otras palabras, los usuarios de los gigantes tecnológicos estamos a merced de las intenciones de manipulación de los dirigentes de tales empresas. La manipulación política y económica apela siempre a la emoción, sea cual sea ésta. Así es como funciona el neuromarketing, las noticias falsas y la videovigilancia.²⁴⁵

Por si fuera poco, las emociones pueden ser contagiosas a partir del sentimiento general de empatía. Así lo comprobó un estudio titulado: “Experimental evidence of massive-scale emotional contagion through social network”, en el cual se manipuló la manera en que

²⁴⁴ Pariser, *El Filtro Burbúja: Cómo La Red Decide Lo Que Leemos y Lo Que Pensamos*.

²⁴⁵ Frederik J. Zuiderveen et al., “Online Political Microtargeting: Promises and Threats for Democracy,” *Utrecht Law Review* 14, no. 1 (2018): 82–96, <https://doi.org/10.18352/ulr.420>; Alan Ware, “The Concept of Manipulation: Its Relation to Democracy and Power,” *British Journal of Political Science* 11, no. 2 (1981): 163–81, <https://doi.org/10.1017/S0007123400002556>; Ruspini and Chaminade, “Manipulación y El Poder de Las Emociones”; Jessica Dawson, “Microtargeting as Information Warfare,” *The Cyber Defense Review* 6, no. 1 (2021): 63–80.

se expuso a personas a expresiones emocionales en su sección de NewsFeed en Facebook. Por un lado, un grupo estuvo expuesto a mensajes mayormente positivos, mientras que otro a mensajes predominantemente negativos. Con esto se comprobó que bastaba la exposición a información con contenido emocional predominante para que las personas cambiaran su propia conducta en sus publicaciones, a la vez que se corroboraba que el funcionamiento indetectable e incontestable de Facebook iba más allá de las pantallas de los dispositivos y entraba en la vida diaria de sus usuarios. Con lo que probable y previsiblemente, se accionaban unas determinadas cualidades de expresión emocional mediante procesos que funcionan más allá de la consciencia de las personas.²⁴⁶ Los investigadores concluyeron los siguiente:

Los estados emocionales pueden transferirse a otros individuos por contagio emocional, haciendo así que las personas experimenten las mismas emociones sin ser conscientes de ello. Los mensajes en línea influyen en nuestra experiencia emocional, lo que puede afectar a diversos comportamientos en el mundo no digital. [Esta es] una de las primeras pruebas experimentales que corroboran la controvertida tesis de que las emociones pueden propagarse a través de una red digital.²⁴⁷

Este tipo de investigaciones y las realizadas por las ciencias del comportamiento que se especializan en saber «cómo las emociones de una persona pueden influir al prójimo y afectar al grupo»,²⁴⁸ abonan aún más a nuestra concepción de manipulación a través de emociones mediante el uso de los productos y servicios de los gigantes tecnológicos.²⁴⁹ Es

²⁴⁶ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Adam D.I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, “Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks,” *Proceedings of the National Academy of Sciences of the United States of America* 111, no. 24 (2014): 8788–90, <https://doi.org/10.1073/pnas.1320040111>.

²⁴⁷ Kramer, Guillory, and Hancock, “Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks.”

²⁴⁸ Ruspini and Chaminade, “Manipulación y El Poder de Las Emociones.”

²⁴⁹ Cass R. Sunstein, “The Age of Behavioral Science,” in *The Ethics of Influence* (Cambridge University Press, 2016), 1–17, <https://doi.org/10.1017/cbo9781316493021.001>.

conocido, por ejemplo, que el uso de contenido visual (video o fotografías) impulsa un mayor uso y popularidad de la información, y por ende de la red social que lo replica.²⁵⁰ Pues se sabe que las emociones o sentimientos a través de imágenes en la comunicación generan un mayor impacto. Es por eso, que las técnicas computacionales para analizar los intercambios sociales en línea han desarrollado tareas específicas, como el análisis de sentimientos, la captura de estados de ánimo, el reconocimiento de emociones y la minería de opiniones.²⁵¹ El interés por conocer las emociones que desencadenan los contenidos ya sean visuales o escritos, proviene del reconocimiento de que la emoción impulsa la toma de decisiones. Esto significa, que las emociones que desencadenan el comportamiento son un componente clave de la inteligencia.²⁵² Sin embargo, y aunque el factor mencionado parezca determinante, el fenómeno que abre la posibilidad a la manipulación política es la asimetría de conocimiento, y por lo tanto de poder.

Regresemos al ejemplo del agente J, y recordemos que el factor determinante que suscitaba la manipulación por parte de P, A o K era el conocimiento, particularmente el de los rasgos de su personalidad o su forma habitual de comportamiento. Conocer algo, sea una persona, una cosa, un animal, un planeta, da cierto control sobre ello. Pero conocer algo de forma cuantitativa da un control aun mayor, dado que se puede medir y estimar movimientos o fuerzas. Si se busca que la manipulación política sea efectiva sobre cierta población es necesario su conocimiento emocional cuantitativo predominante, que definirá la predicción

²⁵⁰ Michelle Henning, "That Liking Feeling : Mood , Emotion , and Social Media Photography," in *Ubiquity. Photography's Multitudes*, ed. Jacob W. Lewis and Kyle Parry (Leuven University Press, 2021), <https://www.jstor.org/stable/j.ctv24cnspsz.15>.

²⁵¹ Klaus R Scherer, Tanja Banziger, and Etienne B Roesch, *Blueprint for Affective Computing: A Sourcebook, Series in Affective Science*, 2010.

²⁵² Mark Andrejevic, *Infoglut: How Too Much Information Is Changing the Way We Think and Know* (New York: Routledge, 2013), <https://doi.org/10.4324/9780203075319>.

del tipo de personalidad. Con ese conocimiento se puede medir la probabilidad estimada de votantes, el tipo de anuncios dirigidos que pueden tener mayor efectividad, así como la configuración de la figura política en orden a satisfacer las necesidades íntimas de la población. En otras palabras, la manipulación política crea una experiencia de control sobre la población, y esto a su vez da un sentido de orden frente a la disonancia democrática, bastante ambicionado por los grupos radicales o extremistas, como los de ultraderecha. Las emociones de la población, aunque son importantes, cobran un sentido más de guía para la creación de ambientes propicios a conveniencia. Con esto, lo que se trata de decir, es que a raíz de la invasión de la privacidad se extrae un nuevo conocimiento fundamentado en los datos de comportamiento y emociones, que son esenciales en la conformación de la identidad de las personas, para luego implementar nuevas medidas inferenciales, predictivas y de manipulación social, política y económica, con la única finalidad de generar nuevos valores (*insights*) que se puedan ofrecer a los anunciantes o partidos políticos, los cuales se traducen en beneficios económicos, políticos y sociales para los gigantes tecnológicos.²⁵³

Dentro de la política, y particularmente en el momento de tomar una decisión en las elecciones, Romain Bouvet de la Universidad de Toulouse lo tiene claro: «La elección por un candidato es algo puramente emocional», pues para él, como seres bastante irracionales que pocas veces toman una decisión política informada y sopesada en el diálogo y discusión con los demás. Es por eso, que las emociones toman un papel determinante en la formación de

²⁵³ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*; Sian Brooke and Carissa Véliz, “Data, Privacy and the Individual,” *Center for the Governance of Change*, vol. 1 (Madrid, 2020); Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Jongepier and Klenk, *Philos. Online Manip.*; Zuiderveen et al., “Online Political Microtargeting: Promises and Threats for Democracy”; Brahim Zarouali et al., “Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media,” *Communication Research*, 2020, <https://doi.org/10.1177/0093650220961965>; Vallejo Ballesteros, Guevara Iñiguez, and Medina Velasco, “Minería de Datos.”

una opinión política, la cual es influenciada por el que mejor maneje los puntos débiles del cerebro.²⁵⁴ Cuanto más se revela el yo, mayor puede ser la manipulación a través de las emociones. En otras palabras, la manipulación solo puede ser llevada a cabo mediante la asimetría de conocimiento, que ha provocado una asimetría de poder. El funcionamiento real de los sistemas de IA, las acciones tomadas por los científicos de los datos o sus principios éticos son en su gran mayoría desconocidos para la población. Contrario al amplio y basto conocimiento que hemos visto que tienen las empresas tecnológicas acerca de las personas. Podemos decir – junto con Véliz –, que el conocimiento de los datos personales y privados de las personas es un nuevo poder ostentado por las empresas tecnológicas y/o gobiernos capaz de predecir y manipular el comportamiento humano. El conocimiento, por lo tanto, es poder.²⁵⁵

Por otro lado, no hemos de olvidar las implicaciones que la manipulación de emociones tiene en la vida personal de cada ser humano, y particularmente en su salud mental. Aunque en este trabajo no profundizaremos en los riesgos que trae consigo este tipo de poder, vale la pena mencionar algunos de ellos.

3.4 Impactos a la salud mental

En la Era Digital es casi imposible desarrollarse individualmente sin algún dispositivo tecnológico, ya sea un ordenador portátil, un smartphone o un asistente digital. Estos dispositivos son requeridos para hacer tareas diarias en el trabajo, escuela o simplemente para

²⁵⁴ Ruspini and Chaminade, “Manipulación y El Poder de Las Emociones.”

²⁵⁵ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*; Carissa Véliz, “The Internet and Privacy,” *Ethics and the Contemporary World*, no. January 2018 (2019): 149–59, <https://doi.org/10.4324/9781315107752-12>; Ruspini and Chaminade, “Manipulación y El Poder de Las Emociones.”

el ocio. Han sido creados para mantener a los individuos ocupados en cualquier situación, y atraer a las personas para que pasen horas de su día concentradas en pantallas tan pequeñas como las palmas de su mano, escribiendo, leyendo o jugando.²⁵⁶ Pero ¿cómo afecta el uso de estos dispositivos social y psicológicamente a las personas?²⁵⁷ Por ahora, tal vez alcancemos a vislumbrar los que ya hemos dilucidado, como el odio generalizado, la falta de espacios propicios para el diálogo, la toma de decisiones políticas basadas en información falsa o distorsionada, entre otros. Sin embargo, en el plano personal entran en juego la propia identidad, intimidad, personalidad, desarrollo humano, y como fundamento de todo ello, la salud mental.

Empecemos por nombrar las problemáticas que trae consigo el solo uso de las tecnologías de la información y la comunicación (TIC) y de una forma particular el uso de los dispositivos móviles y las aplicaciones de ocio, como redes sociales o de juego. En un estudio se exploró la relación entre el uso de Internet y del teléfono móvil y la salud mental. En él se observó una fuerte relación positiva entre el deterioro de la salud mental y el uso problemático de las TIC, especialmente cuando las personas recurrían a ellas para evitar experiencias o sentimientos negativos.²⁵⁸ Un gran número de estudios que intentan encontrar una asociación de correlación entre el detrimento de la salud mental y el uso de las TIC, mencionan principalmente tres problemáticas: Ansiedad^{XLVII}, Depresión y Adicción. Exploremos el primero de ellos.

²⁵⁶ Josefa Ros Velasco and S. Gutiérrez Manjón, “The Expression of Boredom and Unwanted Loneliness on Twitch,” *Icono 20*, no. 1 (2022).

²⁵⁷ Tayana Panova and Alejandro Lleras, “Avoidance or Boredom: Negative Mental Health Outcomes Associated with Use of Information and Communication Technologies Depend on Users’ Motivations,” *Computers in Human Behavior* 58 (2016): 249–58, <https://doi.org/10.1016/j.chb.2015.12.062>.

²⁵⁸ Panova and Lleras.

En una investigación se descubrió que el 45% de los adultos británicos indicaron que se sienten preocupados o incómodos cuando no pueden acceder a su correo electrónico o a los sitios de las redes sociales.²⁵⁹ En otro estudio se descubrió que las generaciones más jóvenes revisan con una frecuencia de cada hora, 15 minutos o todo el tiempo, sus mensajes y redes sociales; y cuando no lo podían hacer se volvían más ansiosas.²⁶⁰ Por si fuera poco, se ha acuñado un término médico a una problemática de este tipo de ansiedad: El síndrome de la vibración fantasma. Este se define como la vibración percibida de un teléfono móvil que no está vibrando. Se ha encontrado que un gran número de personas lo han percibido.²⁶¹ Este síndrome solo es el reflejo de la ansiedad que provocan los teléfonos móviles sobre las personas que están obsesionados con el control de sus redes sociales y mensajes.²⁶² Esta misma ansiedad tiene otra forma de hacerse visible a través del concepto de *Fear of Missing Out* (miedo a perderse algo), popularmente conocido como FoMO. Definido como un temor generalizado o sensación incómoda, y a veces agobiante a que otros puedan estar viviendo experiencias gratificantes de las que uno está ausente; o que ellos poseen más o algo mejor que uno mismo. El FoMO se caracteriza por el deseo de estar continuamente conectado con lo que hacen los demás.²⁶³ Esta aflicción está asociada con un estado de ánimo negativo y un nivel de satisfacción de vida bajo. Investigadores lo identifican con un comportamiento

²⁵⁹ Anxiety UK, “Anxiety UK Study Finds Technology Can Increase Anxiety,” 2012, <http://www.anxietyuk.org.uk/2012/07/for-some-with-anxiety-technology-can-increase-anxiety/>.

²⁶⁰ L. D. Rosen et al., “Is Facebook Creating ‘IDisorders’? The Link between Clinical Symptoms of Psychiatric Disorders and Technology Use, Attitudes and Anxiety,” *Computers in Human Behavior* 29, no. 3 (2013): 1243–54, <https://doi.org/10.1016/j.chb.2012.11.012>.

²⁶¹ Michelle Drouin, Daren H. Kaiser, and Daniel A. Miller, “Phantom Vibrations among Undergraduates: Prevalence and Associated Psychological Characteristics,” *Computers in Human Behavior* 28, no. 4 (2012): 1490–96, <https://doi.org/10.1016/j.chb.2012.03.013>.

²⁶² Amelia Strickland, “Exploring the Effect of Social Media Use on the Mental Health on Young Adults,” *Stars* (University of Central Florida, 2014).

²⁶³ Andrew K. Przybylski et al., “Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out,” *Computers in Human Behavior* 29, no. 4 (2013): 1841–48, <https://doi.org/10.1016/j.chb.2013.02.014>.

compulsivo que tiene la intención de producir cierto alivio en la confianza o seguridad social, pero lo que ocasiona es una generación de más ansiedad.²⁶⁴

También, se ha demostrado que un alto grado de interacción con el teléfono móvil e Internet está relacionado con niveles más altos de ansiedad, especialmente cuando la interacción se basa en texto en lugar del uso de llamadas.²⁶⁵ Esto sucede, dado que la «naturaleza unidimensional de los mensajes de texto es menos agotadora desde el punto de vista cognitivo y emocional, que el comportamiento más comprometido de las llamadas de voz, por lo que parece más atractiva para los individuos ansiosos».²⁶⁶ Por ese motivo, los participantes ansiosos de las investigaciones se sentían más cómodos enviando mensajes de texto que teniendo interacciones en la vida real.²⁶⁷

Podemos darnos cuenta de la existencia de dos variantes. En la primera, las personas que son ansiosas se vuelven aún más ansiosas con el uso de las TIC, mientras que en la segunda las personas que no tenían ansiedad se vuelven ansiosas por el uso de las TIC. Sea cual sea el caso, el hecho es que una alta interacción con los dispositivos y servicios que prestan provoca ansiedad en las personas. Vayamos ahora a revisar la correlación que existe con la depresión.^{XLVIII}

²⁶⁴ Jon D. Elhai et al., “Fear of Missing out, Need for Touch, Anxiety and Depression Are Related to Problematic Smartphone Use,” *Computers in Human Behavior* 63 (2016): 509–16, <https://doi.org/10.1016/j.chb.2016.05.079>.

²⁶⁵ Panova and Lleras, “Avoidance or Boredom: Negative Mental Health Outcomes Associated with Use of Information and Communication Technologies Depend on Users’ Motivations.”

²⁶⁶ N. Park, Y. Hwang, and E. Huh, “Exploring Problematic Mobile Phone Use: Relationships between Adolescents’ Characteristics and Mobile Phone Addiction,” *In Trabajo Presentado En El Annual Meeting of the International Communication Association, Suntec Singapore International Convention & Exhibition Centre*, 2010.

²⁶⁷ Donna J. Reid and Fraser J.M. Reid, “Text or Talk? Social Anxiety, Loneliness, and Divergent Preferences for Cell Phone Use,” *Cyberpsychology and Behavior* 10, no. 3 (2007): 424–35, <https://doi.org/10.1089/cpb.2006.9936>.

Se ha descubierto que el uso del teléfono móvil estaba asociado a la depresión y el uso de drogas permitidas como el tabaco y el alcohol.²⁶⁸ Otro estudio encontró, entre múltiples factores, que el uso del teléfono móvil mostraba una relación significativa con la depresión, los trastornos del sueño y el estrés actual.²⁶⁹ Es posible que aquellas personas con depresión utilicen con mayor frecuencia las redes sociales para tratar de buscar alguna ayuda o alivio con la cual afrontar su situación, sin embargo se ha encontrado que existe una relación entre el estrés y un número elevado de mensajes de texto que da como resultado un menor bienestar emocional,²⁷⁰ a la vez que no existe correlación entre la frecuencia del uso de teléfono móvil y el apoyo social o emocional que puede percibir la persona que así lo requiera.²⁷¹ Se ha descubierto también, que las personas que pasan más tiempo en las redes sociales y realizan más gestiones de imagen en Facebook tienen síntomas clínicos de depresión.²⁷²

Lamentablemente, se ha comprobado que los investigadores de Instagram descubrieron que su aplicación era perjudicial para la salud mental de un porcentaje considerable de jóvenes, sobre todo adolescentes, aumentando los casos de depresión. Sin embargo, Facebook la empresa propietaria de Instagram, ha restado importancia a estos

²⁶⁸ Mercedes Sánchez-Martínez and Angel Otero, “Factors Associated with Cell Phone Use in Adolescents in the Community of Madrid (Spain),” *Cyberpsychology and Behavior* 12, no. 2 (2009): 131–37, <https://doi.org/10.1089/cpb.2008.0164>.

²⁶⁹ Sara Thomée et al., “Prevalence of Perceived Stress, Symptoms of Depression and Sleep Disturbances in Relation to Information and Communication Technology (ICT) Use among Young Adults - an Explorative Prospective Study,” *Computers in Human Behavior* 23, no. 3 (2007): 1300–1321, <https://doi.org/10.1016/j.chb.2004.12.007>.

²⁷⁰ Karla Klein Murdock, “Texting While Stressed: Implications for Students’ Burnout, Sleep, and Well-Being,” *Psychology of Popular Media Culture* 2, no. 4 (2013): 207–21, <https://doi.org/10.1037/ppm0000012>.

²⁷¹ Thomée et al., “Prevalence of Perceived Stress, Symptoms of Depression and Sleep Disturbances in Relation to Information and Communication Technology (ICT) Use among Young Adults - an Explorative Prospective Study”; Strickland, “Exploring the Effect of Social Media Use on the Mental Health on Young Adults.”

²⁷² Rosen et al., “Is Facebook Creating ‘IDisorders’? The Link between Clinical Symptoms of Psychiatric Disorders and Technology Use, Attitudes and Anxiety.”

efectos negativos.²⁷³ Esto lo corroboró un documento confidencial de Facebook de 2017 publicado por el periódico *The Australian*. Era un escrito de ejecutivos de la compañía y dirigido a los clientes anunciantes australianos y neozelandeses, en el cual se describía cómo los sistemas eran capaces de recabar averiguaciones psicológicas sobre 6.4 millones de jóvenes de esos países, principalmente de educación secundaria y superior. A través del conocimiento emocional y de comportamiento con la monitorización de publicaciones, fotos, interacciones y actividad en Internet, que se calculaba cuándo los jóvenes se sentían estresados, derrotados, abrumados, preocupados, nerviosos, estúpidos, ridículos, inútiles y fracasados. De tal manera, que se sabía el momento preciso en el que un joven necesitaba un aluvión de confianza, y por lo tanto, era más vulnerable a una configuración determinada de persuasiones publicitarias.²⁷⁴ Las emociones negativas que provocan depresión son moneda de cambio para las tecnológicas y sus anunciantes. Tanto la ansiedad como la depresión son dos enfermedades mentales que tienen propensiones suicidas y no se le da la debida importancia. El régimen de poder de los datos personales tiene como valor primordial la mayor extracción de beneficios a costa de la vida privada, íntima y mental de las personas.

Ahora hablemos del concepto que abre una nueva realidad para los investigadores en la salud mental: la adicción^{XLIX} a las tecnologías de la información y comunicación. Este tipo de dependencia guarda en sí misma un fenómeno único. Esta adicción se crea y se alimenta de la curiosidad de las personas por saber; y aunque parece ser un principio muy loable, la creación de mecanismos de IA basada en el análisis de la personalidad con el objetivo de que

²⁷³ A Wall Street Journal Investigation, "The Facebook Files," Wall Street Journal, 2021, <https://www.wsj.com/articles/the-facebook-files-11631713039>; McNamee, "Facebook Will Not Fix Itself."

²⁷⁴ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

las personas duren más tiempo en las plataformas o redes sociales sin que ellas apenas se den cuenta, muestra todo lo contrario.

El uso excesivo de las plataformas y redes sociales es usado por las personas para reducir los sentimientos negativos y con ello modificar el estado de ánimo, o bien eliminar el aburrimiento,²⁷⁵ este funcionamiento se vuelve placentero y llega a ser necesario para el disfrute diario. Si esto no sucediera o se impidiera, se sufre de angustia o ansiedad, y se abre la posibilidad de que ello llegue a causar daños en otras áreas de la vida.

«Los estudios señalan que el trasfondo teórico de las necesidades psicológicas innatas de autosuficiencia, determinación, realización, autonomía, reconocimiento, relación y entretenimiento son las principales fuerzas intrínsecas que impulsan a los individuos a participar en diversas actividades».²⁷⁶ Con lo cual, se abre la reflexión acerca de qué tanto la influencia de las redes sociales y su adicción hace satisfacer estas necesidades psicológicas innatas. La realidad también apela a que las personas parecen ser menos vulnerables a estresarse en situaciones que provocan ansiedad cuando tienen acceso a sus TIC, lo que provoca que su uso se vea reforzado. Sin embargo, al terminar recurriendo al uso de estas tecnologías como estrategia de evasión emocional, el patrón se refuerza y puede conducir a problemas de salud mental o agravarlos a largo plazo.²⁷⁷

Se convierte en un círculo casi imposible de salir: La personalización y funcionalidad seduce a un mayor uso de las TIC, esto a su vez provoca ansiedad por FoMO o por el

²⁷⁵ Ros Velasco and Gutiérrez Manjón, “The Expression of Boredom and Unwanted Loneliness on Twitch.”

²⁷⁶ Manoj Kumar Sharma, Nisha John, and Maya Sahu, “Influence of Social Media on Mental Health: A Systematic Review,” *Current Opinion in Psychiatry* 33, no. 5 (2020): 2, <https://doi.org/10.1097/YCO.0000000000000631>.

²⁷⁷ Panova and Lleras, “Avoidance or Boredom: Negative Mental Health Outcomes Associated with Use of Information and Communication Technologies Depend on Users’ Motivations.”

sentimiento de angustia al sentirse atrapado por su uso y llegar a desarrollar el síndrome de la vibración fantasma; se intenta escapar de ello sin tener éxito, luego la persona se siente deprimida y busca alivio o solución en las TIC. De esta manera se regresa al primer momento de seducción y se repite el patrón en modo cíclico. Lo nocivo de la adicción a estas tecnologías es su propensión a la ansiedad y depresión, pero sobre todo que las TIC se presentan en el mundo como indispensables para el desarrollo humano, con lo que es casi imposible dejar su uso deliberadamente. En otras palabras, el uso de estas tecnologías es impuesto por sus creadores y desarrolladores, aunque esto signifique el deterioro mental de las personas.

Con esto – aunque no lo parezca – no se busca dar una postura pesimista, negativa o inclusive que defienda que el regreso a un estado sin dispositivos y plataformas tecnológicas es el mejor. No pretendemos defender una tecnofobia. Es más bien, un análisis explicativo de lo que el uso indiscriminado de los datos personales sin protección ni cuidados, y a su vez la violación a la privacidad puede ocasionar. Tampoco intenta referirse a las tecnologías como instrumentos que provoquen maldad en la humanidad ni cosa parecida. Lo que si intenta es poner a la luz de las herramientas filosóficas de cuestionamiento, crítica, análisis y explicación la realidad tecnológica y de poder que vivimos en nuestro tiempo. Pero regresemos a nuestro análisis de la adicción a las TIC, con la intención de dilucidar el principal hallazgo de nuestra investigación.

Capítulo IV. Doble Poder

El futuro calculable como presente optimizado
no nos causa ninguna preocupación.
Byung-Chul Han, *No-Cosas* (2021)

Hasta ahora, hemos dejado en claro que el poder de las empresas tecnológicas está fundamentado en el conocimiento de los datos personales y privados de las personas, pues les da la posibilidad de crear y manipular la realidad a su conveniencia e intereses, sin importar que esto dañe la vida en comunidad, el diálogo y discusión base de nuestra participación democrática, la salud mental de las personas provocando depresión, ansiedad, adicción e incluso la muerte. Es así, que ahora podemos entender el calado del funcionamiento, posibilidades e intenciones de este tipo de poder de conocimiento. Pero es aquí, donde nace un nuevo cuestionamiento, ¿por qué aunque reconocemos los peligros y riesgos que ocasiona utilizar los productos y servicios de las empresas tecnológicas (Big Tech) seguimos utilizándolos? ¿será que el beneficio tecnológico es mayor que la pérdida de privacidad, abusos de poder, manipulación económica y política, depresión, ansiedad y adicción, para entregar los datos personales sin restricción alguna? ¿o es que solamente nos cobijamos en la idea de la imposición que suponen estas tecnologías, para así negarnos al mínimo atisbo de análisis y cuestionamiento? Algunos dirán que esto querámoslo ver o no, es así. Otros incluso negarán que estas consecuencias estén ocurriendo en el mundo real, víctimas tal vez de las fuentes de información que también lo niegan. Lo cierto es, que este tipo de poder ha evolucionado de tal manera, que ni siquiera nos percatamos que estamos bajo su yugo. Será porque su poder no implica el uso de la violencia, sino la persuasión y manipulación, pero aunque esto pueda tener algo de sentido, aquí no lo consideramos así.

A través del análisis explicativo que hemos realizado en este trabajo, podemos percatarnos que el dominante en este entramado de poder económico, político y social son los gobiernos, las Big Tech o cualquiera que tenga la capacidad de generar un valor mediante el uso de datos personales. Mientras que el rol de la víctima o dominado es la persona (o la sociedad, desde una perspectiva más general) que es persuadida, manipulada y vendida a través de sus datos personales y privados con el afán de mantener un control capaz de ordenar sus decisiones y deseos, es decir, mantener un poder sobre la identidad de la persona.²⁷⁸ Sin embargo, aunque esta posición no le es favorable, dado que atenta contra su propia libertad y autonomía, no existen rasgos que muestren inconformidad ante tal opresión. Un intento de respuesta puede ser aquella que señala que frente al agobiante camino que representa la libertad de elección, cualquier modelo que sustituya esta cualidad humana facilitaría la vida y la haría más eficiente, pues no se perdería tiempo en lo preocupante y angustiante que puede llegar a ser tomar una decisión.²⁷⁹ Por ejemplo, los algoritmos utilizados por YouTube o Netflix evitan el esfuerzo que implica buscar contenido que se adapte a los gustos o intereses de la persona, pues a través del contenido que habitualmente se consume, es que se puede predecir con una alta probabilidad, qué tipo de videos, series o películas le serán de mayor interés, con lo que se genera una lista de sugerencias que la plataforma crea de manera personalizada. Sin embargo, esta respuesta no nos parece convincente. Pues presupone que condiciones humanas para el desarrollo, como la libertad de decisión, pueden estar sometidas a estructuras de control, sin que ello tenga implicaciones éticas, políticas o de salud mental. Otro intento de respuesta es la que señala que el motivo principal por el cual las personas no dan señales de desagrado es porque este tipo de poder es un poder sutil, que no se percibe a

²⁷⁸ Foucault, *Microfísica Del Poder*.

²⁷⁹ Fromm, *El Miedo a La Libertad*.

simple vista, con lo cual revelarse ante algo que ni siquiera se sabe que existe realmente se vuelve complejo. Sin embargo, aquí hemos dado las pruebas fehacientes que muestran el fuerte impacto social, político y personal que tienen estas empresas tecnológicas en la vida cotidiana. Por lo cual, esta respuesta nos parece insuficiente. Los impactos del poder del conocimiento de los datos personales y privados se perciben en la manipulación e influencia de las decisiones personales o políticas. Y aunque no necesita hacer desfilar su poderío – a la manera de los desfiles militares –, porque esto tal vez, significaría la molestia y el disgusto de los que están bajo su imposición, crea mecanismos de control con mayor eficacia que los recursos balísticos. Frente a este tipo de análisis que no aspiran a ser absolutos o respuestas conclusivas, nos atrevemos de la misma manera, a dar los indicios de una postura frente a esta problemática.

Como primer paso, entendamos que el poder tecnológico no es únicamente unilateral, es decir, de las empresas y/o gobiernos para con la sociedad, dado que encuentra su realización en la percepción de poder de sus consumidores. Es decir, para que las TIC tengan y hayan tenido un crecimiento exponencial, sin siquiera conocer por parte de la sociedad qué son o pretenden ser realmente, es necesario dotarlas de cualidades intrínsecas de orden, control y poder;^L cualidades que están íntimamente relacionadas con las ya mencionadas necesidades psicológicas innatas. Con ello, se crea un vínculo determinante de consumo entre los productos y servicios de las Big Tech y la persona. En otras palabras, el consumo de estos productos se genera a través de la alimentación de las percepciones de orden, control y poder en las personas. Es por eso, que a través de la identificación de la manifestación de este tipo de poder, que se inicia desde los desarrolladores tecnológicos y se formaliza con el uso permanente de dispositivos y productos que dotan a quienes los usan de percepción de poder, que podemos concluir la existencia de un poder dual o – como aquí lo definimos – de un

Doble Poder.^{LI} Es una «producción multiforme de relaciones de dominación parcialmente integrables a estrategias de conjunto»²⁸⁰ que parece alejarse de «una estructura binaria con los “dominantes” de un lado y los “dominados” de otro».²⁸¹

Es un poder que logra expandirse de las esferas con mayor dominación a aquellas personas en condiciones de acceso a recibirlo. Inclusive, se llega a parecer a esos pronósticos de aspiración de libertad e igualdad que dieron los desarrolladores de Internet en sus inicios, quiénes afirmaban que la caída de las barreras del acceso a la información traería en consecuencia un equilibrio social. No pudieron estar más equivocados en ello. La realidad de esta expansión de poder o “fuerza” está sostenida en meras percepciones y se desarrolla de diversas maneras, aquí detallamos principalmente dos como condiciones necesarias y una tercera generada por las anteriores, las explicamos a continuación.

La primera es la percepción de orden, que detalla el camino de las dos siguientes. El orden de cosas genera habitualmente en la persona una sensación de calma. Este orden se ve manifestado en la unificación de actividades en los dispositivos. Por ejemplo, el de la comunicación, calendarización, lectura, escritura, investigación, trabajo, ocio, entre otras, que se pueden encontrar en un mismo dispositivo. Evitando así los esfuerzos que esto significaba en el pasado, mientras se ve erradicada la angustia que provoca el desorden.

El segundo es la percepción de control. Cuando lo incontrolable acecha la vida del ser humano, es casi imposible no sentir miedo o angustia. Se sabe impotente y a la deriva que provoca lo otro, aquello que está afuera de las posibilidades del yo. En esos momentos se sabe indefenso frente a lo desconocido. El desarrollo tecnológico desencadena en la persona una sensación de seguridad frente a lo desconocido, se sabe protegido cuando lo otro se

²⁸⁰ Foucault, *Microfísica Del Poder*, 59.

²⁸¹ Foucault, 58.

presente. Las comunicaciones rápidas y eficientes, las relaciones sociales determinadas en una plataforma, las búsquedas a respuestas incómodas, los pronósticos del clima y las copias de seguridad son ejemplos generadores de sensación de control en la persona. No es solo la sensación de que esto puede estar en un mismo dispositivo, sino que además se puede tomar el control de la vida social, laboral, personal, económica o política mediante los usos que se le den.

La fundamentación de la percepción de poder está en el orden y control. Ambos dotan más o menos de un desarrollo individual y casi psicológico de aptitudes acordes al poder. La presentación de estas cualidades se ven manifestadas en los propios fundamentos epistemológicos. El saber reclama orden, y la verdad control. No existe conocimiento sin un orden propio, como tampoco no existe una verdad que no se imponga sobre la falsedad. Como el «ordenamiento general de la naturaleza, que admite una posibilidad de análisis para descubrir el elemento o el origen».²⁸² La unificación de actividades y las facilidades tecnológicas de la eficacia y rapidez generan en principio un poder epistemológico, que luego se transforma para alimentar la sed de exposición social y política. Es decir, el poder que da el conocimiento de las cosas mediante el uso de las TIC da control y orden a la vida cotidiana de las personas; es una genealogía, una relación saber-poder. Es por eso que es requerido el empleo de las tecnologías que solventan tal necesidad que marquen la disciplina de exposición, apertura y confianza ingenua del siglo XXI.²⁸³ Sin embargo, este poder transformado por las necesidades intrínsecas de la persona es vulnerado para ser utilizado como moneda de cambio para la generación de un poder estructural permanente y con

²⁸² Michel Foucault, *Las Palabras y Las Cosas: Una Arqueología de Las Ciencias Humanas*, 2a. (México: Siglo XXI, 2010).

²⁸³ Alberto Constante López and Ramón Chaverry Soto, *World Wide Web y La Formación de La Subjetividad* (Afinita Editorial, 2015).

capacidades de dominación sin precedentes.²⁸⁴ Paradójicamente, en filosofía se ha vislumbrado que la esencia de la técnica recae en la región del des ocultamiento, de la verdad.²⁸⁵ La técnica crea modelos de seguimiento hacia la verdad del orden de las cosas. Mientras que la técnica moderna o tecnología enfoca sus esfuerzos en crear relaciones de poder con el conocimiento de la verdad de las personas. Saber, verdad, técnica (tecnología) y poder conviven en una relación de dependencia. De tal manera, que no se trata de buscar la emancipación de la verdad de todo sistema de poder – por demás una quimera –, sino de buscar la separación del poder de la verdad de las formas de hegemonía que rigen el mundo de lo social, económico y político.²⁸⁶ En este caso, separar el poder del conocimiento de los datos personales de las empresas tecnológicas, pues quien conoce la verdad de las personas tiene el poder de controlarlas.²⁸⁷

Al estar sustentado este poder por los datos privados y personales, las capacidades de desarrollar tal poder por parte de los usuarios de las TIC, se ve reducido a nada frente a la dominación que ejerce quienes las desarrollan. A pesar de que la expansión de este poder puede ser comprobado por sus utilidades y conveniencias tecnológicas, la relación dominador-dominado no deja de existir. Al contrario, crece aún más si se tiene la seguridad de las percepciones o sensaciones de control, orden y poder, pues solo a través de ellas es posible el procesamiento indiscriminado de datos personales sin el mínimo reclamo.

²⁸⁴ Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

²⁸⁵ Martin Heidegger, “La Pregunta Por La Técnica,” in *Filosofía, Ciencia y Técnica*, 3a. (Editorial Universitaria, 1997), 111–48.

²⁸⁶ Foucault, *Microfísica Del Poder*, 45.

²⁸⁷ Véliz, “The Internet and Privacy”; Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

Hemos nombrado percepciones o sensaciones a estas cualidades, con la intención de mostrar más o menos la relación de ilusión o falsedad que guardan las personas con las TIC. Esto no quiere decir que todas las percepciones o sensaciones sean ilusorias o falsas, pero sí, que no todo lo que se percibe es verdadero; y es justamente que en la existencia de la relación con las tecnologías que extraen datos privados que la posibilidad para desarrollar un orden propio es inexistente, pues es mediante el conocimiento del ordenamiento de la persona que se ordena a la misma; se pierde el dominio del orden para permitirle a alguien más que entre por él. Tampoco existe un control sobre lo propio, dadas las condiciones que preparan un ambiente de control de la personalidad basadas en el mismo conocimiento que la persona va desplegando con su huella digital. En consecuencia, el poder que se pretende tener solo existe en la medida en que la persona reconozca su relación con estas tecnologías y profundice en un camino propio de resistencia. De otra manera, se está condenado a creer tener un poderío sobre las cosas, sin darse cuenta de que entre esas cosas está la persona dominada por la estructura de poder que se le superpone. El reconocimiento de esta estructura solo será posible mediante la identificación de la conformación de subjetividades, o como aquí las hemos llamado, realidades particulares o propias. Sin olvidar que el despliegue tecnológico nunca es neutral, siempre se impone por la verdad de su conocimiento hacía tendencias propias de su tiempo.^{288LII}

Si bien es cierto, que el Doble Poder puede ser corroborado por la conveniencia tecnológica y sus raíces profundas que cimientan la vida de hoy, no hemos de prescindir de las herramientas para el des engranaje y destornillamiento de su estructura que nos lleven a profundizar en otras latitudes de nuestro necesario apego tecnológico. Pues, frente a que la

²⁸⁸ Heidegger, “La Pregunta Por La Técnica”; Michel Foucault, *Vigilar y Castigar: Nacimiento de La Prisión*, 2a. (México: Siglo XXI, 2009).

realidad parece llevarnos cada vez más a ilusionarnos con esta ilusión; la ilusión de poder tecnológico y científico, capaz de calmar nuestros miedos y alejarnos de la angustia por lo incierto o desconocido.²⁸⁹ ¿Qué es pues el Doble Poder, sino solo el desarrollo del proceso de la misma ilusión que nos hace querer creer en las capacidades intrínsecas humanas para luego ser utilizadas a conveniencia según los intereses particulares? De eso se trata el poder, de formar sujetos capaces de creer en sus propias capacidades. O bien, ¿qué sentido tendría un poder que solo se dedique a la prohibición?

Si el poder fuera siempre represivo, si nunca hiciera otra cosa que decir no, ¿creen ustedes de verdad que se lo obedecería? Lo que hace que el poder persista, que se lo acepte, es que no pesa solo como una fuerza que dice no, sino que, de hecho, atraviesa, produce cosas, induce placer, forma saber, produce discurso. Hay que considerarlo como una red productiva que atraviesa todo el cuerpo social, mucho más que como una instancia negativa cuya función es reprimir.²⁹⁰

El desarrollo de las capacidades humanas está delimitado – negado – por aquello que se le superpone. Son formadas y dirigidas.²⁹¹ Tal vez, por eso, el diálogo ideal o debate libre y provechoso para el ser persona en sociedad en las redes sociales, pero en el espacio de dominación por excelencia con sus correspondientes dispositivos de poder es, sencillamente, imposible. Pensar que a través de una plataforma que personaliza los contenidos que cada usuario consume, con lo cual cada persona o tipo de personalidad recibe información diferente e incluso contradictoria, creando su propia cámara de eco donde resuenan sus gustos, miedos, fobias y rasgos de personalidad, sea posible realizar un diálogo en comunidad es por demás ingenuo. Pero sobre todo, porque pensar en el hecho de que una empresa privada se convierta en pública solo por prestar servicios a cualquier persona que lo requiera es caer

²⁸⁹ Foucault, *Las Palabras y Las Cosas: Una Arqueología de Las Ciencias Humanas*.

²⁹⁰ Foucault, *Microfísica Del Poder*, 29–30.

²⁹¹ Foucault, *Vigilar y Castigar: Nacimiento de La Prisión*.

en un grave fallo. Los intereses de una empresa privada se regirán siempre por causas y objetivos particulares y no sociales, como la acumulación de mayor capital económico a cuenta de las irregularidades – tal vez no ilícitas, pero si permitidas por la ley «*Permissum videtur in omne quod non prohibitum*» («Parece permitido todo lo que no está prohibido»)²⁹² – de los servicios que presta. Pensar en que las redes sociales son un espacio público o bien, el lugar de diálogo y debate – la nueva ágora – no es más que una ficción. Tales inconsistencias o falsos ideales son solo frutos de la creencia del Doble Poder que moldea las capacidades de los sujetos de los datos.

El absolutismo que proclama esta tecnología algorítmica no es otra cosa que la repetición del miedo a la realidad. La realidad que es movimiento, cambio y relatividad. El anhelo por el control de todo – o casi todo – es el deshacimiento de la persona. El dominio presupone la quietud de todo y el solo movimiento del yo. No es que se quiera dominar, controlar y ordenar todo, es que se quiere huir del miedo que causa el movimiento, lo incontrolado y el desorden. No elegirse persona es elegir que algo o alguien elija las propias decisiones. Se permite de una vez y para siempre que el absolutismo tecnológico permee la vida, la realidad cambiante, que se ve aliviada por el ordenamiento de control algorítmico capaz de crear un cambio – una realidad – sin caos. La inteligencia artificial capaz de crear análisis con mediciones precisas del pensamiento y realidades humanas busca solucionar ese miedo a la realidad del cambio. Sin embargo, la proclamación de ese “cambio sin miedo” contradice a la misma democracia, que apela al miedo por el cambio. Una democracia que exige la elección por la persona humana como el sujeto capaz de crear futuro, desde su presente y lo que ya tiene de su pasado, en libertad; y sobre todo porque su gran novedad

²⁹² Alberto Constante and Ramón Chaverry Soto, *World Wide Web y La Formación de La Subjetivad* (Coyoacán, México: Universidad Nacional Autónoma de México, 2015).

recae en el orden democrático que ha de ser creado y sostenido entre todos. Un orden en movimiento viviente y fluido del cual todos formamos parte. Cuando el hombre se elige persona está ya en sí mismo dicho que las decisiones venideras se harán desde un horizonte que amplie tales capacidades de elección, no que las disminuya. Es el vivir humanamente: «tener que elegir entre las circunstancias». Y sobre todo aquella elección previa y decisiva: «la que se hace uno de sí mismo».²⁹³ Elegir no elegir es negarse persona. Esto sería, en todo caso, alimentar el crecimiento del hombre masa al que su propia realidad le es indiferente y vive de los resultados de los productos sin siquiera conocerlos.²⁹⁴

Por si fuera poco la falsedad de la ilusión del absolutismo tecnológico reabre los caminos de la duda y el sinsentido. Visto desde la realidad, la del día a día, se puede experimentar cada vez más un hartazgo tecnológico, aunado a la incertidumbre que dan la polarización y la vida misma. Es un reconocimiento de la vulnerabilidad del ser persona ante el porvenir incierto, como lo ha sido en la pandemia del COVID-19 de la que nadie en el mundo ha sido ajeno, y ha puesto en evidencia el despliegue de poder del absolutismo tecnológico provocando desinformación y desconfianza social, aburrimiento crónico y el inicio de ansiedad para muchas personas.²⁹⁵ En lo particular, la zozobra y la angustia nos embargan con o sin inteligencia artificial. La cura para el temor al cambio de la realidad no está en la IA.

²⁹³ Zambrano, *Persona y Democracia*, 225.

²⁹⁴ Zambrano, *Persona y Democracia*.

²⁹⁵ Halim Guner, “Moderator Effect of COVID-19 Fear on "mediating Role of Boredom Proneness in Relationship between Internet Addiction and DASS-21," *Educational Process: International Journal* 10, no. 2 (2021): 83–99, <https://doi.org/10.22521/EDUPIJ.2021.102.5>; Leilei Liang et al., “Psychological Distress and Internet Addiction Following the COVID-19 Outbreak: Fear of Missing out and Boredom Proneness as Mediators,” *Archives of Psychiatric Nursing* 40 (2022): 8–14, <https://doi.org/10.1016/j.apnu.2022.03.007>; Ros Velasco and Gutiérrez Manjón, “The Expression of Boredom and Unwanted Loneliness on Twitch.”

Vamos buscando continuamente el alivio que causa saber que se tiene control sobre las cosas que cambian sobre la propia realidad. Ya sea en la política, ya sea en la religión. Sin embargo, en este caso, el poder del absolutismo tecnológico que se tiene sobre la persona alimenta la necesidad de poder sobre el mundo de cosas, y resuelve más o menos el temor ancestral sobre el futuro, esto es, el poder que da el control sobre la realidad.²⁹⁶ Un poder ilusorio, una elección ilusoria, un control ilusorio. El mundo del absolutismo tecnológico es un mundo ficticio creado de ilusiones.

Parece consecuente ahora, ir a la cuestión que interpela esta estructura de poder y busca caminos hacia la resistencia. Pues, «No existen relaciones de poder sin resistencias»,²⁹⁷ sin embargo, cabe preguntarnos: ¿será que los esfuerzos por salir de tal estructura de poder solo son los que la misma estructura permite, convirtiéndose en una quimera pensar en su derrocamiento? Y en última instancia ¿no es acaso que la misma información con la que se formuló este trabajo ha sido condicionada por los servidores que alimentan esta estructura de poder? Entonces, ¿no es que este trabajo solo sigue el discurso propiciado por aquel modelo que él mismo critica y advierte? Antes de respondernos la posibilidad de salida de este absolutismo tecnológico, hemos de revisar las alternativas que se tienen. Cambiar hábitos, servicios o productos, puede ser un buen inicio, pero sobre todo la creación de políticas públicas creadoras de una cultura capaz de revalorar el sentido de intimidad, privacidad y datos personales nos llevarán a un camino de resistencia y renuncia a un progreso tecnológico ya estipulado.²⁹⁸

²⁹⁶ Fromm, *El Miedo a La Libertad*; Zambrano, *Persona y Democracia*.

²⁹⁷ Foucault, *Microfísica Del Poder*, 59.

²⁹⁸ Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.

A manera de resumen final, podemos decir que la privacidad con su correspondiente derecho es un bien común e indispensable para la vida en una sociedad democrática liberal, una forma de su violación es la extracción, acumulación y uso indiscriminado de los datos personales. El conocimiento generado a partir del Big Data y la Inteligencia Artificial en los datos personales, crea una nueva forma de poder. Este se traduce en la obtención de control político, social y económico, en tiempo real y sin fronteras de por medio. Aquí hemos hablado del despliegue de un Doble Poder que crea percepciones ilusorias de poder sobre sus dominados. Mientras mayor sea la seguridad de percepción de poder, el funcionamiento del sistema aumenta a la vez que los dispositivos de control crean lazos más íntimos con sus usuarios. La opción por la resistencia frente al absolutismo tecnológico parece ser una alternativa necesaria. Es por eso, que actualmente diferentes autoras han abogado por una «cultura de la privacidad».

No hay intimidad sin privacidad. Las relaciones que no pueden contar con un escudo de confidencialidad – ya sea porque desconfiamos de los otros o porque desconfiamos de las tecnologías que utilizamos para comunicarnos e interactuar con los otros – están condenadas a ser meramente superficiales. Una cultura de la privacidad es necesaria para disfrutar de conversaciones íntimas con los demás, para tener debates sinceros en entornos cerrados como los hogares y las aulas, y establecer los buenos vínculos sobre los cuales las sociedades están basadas para su buen funcionamiento. Estar en un mundo en el que los datos se convierten constantemente en armas es sentirse perpetuamente amenazado y desconfiado de los otros. Tal miedo genera la conformidad y el silencio.²⁹⁹

Aún quedan cuestiones por hacer y tal vez responder, como el de la idea de progreso que parece ser una rueda importante para el movimiento de lo tecnológico, como un ordenamiento de sucesión que la historia nos presenta capaz de descubrir el principio de

²⁹⁹ Véliz, 80.

regularidad en su formación, como si se tratara de una secuencia matemática con la que se pueda predecir el resto de la serie.³⁰⁰ O bien, lo que parece ser el fin e inicio de una nueva era de la humanidad, con lo cual la realidad del hombre tal y como la hemos conocido se verá destruida para dar paso al nacimiento de una nueva. O inclusive pasar de una visión de mundo homocéntrica a una visión del mundo datacéntrica.³⁰¹ Con esto el «Conócete a ti mismo» se verá remplazado por un «Conócete por algoritmos». Tal vez todos los esfuerzos por asegurar la predominancia y supervivencia de lo humano demuestran una sola cosa: que nos cuesta trabajo el proceso de aceptación a la adaptación de una realidad llena de subjetividades creadas y dominadas, vigilada, personalizada, con aspiraciones universalistas y absolutistas, que se aleja de la exaltación romantizada por las cualidades humanas sintientes, de conciencia y de comportamiento. Tal vez solo sea que estamos tan ensimismados en la creatura humana y su desarrollo que no alcanzamos a ver más allá. Esto solo puede ser comprobado en la historia, dejándonos sin la posibilidad de predicción.

El ser humano tomado como la conformación de todos los saberes que han existido es una creación propia de una era. La nuestra, puede estar llegando a su fin con la desaparición de las condiciones y disposiciones necesarias, tal como llegaron a aparecer. No lo podemos predecir – al menos por medios humanos –, pero sí presentir. Puede presentirse que «el hombre se borraría, como en los límites del mar un rostro de arena».³⁰²

³⁰⁰ Popper, *La Miseria Del Historicismo*.

³⁰¹ Noah Harari, *Homo Deus. Breve Historia Del Mañana*.

³⁰² Foucault, *Las Palabras y Las Cosas: Una Arqueología de Las Ciencias Humanas*, 398.

Conclusión

La visión de mundo construida por el poder tecnológico que aquí hemos explorado es una visión coartada, sesgada, pero sobre todo creadora de realidades alternas que violan el derecho a la privacidad. Es casi imposible pensar la tecnología de hoy sin manipulación. El camino que sigue este poder tecnológico nos sugiere un método inductivo que se origina en las cualidades de las individualidades personales extrayendo, almacenando, vigilando y analizando lo privado, lo íntimo; para luego lograr inferencias, predicciones y manipulaciones de control. Mediante el modelo del Big Data se crea una reconfiguración de lo privado para ser transformado en datos. Nuestra privacidad es información que da poder a quien la tiene. Se manipula la privacidad para sacar el mayor provecho capitalista posible. La realidad y visión de mundo de cada persona es moneda de cambio.

Aquí hemos dilucidado una continua lucha – digámoslo así – entre contrarios, un modelo hegeliano que encuentra su síntesis en concepciones utilizadas por este poder tecnológico. La primera de ellas se encuentra precisamente en el espacio de lo propio: lo privado. Es la privacidad aquello que medía ser en sí y ser para otro. La segunda de ellas es la información: el proceso histórico de lo analógico a lo digital; como aquello que transforma lo cualitativo en cuantitativo, y por lo tanto en manipulable. Después nos encontramos con los datos personales y privados como concepción que nos adentra de manera directa a las abstracciones de las actividades espontáneas de las personas y de las cosas que suceden. Y por último, como originadores del funcionamiento de este poder se encuentran el conocimiento iniciador de la curiosidad humana y la ilusión de poder creada por el orden y control del desarrollo vital dado por la tecnología. Ambos, conocimiento e ilusión de poder, encuentran su síntesis en nuestra idea de Doble Poder.

Aunque nuestras ideas tratan de dar claridad a esta cotidianeidad, no nos deja de interpelar la cuestión por la imprescindible resistencia al poder. Una pregunta que busca respuestas inmediatas, pero sobre todo efectivas, funcionales. No logramos concebir que una realidad tan atrofiada como la tecnológica, siga sin el menor atisbo de lucha y resistencia. Porque al final, siempre se desvela esa libertad primera, la del pensamiento, la que busca una rendija para asomarse. En eso consiste el crecimiento humano, en salir, buscar, pensar, gritar, luchar.

Frente a este poder que nos procura y nos hace pensar que cuida lo propio, en tanto su cualidad de Doble Poder, solo veo una respuesta posible: la del saberse ahí. Es decir, saber que nuestro desarrollo personal en libertad utilizando los medios de este poder está condicionado a la inferencia de datos sensibles, la predicción de comportamiento, la manipulación política y económica, y a afecciones a la salud mental. Saberse que frente a los medios convencionales tecnológicos, nuestra realidad tal y como la hemos concebido, está propensa a cambiar en cualquier momento obedeciendo a intereses económicos, políticos e incluso, biopolíticos; haciéndose valer de nuestra privacidad para ello. Y si después de reconocernos dominados y una simple moneda de cambio para las empresas tecnológicas y gobiernos, surgiera la necesidad de resistir busquemos en comunidad los caminos para lograrlo. Las iniciativas o cambios individualizados nunca serán suficientes si lo que se quiere lograr es un cambio en sociedad, para ello necesitamos compartir la urgencia del debate por la privacidad, cambiar hábitos que atentan contra la privacidad de las personas, inclusive generar grupos interesados en alternativas tecnológicas. La resistencia a este poder implica un esfuerzo mayor, sin embargo, a cambio se obtiene seguridad, libertad de expresión, autonomía, protección de los abusos de poder y sobre todo una democracia sana. No dejemos que lo verdaderamente nuestro, nuestra privacidad y libertad, sea robada,

ultrajada, vendida o utilizada en nuestra contra. Recordemos que la tecnología y su desarrollo solo tienen sentido si van acordes a los paradigmas y normas sociales, es decir, la tecnología no se crea por sí sola, no se engendra a ella misma, está siempre atada a la voluntad y anhelo humanos, por lo tanto su progreso depende de las decisiones humanas. Retomemos el control de la tecnología, con la esperanza de que no sea demasiado tarde. Es así que solo a la luz de la filosofía que señala y encuentra el entramado de ideas y realidades que se entretrejen y crean mundo es que nuestra realidad angustiante puede ser cuestionada, analizada, criticada, interpretada y llevada a buen puerto a través de la ética.

Referencias bibliográficas

- Online Library Learning Center. "A Brief History of the Internet." Accessed September 18, 2022. https://doi.org/10.1007/978-3-642-13247-6_1.
- Academy, Khan. "Ley de Gravitación Universal de Newton." Khan Academy. Accessed October 22, 2022. <https://es.khanacademy.org/science/hs-physics/x215e29cb31244fa1:types-of-interactions/x215e29cb31244fa1:newton-s-law-of-universal-gravitation/a/newtons-law-of-universal-gravitation>.
- Alexy, Robert. *Teoría de Los Derechos Fundamentales*. Madrid: Centro de Estudios Constitucionales, 1993.
- Amazon.com, Inc. "FORM 10-K." Washington, D.C.: United States Securities and Exchange Commission, 2014. <https://doi.org/10.4135/9781608712380.n519>.
- Ambrose, Jillian. "Lights Stay on despite Cyber-Attack on UK's Electricity System." *The Guardian*, 2020. <https://www.guardian2zotagl6tmjucg3lrhxdk4dw3lhbqnkvvkywawy3oqfoprid.onion/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system>.
- Andrejevic, Mark. *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge, 2013. <https://doi.org/10.4324/9780203075319>.
- Apple Inc. "FORM 10-K." Washington, D.C.: United States Securities and Exchange Commission, 2021. <https://doi.org/10.4135/9781608712380.n519>.
- Applebaum, Anne. *El Ocaso de La Democracia*. México: Penguin Random House, 2021.
- Arendt, Hannah. *Entre El Pasado y El Futuro. Ocho Ejercicios Sobre La Reflexión Política*. Barcelona: Península, 1996.
- . *La Condición Humana*. 1a ed. Buenos Aires: Paidós, 2003.
- . *La Promesa de La Política*. Ciudad de México: Paidós, 2005.
- Argüelles, Alexandra, and Brenda Battaglia. *Violencia Digital En México: El Estado vs La Sociedad Civil*. México: Malpaís, 2021.
- Aristóteles. *Ética Nicomáquea Ética Eudemia*. Madrid: Gredos, 1985.
- . *Tratados de Lógica (Organon)*. 12a ed. México, D. F.: Porrúa, 2008.
- Baer, Drake. "Why Data God Jeffrey Hammerbacher Left Facebook To Found Cloudera." Fast Company, 2013. <https://www.fastcompany.com/3008436/why-data-god-jeffrey-hammerbacher-left-facebook-found-cloudera>.
- BBC. "Facebook Fined £500,000 for Cambridge Analytica Scandal." *BBC*, 2018. <https://www.bbc.com/news/technology->

- 45976300?intlink_from_url=https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-data-scandal&link_location=live-reporting-story.
- Ben-Shahar, Omri, and Carl E. Schneider. “The Failure of Mandate Disclosure, Part 4.” *Actual Problems of Economics and Law* 11, no. 4 (2017): 146–69.
<https://doi.org/http://dx.doi.org/10.21202/1993-047X.11.2017.4.146-169>.
- Bohannon, John. “Facebook Preferences Predict Personality Traits.” *Science Now*, 2013, 1.
<https://doi.org/10.1126/article.26288>.
- . “Your Computer Knows You Better than Your Friends Do.” *Science*, 2015, 10–12.
<https://doi.org/10.1126/science.aaa6329>.
- Brin, Sergey, and Larry Page. “The Anatomy of a Large-Scale Hypertextual Web Search Engine.” *Computer Networks and ISDN Systems* 30, no. 1–7 (1998): 107–17.
[http://dx.doi.org/10.1016/S0169-7552\(98\)00110-X%5Cnhttp://apps.webofknowledge.com/full_record.do?product=UA&search_mode=GeneralSearch&qid=6&SID=X1pOWPMuSmOv1SlwJ6f&page=1&doc=2](http://dx.doi.org/10.1016/S0169-7552(98)00110-X%5Cnhttp://apps.webofknowledge.com/full_record.do?product=UA&search_mode=GeneralSearch&qid=6&SID=X1pOWPMuSmOv1SlwJ6f&page=1&doc=2).
- Brooke, Sian, and Carissa Véliz. “Data, Privacy and the Individual.” *Center for the Governance of Change*. Vol. 1. Madrid, 2020.
- Burr, Christopher, and Nello Cristianini. *Can Machines Read Our Minds? Minds and Machines*. Vol. 29. Springer Netherlands, 2019. <https://doi.org/10.1007/s11023-019-09497-4>.
- Cadwalladr, Carole, and Emma Graham-Harrison. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” *The Guardian*, 2018.
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- Carole Cadwalladr. “‘I Made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower.” *The Guardian*, 2018. <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.
- Castilla del Pino, Carlos. “Teoría de La Intimidación.” *Revista de Occidente* 182–183 (1996): 15–30.
- Castillo, Carlos Del. “Así Trabaja Una Empresa Española Que Compra y Vende Datos Personales Para Hacer Publicidad: ‘Recogemos Toda La Información Posible.’” *Diario.Es*, October 21, 2019. https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_1_1297691.html.
- Cisneros Arellano, José Luis. *Filosofía Del Pensamiento Complejo. Una Reflexión Sobre Edgar Morín*. Monterrey, N.L.: Centro de Estudios Humanísticos, UANL, 2020.
- . “La Asesoría y La Consultoría Filosófica Frente a La Corrupción.” In *Humanidades Inter y Transdisciplinarias En Contextos de Incertidumbre: Nuevas Ideas, Nuevos Enfoques, Nuevos*

- Temas.*, edited by Ludivina Cantú Ortiz, 865–90. Monterrey: Facultad de Filosofía y Letras, UANL, 2021.
- . “La Investigación Filosófica Desde La Relación: Una Mirada Panorámica a La Luz de Una Propuesta Metodológica.” *Tesis (Lima)* 14, no. 18 (2021): 491–509.
<https://doi.org/10.15381/tesis.v14i19.20516>.
- Clarke, Roger. “Internet Privacy Concerns Confirm the Case for Intervention.” *Communications of the ACM* 42, no. 2 (1999): 60–67. <https://dl.acm.org/doi/pdf/10.1145/293411.293475>.
- Coeckelbergh, Mark. *Ética de La Inteligencia Artificial*. Madrid: Cátedra, 2021.
- Constant, Benjamin. “De La Libertad de Los Antiguos Comparada Con La de Los Modernos.” In *Del Espíritu de Conquista*, 64–93. Madrid: Tecnos, 1989.
- Constante, Alberto, and Ramón Chaverry Soto. *World Wide Web y La Formación de La Subjetivad*. Coyoacán, México: Universidad Nacional Autónoma de México, 2015.
- Constante López, Alberto, and Ramón Chaverry Soto. *World Wide Web y La Formación de La Subjetividad*. Afinita Editorial, 2015.
- Corporation, Microsoft. “FORM 10-K.” Washington, D.C.: United States Securities and Exchange Commission, 2022. <https://doi.org/10.4135/9781608712380.n519>.
- Council, National Intelligence. “Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interest Out to 2025,” 2008. <http://www.fas.org/irp/nic/disruptive.pdf>.
- Davara Fernández de Marcos, Isabel. *Diccionario de Protección de Datos Personales. Conceptos Fundamentales*. Ciudad de México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 2019.
- Dawson, Jessica. “Microtargeting as Information Warfare.” *The Cyber Defense Review* 6, no. 1 (2021): 63–80.
- Dewey, John. *Liberalism and Social Action*. New York: G.P. Puntam’s Sons, 1935.
- Drouin, Michelle, Daren H. Kaiser, and Daniel A. Miller. “Phantom Vibrations among Undergraduates: Prevalence and Associated Psychological Characteristics.” *Computers in Human Behavior* 28, no. 4 (2012): 1490–96. <https://doi.org/10.1016/j.chb.2012.03.013>.
- Dworskin, Elizabeth. “FTC: Data Brokers Can Buy Your Bank Account Number for 50 Cents.” *The Wall Street Journal*, 2014. <https://www.wsj.com/articles/BL-DGB-39567>.
- Elhai, Jon D., Jason C. Levine, Robert D. Dvorak, and Brian J. Hall. “Fear of Missing out, Need for Touch, Anxiety and Depression Are Related to Problematic Smartphone Use.” *Computers in Human Behavior* 63 (2016): 509–16. <https://doi.org/10.1016/j.chb.2016.05.079>.
- Española, Real Academia. “Diccionario de La Lengua Española.” 23, [versión 23.5 en línea], 2022. <https://dle.rae.es>.

- Europa, Consejo de. Convenio 108 (1981).
- Europea, Comisión. Reglamento General de Protección de Datos, Diario Oficial de la Unión Europea § (2016). <https://doi.org/10.2307/j.ctv17hm980.4>.
- Floridi, Luciano. *The Onlife Manifesto. Being Human in a Hyperconnected Era*. Edited by Luciano Floridi. Oxford, UK: Springer Open, 2015. https://doi.org/10.1007/978-3-319-04093-6_21.
- Foucault, Michel. *Las Palabras y Las Cosas: Una Arqueología de Las Ciencias Humanas*. 2a. México: Siglo XXI, 2010.
- . *Microfísica Del Poder*. Buenos Aires: Siglo Veintiuno, 2019.
- . *Vigilar y Castigar: Nacimiento de La Prisión*. 2a. México: Siglo XXI, 2009.
- Fromm, Erich. *El Miedo a La Libertad*. 6a ed. México: Paidós, 2012.
- Gelman, Robert. “Draft Proposal: Declaration of Human Rights in Cyberspace.” The digital Be-In, 1997. <https://www.be-in.com/10/rightsdec.html>.
- Gibbs, Samuel. “40 Years of Apple - in Pictures.” *The Guardian*, 2016. <https://www.theguardian.com/technology/gallery/2016/apr/01/40-years-of-apple-in-pictures>.
- Gibbs, Samuel, and Alex Hern. “Google at 20: How Two ‘obnoxious’ Students Changed the Internet.” *The Guardian*, 2018. <https://www.theguardian.com/technology/2018/sep/24/google-at-20-larry-page-sergey-brin-internet>.
- Goizueta, Javier. “El RGPD Pone En Jaque El Gran Negocio Del Siglo XXI.” *El Confidencial*, September 13, 2018. https://blogs.elconfidencial.com/espana/tribuna/2018-09-13/datos-rgpd-gran-negocio-sigloxxi_1614624/.
- Gómez-Feria Prieto, Ildefonso. “Glosario de Términos Psicopatológicos e Históricos Psiquiátricos.” *Psiquiatria.com*, 2022. <https://psiquiatria.com/glosario/index.php>.
- Google. “Real-Time Bidding.” GOOGLE INC. Accessed February 19, 2022. <https://developers.google.com/authorized-buyers/rtb/start>.
- Greenberg, Andy. “How Hacked Water Heaters Could Trigger Mass Blackouts.” *Wired*, 2018. <https://www.wired.com/story/water-heaters-power-grid-hack-blackout/>.
- Grupo de Trabajo del Artículo 29. “Dictamen 4/2007 Sobre El Concepto de Datos Personales,” 2007, 1–29. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.
- Guner, Halim. “Moderator Effect of COVID-19 Fear on "mediating Role of Boredom Proneness in Relationship between Internet Addiction and DASS-21.” *Educational Process: International Journal* 10, no. 2 (2021): 83–99. <https://doi.org/10.22521/EDUPIJ.2021.102.5>.
- Han, Byung-Chul. *No-Cosas*. Ciudad de México: Penguin Random House, 2021.
- Hao, Karen. “She Risked Everything to Expose Facebook. Now She’s Telling Her Story.” *MIT*

- Technology Review*, 2021.
<https://www.technologyreview.com/2021/07/29/1030260/facebook-whistleblower-sophie-zhang-global-political-manipulation/>.
- Hegel, G. W. F. *Filosofía Del Derecho*. 5a. Buenos Aires: Claridad, 1968.
- Heidegger, Martin. “La Pregunta Por La Técnica.” In *Filosofía, Ciencia y Técnica*, 3a., 111–48. Editorial Universitaria, 1997.
- Heikkilä, Melissa. “Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms.” *Politico*, 2022. <https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/amp/>.
- Henning, Michelle. “That Liking Feeling : Mood , Emotion , and Social Media Photography.” In *Ubiquity. Photography’s Multitudes*, edited by Jacob W. Lewis and Kyle Parry. Leuven University Press, 2021. <https://www.jstor.org/stable/j.ctv24cnspsz.15>.
- Hilbert, Martin, and Priscila López. “The World’s Technological Capacity to Store, Communicate, and Compute Information.” *Science* 332, no. 6025 (2011): 60–65.
<https://doi.org/10.1126/science.1200970>.
- Hitler, Adolf. “Adolf Hitler Speech of January 27, 1932,” 2022.
- IFAI. *Protección de Datos Personales. Compendio de Lecturas y Legislación*. 1a. México: Tiro Corto Editores, 2010.
- INAI. “Resolución Del Procedimiento de Verificación 3S.07.02-039/2017,” 2017.
https://inicio.inai.org.mx/pdf/resoluciones/2017/03S_02-039.pdf.
- Inc., Alphabet. “United States Securities and Exchange Commission. Form 10-K. Annual Report.” Washington D.C., 2021.
https://abc.xyz/investor/static/pdf/20220202_alphabet_10K.pdf?cache=fc81690.
- Inc., Google. “United States Securities and Exchange Commission. Form 10-K. Annual Report.” Washington D.C., 2005.
<https://www.sec.gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm>.
- Information Commissioner’s Office. “Update Report into Adtech and Real Time Bidding,” 2019.
<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>.
- Institute, The Alan Turing. “What Is an Algorithm?” YouTube, 2021.
https://www.youtube.com/watch?v=i76WAFOut_Y.
- Intelligence Unit, The Economist. “Democracy Index 2019. A Year of Democratic Seatbacks and Popular Protest.” London, 2019.

- Investigation, A Wall Street Journal. "The Facebook Files." Wall Street Journal, 2021.
<https://www.wsj.com/articles/the-facebook-files-11631713039>.
- Isaak, Jim, and Mina J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." *Computer* 51, no. 8 (2018): 56–59. <https://doi.org/10.1109/MC.2018.3191268>.
- Isikoff, Michael. "NSA Program Stopped No Terror Attacks, Says White House Panel Member." *NBC News*, 2013. <http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588>.
- ITU. *2021 Measuring Digital Development: Facts and Figures*. ITU Publications. Geneva: International Telecommunication Union, 2021.
[https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU Facts and Figures 2019 - Embargoed 5 November 1200 CET.pdf%0Ahttps://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx](https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU_Facts_and_Figures_2019_-_Embargoed_5_November_1200_CET.pdf%0Ahttps://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx).
- "Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights." *Human Rights Watch*, 2020.
<https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight>.
- Jongepier, Fleur, and Michael Klenk. *The Philosophy of Online Manipulation. The Philosophy of Online Manipulation*. New York: Routledge, 2022. <https://doi.org/10.4324/9781003205425>.
- Kaiser, Brittany. *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook Broke Democracy*. London: HarperCollins, 2019.
- Kant, Immanuel. *La Metafísica de Las Costumbres*. 4ta. Madrid: Tecnos, 2008.
- Kari, Paul. "Facebook Announces Name Change to Meta in Rebranding Effort." *The Guardian*, 2021. <https://www.theguardian.com/technology/2021/oct/28/facebook-name-change-rebrand-meta>.
- Kelion, Leo. "Google-Nest Merger Raises Privacy Issues." *BBC News*, 2018.
<http://www.bbc.co.uk/news/technology-42989073>.
- Khalil, Lydia. "Digital Authoritarianism , China and COVID." *Lowy Institute for International Policy*, 2020.
- Kosinski, Michal, David Stillwell, and Thore Graepel. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (2013): 5802–5.
<https://doi.org/10.1073/pnas.1218772110>.
- Kramer, Adam D.I., Jamie E. Guillory, and Jeffrey T. Hancock. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *Proceedings of the National*

- Academy of Sciences of the United States of America* 111, no. 24 (2014): 8788–90.
<https://doi.org/10.1073/pnas.1320040111>.
- Lambiotte, Renaud, and Michal Kosinski. “Tracking the Digital Footprints of Personality.”
Proceedings of the IEEE 102, no. 12 (2014): 1–6.
<https://doi.org/10.1109/JPROC.2014.2359054>.
- Laurant, Cédric, and Renato Opice Blum. “Recent Cyber-Crime Court Decisions from Latin America Legal & Policy Developments,” 2010. https://issuu.com/cedriclaurant/docs/100920-htcia-cybercrime_court_decisions_from_latam.
- Lee, Jennifer. “Postcards From Planet Google.” *The New York Times*, 2002.
<https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ybbb2dj3x62d2lljsciidy.onion/2002/11/28/technology/postcards-from-planet-google.html>.
- León Pluas, Edwin, Esmeralda Proaño Arias, Viena Muirragui Irrazábal, and Jaime Cajamarca Yunga. “Minería de Datos En El Análisis de Tendencias Políticas En Redes Sociales.” *Ciencia Digital* 3, no. 3.4. (2019): 91–103. <https://doi.org/10.33262/cienciadigital.v3i3.4..837>.
- LePan, Nicholas. “Visualizing the Length of the Fine Print, for 14 Popular Apps.” Visual Capitalis, 2020. <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>.
- Liang, Leilei, Chuanen Li, Cuicui Meng, Xinmeng Guo, Jianping Lv, Junsong Fei, and Songli Mei. “Psychological Distress and Internet Addiction Following the COVID-19 Outbreak: Fear of Missing out and Boredom Proneness as Mediators.” *Archives of Psychiatric Nursing* 40 (2022): 8–14. <https://doi.org/10.1016/j.apnu.2022.03.007>.
- Llácer, M. R., M. Casado, and L. Buisan. “Document Sobre Bioética i Big Data de Salut: Explotació i Comercialització de Les Dades Dels Usuaris de La Sanitat Pública.” Barcelona: Publicacions i Edicions de la Universitat de Barcelona, 2015.
- Locke, John. *Segundo Tratado Sobre El Gobierno Civil*. Madrid: Alianza, 2004.
- Lyotard, Jean-François. *La Condición Postmoderna*. <https://medium.com/>. Buenos Aires: Cátedra, 1987.
- Macintyre, Amber. “Who’s Working for Your Vote?” *Tactical Tech*, 2018.
<https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote/>.
- Manota, Anthony. “Big Data: Qué Es y Para Qué Sirve,” 2021. <https://platzi.com/blog/big-data/>.
- Markoff, John. “THREATS AND RESPONSES: INTELLIGENCE; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans.” *The New York Times*, 2002.
<http://www.nytimes.com/2002/11/09/politics/09COMP.html>.
- Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data. La Revolución de Los Datos Masivos*,

- 2013.
- Mcnamee, Roger. "Facebook Will Not Fix Itself." *Time*, 2021. <https://time.com/6104863/facebook-regulation-roger-mcnamee/>.
- Meta Platforms, Inc. "FORM 10-K." Washington, D.C.: United States Securities and Exchanges Commission, 2021.
- Metz, Rachel. "The Smartphone App That Can Tell You're Depressed before You Know It Yourself." *MIT Technology Review*, 2018. <https://www.technologyreview.com/s/612266/the-smartphone-app-that-can-tell-youre-depressed-before-you-know-it-yourself/>.
- Meyer, Melanie A. "Healthcare Data Scientist Qualifications, Skills, and Job Focus: A Content Analysis of Job Postings." *Journal of the American Medical Informatics Association* 26, no. 5 (2019): 383–91. <https://doi.org/10.1093/jamia/ocy181>.
- Mill, John Stuart. *Sobre La Libertad*. Madrid: Alianza, 1993.
- Moll, Joana. "The Dating Brokers: An Autopsy of Online Love." *Tactical Tech*, 2018. <https://datadating.tacticaltech.org/viz>.
- Montagnani, Maria Lilla, and Mark Verstraete. "What Makes Data Personal?" *UC Davis Law Review* 56, no. 3 (2022): 53. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13958/10070>.
- Montgomerie, Johnna, and Samuel Roscoe. "Owning the Consumer-Getting to the Core of the Apple Business Model." *Accounting Forum* 37, no. 4 (2013): 10. <https://doi.org/10.1016/j.accfor.2013.06.003>.
- Murdock, Karla Klein. "Texting While Stressed: Implications for Students' Burnout, Sleep, and Well-Being." *Psychology of Popular Media Culture* 2, no. 4 (2013): 207–21. <https://doi.org/10.1037/ppm0000012>.
- Nix, Alexander. "The Power of Big Data and Psychographics." *Concordia Summit*, 2018. <https://archive.org/details/CambridgeAnalyticaThePowerOfBigDataAndPsychographics>.
- Noah Harari, Yuval. *Homo Deus. Breve Historia Del Mañana*. 10ma. México: Penguin Random House, 2018.
- ONU, Asamblea General de las. "Declaración Universal de Derechos Humanos," 1948. <https://doi.org/10.1017/S0031819117000274>.
- Organización de Estados Americanos [OEA]. "Convención Americana Sobre Derechos Humanos o Pacto de San José de Costa Rica." *Tratados Multilaterales Interamericanos*, no. 9460 (1978): 24. http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf.
- Panova, Tayana, and Alejandro Lleras. "Avoidance or Boredom: Negative Mental Health Outcomes

- Associated with Use of Information and Communication Technologies Depend on Users' Motivations." *Computers in Human Behavior* 58 (2016): 249–58.
<https://doi.org/10.1016/j.chb.2015.12.062>.
- Pariser, Eli. *El Filtro Burbúja: Cómo La Red Decide Lo Que Leemos y Lo Que Pensamos*. Edited by Mercedes Vaquero. Barcelona: Penguin Random House, 2017.
- Park, N., Y. Hwang, and E. Huh. "Exploring Problematic Mobile Phone Use: Relationships between Adolescents' Characteristics and Mobile Phone Addiction." *In Trabajo Presentado En El Annual Meeting of the International Communication Association, Suntec Singapore International Convention & Exhibition Centre*, 2010.
- Parraguez Kobek, Luisa, and Erick Caldera. "Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection." *Oasis* 0, no. 24 (2016): 109–28.
<https://doi.org/http://dx.doi.org/10.18601/16577558.n24.07>.
- Peces-Barba Martínez, Gregorio. *Derecho Positivo de Los Derechos Humanos*. México: Debate, 1987.
- Perea, Juan. "Divide y Vencerás, Una Estrategia Política Generalizada." *El Confidencial*, December 2, 2014. https://www.elconfidencial.com/alma-corazon-vida/2011-09-30/divide-y-venceras-una-estrategia-politica-generalizada_522447/.
- Pérez Luño, Antonio Enrique, Gregorio Peces-Barba Martínez, Francisco Javier Ansuátegui Roig, José Manuel Rodríguez Uribez, and Eusebio Frenandéz García. *Historia de Los Derechos Fundamentales Tomo II: Siglo XVIII. Vol. II: La Filosofía de Los Derechos Humanos*. Madrid: Dykinson, 2001.
- Perry Barlow, John. "Declaration of Human Rights in Cyberspace." Davos, Switzerland: Electronic Frontier Foundation, 1996. <https://www.eff.org/cyberspace-independence>.
- Platón. *Diálogos II. Gorgias, Menéxeno, Eutidemo, Menón, Crátilo. Biblioteca Clásica Gredos*. Madrid: Editorial Gredos, 1987.
- Popper, Karl R. *La Miseria Del Historicismo*. 3a ed. Madrid: Alianza, 2014.
- . *The Open Society and Its Enemies: The Spell of Plato*. 4th ed. Vol. I. London: Routledge & Kegan Paul, 1962. <https://doi.org/10.5840/thought1952272108>.
- Post, Robert C. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77, no. 5 (1989): 957–1010.
<https://doi.org/10.4159/9780674276994-004>.
- Prokop, Andrew. "Cambridge Analytica Shutting down: The Firm's Many Scandals, Explained." *Vox*, 2018. <https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller>.

- Przybylski, Andrew K., Kou Murayama, Cody R. Dehaan, and Valerie Gladwell. “Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out.” *Computers in Human Behavior* 29, no. 4 (2013): 1841–48. <https://doi.org/10.1016/j.chb.2013.02.014>.
- Radin, Margaret Jane. “Property and Personhood.” *Stanford Law Review* 34, no. 5 (1982): 957–1015. <http://www.jstor.org/stable/1228541>.
- Red Iberoamericana de protección de datos. “Estándares De Protección De Datos Personales Para Los Estados Iberoamericanos,” no. 1 (2017): 1–29. https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.
- Reid, Donna J., and Fraser J.M. Reid. “Text or Talk? Social Anxiety, Loneliness, and Divergent Preferences for Cell Phone Use.” *Cyberpsychology and Behavior* 10, no. 3 (2007): 424–35. <https://doi.org/10.1089/cpb.2006.9936>.
- Risen, James, and Eric Lichtblau. “Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring.” *The New York Times*, 2005. <https://doi.org/10.4324/9781315549293-15>.
- Ros Velasco, Josefa, and S. Gutiérrez Manjón. “The Expression of Boredom and Unwanted Loneliness on Twitch.” *Icono* 20, no. 1 (2022).
- Rosen, L. D., K. Whaling, S. Rab, L. M. Carrier, and N. A. Cheever. “Is Facebook Creating ‘IDisorders’? The Link between Clinical Symptoms of Psychiatric Disorders and Technology Use, Attitudes and Anxiety.” *Computers in Human Behavior* 29, no. 3 (2013): 1243–54. <https://doi.org/10.1016/j.chb.2012.11.012>.
- Rubel, Alan, Clinton Castro, and Adam Pham. *Algorithms and Autonomy*. Cambridge: Cambridge University Press, 2021. <https://doi.org/10.1017/9781108895057>.
- Ruspini, Sonia, and Thierry Chaminade. “Manipulación y El Poder de Las Emociones.” *DW Documental*, 2022. <https://www.youtube.com/watch?v=RRxJ7U0-G90>.
- Sánchez-Martínez, Mercedes, and Angel Otero. “Factors Associated with Cell Phone Use in Adolescents in the Community of Madrid (Spain).” *Cyberpsychology and Behavior* 12, no. 2 (2009): 131–37. <https://doi.org/10.1089/cpb.2008.0164>.
- Sánchez Rojo, Alberto. “Educación y Derecho a La Privacidad En La Sociedad Del Conocimiento.” Tesis Doctoral, Universidad Complutense de Madrid, 2015. <https://doi.org/10.14201/14771>.
- Sanz García, Rosa María. “Redes Sociales Online: Fuentes de Acceso Público Ficheros de Datos Personales Privados (Aplicación de Las Directivas de Protección de Datos y Privacidad En Las Comunicaciones Electrónicas).” *Revista de Derecho Político* 81 (2011): 101–54. <http://e-spacio.uned.es/revistasuned/index.php/derechopolitico/article/view/9151>.
- Savage, Charlie. “Declassified Report Shows Doubts About Value of N.S.A.’s Warrantless

- Spying.” *The New York Times*, 2015.
- Scherer, Klaus R, Tanja Banziger, and Etienne B Roesch. *Blueprint for Affective Computing: A Sourcebook. Series in Affective Science*, 2010.
- Sen, Amartya. “Human Rights and Capabilities.” *Journal of Human Development* 6, no. 2 (2005): 151–66. <https://doi.org/10.1080/14649880500120491>.
- Sharma, Manoj Kumar, Nisha John, and Maya Sahu. “Influence of Social Media on Mental Health: A Systematic Review.” *Current Opinion in Psychiatry* 33, no. 5 (2020): 467–75. <https://doi.org/10.1097/YCO.0000000000000631>.
- Silverman, Craig, Ryan Mac, and Pranav Dixit. “‘I Have Blood on My Hands’: A Whistleblower Says Facebook Ignored Global Political Manipulation.” BuzzFeed News, 2020. <https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo>.
- Snowden, Edward. *Permanent Record*. New York: Metropolitan Books, 2019.
- Solove, Daniel. “Autogestión de La Privacidad y El Dilema Del Consentimiento.” *Revista Chilena de Derecho y Tecnología* 2, no. 3 (2014): 11–48. <https://doi.org/10.5354/0719-2584.2013.30308>.
- Solove, Daniel J. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *The Individual and Privacy: Volume I*, 2016, 745–72. <https://digital.sandiego.edu/cgi/viewcontent.cgi?article=2790&context=sdlr>.
- Soto, Yasmina. “Datos Masivos Con Privacidad y No Contra Privacidad.” *Revista de Bioética y Derecho* 0, no. 40 (2017): 101–14. <https://doi.org/10.1344/rbd2017.40.19165>.
- Strickland, Amelia. “Exploring the Effect of Social Media Use on the Mental Health on Young Adults.” *Stars*. University of Central Florida, 2014.
- Sunstein, Cass R. “The Age of Behavioral Science.” In *The Ethics of Influence*, 1–17. Cambridge University Press, 2016. <https://doi.org/10.1017/cbo9781316493021.001>.
- Tavani, Herman. “Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy.” *Metaphilosophy* 38, no. 1 (2007): 1–22. <http://www.jstor.org/stable/24439672>.
- Tavani, Herman T. “Informational Privacy, Data Mining, and the Internet.” *Ethics and Information Technology* 1, no. 2 (1999): 137–45. <https://doi.org/10.1023/A:1010063528863>.
- Thomée, Sara, Mats Eklöf, Ewa Gustafsson, Ralph Nilsson, and Mats Hagberg. “Prevalence of Perceived Stress, Symptoms of Depression and Sleep Disturbances in Relation to Information and Communication Technology (ICT) Use among Young Adults - an Explorative Prospective Study.” *Computers in Human Behavior* 23, no. 3 (2007): 1300–1321. <https://doi.org/10.1016/j.chb.2004.12.007>.

- Toscano, Manuel. “Sobre El Concepto de Privacidad: La Relación Entre Privacidad e Intimidad.” *Isegoria*, no. 57 (2017): 533–52. <https://doi.org/10.3989/isegoria.2017.057.06>.
- UK, Anxiety. “Anxiety UK Study Finds Technology Can Increase Anxiety,” 2012. <http://www.anxietyuk.org.uk/2012/07/for-some-with-anxiety-technology- can- increase- anxiety/>.
- Unidas, Asamblea General de las Naciones. “Directrices Para La Regulación de Los Archivos de Los Datos Personales Informatizados,” 1990.
- Unión, Cámara de Diputados del Congreso de la. Constitución Política de los Estados Unidos Mexicanos, Pub. L. No. 28-05–2021, Diario Oficial de la Federación 354 (1917). <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>.
- . Ley Federal de Protección de Datos Personales en posesión de los particulares, Pub. L. No. 05-07–2010, 18 (2010).
- . Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Pub. L. No. 26-01–2017, Diario Oficial de la Federación 52 (2017).
- Unión Europea. “Reglamento General de Protección de Datos,” 2019.
- United States Government. “The USA PATRIOT Act : Preserving Life and Liberty.” *USA Department of Justice*, 2001. http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.
- Vallejo Ballesteros, Henry Fernando, Edelmira Guevara Iñiguez, and Segundo Rafael Medina Velasco. “Minería de Datos.” *Recimundo 2* (2018): 339–49. <https://doi.org/10.26820/recimundo/2.esp.2018.339-349>.
- Vasak, Karel. “A 30-Year Struggle. The Sustained Efforts to Give Force of Law to the Universal Declaration of Human Rights.” *The UNESCO Courier*. París: UNESCO, 1977.
- Véliz, Carissa. “La Privacidad Como Instrumento de Resistencia Colectiva.” *Anuario Internacional CIDOB 2021*, 2021, 21–27.
- . “London Speaker Bureau. Interview Series,” 2021. <https://londonspeakerbureau.com/interview-carissa-veliz/>.
- . “Más Sobre Privacidad. Respuesta a Los Comentarios Sobre ‘Privacidad Es Poder.’” *EUNOMÍA. Revista En Cultura de La Legalidad*, no. 21 (2021): 431–34. <https://doi.org/10.20318/eunomia.2021.6366>.
- . *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. London: Bantam Press, 2020.
- . “The Internet and Privacy.” *Ethics and the Contemporary World*, no. January 2018 (2019): 149–59. <https://doi.org/10.4324/9781315107752-12>.
- Viljoen, Salome. “A Relational Theory of Data Governance.” *Yale Law Journal* 131, no. 2 (2021):

573–654.

- Wall, Matthew. “5G: ‘A Cyber-Attack Could Stop the Country’ - BBC News.” BBC, 2018. <https://www.bbc.co.uk/news/business-45952693>.
- Ware, Alan. “The Concept of Manipulation: Its Relation to Democracy and Power.” *British Journal of Political Science* 11, no. 2 (1981): 163–81. <https://doi.org/10.1017/S0007123400002556>.
- Wark, Mckenzie. “Manifiesto Hacker.” Accessed November 5, 2021. http://subsol.c3.hu/subsol_2/contributors0/warktext.html.
- Warren, Samuel, and Louis Brandeis. *El Derecho a La Intimidación*. Edited by Benigno Pendás and Pilar Baselga. 1a ed. Madrid: Civitas, 1995.
- Weaver, Matthew. “Facebook Scandal: I Am Being Used as Scapegoat – Academic Who Mined Data.” *The Guardian*, 2018. <https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica>.
- Westin, Alan F. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59, no. 2 (2003): 431–53. www.forstbuch.de.
- World Health Organization. “WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance,” 2020. <https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance>.
- Wolff, Jonathan. “The Lure of Fascism.” Aeon, 2020. <https://doi.org/10.4324/9780203007259-32>.
- Wylie, Christopher. *Mindf*ck Cambridge Analytica: La Trama Para Desestabilizar*. Barcelona: Roca Editorial, 2020.
- Zambrano, María. *Persona y Democracia*. España: Alianza, 2019.
- Zarouali, Brahim, Tom Dobber, Guy De Pauw, and Claes de Vreese. “Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media.” *Communication Research*, 2020. <https://doi.org/10.1177/0093650220961965>.
- Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019.
- Zuiderveen, Frederik J., Judith Möller, Sanne Kruikemeier, Ronan Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo, and Claes de Vreese. “Online Political Microtargeting: Promises and Threats for Democracy.” *Utrecht Law Review* 14, no. 1 (2018): 82–96. <https://doi.org/10.18352/ulr.420>.

Anexos

^I El asesor de esta tesis, el Doctor José Luis Cisneros Arellano, ha realizado una revisión argumentativa lógica de este trabajo en la cual concluye que tanto los silogismos, el dilema generado y la argumentación propuesta son válidas, y por lo tanto es un trabajo científicamente válido.

Se notó que el primer proceso argumentativo es de corte silogístico hipotético, es decir

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \therefore \\ p \rightarrow r \end{array}$$

Esto es: privacidad y sus características, como condición para la democracia. La democracia como condición para el respeto de los derechos y el ejercicio auténtico del poder individual y colectivo. Por tanto, al haber privacidad, hay derechos.

Luego se plantea un nuevo escenario: las empresas tecnológicas (Big Tech) basadas en el conocimiento de los datos personales son condición para la cuantificación de la privacidad. La cuantificación es condición para la inferencia, predicción y manipulación. Por tanto, las Big Tech producen manipulación.

Al final se hace una unión de todo con un dilema constructivo:

$$\begin{array}{l} (p \rightarrow q) \wedge (r \rightarrow s) \\ p \vee r \\ \therefore \\ q \vee s \end{array}$$

Esto es: hay privacidad entonces hay derechos, y luego hay Big Tech entonces hay manipulación (relación hipotética).

Con ello el argumento muestra que se tiene privacidad o empresas tecnológicas, por tanto se tiene derechos o manipulación. Sin embargo, al generar el concepto de Doble Poder ambas concepciones (realidades) existen en una disyunción inclusiva y en un movimiento hegeliano, esto no se deduce de los silogismos ni del dilema, sino de la unión de una proposición como $q \vee s$ –qu o s– y por lo tanto, alcanza el grado de lógica de segundo orden. Por tal motivo, Cisneros Arellano reconoce que el concepto de Doble Poder es metafísico porque da un sentido que engloba todo este trabajo investigativo. Está en el nivel del metalenguaje. [José Luis Cisneros Arellano, “La Investigación Filosófica Desde La Relación: Una Mirada Panorámica a La Luz de Una Propuesta Metodológica,” *Tesis (Lima)* 14, no. 18 (2021): 491–509, <https://doi.org/10.15381/tesis.v14i19.20516>.] [José Luis Cisneros Arellano, *Filosofía Del Pensamiento Complejo. Una Reflexión Sobre Edgar Morín* (Monterrey, N.L.: Centro de Estudios Humanísticos, UANL, 2020).]

^{II} Vale la pena señalar la relevancia que cobran en esa confusión las traducciones hechas del inglés al español, dado que la gran mayoría de estudios e investigaciones referentes a la privacidad han sido realizados por autores de habla inglesa. En las traducciones que se han hecho a nuestro idioma la palabra privacidad es traducida como intimidad, generando así que estas palabras se tornen

equivalentes o sinónimos, siendo que no es así. Para ello cabe echar un vistazo al diccionario de la Real Academia Española. Privacidad es entendida como ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Intimidad es la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia. [Real Academia Española, “Diccionario de La Lengua Española,” 23, [versión 23.5 en línea], 2022, <https://dle.rae.es.>]

^{III} Pensar en la idea del common law desde la evolución que responde a las necesidades actuales, nos hace pensar en la capacidad que se tiene para dar respuesta a las problemáticas de hoy con respecto a la privacidad, como lo fue en 1890, cuando se pensó en la protección de tal derecho.

^{IV} A pesar de que todo ello tiene sentido y guarda relación con nuestra idea de privacidad en la vida de la sociedad democrática, no podemos reducir la privacidad en términos de no injerencia o del derecho a no ser molestado, pues como dice Tavani puede suceder que se confunda la condición o el contenido de la privacidad con el derecho a la privacidad, de la misma manera que al definir la privacidad como estar libre de intrusiones se confunde la privacidad con la libertad [Herman Tavani, “Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy,” *Metaphilosophy* 38, no. 1 (2007): 5, <http://www.jstor.org/stable/24439672>]. Sin embargo, esta propuesta de privacidad dada por varios autores encuentra su sentido y significado en la respuesta a la problemática con que se enfrenta en su contexto actual. Así que, ciertamente es probable tal confusión con otros conceptos, sin embargo no por ello hemos de despreciar estos análisis y señalamientos acerca de la privacidad dada su correspondencia casi directa en la suma con otros análisis con la jurisprudencia guiada por las declaraciones de derechos humanos y las constituciones de cada Estado.

^V Solove nos invita a pensar en lo confuso e indefinible que es nuestro concepto: «Los académicos han proclamado que la privacidad es un concepto tan confuso que tiene poca utilidad. Según Arthur Miller, la privacidad es "exasperantemente vaga y evanescente". Como declara Hyman Gross, "el concepto de privacidad está infectado de perniciosas ambigüedades". Colin Bennett señala de forma similar que "los intentos de definir el concepto de 'privacidad' no han tenido generalmente ningún éxito.” Robert Post declara que "la privacidad es un valor tan complejo, tan enredado en dimensiones competitivas y contradictorias, tan cargado de significados diversos y distintos, que a veces desespere de que pueda ser abordado de forma útil". "Quizá lo más sorprendente del derecho a la privacidad", observa Judith Jarvis Thomson, "es que nadie parece tener una idea muy clara de lo que es"» [Daniel J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *The Individual and Privacy: Volume I*, 2016, 754, <https://digital.sandiego.edu/cgi/viewcontent.cgi?article=2790&context=sdlr>.]

^{VI} La recopilación de datos puede matar. Los holandeses tuvieron la mayor tasa de mortalidad de judíos en la Europa ocupada: el 73%. De los 140.000 judíos holandeses estimados, más de 170.000 fueron deportados, y 102.000 de ellos fueron asesinados. [Carissa Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data* (London: Bantam Press, 2020).]

^{VII} Tal definición fue expuesta por Moor, James H. 1997. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27, no. 3 (Septiembre): 27-32.

^{viii} Con el pronunciamiento del derecho a la protección de los datos personales nace también un término análogo al Habeas Corpus, que hace referencia precisamente al control en los datos personales: el Habeas Data; es una noción jurídica que protege toda la información relativa al individuo, desde la personal hasta la financiera, dándole el poder de decidir cómo y dónde pueden utilizarse esos datos. Esto quiere decir también, que una persona puede solicitar ver toda la información que una empresa o agencia gubernamental tiene sobre ella. El derecho de Habeas Data se remonta a la primera ley de protección de datos llamada Bundesdatenschutzgesetz que se promulgó en Alemania el 7 de octubre de 1970. Los esfuerzos se dirigen principalmente en la creación de legislaciones de control propias para la protección de los datos personales. En la Convención en Ciberdelincuencia en 2001 se propuso crear: “reglamentos y políticas; inspecciones financieras protección de datos y privacidad; preparación de fiscales y jueces; cooperación internacional con más de 120 países; aplicación de la ley; creación de talleres parlamentarios regionales en América Latina; y fortalecimiento de las legislaciones en más de 100 países” [Cédric Laurant and Renato Opice Blum, “Recent Cyber-Crime Court Decisions from Latin America Legal & Policy Developments,” 2010, https://issuu.com/cedriclaurant/docs/100920-htcia-cybercrime_court_decisions_from_latam.] Cabe resaltar las características que marcan diferencia entre el Derecho a la Privacidad, el Habeas Data y la Protección a los datos personales. La primera es la enmarcada dentro de la Declaración de los Derechos Humanos promulgada por la Asamblea General: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.» [Asamblea General de las ONU, “Declaración Universal de Derechos Humanos,” 1948, <https://doi.org/10.1017/S0031819117000274>.] La segunda precisamente se refiere al derecho legal de un ciudadano sobre su propia información, mientras que la protección de datos denota cómo debe obtenerse, procesarse y protegerse la información. [Luisa Parraguez Kobek and Erick Caldera, “Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection,” *Oasis* 0, no. 24 (2016): 109–28, <https://doi.org/http://dx.doi.org/10.18601/16577558.n24.07>.] En México el artículo dieciséis constitucional protege el derecho a la privacidad y a la protección de los datos personales: «Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros». [Cámara de Diputados del Congreso de la Unión, “Constitución Política de Los Estados Unidos Mexicanos,” Pub. L. No. 28-05–2021, Diario Oficial de la Federación 354 (1917), <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>.]

^{ix} El London Speaker Bureau es un recurso global para corporaciones y gobiernos, proporcionando oradores, clases magistrales de aprendizaje para ejecutivos y asesores de sala de juntas. Representan a algunos de los líderes empresariales y políticos más influyentes del mundo. Actualmente son 110 colegas en 18 países de Europa, Oriente Medio, África, Asia y Norteamérica. Son la mayor red internacional de expertos y asesores para empresas y gobiernos de todo el mundo. [<https://londonspeakerbureau.com/>]

^X Profesora asociada del Instituto de Ética en Inteligencia Artificial y miembro del Hertford College de la Universidad de Oxford, además es autora del libro “Privacy is Power” [Privacidad es Poder] publicado en 2020 en Bantam Press. El libro sostiene que la gente debe proteger su privacidad porque la privacidad es un tipo de poder. Si cedemos demasiados datos a las empresas, los ricos gobernarán. Si damos demasiados datos personales a los gobiernos, corremos el riesgo de caer en el autoritarismo. Carissa ha sido miembro del Grupo de Expertos encargado de redactar una Carta de Derechos Digitales en el Ministerio de Economía y Transformación Digital de España. Es testigo del Comité Selecto de Comunicaciones y Digital de la Cámara de los Lores, así como miembro del Grupo Asesor de Alto Nivel sobre Tecnología y Orden Global del Ministerio de Asuntos Exteriores en España. Ha publicado artículos en The Guardian, The New York Times, New Statesman, The Independent y El País. Su trabajo académico se ha publicado en The Harvard Business Review, Nature Electronics, Nature Energy, AI & Society y The American Journal of Bioethics, entre otros. [Carissa Véliz, “London Speaker Bureau. Interview Series,” 2021, <https://londonspeakerbureau.com/interview-carissa-veliz/>.]

^{XI} «Edward Snowden nació en Elizabeth City, Carolina del Norte, y creció a la sombra de Fort Meade. Ingeniero de sistemas de formación, fue oficial de la Agencia Central de Inteligencia (CIA) y trabajó como contratista para la Agencia de Seguridad Nacional (NSA). Ha recibido numerosos premios por su servicio público, como el Right Livelihood Award, el German Whistleblower Prize, el Ridenhour Prize for Truth-Telling y la Carl von Ossietzky Medal de la Liga Internacional de Derechos Humanos. En la actualidad, es presidente del consejo de administración de la Fundación para la Libertad de Prensa.»
[Edward Snowden, *Permanent Record* (New York: Metropolitan Books, 2019).]

^{XII} Esta definición es acorde a la dada por el Convenio 108 del Consejo Europeo promulgado el 28 de enero de 1981 el cual trata de la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este documento fue pionero en el cuidado del tratamiento de datos personales a través de modelos automatizados. En él se lee lo siguiente: “«Datos de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»)» [Consejo de Europa, “Convenio 108” (1981).]

^{XIII} El Reglamento general de protección de datos (RGPD) actualiza y moderniza los principios consagrados en la Directiva sobre protección de datos de 1995 para garantizar el derecho a la intimidad. Fue creado por y para la Unión Europea, sin embargo su calado ha tenido fuerte impacto en otras regiones del mundo.

Este Reglamento es una medida crucial para reforzar los derechos fundamentales de los ciudadanos en la era digital y facilitar la actividad empresarial simplificando la normativa para las empresas en el mercado único digital. Con un único acto legislativo se eliminarán la actual fragmentación y la onerosa carga administrativa. El Reglamento presta especial atención a:

- reforzar los derechos de las personas;
- fortalecer el mercado interior de la UE;
- garantizar un cumplimiento más estricto de las normas;
- simplificar las transferencias internacionales de datos personales; y
- establecer normas internacionales de protección de datos.

Gracias a estos cambios, los ciudadanos tendrán más control sobre sus datos personales y podrán acceder más fácilmente a ellos. Se pretende así garantizar la protección de los datos personales, con independencia de su lugar de envío, tratamiento o conservación, incluso cuando ese lugar está fuera de la UE, como ocurre a menudo en Internet. Este reglamento está en vigor desde el 25 de mayo del 2019. [Unión Europea, “Reglamento General de Protección de Datos,” 2019. https://www.eeas.europa.eu/eeas/reglamento-general-de-proteccion-de-datos_es?s=40]

^{xiv} Además de estas categorías de datos personales existen otras, como datos relativos a la salud, datos genéticos [Comisión Europea. (2017). Reglamento General de Protección de Datos. Diario Oficial de la Unión Europea. Art. 4], inclusive una nueva generación de datos relativos a la información neuronal y cerebral de las personas (Cfr. OECD, Recommendation of the Council on Responsible Innovation in Neurotechnology, OECD/LEGAL/0457). Sin embargo, y para los propósitos de este trabajo, solo se tomarán en cuenta los ya definidos dado el valor que aportan al sustento de la argumentación principal.

^{xv} En esencia, un algoritmo es una secuencia de reglas o normas que una computadora utiliza para completar una tarea específica. Es el seguimiento – como en el caso de alguna receta de cocina o la secuencia del armado de un cubo de Rubik – de un conjunto de instrucciones para resolver eficazmente un problema. En el caso de los algoritmos computacionales, son programados a través de código informático y son usados en las redes sociales, los smartphones, las navegaciones por Internet o en las aplicaciones de citas. También hacen predicciones y toman decisiones en diversos ámbitos de la vida humana. [The Alan Turing Institute, “What Is an Algorithm?,” YouTube, 2021, https://www.youtube.com/watch?v=i76WAFOUT_Y.] En el caso de la intervención de esta tecnología en la vida humana ya no solo se le cataloga como un siempre conjunto de instrucciones que resuelven un problema, sino que en este sentido, los algoritmos se entienden mejor como partes constitutivas de sistemas socio-técnicos, los cuales son utilizados por individuos y grupos que afectan a otros individuos y grupos, de modo que constituyen un sistema interrelacionado que es a la vez social y tecnológico. [Alan Rubel, Clinton Castro, and Adam Pham, *Algorithms and Autonomy* (Cambridge: Cambridge University Press, 2021), <https://doi.org/10.1017/9781108895057>.]

^{xvi} Mediante este tipo de procedimientos y protocolos ya establecidos los anunciantes buscan ganar a toda costa mayores visitas a sus sitios web a través de diversas artimañas de atracción; lo que importa es que la finalidad se cumpla: atraer nuevos clientes haciendo uso de los medios que sean necesarios. Para señalar esta manera de proceder en la programación de las tecnologías de anuncios existe un término muy sonado últimamente: Clickbait. Precisamente este concepto nos habla acerca de la lucha constante por ganar más y nuevos clics [Rubel et al., 2021, *Algorithms and Autonomy*, Cambridge, Cambridge University Press, p. 111] que lleven a más información clave para conocer a sus futuros clientes. Como se hace en el RTB, el anunciante cruza su información con la que le es vendida por Google para deducir quienes serán sus futuros clientes. Curiosamente para el científico de datos Jeffrey Hammerbacher – que es fundador de la empresa de análisis de datos Cloudera – quien anteriormente había trabajado en Facebook haciendo estadísticas, dijo en una entrevista: "Las mejores mentes de mi generación están pensando en cómo hacer que la gente haga clic en los anuncios". Cuando trabajaba en Facebook su trabajo consistía en construir una infraestructura escalable para el almacenamiento y el análisis de datos en la mayor red social del mundo. En definitiva su salida de

esta empresa dejó en claro que sus aspiraciones como científico de datos no consistían en crear un sistema de ingeniería que ganara la mayor cantidad de clics. [Baer, 2013, Why Data God Jeffrey Hammerbacher Left Facebook To Found Cloudera, Fast Company, <https://www.fastcompany.com/3008436/why-data-god-jeffrey-hammerbacher-left-facebook-found-cloudera>.]

^{xvii} En la actualidad existe un sistema de anuncios desarrollado por Google, el cual parece ser un buen ejemplo que representa el funcionamiento de los anuncios dirigidos: Oferta en Tiempo Real (mejor conocido como Real-Time Bidding). Es un conjunto de tecnologías y prácticas utilizadas en la publicidad programática. Se apoya en la tecnología publicitaria (adtech), permitiendo a los anunciantes competir por el espacio publicitario digital disponible en milisegundos, colocando miles de millones de anuncios online en páginas web y aplicaciones. [Information Commissioner's Office, "Update Report into Adtech and Real Time Bidding," 2019, <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>.] El RTB funciona de la siguiente manera:

- Se realiza un envío de los datos personales de los usuarios de las páginas web para interesar a los anunciantes.
- Luego, el anunciante reconoce al usuario a través de los datos personales como un visitante de su página web.
- El anunciante está dispuesto a pagar más y así atraer a la persona que ya ha visitado su sitio web.
- Finalmente se muestra el anuncio al usuario que con altas probabilidades realizará la compra en el sitio web del anunciante. [Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*.] Todo este procedimiento de "subasta" de datos sucede en tiempos minúsculos. "Google espera entre 80 y 1000 ms para que la aplicación de oferta responda, dependiendo del formato y del tipo de subasta." [Google, "Real-Time Bidding," GOOGLE INC., accessed February 19, 2022, <https://developers.google.com/authorized-buyers/rtb/start>.]

^{xviii} En esencia, la tecnología de la minería de datos combina la inteligencia artificial, el análisis estadístico, la adquisición de conocimientos a partir de sistemas expertos, la visualización de datos, el descubrimiento de máquinas y el reconocimiento de patrones. Cavoukian define la minería de datos como un "conjunto de técnicas automatizadas que se utilizan para extraer información oculta o desconocida de grandes bases de datos "1. Es una técnica para el descubrimiento eficiente de información valiosa y no obvia. Mediante las técnicas de minería de datos es posible desenterrar patrones y relaciones, que antes eran desconocidos, y utilizar esta "nueva" información, es decir, nuevos hechos y relaciones en los datos para tomar decisiones y hacer previsiones. En su sentido más amplio, la minería de datos es el proceso de (A) encontrar patrones o correlaciones en los datos (por ejemplo, registros) almacenados en grandes bases de datos y (B) analizar esos datos desde diferentes perspectivas, categorizarlos y resumirlos en información útil. [Herman T. Tavani, "Informational Privacy, Data Mining, and the Internet," *Ethics and Information Technology* 1, no. 2 (1999): 137–45, <https://doi.org/10.1023/A:1010063528863>.]

^{xix} Según Álvaro del Castillo, fundador y director ejecutivo de TapTap, (empresa Data Broker) – en conversación con eldiario.es. – el valor añadido entre la compra y la venta es la posibilidad de aumentar la efectividad de la publicidad, haciendo que llegue a personas interesadas en ella mientras

se descartan contextos poco favorables para ese anuncio en concreto. “Tenemos un ratio de retención de clientes del 100%”, presume. [Carlos Del Castillo, “Así Trabaja Una Empresa Española Que Compra y Vende Datos Personales Para Hacer Publicidad: ‘Recogemos Toda La Información Posible,’” *Diario.Es*, October 21, 2019, https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_1_1297691.html.]

^{xx} Las ‘Cookies’ son ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web. Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades. [Rosa María Sanz García, “Redes Sociales Online: Fuentes de Acceso Público Ficheros de Datos Personales Privados (Aplicación de Las Directivas de Protección de Datos y Privacidad En Las Comunicaciones Electrónicas),” *Revista de Derecho Político* 81 (2011): 124, <http://e-spacio.uned.es/revistasuned/index.php/derechopolitico/article/view/9151>.]

^{xxi} Una web beacon o web bug es una diminuta imagen en una página web o en un mensaje de correo electrónico que se diseña para controlar quién lee el mensaje. Su tamaño es inapreciable, pudiendo ser un píxel en formato GIF y transparente. Se representan como etiquetas HTML. Una web beacon permite tener cierta información sobre el usuario (o del visitante de una página web o del lector de mensaje de correo electrónico). [Sanz García, 124.]

^{xxii} Dentro de estos dispositivos y sistemas podemos mencionar los dispositivos Smart-Home Nest: «Nest ha funcionado como una unidad independiente desde su adquisición por parte de Alphabet de 3.200 millones de dólares (2.300 millones de libras) en 2014. Sus productos para el hogar inteligente se benefician de la recopilación de datos sobre sus usuarios. Los productos de Nest incluyen:

- cámaras de seguridad conectadas a Internet para el interior y el exterior del hogar
- termostatos que utilizan sensores de detección de movimiento para detectar cuando los propietarios están cerca
- un timbre equipado con cámara - un sistema de alarma que detecta el movimiento y un detector de humo

Además, la aplicación de la división puede configurarse para recopilar datos de otros productos - como coches, hornos, rastreadores de fitness e incluso camas equipadas con sensores- para ayudar a "ahorrar energía... y estar seguros"» [Leo Kelion, “Google-Nest Merger Raises Privacy Issues,” *BBC News*, 2018, <http://www.bbc.co.uk/news/technology-42989073>.] Estos dispositivos recogen datos sobre su uso y su entorno. Utilizan sensores de movimiento y computación para «aprender» los comportamientos de los habitantes de una casa. Esos sistemas pueden activar luces, por ejemplo, si se detecta un movimiento anómalo, indicar que se grabe en vídeo y audio lo que está ocurriendo, e incluso enviar notificaciones a los propietarios o a otras personas. [Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019), 6.]

En diversas ocasiones los encargados de las tareas principales en Google dan declaraciones demasiado optimistas al respecto del desarrollo de sus productos y plataformas, como es el caso de

la declaración dada en 2017 por Sundar Pichai director ejecutivo de la compañía: «Pichai anunció en aquella ocasión que siete de los más destacados “productos y plataformas” de la compañía atraen a 1.000 millones de usuarios activos al mes: hablamos de Gmail, Android, Chrome, Maps, el buscador de Google, YouTube y Google Play Store. Habló también de que había ya 2.000 millones de dispositivos Android activos; 800 millones de usuarios activos mensuales de Google Drive, donde se subían unos 3.000 millones de objetos a la semana; 500 millones de usuarios de la aplicación Fotos, que subían diariamente 1.200 millones de fotografías; y 100 millones de dispositivos que usaban el asistente de Google. Cada dispositivo se reestructura para convertirse en un vehículo de ese asistente, que está disponible así “durante todo el día, en casa y fuera de casa” para toda clase de tareas o funciones sociales. Pichai dijo que quería más aún y pidió a su equipo un esfuerzo adicional para conseguirlo: “Debemos ir más a fondo”. El asistente debería estar en cualquier lugar “donde las personas puedan querer pedir ayuda”». [Zuboff, 418.]

^{xxiii} Como ya se ha mencionado anteriormente, la privacidad es una cualidad humana, intrínsecamente personal. Por tal motivo consideramos que la caracterización del trato al sujeto como usuario despersonaliza a quien ingresan a un sitio web. En este sentido la palabra usuario, será remplazada en varias ocasiones por persona, con el único propósito de reconocimiento entre privacidad y persona.

^{xxiv} Por poner un ejemplo, la propia dirección IP de los dispositivos es reconocida como datos personal, puesto que puede asociarse a una persona identificable, a través del contenido de la información sobre los usos y hábitos en Internet de la persona. [Sanz García, “Redes Sociales Online: Fuentes de Acceso Público Ficheros de Datos Personales Privados (Aplicación de Las Directivas de Protección de Datos y Privacidad En Las Comunicaciones Electrónicas),” 124–25.]

^{xxv} La gran mayoría de las personas no leen las notificaciones de privacidad. Uno de los factores más importantes de esta problemática es lo largo que puede ser su extensión. Por ejemplo, el documento de los términos y condiciones de Microsoft está conformado por 15,260 palabras (en inglés) lo cual toma 63.5 minutos de lectura tomando como base una lectura de 240 palabras por minuto. Por otro lado, el documento de menor extensión es el de la red social Instagram que cuenta con 2451 palabras (en inglés) y toma 9.42 minutos de lectura. Por este motivo y seguramente, por el más obvio, que al final si no se aceptan los términos y condiciones no es posible acceder a los servicios que se ofrecen. Es decir, no existe una opción de común acuerdo; es un acuerdo si y solo si la decisión que se toma está en concordancia con lo estipulado en el documento de la misma plataforma. Así que de poco o nada sirve leer tales documentos si al final se tiene que estar de acuerdo con las condiciones para hacer uso de sus servicios, los cuales, muchas veces son necesariamente requeridos por los centros escolares o de trabajo. Es por eso, que un estudio realizado por Vizualist Capitalist arrojó como resultado que el 97% de las personas en los rangos de edad de 18 a 34 años está de acuerdo con los términos y condiciones de las plataformas y sitios web sin haberlos leído. [Nicholas LePan, “Visualizing the Length of the Fine Print, for 14 Popular Apps,” Visual Capitalis, 2020, <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>.] [Omri Ben-Shahar and Carl E. Schneider, “The Failure of Mandate Disclosure, Part 4,” *Actual Problems of Economics and Law* 11, no. 4 (2017): 146–69, <https://doi.org/http://dx.doi.org/10.21202/1993-047X.11.2017.4.146-169>.]

^{xxvi} Problemáticas cognitivas: «La autogestión de la privacidad supone una persona racional e informada que toma decisiones apropiadas respecto a consentir o no en las múltiples formas de recolección, uso y divulgación de datos personales. Pero tanto evidencia empírica como estudios en ciencias sociales muestran que la capacidad de las personas para tomar estas decisiones informadas y racionales ni siquiera se acercan a la visión contemplada por la autogestión de la privacidad». Los obstáculos para que se realice a cabalidad este ideal son: «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». [Daniel Solove, “Autogestión de La Privacidad y El Dilema Del Consentimiento,” *Revista Chilena de Derecho y Tecnología* 2, no. 3 (2014): 17–23, <https://doi.org/10.5354/0719-2584.2013.30308>.]

Problemáticas estructurales: Estos problemas «impiden evaluar adecuadamente los costos y beneficios de consentir las diversas formas de recolección, uso y divulgación de información personal» Uno de ellos es el problema de escala: la existencia de innumerables entidades que tratan datos personales sin que la gente se dé cuenta genera que las personas tengan dificultades para administrar su privacidad con entidades que no conocen. Otro es el problema de agregación: dadas las clases de nueva información que pueden ser obtenidas a partir del análisis de información existente y las predicciones que pueden ser realizadas a partir de estos datos, lo complejo y lo vasto de estos nuevos datos evolucionan demasiado rápido como para que las personas puedan evaluar completamente los riesgos y beneficios involucrados. [Solove, 23–29.] Y aunque la legislación reciente se esfuerza por que esta autogestión de la privacidad sea eficaz, como se ve a continuación: «El Reglamento General de Protección de Datos obliga a los proveedores de sitios web a hacer obvia y explícita su personalización mediante cookies de seguimiento. Los sitios web tienen que informar a los usuarios de la Unión Europea de sus mecanismos de seguimiento y los usuarios pueden optar por continuar en el sitio web y rechazar las cookies de seguimiento que no son necesarias para el funcionamiento básico del sitio web (...) La necesidad de aceptar las cookies de rastreo funciona como una advertencia que puede disminuir la confianza en un sitio web y, por lo tanto, compensa algunos de los efectos del diseño fácil de usar». [Fleur Jongepier and Michael Klenk, *The Philosophy of Online Manipulation, The Philosophy of Online Manipulation* (New York: Routledge, 2022), 306, <https://doi.org/10.4324/9781003205425>.] la realidad es que sus esfuerzos siguen arrastrando las problemáticas que ya hemos mencionado.

^{xxvii} Meta Inc. se describe a sí misma de la siguiente manera: «Nuestra misión es dar a las personas el poder de construir una comunidad y acercar el mundo. Todos nuestros productos, incluidas nuestras aplicaciones, comparten la visión de ayudar a dar vida al metaverso. Construimos tecnología que ayuda a las personas a conectarse, a encontrar comunidades y a hacer crecer sus negocios. Nuestros útiles y atractivos productos permiten a las personas conectarse y compartir con sus amigos y familiares a través de dispositivos móviles, ordenadores personales, auriculares de realidad virtual (RV), wearables y dispositivos domésticos. También ayudamos a las personas a descubrir y aprender sobre lo que ocurre en el mundo que les rodea, permitimos que las personas compartan sus opiniones, ideas, fotos y vídeos, y otras actividades con audiencias que van desde sus familiares y amigos más cercanos hasta el público en general, y que se mantengan conectadas en cualquier lugar accediendo a

nuestros productos. Meta va más allá de las pantallas 2D y se acerca a experiencias inmersivas como la realidad aumentada y virtual para ayudar a construir el metaverso, que creemos que es la próxima evolución de la tecnología social.» Su negocio de publicidad se realiza de la siguiente manera: «Los anuncios en nuestras plataformas permiten a los comerciantes llegar a las personas en función de una serie de factores como la edad, el sexo, la ubicación, los intereses y los comportamientos. Los comercializadores compran anuncios que pueden aparecer en múltiples lugares, incluyendo en Facebook, Instagram, Messenger y aplicaciones y sitios web de terceros. RL (Reality Labs) genera ingresos a partir de las ventas de productos de hardware de consumo, software y contenido». «Los ingresos por publicidad se generan al mostrar productos publicitarios en Facebook, Instagram, Messenger y en sitios web o aplicaciones móviles de terceros afiliados, y en sitios web o aplicaciones móviles de terceros. Los comercializadores pagan por los productos publicitarios, ya sea directamente o a través de sus relaciones con agencias de publicidad o revendedores, en función del número de impresiones entregadas o del número de acciones, como los clics, realizadas por nuestros usuarios». «También contamos con una fuerza de ventas global que se centra en atraer y retener a los anunciantes y proporcionarles apoyo en todas las etapas del ciclo de marketing, desde la toma de decisiones previas a la compra hasta las optimizaciones en tiempo real y los análisis posteriores a la campaña. Trabajamos directamente con estos anunciantes, así como a través de agencias de publicidad y revendedores. Operamos en más de 80 ciudades de todo el mundo, la mayoría de ellas con presencia comercial. También invertimos en herramientas de autoservicio y nos apoyamos en ellas para ofrecer asistencia directa a nuestros usuarios y socios» para el 31 de diciembre de 2021, su capital humano era de 71.970 empleados, lo que representa un aumento del 23% con respecto al año anterior. «La mayor parte de nuestros ingresos proceden de la publicidad. La pérdida de anunciantes, o la reducción del gasto de los mismos, podría perjudicar seriamente nuestro negocio». Las ganancias totales del año fiscal que terminó el 31 de diciembre de 2021 fueron de \$165, 987 millones de dólares. [Meta Platforms Inc., “FORM 10-K” (Washington, D.C.: United States Securities and Exchanges Commission, 2021).]

^{xxviii} «El director general de Facebook, Mark Zuckerberg, ha anunciado que el gigante de las redes sociales cambiará el nombre de su holding por el de Meta; Zuckerberg reveló el nuevo nombre en la conferencia anual de AR/VR de Facebook, donde esbozó la visión de realidad virtual de la compañía para el futuro. También dio a conocer sus planes para construir el "metaverso", un mundo digital construido sobre el nuestro, compuesto por cascos de realidad virtual y realidad aumentada. "Creemos que el metaverso será el sucesor de la Internet móvil", dijo Zuckerberg. "Podremos sentirnos presentes: como si estuviéramos allí con la gente, sin importar lo lejos que estemos en realidad". Con un símbolo de infinito azul como logotipo, el nuevo holding Meta englobará a Facebook, su mayor filial, así como a aplicaciones como Instagram, WhatsApp y la marca de realidad virtual Oculus. Zuckerberg dijo que espera que el metaverso llegue a mil millones de personas en la próxima década. En los últimos informes de resultados, la empresa anunció que su segmento de realidad virtual había crecido tanto que ahora declarararía sus ingresos por separado, dividiendo sus productos en dos categorías. El esfuerzo de cambio de marca de Facebook no es inédito en el espacio tecnológico: en 2015, Google lo hizo con su cambio a Alphabet». [Paul Kari, “Facebook Announces Name Change to Meta in Rebranding Effort,” *The Guardian*, 2021, <https://www.theguardian.com/technology/2021/oct/28/facebook-name-change-rebrand-meta>.]

^{xxix} Apple Inc. es una empresa estadounidense que diseña, fabrica y comercializa teléfonos inteligentes, ordenadores personales, tabletas, wearables y accesorios, y vende una variedad de servicios relacionados. Sus productos principales son iPhone, iPad y Mac, Sus servicios se distribuyen en publicidad, los cuales incluyen varios acuerdos de licencia de terceros y las plataformas publicitarias propias de la empresa; AppleCare, Cloud services, Contenido Digital y Servicios de Pago. La venta total de productos y servicios durante el 2021 fue de \$ 365,817 millones de dólares. A fecha de 25 de septiembre de 2021 la compañía contaba con aproximadamente 154,000 empleados de tiempo completo. La sede de la empresa está en Cupertino, California. Actualmente, el CEO (Chief Executive officer and Director) es Timothy D. Cook. [Apple Inc., “FORM 10-K” (Washington, D.C.: United States Securities and Exchange Commission, 2021), <https://doi.org/10.4135/9781608712380.n519>.] Apple nace en 1976 con la creación de Apple I, construido por el cofundador de Apple, Steve Wozniak. Mientras que Steve Jobs el amigo de Wozniak, tuvo la idea de vender el ordenador. [Samuel Gibbs, “40 Years of Apple - in Pictures,” *The Guardian*, 2016, <https://www.theguardian.com/technology/gallery/2016/apr/01/40-years-of-apple-in-pictures>.] «El modelo de negocio de Apple está diseñado para atraer a los consumidores a su ecosistema y retenerlos en él, lo que ha tenido un enorme éxito hasta la fecha y ha permitido a Apple ejercer un enorme poder en la cadena de suministro de extremo a extremo». [Johnna Montgomerie and Samuel Roscoe, “Owning the Consumer-Getting to the Core of the Apple Business Model,” *Accounting Forum* 37, no. 4 (2013): 10, <https://doi.org/10.1016/j.accfor.2013.06.003>.] Por otro lado, Apple ha trazado unos límites (que, hasta la fecha, ha respetado), pues se ha comprometido a no realizar prácticas de vigilancia usando los datos personales. [Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.]

^{xxx} Microsoft Inc. es una empresa fundada en 1975 y está enfocada en desarrollar y dar soporte a software, servicios y dispositivos. Ofrece una serie de servicios, incluyendo soluciones basadas en la nube que proporcionan a los clientes software, servicios, plataformas y contenidos. También ofrece publicidad online relevante a una audiencia global. A fecha de 30 de junio de 2022, emplean a unas 221.000 personas a tiempo completo, 122.000 en Estados Unidos y 99.000 a nivel internacional. Actualmente su director ejecutivo es Satya Nadella. El negocio de la publicidad en búsquedas está diseñado para ofrecer publicidad relevante dependiendo las búsquedas y el lugar geográfico donde se realiza. A través de Yahoo se proporciona y monetiza las consultas de búsqueda. El 6 de junio de 2022, Microsoft Inc. adquirió Xandr, Inc. una plataforma tecnológica con herramientas para acelerar la entrega de soluciones de publicidad digital. Durante el año fiscal de 2021 a 2022 que concluyó el 30 de junio la empresa generó una ganancia de 365,840 millones de dólares. [Microsoft Corporation, “FORM 10-K” (Washington, D.C.: United States Securities and Exchange Commission, 2022), <https://doi.org/10.4135/9781608712380.n519>.]

^{xxxI} Amazon busca ser la empresa más centrada en el cliente de la Tierra. Se guían por cuatro principios: obsesión por el cliente y no por la competencia pasión por la invención, compromiso con la excelencia operativa y pensamiento a largo plazo. Actualmente cuenta con 1,608,000 empleados de tiempo completo. Su director ejecutivo es Jeff Bezos, fundador de Amazon.com en 1994. Proporciona servicios de publicidad a vendedores, proveedores, editores, autores y otros, a través de programas como anuncios patrocinados, publicidad en pantalla y en vídeo. Los ingresos se reconocen a medida que se entregan los anuncios en función del número de clics o impresiones. Durante el 2021

las ventas de la compañía fueron de \$ 469,822 millones de dólares de los cuales \$31,160 millones fueron de servicios de publicidad los cuales incluye la venta de servicios de publicidad a vendedores, proveedores, editores, autores y otros, a través de programas como los anuncios patrocinados, la visualización y la publicidad en vídeo. [Amazon.com, Inc., “FORM 10-K” (Washington, D.C.: United States Securities and Exchange Commission, 2014), <https://doi.org/10.4135/9781608712380.n519>.]

^{xxxii} “Hackear es la actividad que le corresponde a un hacker, y éste es entendido como una persona apasionada por analizar, resolver problemas, desarrollar su intelecto y ofrecer el fruto de su trabajo intelectual para el bien común. No existe un término latino o castizo que pudiera utilizarse como traducción. Aunque la palabra hacker no está incluida en el diccionario de la Real Academia Española, es amplia su utilización en el castellano usual actual. Desafortunadamente, el término se asocia con expertos en computación, y suele traducirse como pirata informático.” [Mckenzie Wark, “Manifiesto Hacker,” accessed November 5, 2021, http://subsol.c3.hu/subsol_2/contributors0/warktext.html.] Apple Inc. ha padecido la problemática de ciberseguridad en sus servidores: «La empresa sufre regularmente ataques maliciosos y otros intentos de acceso no autorizado a sus sistemas. Estos ataques buscan comprometer la confidencialidad, integridad o disponibilidad de la información confidencial o interrumpir las operaciones comerciales normales (...) Aunque los ataques maliciosos perpetrados para acceder a información confidencial, incluida la información personal, afectan a muchas empresas de diversos sectores, la empresa corre un riesgo relativamente mayor de ser objeto de ellos debido a su alto perfil y al valor de la información confidencial que crea, posee, gestiona, almacena y procesa». [Apple Inc., “FORM 10-K,” 19.] «Los ciberataques descubiertos a finales de 2020 conocidos como "Solorigate" o "Nobelium" son un ejemplo de ataque a la cadena de suministro en el que se introdujo malware a los clientes de un proveedor de software, incluidos nosotros (Microsoft Inc.), a través de actualizaciones de software. Los atacantes fueron capaces de crear posteriormente credenciales falsas que parecían legítimas en los sistemas de ciertos clientes. Es posible que seamos objeto de otros ataques similares a los de Solorigate/Nobelium, tanto como proveedores como consumidores de TI». [Corporation, “FORM 10-K.”]

^{xxxiii} Desde la creación del ciberespacio hasta hoy, la seguridad en los protocolos de acceso y cuidado de la información ha sido todo un reto. A esta seguridad encargada del cuidado en el almacenamiento de la información y la mejora continua de las normativas que creen un espacio seguro podemos denominarla ciberseguridad. En la actualidad, y después de la pandemia del coronavirus, los ciberataques se elevaron al tener un superficie de ataque disponible con tanta gente trabajando desde casa con redes Wi-Fi y dispositivos inseguros [Véliz, *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, 142.] Podemos dar dos ejemplos claros de esto, uno es el ataque que recibió el sistema eléctrico de Gran Bretaña durante la época de confinamiento [Ambrose, 2020, Lights stay on despite cyber-attack on UK's electricity system, *The Guardian*, <https://www.guardian2zotagl6tmjucg3lrhxdk4dw3lhbqknkvkywawy3oqfoprid.onion/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system>] y otro fue un incremento en los ataques a la Organización Mundial de la Salud [Organization, 2020, WHO reports fivefold increase in cyber attacks, urges vigilance, *World Health Organization*, <https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges->

vigilance.] De la misma forma han existido diversas advertencias frente la hiper-conectividad que está viviendo el mundo [Cfr. Wall, 2018, 5G: 'A cyber-attack could stop the country' - BBC News, BBC, <https://www.bbc.co.uk/news/business-45952693>] [Cfr. Greenberg, 2018, How Hacked Water Heaters Could Trigger Mass Blackouts, Wired, <https://www.wired.com/story/water-heaters-power-grid-hack-blackout/>]

La ciberdelincuencia, como se le cataloga a toda aquella forma de ilegalidad realizada dentro del ciberespacio, abarca desde ataques financieros hasta el espionaje, las violaciones de la información y los datos. En Latinoamérica el mercado del cibercrimen ha aumentado enormemente: “Latin America and the Caribbean have the fastest growing Internet population in the world, with 147 million users in 2013 ... only in Brazil, the cost of cybercrime reached 8 billion USD, followed by Mexico with 3 billion USD and Colombia with 464 million USD” [Parraguez Kobek and Caldera, “Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection,” 110.]

^{xxxiv} Siguiendo el método de los corredores de bolsa, en estas empresas se compran datos a un precio bajo en un sitio para luego venderlos a otro sitio a una tarifa mayor, después de haberlas cruzado con otras bases de datos para segmentar la publicidad digital, principalmente en los móviles. [Del Castillo, Carlos. (21 de octubre de 2019) Así trabaja una empresa española que compra y vende datos personales para hacer publicidad: “Recogemos toda la información posible”. Diario.es https://www.eldiario.es/tecnologia/trabaja-empresa-compra-venta-personales-sentido_1_1297691.html]

^{xxxv} Se estima que solo en la Unión Europa hay alrededor de 50 grandes empresas ‘data brokers’ (empresas de comercio de datos) y el precio por la cesión de los datos puede ser realmente elevado cuando se ceden datos personales de muchos usuarios, especialmente si se aporta información adicional que permite crear un perfil del usuario. Tanya O’Carroll, asesora de Tecnología y Derechos Humanos de Amnistía Internacional, expuso hace unos meses que “el comercio con datos privados es un negocio floreciente” y “el inmenso avance experimentado por el 'big data' en la última década ha permitido que los 'data brokers' lo sepan todo de ti”. [Javier Goizueta, “El RGPD Pone En Jaque El Gran Negocio Del Siglo XXI,” *El Confidencial*, September 13, 2018, https://blogs.elconfidencial.com/espana/tribuna/2018-09-13/datos-rgpd-gran-negocio-sigloxxi_1614624/.]

^{xxxvi} La PSP era una orden ejecutiva, es decir, un conjunto de instrucciones estipuladas por el presidente estadounidense que el Gobierno debe considerar equivalente al derecho público. El PSP capacitaba a la Agencia de Seguridad Nacional (NSA) para recopilar comunicaciones por teléfono e Internet entre Estados Unidos y el extranjero. Con ello se facultaba a la NSA a hacer tal cosa sin que fuese necesario obtener ninguna orden judicial especial del Tribunal estadounidense de Vigilancia de Inteligencia Extranjera. La administración Bush aseguró que el PSP fue terminado en 2007 después de las protestas suscitadas luego de su conocimiento público, pero esto fue mentira. Pues a través de las legislaciones a probadas – las leyes Protect America Act de 2007 y FISA Amendments Act de 2008 – se daba inmunidad retroactiva a los proveedores de servicios de telecomunicaciones e Internet que hubiesen participado en el PSP. Estas legislaciones facultaban a la NSA para recopilar sin orden judicial comunicaciones por teléfono e Internet hacia el exterior que se originasen dentro de las

fronteras estadounidenses. [Snowden, 2019, *Permanent Record*, Metropolitan Books, New York p. 172]

xxxvii STELLARWIND recopiló comunicaciones desde el comienzo del PSP en 2001. Según el informe clasificado encontrado por Snowden: TOP SECRET // STLW // HCS / COMINT // ORCON / NOFORN la NSA había recibido la orden de realizar una «recopilación indiscriminada», esto representó el inicio por conseguir el acceso completo a los registros de todas las comunicaciones digitales existentes y adueñarse clandestinamente de ellos. [Snowden, 175–77.]

xxxviii El término “Big Tech” hace referencia a las cinco compañías más poderosas de tecnología actualmente: Google, Microsoft, Amazon, Apple y Meta.

xxxix Por “Internet of Things” (“IoT”) o Internet de las cosas entendemos: el sistema de tecnología de sensores y todo aquello dispositivo o aparato electrodoméstico que este permanentemente conectado a una red; que sean legibles, reconocibles, localizables, direccionables y controlables a través de Internet, ya sea mediante RFID, LAN inalámbrica, red de área amplia, red 5G u otros medios. [National Intelligence Council, “Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interest Out to 2025,” 2008, <http://www.fas.org/irp/nic/disruptive.pdf>.]

xl Por científico de datos entendemos un profesional que tiene los conocimientos y las habilidades para realizar trabajos de ciencia de datos, en ella extraen conocimientos de los datos para impulsar la acción. «Las áreas de conocimiento importantes incluyen la estadística (es decir, un conocimiento práctico de la probabilidad, las distribuciones, las pruebas de hipótesis y el análisis multivariante); la informática, que abarca la comprensión de las estructuras de datos, los algoritmos y los sistemas de bases de datos (por ejemplo, Hadoop); y la formulación de problemas (es decir, la capacidad de formular problemas para aportar soluciones eficaces)». [Melanie A. Meyer, “Healthcare Data Scientist Qualifications, Skills, and Job Focus: A Content Analysis of Job Postings,” *Journal of the American Medical Informatics Association* 26, no. 5 (2019): 383–91, <https://doi.org/10.1093/jamia/ocy181>.]

xli La fuerza de la gravedad F_g es siempre atractiva y depende solo de las masas involucradas y la distancia entre ellas. Cada objeto en el universo atrae a todos los otros objetos con una fuerza a lo largo de una recta imaginaria entre ellos.

La ecuación para la gravitación de Newton es:

$$F_g = G \frac{m_1 m_2}{r^2}$$

Donde: F_g es la fuerza gravitacional entre m_1 y m_2 ,

G es la constante gravitacional, que es igual a $6.67 \times 10^{-11} \frac{\text{m}^3}{\text{kg} \cdot \text{s}^2}$ y m_1 y m_2 son masas.

La fuerza es directamente proporcional al producto de las masas. También es inversamente proporcional al cuadrado de la distancia entre los centros de masa. A esto a veces se le llama una ley del inverso al cuadrado. [Khan Academy, “Ley de Gravitación Universal de Newton,” Khan Academy, accessed October 22, 2022, <https://es.khanacademy.org/science/hs->

physics/x215e29cb31244fa1:types-of-interactions/x215e29cb31244fa1:newton-s-law-of-universal-gravitation/a/newtons-law-of-universal-gravitation.]

^{XLII} Entendemos aquí por IA «una inteligencia desplegada o simulada por un código (algoritmos) o por una máquina». Tal inteligencia es comprendida bajo los estándares de la inteligencia humana, por tanto se busca que las máquinas basadas en IA sean capaces de pensar y (re)accionar como lo hacen los seres humanos. El término como tal, fue acuñado por John Mcharthy en el seminario Dartmouth de 1956 en Hannover, New Hampshire. Hoy en día la IA solo puede operar en ámbitos específicos, como el ajedrez o la clasificación de imágenes, pero cada vez su desarrollo va en progreso. La base de la inteligencia de una IA es el software: un algoritmo o una combinación de algoritmos que le dice qué hacer al ordenador, smartphone, máquina, robot, o cualquier cosa en la que esté integrado, el cual conduce a un resultado (output) particular basándose en la información disponible (input), por lo tanto se resuelve un problema. Sin duda, la IA es «un enfoque multidisciplinar para la comprensión, modelado y reproducción de la inteligencia y los procesos cognitivos mediante el usos de varios principios y dispositivos computacionales, matemáticos, lógicos, mecánicos e, incluso biológicos». [Mark Coeckelbergh, *Ética de La Inteligencia Artificial* (Madrid: Cátedra, 2021).]

^{XLIII} Este análisis fue concebido por Alexander Nix como OCEAN, por sus siglas en inglés de los perfiles de personalidad (Openess, Conscientiousness, Extraversion, Agreeableness, Neuroticism) en su conferencia en el Concordia Summit de 2018 titulada “The Power of Big Data and Psycographics”, con lo cual explicó abiertamente y sin ningún sentido de ética social el funcionamiento de Cambridge Analytica [Alexander Nix, “The Power of Big Data and Psycographics” (Concordia Summit, 2018), <https://archive.org/details/CambridgeAnalyticaThePowerOfBigDataAndPsychographics.>]

^{XLIV} Como Bot, entendemos un robot o programa computacional que actúa automáticamente y de forma repetitiva. Son usados comúnmente en las redes sociales para hacer comentarios racistas o de odio y así generar que el discurso sea replicado manteniéndose en el colectivo online.

^{XLV} Alexander Nix se refiere al Big Data como «el conjunto de tantos puntos de datos individuales como sea posible, que se sintetizan en una base de datos de registro limpio, que luego son utilizados para informar y crear una visión de su público objetivo». [Nix.]

^{XLVI} Vale la pena mencionar los casos de las denunciantes (whistleblowers) Sophie Zhang y Frances Huagen ambas extrabajadoras de la empresa Facebook (actualmente Meta). La primera de ellas denunció en 2020 como la empresa permitía con una actitud omisiva la creación de páginas o perfiles falsos en Facebook para la propagación de información con intenciones de manipulación política en países como India, México, Afganistán, Corea del Sur, Honduras, entre otros. En este último, durante nueve meses se dirigió una campaña coordinada que impulsaba al presidente Juan Orlando Hernández de forma masiva para engañar al pueblo hondureño. En Azerbaiyán, el partido político en el poder utilizaba cuentas falsas para acosar masivamente a la oposición. En 2019 se detectó más de 10.5 millones de cuentas falsas que seguían a políticos de Brasil y Estados Unidos. Tras el inicio de la pandemia de COVID-19 la página de Facebook del Ministerio de Sanidad español inició una coordinada manipulación sustentada por 672.00 cuentas falsas, las cuales también actuaban sobre objetivos similares a nivel mundial. [Karen Hao, “She Risked Everything to Expose Facebook. Now She’s Telling Her Story.” *MIT Technology Review*, 2021, <https://www.technologyreview.com/2021/07/29/1030260/facebook-whistleblower-sophie-zhang->

global-political-manipulation/; Craig Silverman, Ryan Mac, and Pranav Dixit, “‘I Have Blood on My Hands’: A Whistleblower Says Facebook Ignored Global Political Manipulation,” BuzzFeed News, 2020, <https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo>.] Por otra lado, Haugen denunció sustentándose en documentos de la propia compañía, la ineptitud de la inteligencia artificial de Facebook para erradicar los discursos de odio y la violencia excesiva. No es capaz de «identificar sistemáticamente los vídeos de tiroteos en primera persona, los desplantes racistas e incluso, en un episodio notable, la diferencia entre las peleas de gallos y los accidentes de tráfico, según los documentos» A pesar de conocer los daños que estaba causando por los grandes sesgos en su inteligencia artificial, así como lo que esto significaba para que los discursos de odio se maximizaran, Facebook optó por redoblar sus esfuerzos sin importar el daño que esto estaba ocasionando. [A Wall Street Journal Investigation, “The Facebook Files,” Wall Street Journal, 2021, <https://www.wsj.com/articles/the-facebook-files-11631713039>; Roger McNamee, “Facebook Will Not Fix Itself,” *Time*, 2021, <https://time.com/6104863/facebook-regulation-roger-mcnamee/>.]

^{XLVII} La palabra angustia está emparentada con el latín *angustus* que significa estrecho. El sentimiento de angustia patológico o neurótico puede manifestarse por síntomas somáticos, conductuales y subjetivos. Los síntomas somáticos pueden ser cardiovasculares (taquicardia, palpitaciones, dolor precordial, palidez, accesos de calor), respiratorios (disnea, hiperventilación, suspiros, sensación de ahogo, opresión torácica), digestivos (bolo esofágico, náuseas, vómitos, diarreas, aerofagia, dispepsia), genitourinarios (polaquiuria, eyaculación precoz, frigidez, incontinencia), neuromusculares (tensiones musculares, temblor, cefalea tensional). La angustia se puede exteriorizar a nivel conductual en forma de inhibición o inquietud psicomotriz, incapacidad para estar sentado, restregamiento de las manos, movimientos continuos, etc. A nivel subjetivo la ansiedad se manifiesta por el temor a volverse loco o morir, la sensación de espera de lo peor, de que algo malo le pueda sobrevivir a él o a un familiar, la dificultad de concentración, los sobresaltos a los ruidos, etc. La angustia patológica no sólo se manifiesta en las enfermedades neuróticas. Toda enfermedad psiquiátrica puede presentar angustia y en algunas de ellas, como en los trastornos depresivos, puede ser un síntoma dominante. Mientras que la angustia es más precordial, más epigástrica, más profunda, la ansiedad es más respiratoria. J.J.López Ibor consideró que en la angustia hay sobrecogimiento, inmovilización y en la ansiedad movilización, sobresalto. A veces, se mezclan las vivencias de angustia y ansiedad. [Ildefonso Gómez-Feria Prieto, “Glosario de Términos Psicopatológicos e Históricos Psiquiátricos” (Psiquiatria.com, 2022), <https://psiquiatria.com/glosario/index.php>.]

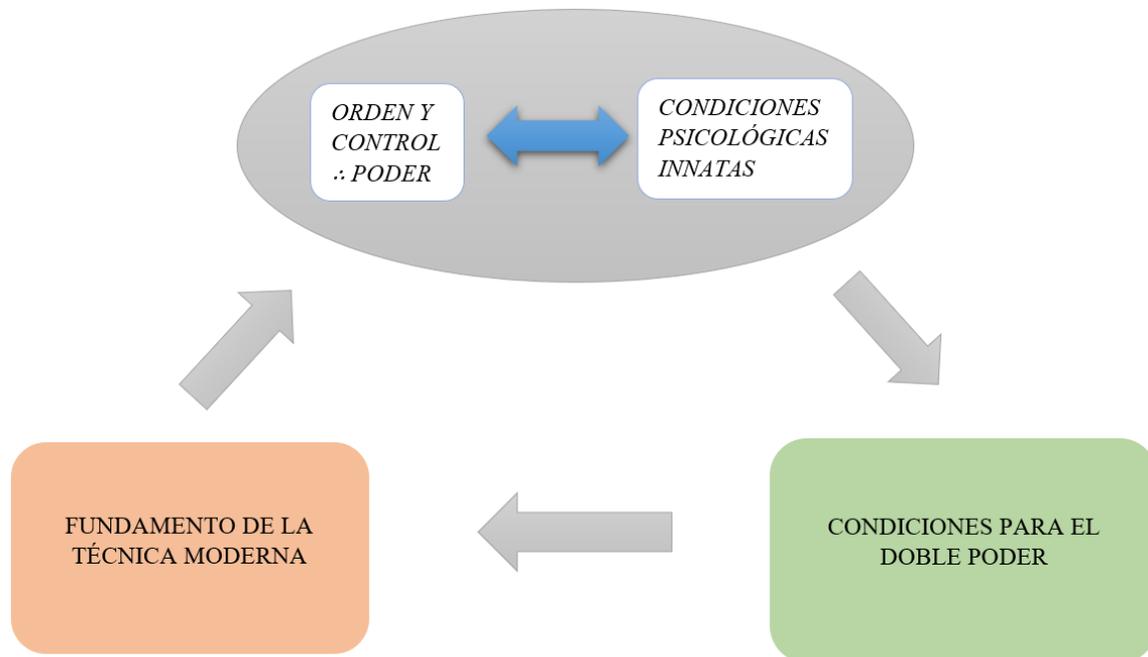
^{XLVIII} Trastorno afectivo caracterizado por la tristeza y la pérdida de interés o de la capacidad para experimentar placer. El término depresión mental (depresión of mind) fue utilizado por primera vez por el psiquiatra escocés Robert Whytt (1714-1766), uno de los fundadores de la neurofisiología. A veces se ha utilizado como síntoma, sinónimo de tristeza, sobre todo con el adjetivo deprimido. [Gómez-Feria Prieto.]

^{XLIX} Dependencia de sustancias o actividades nocivas para la salud o el equilibrio psíquico. [Española, “Diccionario de La Lengua Española.”]

^l Con las cualidades de orden, control y poder no pretendemos agotar el discurso unificador del desarrollo de este tipo de poder. Lo que sí, es que estas cualidades, nos parecen las más significativas hasta ahora y guardan mayor relevancia para la justificación de nuestro incipiente análisis. Por ahora,

vale la pena mencionar las características de disciplina, vigilancia en tiempo real e incluso identidad, solo por no dejar de lado la estructura sobre la cual recae este tipo de poder.

^{LI} El aquí denominado “Doble Poder” es generado por las Big Tech y está fundamentado en un nuevo nivel de progreso de orden ontológico creado a partir de una relación compleja de condiciones. El orden y control que fundamentan el poder son condición necesaria y suficiente para el desarrollo de las disposiciones psicológicas innatas. De la misma manera que las disposiciones psicológicas innatas reclaman orden y control de la realidad, obteniendo poder y consiguiendo alejarse del miedo al caos.



^{LII} Como un intento de mapear las ideas principales, a la vez que pudimos detectar un método hegeliano dentro del mismo mecanismo del funcionamiento del flujo de datos personales en la Era digital es que generamos este esquema que nos permite señalar el reconocimiento de la afirmación de la realidad personal y social en lo cualitativo en sí mismo (la tesis hegeliana), señalar la negación del mundo de las cosas en lo cuantitativo que representan los datos personales (la delimitación hegeliana de la antítesis) y el punto que genera la unión entre ambos (síntesis), la cual desemboca en una nueva identificación de poder y su afirmación primera: Doble Poder. Lo título: “Esquema hegeliano del flujo de los datos personales en la Era digital y sus implicaciones de poder” es de mi autoría con la ayuda de mi asesor.

