Universidad Panamericana

Facultad de Derecho

Ricardo Meneses Calzada

El Derecho a la Privacidad en Internet y el Perfilamiento Algorítmico

Tesis para Doctorado en Derecho dirigida
por el Dr. Guillermo Antonio Tenorio Cueto

Ciudad de México a 17 de noviembre de 2025

Table of Contents

INTRODUCCIÓN

En una era dominada por avances tecnológicos sin precedentes, la influencia omnipresente del perfilado algorítmico se erige como una piedra angular de nuestra sociedad digital (*inter-networked)* interconectada. A medida que las personas navegamos por la tecnología digital, sus apps, sus navegadores, sus redes; nuestras actividades en línea dejan tras de sí un rastro de datos recopilados por algoritmos sofisticados. Estos algoritmos, alimentados por el aprendizaje automático e inteligencia artificial, se esfuerzan por desentrañar la intrincada trama del comportamiento humano, preferencias e interacciones que dan como resultado un perfilamiento sociológico, comercial, psicológico, político, entre otros. Si bien las promesas de servicios personalizados y recomendaciones específicas son atractivas, el ascenso del perfilado algorítmico plantea profundas preocupaciones, especialmente en lo que respecta a su impacto en el ámbito de la privacidad.

Esta investigación doctoral hará una exploración integral de la intrincada relación entre el perfilado algorítmico y la privacidad en el ámbito digital contemporáneo, ya que a medida que el ecosistema digital evoluciona, lo hacen también los mecanismos utilizados para el aludido perfilamiento, más allá de los límites y paradigmas tradicionales del derecho a la privacidad.

Esta investigación tiene como objetivo examinar las dimensiones legales que rodean al perfilado algorítmico, centrándose en comprender su impacto en la privacidad en el contexto de los entornos digitales contemporáneos.

Tesis Central:

La hipótesis sostiene que la proliferación del perfilado algorítmico, impulsada por las vastas cantidades de datos generados en el ámbito digital, tiene el potencial de erosionar los derechos de privacidad consagrados en los marcos legales existentes. Esta erosión está impulsada por la opacidad inherente de los algoritmos, la complejidad de los mecanismos de procesamiento de datos y la falta de marcos regulatorios integrales capaces de abordar de manera efectiva los problemas multifacéticos derivados del perfilado algorítmico.

Esta investigación busca desentrañar las complejidades asociadas con el perfilado algorítmico, así como promover una comprensión de sus implicaciones para la privacidad. Analizaremos el contexto donde surgen los diversos conflictos jurídicos en el ámbito digital, abodaremos el concepto de privacidad, su naturaleza jurídica, sus valores y contravalores, los ámbitos de la privacidad para llegar al estudio de la privacidad en la era digital y llegar a nuestro tema del perfilamiento algorítmico.

La investigación tiene como objetivo aportar ideas valiosas al discurso sobre la privacidad en la era digital, ofreciendo una base para que los responsables de políticas, profesionales legales y desarrolladores de tecnología naveguen por los desafíos planteados por el perfilamiento algorítmico, al tiempo que se defienden los derechos fundamentales de privacidad sin descuidar la innovación tecnológica. La abundancia de información en el ciberespacio se fundamenta en su estructura interconectada. Esta interconexión engendra una comunicación constante entre millones de individuos y la creación de recursos compartidos que, en última instancia, democratiza el acceso a la información para cualquier persona con conexión a la red. Sin embargo, la recolección de

datos con la aplicación de la inteligencia artificial conlleva la aparición de una serie de cuestiones legales y disputas jurídicas, sobre todo ante el llamado perfilamiento algorítmico.

Internet funciona a partir de sistemas conducidos por algoritmos, estos sistemas originalmente persiguen la consecución de una eficiencia colectiva derivada de la suma de dos factores: la inteligencia colectiva y la experiencia colectiva. La capacidad de acceder a billones de datos en cuestión de segundos y el intercambio de información desde cualquier punto del mundo tiene efectos profundos en todos los estratos de la sociedad; pocos conocen el rastro digital que dejan y que alimenta grandes bases de datos que pueden ser usados para diversos efectos, como el perfilado algorítmico dando lugar al Capitalismo de Vigilancia que "unilateralmente reclama la experiencia humana como materia prima gratuita para ser traducida en datos de comportamiento" Zuboff (2019)[1]

En este contexto de avalancha informativa, resurge el conocido aforismo jurídico que postula que "el hecho siempre antecede al Derecho", tanto el rápido desarrollo como la implementación de tecnologías de perfilado algorítmico en la sociedad a menudo ocurren antes de que exista una regulación legal adecuada para manejar sus implicaciones. Esto significa que los avances tecnológicos, como el perfilado algorítmico, pueden presentar desafíos éticos y de privacidad antes que los marcos legales puedan adaptarse y proporcionar las salvaguardias necesarias. En esencia, la ley a menudo tiene que ponerse al día con las innovaciones y realidades tecnológicas nuevas para proteger efectivamente los derechos de los individuos. Los sistemas de inteligencia artifical que prometen rebasar la capacidad humana en algunas actividades o toma de decisiones, amenazan con

[1] Zuboff, S. *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós, Editorial Planeta. Barcelona, 2019, p. 15

sustituir a los humanos en toma de decisiones, por ejemplo en temas de permisos de inmigración o salud. El Derecho juega un papel primordial para marcar los senderos que seguirá Internet al fomentar, regular o inhibir este intercambio que ha transformado la manera en que creamos, editamos, publicamos, usamos y distribuimos información, esto puede llevarse a cabo al regular la conducta de las empresas tecnológicas que, a través de sus algoritmos patentados, tienen todo el control de lo que vemos y escuchamos en internet. Los académicos se preguntan si hay que crear un Derecho de los Algoritmos[2] como aquél que limite el caos creativo generado por internet; nuestra opinión es que las nuevas situaciones jurídicas originadas por la tecnología en internet deben ser resueltas con las figuras legales ya creadas y sólo en donde se queden cortas para resolver los casos deben proponerse reformas específicas. En general, debemos identificar la tecnología que permite dar la vuelta al límite que marca el derecho y que, muchas veces, deja desprotegido al bien jurídico que se desea tutelar; a saber, la información privada. Partimos del hecho que el individuo siempre está en un espacio real aun cuando esté en el mundo virtual de internet. El Derecho siempre marca como fin claro la protección de bienes jurídicos. No debemos caer en la excesiva regulación que inhiba el bien de la sociedad y las personas que la componen. Algunos aspectos positivos del perfilado algorítmico son una personalización eficaz que permite servicios y recomendaciones a la medida, mejorar la experiencia del usuario en varios sectores como el comercio minorista, el entretenimiento y las redes sociales: o bien, la detección de fraudes a partir de los patrones de comportamiento financiero de los usuarios de la banca electrónica.

[2] Barfiel, Woodrow. *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, UK 2021, p. 3.

Los problemas jurídicos derivados del perfilamiento algorítmico son diversos, el principal es la recolección y uso de datos personales para el perfilado que pueden entrar en conflicto con los derechos de privacidad, especialmente si se hace sin consentimiento informado como en el caso de los *Data Brokers* que son empresas que recopilan datos de personas para predecir el comportamiento futuro y con ellos hacer negocio al vender datos a las empresas interesadas. Los algoritmos pueden perpetuar o amplificar sesgos existentes, llevando a resultados discriminatorios en áreas como empleo, crédito y aplicación de la ley. Además, a menudo, el funcionamiento interno de los algoritmos, casi secreto, dificulta la rendición de cuentas por decisiones o acciones erróneas basadas en el perfilado. Otro tema es la ciber seguridad que desencadena el potencial para violaciones de datos y mal uso de información sensible.

Los juristas nos preguntamos dónde comienza el derecho del Estado para regular y limitar el uso de los algoritmos patentados para perfilar a las personas para diversos fines, muchas veces contrarios a la ética y la justicia. Andrew Tutt, asesor jurídico del Departamento de Justicia de EUA ha propuesto una institución semejante a la *Food and Drugs Administration* para Algoritmos[3], en virtud de que, en su opinión, ni el derecho civil, ni el derecho penal podrá regular la problemática que los algoritmos pueden generar. Tutt sugiere que tal institución tenga tres poderes: a) Capacidad para organizar y clasificar los algoritmos en diversas categorías a partir de su diseño, complejidad y potencial de daño tanto ne su uso convencional como en posibles abusos b) Se postula que dicha entidad debería contar con el poder de evitar la introducción de algoritmos al mercado hasta que su seguridad y eficacia sean verificadas a partir de ensayos

[3] Aludido por Barfiel, Woodrow. *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, UK 2021, p. 14-15.

precomerciales respaldados por hechos y pruebas que prueben que no perjudicarán los derechos de terceros, como la privacidad[4].

Es importante detectar las implicaciones jurídicas de la inteligencia artifical (*AI*) para preservar la privacidad y proteger información personal para todos aquellos que la usan. La era del llamado *big data* implica que diariamiente se generan millones de datos que alimentan los avances de las tecnologías de inteligencia artificial, necesariamente en esos millones de datos se contiene información privada cuya difusión violaría derechos a la protección de datos. Vicancos[5] define *Big Data* con 5 Vs: **Volumen**, si bien no hay una medición cuántica, sí hablamos de *terabytes, petabytes, exobytes*. **Velocidad**: Los procesadores son de altísima potencia -no en vano ha sido el crecimiento de Nvidia el procesador que potencia la IA. La velocidad se puede observar ante cualquier prompt en ChatGPT o Gemini. **Variedad**: El *Big Data* va más allá de los datos relacionados en una hoja de cálculo o cualquier programa; son datos no estructurados que incluye videos, audio, imágenes, geo localización, entre otros. **Veracidad**: Observamos, cada vez más, la integridad de los datos. Por ejemplo, con la tecnología de face recognition al ingresar a un país. Aún cuando nos dan la garantía que nuestra imagen no quedará almacenada, lo cual es dudoso. Aquí el peligro de las *fake news o fake videos* alerta de la manipulación que se puede hacer con fines no éticos. **Valor**: El *Big Data* aporta valor a través de la analítica que permite perfilar gustos, aficiones, deseos de compra, inclinaciones políticas entre otras cosas. El comercio, la mercadotecnia, las patentes, la música, las películas, los contenidos, los periódicos; todos se ven beneficiados o amenazados ante la ola

[4] Barfield, *Supra* p. 15
[5] Vicancos, D. Citado por Serrano, Antonio en Muñoz, Ana, *etal*. Revolución Digital, Derecho Mercantil y Token Economía, Ed. Tecnos, España 2019. Cap. 3: El *Big Data* en el Contexto de la Normativa de Protección de Datos, p. 112-114

avasalladora de la inteligencia artifical. Olier redefine la ley de la escasez: "No se trata únicamente de la lucha por los recursos, sino que se adentra en los equilibrios geopolíticos actuales que encierran un modelo nuevo de guerra económica que busca el predominio tecnológico y el dominio de los mercados, a la vez que trata de proteger los sistemas productivos propios… ya no es la informática, son los datos y su análisis con complejos algorítmos los que dan o quitan poder y, en consecuencia, los que determinan lo que es escaso y lo que no lo es."[6] Lawrence Lessig nos hace reflexionar acerca de quién es dueño de Internet, o por lo menos quién lo gobierna, quién instaura los protocolos, quién diseña la arquitectura que, a final de cuentas, es una forma de regular[7].

Las implicaciones de la regulación jurídica o sus lagunas por lo menos alcanzan cuatro áreas específicas: a) El impacto político-socio-cultural de las nuevas tecnologías de internet y cómo los cambios de disposiciones legales afectan estos tres ámbitos fundamentales de la vida humana. Se observó el impacto del eficaz manejo del *machine learning* y el perfilado algorítmico en la elección presidencial del 2012 en EUA. Barak Obama contrató a Rayid Ghani[8] como chief scientist que consolidó la información de los votantes en una sola base de datos, la combinó con sus redes sociales e integró campañas de *marketing* político para predecir la forma en que cada persona podría apoyar a Obama, a partir de los temas que a cada uno le interesaban. Ya desde su campaña en 2011 se promovió a través de Twitter con 8.7 millones de seguidores al 18 de junio del 2011

[6] Citado por Serrano, Antonio en Muñoz, Ana, *etal*. Revolución Digital, Derecho Mercantil y Token Economía, Ed. Tecnos, España 2019. Cap. 3: El *Big Data* en el Contexto de la Normativa de Protección de Datos, p. 109

[7] Ver Lessig, Lawrence, *Code* v.2.0 *Basic Books*, New York, 2006

[8] Prastien, L. (2019, 28 de agosto). Rayid Ghani, pioneer in applying AI to social issues, joins Carnegie Mellon. Carnegie Mellon University.
https://www.cmu.edu/news/stories/archives/2019/august/ai-pioneer-joins-faculty.html

según Liz Gannes[9]. Camino a las elecciones 2013, su campaña creó el *trending topic* #Obama2012 en Twitter. A la fecha cuenta con 130.1 millones de seguidores en su Twitter[10]. Trump aprendió bien y usó la tecnología para ganar las elecciones en el 2016.

Antaño, teníamos la capacidad de sumergirnos en la lectura, explorar y adquirir conocimiento en la tranquilidad de una biblioteca; en la actualidad, nuestras búsquedas, lecturas de libros digitales y descargas están siendo rastreadas con objetivos comerciales, individuales o gubernamentales, convirtiéndonos en componentes esenciales del vasto conjunto de datos conocido como *big data* que se traducen en información cuando se usan los algoritmos y el perfilado. En este momento, nuestra información adquiere un valor significativo y, al mismo tiempo, se percibe como vulnerable debido a la aparente inacción de las normativas legales. Este fenómeno conduce a una reflexión profunda sobre el concepto de privacidad, que va más allá de simplemente ocultar datos, abarcando una esfera más amplia que incluye los derechos de autonomía e integridad personal. En este contexto, el perfilamiento algorítmico emerge como un componente crucial, ya que nuestras actividades en línea son analizadas y utilizadas para modelar patrones de comportamiento, lo que plantea desafíos adicionales a la preservación de nuestra privacidad y autonomía.

El gobierno, al ser percibido como el "gran ojo que todo lo ve", podría emplear técnicas de perfilamiento algorítmico para recopilar y analizar información sobre la población en diversas áreas como impuestos, seguridad nacional y salud. El ataque del 11 de septiembre a las Torres Gemelas de Nueva York destaca la paradoja de cómo las medidas

[9] Gannes, Liz. *"Four Years Later, Obama Will Start Tweeting Himself," AllThingsD*, https://allthingsd.com/20110617/four-years-later-obama-will-start-tweeting-himself/ consultado el 15 de marzo de 2023.
[10] https://x.com/BarackObama consultado el 15 de octubre de 2025

intrusivas en la privacidad, a pesar de implementarse en nombre de la seguridad ciudadana, no garantizan la protección efectiva de los ciudadanos. Además, la mencionada paradoja de tratar a ciudadanos respetuosos de la ley como potenciales amenazas, mientras los verdaderos terroristas eluden dicha vigilancia, sugiere una reflexión sobre la efectividad y la ética del perfilamiento algorítmico en la preservación de la seguridad pública. En este contexto, se plantea la preocupación sobre cómo se equilibran la seguridad y la privacidad en la implementación de estas tecnologías de vigilancia algorítmica.

Esta tesis llama a un debate más profundo a nivel social, político y jurídico sobre cómo se están utilizando esta tecnología invasiva llamada perfilamiento algorítmico.

La referencia a programas de entretenimiento donde las personas revelan detalles íntimos de sus vidas frente a las cámaras y concursos como "big-brother" resalta la paradoja de una sociedad que parece dispuesta a compartir abiertamente información personal, a veces a cambio de premios, mientras simultáneamente se preocupa por la invasión de la privacidad. El perfilamiento algorítmico presenta diversos desafíos para la privacidad, como la ignorancia de los usuarios de Internet, la protección del derecho a la información, los conflictos con otros intereses jurídicos como la seguridad del Estado, y la libertad de expresión, que a veces se interpreta como el derecho no solo a recopilar datos a través de la invasión a la privacidad, sino también a la publicación masiva de esa información.

La inclusión de las empresas privadas y sus intereses financieros en la recopilación de datos de millones de usuarios en la web, como se evidencia en el modelo de marketing en internet conocido como Google Ads, evidencia el uso del perfilamiento algorítmico. Este

último se basa en el análisis de grandes cantidades de datos para comprender y predecir el comportamiento del usuario, a menudo con fines publicitarios. La amplia gama de aspectos que abarca el término "privacidad", desde derechos constitucionales individuales hasta la protección contra el correo no deseado (spam), subraya la complejidad del debate en torno a la privacidad en la era digital y la necesidad de considerar estos temas desde múltiples perspectivas.

El creciente intercambio de datos en internet afecta la esfera jurídica del individuo. Hoy la tendencia legislativa e informática en el mundo se inclina hacia el hecho de que la información esté estrechamente rastreada. Hay cámaras en todos lados –públicos o privados-, nuestros datos personales están almacenados no sólo en servidores estatales; sino privados, tales como bancos, hospitales, escuelas, entre otros. Es frecuente la venta de bases de datos sin el consentimiento del afectado, así como la colocación de *cookies* para rastrear nuestra actividad y hábitos en línea con el objetivo de tener un perfilamiento algorítmico eficaz a los fines de las empresas. Como sociedad nos corresponde inducir los valores que deseamos ver y definir las características de los algoritmos esenciales para garantizar la transparencia y el respeto al derecho a la privacidad de las personas. En Estados Unidos, la Unión Europea y Asia han hecho varios esfuerzos por regular los sistemas de algoritmos[11]. En 2007 el gobierno de Corea del Sur propuso el *Robot Ethics Charter*, en 2011 el *The Engineering and Physical Sciences Research Council* del Reino Unido publicó cinco principios éticos para la industria y en 2017 la Association for Computing Machinery de Estados Unidos publicó siete principios para la transparencia y

[11] Barfiel, Woodrow. *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, UK 2021, p. 3.

responsabilidad algorítmica[12]. Los algoritmos son punto de litigio en patentes, derecho civil, mercantil, penal, entre otros.

Así como los derechos humanos han evolucionado para incluir no solo aspectos físicos sino también incorpóreos y espirituales, el derecho también debe evolucionar para abordar los desafíos planteados por el perfilamiento algorítmico. Este tipo de tecnología afecta no solo la privacidad física, sino también aspectos más intangibles de la privacidad, como los patrones de comportamiento y las preferencias personales. Por lo tanto, la ley debe extender su protección para salvaguardar estos aspectos de la privacidad en la era digital, reconocer y adaptarse a las nuevas realidades creadas por el avance tecnológico.

Diversos autores[13] se polarizan o unifican en torno al tema de la privacidad y la vigilancia (*surveillance*). El ojo que todo lo ve, sin ser visto. Asimetría que encrespa los ánimos de la gente común, nos preguntamos cuánta información tienen de nosotros, tanto el gobierno como otras empresas. El Estado controla, a través del perfilamiento algorítmico, no sólo las instituciones, sino las comunicaciones públicas y privadas; estas prácticas pueden afectar la privacidad individual, una preocupación similar a la vigilancia estatal en un régimen totalitario, donde no hay esfera individual que pueda escapar del ojo estatal. Se constituye una red de informantes en pro del Estado y se vigila toda relación privada. ¿Cómo? La tecnología es el medio para lograrlo, muchas veces ignorada por el ciudadano común, se tiene información de cada ciudadano, sus actividades, sus registros. Se desintegran comunidades, hay desconfianza, hay difamación, chantaje.

[12] Woodrow, *Supra*
[13] Bentham, Jeremy. *Panopticon* publicada en 1787; Orwell, George. *Nineteen Eighty Four*. Burwood, N.S.W.: *Royal Blind Society of New South Wales*, 1963. Foucault, Michel. *Power / Knowledge: Selected Interviews* An. Brighton, Sussex: The Harvester press, 1980.

Contrariamente, en un estado democrático que valora los derechos humanos de libertad, igualdad, propiedad y seguridad jurídica, se da un equilibrio cuidadoso para asegurar que el uso del perfilamiento algorítmico no comprometa derechos fundamentales como la libertad y la privacidad. La privacidad, en este Estado democrático, es el ámbito donde el individuo puede reflexionar, pensar, discutir, proponer ideas, alejado del ojo estatal y sin miedo a represalias. Cuando un estado pierde la seguridad jurídica, sus libertades básicas ceden ante la tiranía.

I. Concepto de la privacidad y su relación con los algoritmos

La privacidad constituye un **derecho humano** y, por ende, es un derecho **subjetivo** entendido como un interés jurídicamente protegido que se puede hacer valer frente al Estado y otras personas. Es parte de los derechos **individuales** al poseer como valor esencial de la persona, incluso fundamental, inherente a ella, constitutivo de su dignidad[14]. Es un derecho **de la personalidad** porque está ligado indisolublemente a la personalidad del hombre; Castán Tobeñas distingue derecho de la personalidad de la personalidad misma, entendida ésta como la abstracta posibilidad de tener derechos subjetivos; en tanto los primeros son "facultades concretas de que está investido aquél que tiene personalidad"[15]. Jacqueline Onassis pudo evitar que una empresa publicara anuncios que contenían la foto de una modelo que lucía como Onassis[16]. Bette Midler recuperó $400,000 dólares por daños cuando Ford Motor Co usó una cantante que imitaba el tono de Midler. Esta protección va incluso a los herederos de las personas cuya privacidad se protege. Esto verdaderamente contrasta con otros intereses relacionados con la privacidad. Los derechos de la personalidad fueron reconocidos formalmente por el *Civil Law* al enfatizar el ámbito privado donde el bien jurídico es la reputación. Es hasta las constituciones promulgadas con la caída de las dictaduras en Grecia, España y

[14] Quijano, Carmen. Derecho a la Privacidad en Internet, Ed. Tirant Lo Blanch, México, 2022 p. 54
[15] Aludido por Muñozcano Eternod, A. (2010). El derecho a la intimidad frente al derecho a la información. Editorial Porrúa p. 45.
[16] *Lexis Nexis, "Onassis v. Christian Dior-New York, Inc. - 122 Misc. 2d 603, 472 N.y.s.2d 254 (Sup. Ct. 1984)," Community, accessed March 21, 2023, https://www.lexisnexis.com/community/casebrief/p/casebrief-onassis-v-christian-dior-new-york-inc.*

Portugal (hacia 1945)[17] en que se clarifica la relación entre lo público y su relación con lo privado. El derecho a no ser molestado como parte de los derechos de la personalidad contenía un bien jurídico intangible, sin cuantificación económica. Carrillo enfatiza que este movimiento constitucional se fundamenta en La Ilustración y los primeros Estados liberales donde se reconoce el poder político de la burguesía que ansiaba la protección de tales derechos de la personalidad[18]. Ya Stuart Mill[19] en su obra *On Liberty* señaló la lucha constante entre libertad y autoridad como la más conspicua batalla entre las personas y la autoridad política. Es S. Warren y L. Brandeis en su Right to Privacy (1890) que atribuyen entidad propia al derecho a la privacidad versus cualquier intromisión injustificada de la autoridad pública. Este legendario artículo sirvió para la correcta interpretación de la Cuarta Enmienda introducida por James Madison en 1789 que protege al ciudadano en su derecho a la privacidad y a no sufrir una detención arbitraria. Carrillo señala "... la *privacy* personal y familiar se convirtió en un límite para el Estado, y disponer de este derecho de la personalidad devino un privilegio social, un privilegio de clase. Una consecuencia de ello fue, claro está, que todo lo público era definido a partir de lo privado. Un ámbito definido por una minoría social"[20].

Los derechos humanos se basan en **normas jurídicas objetivas** que regulan a la sociedad y que son su cimiento para la convivencia. Piñar y Recio opinan que la Constitución Política Mexicana distingue entre derecho a la protección de datos y el derecho a la privacidad; el primero se protege en el Artículo 6 Ap. A fr. II Constitucional "La información que se refiere a la vida privada y los datos personales será protegida en los

[17] Carrillo, Marc. *La intimidad, las celebridades y el derecho a la intimidad.* Diario La Ley, Nº 6979, Sección Doctrina, 1 Jul. 2008, Año XXIX, Editorial LA LEY, p. 3
[18] *Supra*, p. 3
[19] Mill, Stuart. *On liberty*. Yale University Press, NY 2003, p. 84
[20] Carrillo, Marc. *Op. Cit*. p. 4

términos y con las excepciones que fijen las leyes…" y el segundo en el Art. 16 Const. "… nadie puede ser molestado…". La distinción es ontológica, la privacidad es ser, los datos son tener. La privacidad es reserva personal, la protección de datos es control sobre nuestra información. La persona sólo podrá construir y desarrollar su personalidad propia a partir de la capacidad de mantener ciertos aspectos, información, circunstancias y situaciones en privado. La definición de privacidad ha sido estudiada por filósofos, juristas, sociólogos, politólogos; más la evolución de la tecnología ha ampliado su estudio a ingenieros expertos en información, perfilamiento, comunicólogos, psicólogos y hasta antropólogos. No existe una definición aceptada por todos los expertos, pero podemos afirmar que en toda sociedad que respeta los derechos humanos, la privacidad se entiende como la facultad que tiene una persona de decidir sobre sus pensamientos, información personal, relaciones, comportamientos confidenciales, sin injerencia de terceros. Quijano[21] destaca que, las teorías sobre la privacidad se pueden agrupar en seis grupos: 1. Derecho a ser dejado solo, es decir la libertad de no ser molestado. 2. Control sobre el acceso a uno mismo, entendido como la capacidad de limitar quién puede acercarse a la persona. 3. Secrecía, mantener asuntos ocultos de los otros. 4. Control de la información personal. La autonomía sobre cómo se use y se comparta la información de la persona. 5. Protección de la personalidad y dignidad, un escudo que resguarda la identidad y el valor de la persona. 6. Derecho a la intimidad: la potestad de controlar las relaciones interpersonales y cualquier aspecto considerado íntimo de la vida de la persona.

En el mundo vemos dos concepciones muy claras, la norteamericana y la europea. La concepción norteamericana que comienza en una concepción individualista de la privacidad sin contemplar grandes cantidades de datos de personas en pro de construir

[21] *Supra*, Quijano, p. 55

mejores políticas económicas y sociales. Es hasta la creación de los Principios de Prácticas Justas de Información (FIPPs en inglés) por el Departamento de Salud, Educación y Bienestar de Estados Unidos de América en 1973 que se establecen los conceptos de transparencia, control individual y seguridad de datos. Estos principios son tomados por la Organización para la Cooperación y Desarrollo Económico en 1980 para las directrices sobre la Protección de la Privacidad y los Flujos Transfronterizos de los Datos Personales que se aplicaron a nivel de sus miembros[22].

La legislación norteamericana está más bien distribuida en diferentes leyes, es curioso que ni la palabra *privacy* o *intimacy* existe en la Constitución norteamericana.

En Europa existe un marco general de protección a la privacidad desde la propia constitución europea, la Corte Europea de Derechos Humanos (*ECHR*) y la Convención Europea de Derechos Humanos (*ECHR*).

La concepción europea se basa en un enfoque más social al elevar el derecho a la privacidad como un derecho humano que, aunque es el más alto rango de derechos, nunca es absoluto. Los derechos humanos son generalmente considerados derechos subjetivos, es cada persona las que posee la facultad de exigir su respeto y protección porque existen normas jurídicas objetivas que obligan a todos los miembros de la sociedad a respetar. El derecho a la privacidad es un derecho humano, por ende, subjetivo que faculta a la persona a exigir el respeto a su esfera privada con base en los ordenamientos jurídicos, a saber, derecho objetivo. Los orígenes de la protección de datos vienen de la tradición europea que toma fuerza en varios países hacia los 70´s y las resoluciones del Consejo de Europa respecto al proceso de datos. El concepto de privacidad implica controlar nuestra

[22] Van der Sloot, Bart. *Op. Cit.* p. 83.

información, nuestro espacio, nuestras decisiones principalmente por los efectos que pudiera tener en nuestros bienes jurídicos.

Privacidad toma identidad cuando se contrapone a lo público[23], esta relación ha evolucionado a través del tiempo desde el ágora griega a la sociedad de la información donde la tecnología digital permite la invasión a la privacidad en el ciber espacio. El interés por nuestros datos ha crecido a través de diversos fines no sólo en el ámbito estatal sino privado donde una empresa puede recolectar nuestros datos con fines comerciales sin que nosotros estemos conscientes de tal apropiación de nuestros datos. Hay una línea que separa a la privacidad de su invasión que es precisamente lo mío, mi casa, mi computadora, mis datos, mis decisiones[24].

De acuerdo a Robert C. Neville hay dos factores esenciales al proteger la privacidad. El primero es que las cosas importantes son aquellas que aumentan nuestra posición económica y propiedad. El segundo es la contribución relevante que tengan para la vida política o qué tanto incrementa o disminuye el poder político[25].

Es decir, según Neville el interés jurídico para proteger la privacidad es económico y el conflicto de intereses de la privacidad con algún otro deberá resolverse bajo la balanza de cuál contribuye más al poder político.

Los factores de Neville son extremadamente pragmatistas, Neville[26] sostiene que los asuntos privados son aquellos que tienen que ver con la creatividad personal; en cambio, los asuntos públicos son aquellos que tienen que ver con establecer y mantener un ambiente que permita esos niveles de creatividad, entendida ésta como la definen algunos

[23] Neville, Robert C. *Various Meanings of Privacy: A Philosophical Analysis*, in *Privacy: A Vanishing Value?* Ed. William C.S.J. Bier (New York: Fordham University Press, 1980), p.22
[24] La Cuarta Enmienda Norteamericana versa sobre este tema de la no invasión al hogar.
[25] Neville, Robert C. *Op. Cit.*, p. 25.
[26] Citado por Bier, William Christian, *Privacy, a Vanishing Value?* Fordham University Press, 1980, p. 27

filósofos (Hartshorne, Neville, Whitehead[27]) como una serie de experiencias que las personas tenemos, las cuales se acumulan a través del tiempo y que son usadas para crear nuevas ideas. Este concepto es rescatado por Alfred Korzybski al definirlo como *time-binding*[28], el conocimiento se pasa de generación en generación a través del lenguaje.

La relevancia de contraponer lo público y lo privado para la construcción del concepto de privacidad se basa en que, a partir los límites que se tengan, se dará la importancia necesaria a la protección de nuestro derecho a la privacidad. La vida privada siempre se da en un ambiente cuyo mantenimiento es responsabilidad pública. La vida privada se puede tornar pública cuando implica un efecto a dicho ambiente equilibrado.

Los medios de comunicación digitales los que permitirán recolectar datos de todos esos segmentos de la sociedad para potenciar la manipulación, muchas veces sin respeto a la privacidad de los ciudadanos.

Tanto la acción privada como la pública deben tener una obligación jurídica de responsabilidad impuesta incluso desde el ámbito constitucional. El individuo debe ser responsable al permitir que su información personal salga de su ámbito. Pero también el Estado debe hacer uso responsable de la información que necesariamente recopila desde efectos censales hasta fiscales y donde se fortalecen conceptos como consentimiento informado o consentimiento confidencial. Si **privacidad** en la más simple de las definiciones consiste en inhibir la invasión o el acto de molestia en nuestros asuntos privados o personales, siempre hay situaciones límite cuando estos datos deben ser accedidos por instituciones que nos otorgarán un servicio físico o digital, estas instituciones pueden ser públicas o privadas. En todo caso, estas instituciones realizan

[27] *Supra* p. 28
[28] Korzybski, Alfred. *Science and Sanity*, Ed. Institute of General Semantics, NY 1998. p. 376

una acción de investigación que debe respetar a la persona que goza el derecho a la privacidad. Es ahí donde surge la confidencialidad que enfatiza la acción del investigador. El primer paso es obtener el **consentimiento informado** del titular del derecho a la privacidad para tener acceso a sus datos, este consentimiento debe estar condicionado a explicar de forma verbal y por escrito tanto el manejo como el alcance que se dará a esos datos por la institución. La **confidencialidad** consiste en el acuerdo de voluntades entre el titular del derecho de protección de datos o privacidad y la institución que tiene necesidad de recabar sus datos. Este acuerdo debe ser tan amplio que incluya la manera en que se captará, almacenará, manejará y difundirá la información del titular de la misma. Aquí cobra relevancia la encriptación de datos sobretodo al ser transmitidos por medios digitales.

Cuando una persona tiene acceso al ámbito privado de otra, puede recopilar alguna información o datos, pero cuando la tecnología digital permite procesar miles de datos, casi al inifnito, los riesgos a la invasión de la privacidad de las personas se incrementan. El instrumento para analizar tales cantidades enormes de datos es un algoritmo, definido por Domingos como "una secuencia de instrucciones que indica a una computadora qué hacer….lo crean o no, cada algoritmo sin importar qué complejo sea, puede ser reducido a Y, O y NO -*AND, OR OR NOT*-"[29]. Es decir, simple lógica. Por eso se afirma que realmente no puedes entender algo, sino eres capaz de expresarlo en un algoritmo. Los algoritmos ayudan a realizar muchas funciones y, poco a poco, los algoritmos se combinan con otros algoritmos creando un ecosistema digital tan complejo como la vida

[29] Domingos, Pedro, *The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake our World*, New York, NY: Ed. Basic Books, 2018 p. 8

misma[30]. Cuando los algoritmos son capaces de crear otros algoritmos nace el denominado *machine learning*. El ser humano quiere conocer la verdad, ésta lucha por salir a la luz; sin embargo, este esfuerzo requiere tener acceso a lo conocido. Como personas, no podemos entender, estudiar o investigar un tema o fenómeno del que conocemos nada.

Conforme el desarrollo de la tecnología digital y la inteligencia artificial (IA) se integra de manera cada vez más generalizada en la sociedad, los algoritmos se entrelazan aún más con nuestras vidas, desempeñando roles cruciales como guardianes en la recopilación de información, la selección de contenido y el análisis predictivo. Estos algoritmos se erigen como mediadores fundamentales a través de los cuales los sistemas algorítmicos moldean la vida individual, social, política y económica. En plataformas de redes sociales, los algoritmos organizan las publicaciones en las historias o *feeds* de los usuarios. Mediante estos algoritmos, las aplicaciones de medios de noticias priorizan las noticias que los usuarios leen en sus *feeds*. En el ámbito del entretenimiento, plataformas de transmisión como Spotify, Netflix y Hulu hacen uso de algoritmos para impulsar sus operaciones, destacándose al ofrecer contenido digital personalizado para cada usuario[31].

En concreto, la privacidad se concibe como el derecho de las personas a controla la información que existe sobre sí mismos, pero el advenimiento del perfilamiento algorítmico representa varios retos a este derecho, sobre todo porque frecuentemente dicho perfilamiento se hace de manera invisible contra el principio de transparencia que

[30] Domingos, *Supra* p. 9
[31] Shin, Donghee, Kerk F. Kee, and Emily Y. Shin. "*Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms*?" *International Journal of Information Management* 65 (2022): 102494, p. 1

el derecho exige a la tecnología[32]. Las personas generalmente no están conscientes que están siendo sujetas a un perfilamiento a partir del análisis de sus datos, ni el objetivo de dicho perfilamiento.

El perfilamiento algorítmico también amenaza el derecho a la autonomía, entendido como la capacidad y el derecho de una persona para tomar sus propias decisiones libres de coerción o influencia indebida. Este derecho está intrínsecamente relacionado con los principios de dignidad humana y libertad personal, y se manifiesta en varios aspectos de la ley y la sociedad. El perfilamiento algorítmico puede ser inexacto respecto a las personas, inhibiendo las oportunidades de empleo, crédito, residencia en temas migratorios, entre otros. Nucci previene del riesgo que representan estas nuevas formas de comunicación "para el desarrollo de nuestros derechos fundamentales[33]", destaca la necesidad de "proteger los derechos de la personalidad, personales o personalísimos (derecho a la identidad, vida privada o intimidad, honor y propia imagen) en el Internet y las redes sociales ante el vacío legislativo que actualmente existe en nuestro país"[34].

1.0. Evolución histórica del concepto de Privacidad. Perspectiva interdisciplinaria de la Privacidad

El análisis de la privacidad, sus múltiples dimensiones y desafíos han sido una constante a lo largo de la historia, reflejando nuestra inherente dualidad: por un lado, la dimensión social que facilita nuestra supervivencia mediante habilidades adquiridas colectivamente; y por otro, la dimensión individual, que confiere a cada ser humano su singularidad y permanencia. Ambos aspectos son cruciales para el desarrollo pleno del individuo. La

[32] Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo (GDRP). EUR-Lex https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa, Cap. II, Principios, Art. 5.
[33] Nucci, Hilda. *Los derechos de la personalidad en el internet y las redes sociales: propuesta de regulación*. Ed. Conacyt , México CDMX, 2022, p. 28
[34] Nucci, *Supra* p. 29

naturaleza social del hombre parece contraponerse a su necesidad por el respeto a su privacidad, sin embargo, la participación social y la privacidad son complementarias. Las ideas e ideales de la privacidad han sido siempre una muestra de la evolución de las culturas.

Levine[35] subraya la complejidad de la privacidad, especialmente en el contexto de la diversidad de subculturas y estratos sociales presentes en el Occidente, identificando tres aspectos clave en la comprensión contemporánea de la privacidad: primero, la concepción de la privacidad como un derecho ligado al espacio y la territorialidad; segundo, el fenómeno del exhibicionismo moderno, que parece sugerir una renuncia voluntaria a la privacidad; y tercero, la erosión de la privacidad provocada por avances tecnológicos, entendida dentro de su contexto sociocultural y su significado inherente.

En este contexto, el perfilamiento algorítmico emerge como un desafío particularmente significativo. Este proceso implica el uso de algoritmos para analizar datos personales con el fin de evaluar, predecir o influir en comportamientos, preferencias y decisiones individuales. Aunque puede ofrecer beneficios en términos de eficiencia y personalización de servicios, también plantea preocupaciones sustanciales sobre la privacidad y la autonomía individual, especialmente cuando se realiza sin consentimiento explícito o comprensión de los afectados.

La tarea, entonces, consiste en equilibrar los potenciales beneficios del perfilamiento algorítmico con la protección de la privacidad individual, un reto que exige una revisión constante de las normativas y políticas, así como un diálogo continuo entre tecnólogos, legisladores, académicos y la sociedad en general. Este equilibrio debe buscar preservar

[35] Bier, William C. *Privacy: A Vanishing Value*, Ed. Forham University Pres, NY, NY 1980, Artículo escrito por Levine, Morton H. *Privacy in the Tradition of the Western World*, p. 3

la capacidad de los individuos para controlar su información personal, al tiempo que permite innovaciones tecnológicas que pueden mejorar la vida social y económica. En este sentido, el derecho y la ética juegan roles fundamentales en la definición de los límites y responsabilidades asociados al uso de tecnologías de perfilamiento algorítmico, asegurando que la evolución tecnológica avance de manera que respete y fomente la dignidad y los derechos de todos los individuos.

Es interesante conocer el enfoque que los griegos dieron a la privacidad, sobre todo por la influencia que tuvo en el pensamiento occidental a través de la historia. En el periodo arcaico (776 AC – 499 AC) y preclásico (500 AC – 400 AC) de los griegos, sólo los aristócratas tenían vida pública[36]. Sus conceptos de sí mismos y actividad sólo se relacionaban con las responsabilidades, virtudes y rituales de la vida pública. Los no aristócratas y las mujeres no tenían vida pública ni para la política, ni para el comercio. Aristóteles (382-322 AC) es esencial para comenzar con el análisis histórico del concepto al ser el primer autor que habla sobre el ámbito privado. El estagirita hace la distinción entre la esfera doméstica privada de la familia, *oikos*; y la esfera pública de la actividad política, *polis*[37]. El hogar -oikos- es la base de la polis griega, esta unidad debe ser autosuficiente en la producción-consumo de alimentos para la supervivencia. Este hogar no es el concepto actual de hogar, sino un grupo de vecinos, familias que tienen una extensión de terreno para vivir en búsqueda de la virtud para alcanzar la felicidad[38]. Así, Aristóteles ve la *polis* griega en dos sentidos, el primero como un grupo de comunidades

---

[36] Bier, William C. *Privacy: A Vanishing Value*, Ed. Forham University Pres, NY, NY 1980, Artículo escrito por Neville, Robert C. *Various Meanings of Privacy: A Philosophical Analysis.* p. 22 y sigs.
[37] DeCew, Judith. "*Privacy*." *Stanford Encyclopedia of Philosophy*. Stanford University, January 18, 2018. https://plato.stanford.edu/archives/spr2018/entries/privacy/, consultado el 30 de marzo de 2024
[38] Nagle, Brendan D. *The Household as the Foundation of Aristotle's Polis*. Cambridge, UK: Cambridge university press, 2006, p. 31

familiares -*oikiai*- agrupados como vecinos -*komai*-. La base es la familia; el segundo como un grupo de ciudadanos -*plethos*- que forman la polis política. La base es el ciudadano[39]. Esta evolución de la Polis con base en el ámbito privado-público ha sido retomada por Bourriot para explicar la formación de Francia compuesta por todas las villas y personas que conforman la nación[40]. Fustel de Coulanges destaca la privación de derechos que tenían las mujeres sobre todo en el ámbito público[41] y la privatización del *oikos* como resultado de la ascensión de la *Polis*. Barrington Moore, el sociólogo de los regímenes totalitarios escribió una historia socio-cultural de la privacidad al enfatizar que los gobiernos autoritarios siempre han negado a sus gobernados el derecho a la privacidad; dicho control tiene todo que ver con los artefactos que la tecnología aporta para llevar a cabo ese *surveillance* (vigilancia)[42]. Hanna Arendt (1906-1975) retoma la distinción en su obra La Condición Humana[43] al hablar del ámbito del hogar como centro de la tendencia natural del ser humano a asociarse (*oikia*) diferenciado de aquél de la organización política (*polis*); la esfera pública es el ámbito de la acción política, donde los individuos actúan y hablan juntos, revelando quiénes son. Por otro lado, la esfera privada es el dominio de la vida doméstica y el cuidado personal, protegido de la vista pública y liberado de las necesidades de actuar políticamente. El estado intenta persuadir a las personas de que cedan su privacidad en aras de fomentar un comportamiento colectivo uniforme a la par de consolidar su autoridad.

[39] Nagle, Brendan D. *Supra* p. 29
[40] Aludido por Nagle, *Supra* p. 29
[41] Fustel de Coulanges, Numa Denis. *The Ancient City*. Ontario, Canada: Batoche Books, 2001. p. 270
[42] Mencionado por Keulen, Sjoerd y Kroeze, Ronald en su capítulo de *Privacy from a Historical Perspective*, como parte del *Handbook of Privacy Studies*, editado por Van Der Sloot, Bart y De Groot, Aviva. Amsterdam University Press, 2018, p.
[43] Arendt, Hannah. La Condición Humana. Argentina: Paidós, 2003. p. 39 y siguientes.

La privacidad claramente es una creación humana para exigir de los otros individuos el respeto a lo que entendamos por nuestra esfera privada. Sólo el hombre es capaz de exigir privacidad, ningún animal podría exigirlo. A la par la autora distingue entre labor –proceso biológico-, de trabajo –artificial mundo de cosas creadas por el hombre- y de acción –condición humana de pluralidad, que implica el pensamiento filosófico-. Esta última es el fundamento de la vida política y, por ende, jurídica[44]. Los hombres están condicionados por su entorno, y todo aquello con lo que interactúan pasa a ser una condición de su existencia. La privacidad es una condición que surge hacia el otro al intentar proteger lo nuestro versus los demás. Lo que rescata a cada ser humano de la historia cíclica de otros es precisamente sus acciones y su discurso en torno a las condiciones que enfrenta, precisamente eso le revela su yo único. La privacidad sólo surge a partir de la condición de que los hombres vivimos en sociedad. Y esa vida privada le es dada junto con su "… bios politikos. Ahora todo ciudadano pertenece a dos órdenes de existencia, y hay una tajante distinción entre lo que es suyo (idion) y lo que es comunal (koinon)."[45] La grandeza de los héroes en toda época sólo se entiende por sus acciones y discursos en la esfera política. Por ello, podemos afirmar que la revelación del agente es menos completa en lo privado que en lo público. Lo público es el reino de la apariencia y recuerdos organizados; el discurso manipulador. Entonces, hablaremos de esfera pública y privada, pero también de polis y familia. La sociedad es una súper familia y su organización engendra la nación. Desde la antigüedad, la esfera privada ha sido sacrificada en aras de la esfera pública.

[44] Arendt, Hannah. La Condición Humana. Barcelona: Paidós, 2003.. 23
[45] Arendt, *Ibídem* p. 39

Para Arendt el primer explorador de la intimidad fue Jean-Jacques Rousseau para quien "lo íntimo y lo social eran más bien modos subjetivos de la existencia humana[46]". Tal afirmación de Arendt respecto a Rousseau me llevó a consultar a Cladis que destaca la obra *Reveries* de Rousseau que comienza "Yo, separado del mundo entero, ¿qué soy? ¿Qué somos divorciados de nuestros lazos y relaciones sociales? ¿Qué somos cuando rechazamos la compañía de otros?"[47]. En esta obra, Rousseau descubre el camino a la privacidad, al amarse uno mismo, sin hacer daño a otros. Se reconoce sufrimiento en tal privacidad al tener soledad. Rousseau sostiene que este camino a la privacidad es un mal sueño del que despertaremos para estar, de nuevo, en el ámbito social. Interesante reflexión de Rousseau, pues hoy parece que la privacidad es un sueño al que queremos aspirar para poder vivir con nosotros mismos, moldear nuestro destino, liberarnos de las emociones y sentimientos que nos da estar frente a otros. Este sueño, siempre tendrá la manera de ser despertado y desenmascarar nuestra privacidad. Quizá esté sea el fundamento para que el derecho sustantivo proteja nuestra capacidad de soñar, nuestra capacidad de tener privacidad. A partir de esto, si la gente quiere entrar a nuestra esfera privada, insistiremos en tener por lo menos cierto control sobre ello. Si alguien se atreve a transgredir esos límites, estará cometiendo una violación a nuestra privacidad.

En relación a la esfera privada, Arendt[48] interpreta el original sentido privativo. Explica, vivir una vida privada implica privarse de cosas esenciales a una verdadera vida humana: estar privado de ser visto u oído por los demás, estar privado de una relación con los otros. Es decir, la privación de lo privado radica en la ausencia de los demás. Es como si

[46] Arendt, *Supra* p. 50
[47] Cladis, Mark Sydney. *Public Vision, Private Lives: Rousseau, Religion, and 21st-Century Democracy*. Oxford: Oxford University Press, 2003. p. 168
[48] Arendt … *Supra* p. 67

no existiera, por lo que cualquier cosa que hiciera carece de impacto para el resto de la sociedad. En el ámbito privado, lo que nos importa, no les importa a los demás. Sólo al haber propiedad puede haber privacidad en el ámbito físico. Arendt emite un juicio duro sobre la distinción entre lo público y lo privado al hacerlo coincidir con varias dicotomías: necesidad y libertad, futilidad y permanencia, vergüenza y honor. "Sólo lo necesario, fútil y vergonzoso tendrán su lugar adecuado en la esfera privada[49]". Es el cristianismo el que aumenta una dimensión a lo privado con la bondad que enseñó Jesús con palabra y hechos, sostiene Arendt[50], y que acoge una tendencia a no ser vista ni oída. Puesto que, si una acción bondadosa se hace pública y conocida, pierde el carácter de bondadosa. Es aquí donde Arendt rescata dos aspectos positivos de la privacidad, los actos bondadosos y la propia sabiduría. Que, curiosamente parten de dos hechos radicales, nadie es bueno y nadie es sabio. Y la paradoja es que la bondad debe reflejarse en el otro, de la misma manera que pensar nunca es completo sin el diálogo. Arendt se refiriere a Maquiavelo quien sostuvo que la maldad que surge de lo oculto es impúdica y destruye directamente al mundo común; la bondad que surge de lo oculto y asume un papel público ya no es buena sino corrupta en sus propios términos[51].

1.0.1. El pensamiento de Arendt y el perfilamiento algorítmico

La relevancia de Arendt para la privacidad se manifiesta en su énfasis en la importancia de tener un espacio privado para el desarrollo del individuo. Ella sostiene que sin un espacio privado, protegido de las miradas del mundo, los individuos no pueden tener un verdadero refugio para la reflexión personal o el desarrollo del carácter. La privacidad, en

[49] Arendt … *Supra* p. 78
[50] Arendt … *Supra* p. 79
[51] Arendt … *Supra* p. 82

este sentido, es vista como esencial para la dignidad humana y la autonomía individual. Arendt advierte sobre los peligros de la erosión de las fronteras entre lo público y lo privado. En sociedades donde estas fronteras se desvanecen, la individualidad y la libertad pueden ser socavadas. Este pensamiento es especialmente profético en la era digital, donde la tecnología ha borrado muchas de las divisiones tradicionales entre estos dos ámbitos, llevando a preocupaciones sobre la vigilancia masiva, el perfilamiento algorítmico y la pérdida de autonomía personal.

Desde la perspectiva de Arendt, el desafío de la privacidad en la era moderna no es simplemente una cuestión de proteger datos o información personal, sino de preservar un espacio en el que los individuos pueden ser verdaderamente libres para desarrollarse lejos del escrutinio público. En este sentido, el debate sobre privacidad es fundamentalmente un debate sobre la naturaleza de la sociedad y la condición humana, en el que se juegan la libertad individual y la capacidad de participación política.

En conclusión, Hannah Arendt nos invita a reflexionar sobre la importancia de mantener espacios privados como condiciones esenciales para la libertad y la autenticidad humanas. En una era caracterizada por avances tecnológicos que amenazan con penetrar cada vez más en nuestra esfera privada, su pensamiento ofrece una guía valiosa para navegar los desafíos contemporáneos de la privacidad, recordándonos la necesidad de proteger esos espacios donde podemos ser nosotros mismos, libres de la imposición de la mirada pública. La conexión entre el pensamiento de Hannah Arendt sobre la privacidad y el desafío contemporáneo del perfilamiento algorítmico es profunda y significativa. Arendt, al diferenciar claramente entre las esferas pública y privada, subraya la importancia de mantener un espacio íntimo protegido de la incursión pública para el

desarrollo individual y la autonomía. En este contexto, el perfilamiento algorítmico representa una amenaza contemporánea a este espacio privado, al erosionar las fronteras que Arendt consideraba esenciales para la libertad y la dignidad humana. El perfilamiento algorítmico, que implica la recolección y análisis de grandes cantidades de datos personales para predecir comportamientos y preferencias, se realiza a menudo sin el consentimiento explícito o incluso el conocimiento de las personas afectadas. Esto representa una intrusión tecnológica en la esfera privada que Arendt advirtió podría socavar la individualidad y la libertad. En la práctica, el perfilamiento algorítmico puede limitar la capacidad de los individuos para actuar libremente, al encerrarlos en categorías predefinidas y exponer aspectos de su vida privada que preferirían mantener alejados del dominio público. Desde la perspectiva arendtiana, el perfilamiento algorítmico podría interpretarse no solo como una invasión de la privacidad, sino como una amenaza a la capacidad de los individuos para participar genuinamente en la esfera pública. Arendt valoraba la esfera pública como un espacio de acción y discurso donde los individuos pueden revelarse entre sí como únicos y distintos. Sin embargo, si las acciones y opiniones de las personas son predecidas y manipuladas por algoritmos, la autenticidad de esa participación pública podría verse comprometida. Además, la omnipresencia del perfilamiento algorítmico podría conducir a una forma de conformismo, donde las personas se sienten presionadas a adaptarse a las normas y expectativas generadas por análisis de datos, restringiendo así la pluralidad y la libertad que Arendt consideraba vitales para la política y la sociedad. Para abordar estos desafíos, sería necesario invocar los principios arendtianos de protección de la esfera privada y promoción de una esfera pública vibrante y genuina. Esto implicaría desarrollar y aplicar regulaciones más

estrictas sobre la recolección y uso de datos personales, asegurando que los individuos retengan el control sobre su información personal y que su consentimiento sea informado y genuino. Asimismo, sería esencial fomentar un debate público crítico sobre los límites éticos del perfilamiento algorítmico y la importancia de preservar espacios para la individualidad y la libertad fuera del alcance de la tecnología. En resumen, al relacionar el pensamiento de Hannah Arendt con el perfilamiento algorítmico, nos enfrentamos a la tarea crítica de revisar y reafirmar los valores de privacidad, libertad y autenticidad en una era dominada por tecnologías invasivas. Esto requiere un compromiso colectivo para proteger los espacios privados que permiten la individualidad y asegurar que la esfera pública siga siendo un lugar de encuentro auténtico y libre para todos.

1.0.2. Hobbes, Locke, Marx y el perfilamiento algorítmico

Relacionar el pensamiento de filósofos tan fundamentales y diversos como John Locke, Thomas Hobbes y Karl Marx con el fenómeno contemporáneo del perfilamiento algorítmico implica un reto que cruza siglos de teoría política para abordar uno de los desafíos más significativos de nuestra era digital. Aunque ninguno de estos pensadores pudo haber imaginado la tecnología actual, sus ideas sobre el estado, la sociedad y la economía ofrecen perspectivas valiosas sobre las implicaciones políticas y sociales del perfilamiento algorítmico.

John Locke. Conocido por su énfasis en los derechos individuales y la propiedad privada, podría verse como un defensor de la protección de los datos personales como una extensión de la propiedad privada. Locke subraya que, aunque los ciudadanos deben adherirse a las leyes establecidas por el Estado, tienen el derecho a resistir en situaciones

donde el Estado infrinja su privacidad[52]. En su teoría, la propiedad surge del trabajo personal sobre los recursos naturales, lo que podría extenderse metafóricamente a los datos personales en la era digital: los individuos "laboran" al generar datos a través de sus acciones y elecciones en línea, por lo que estos datos deberían pertenecerles y estar protegidos por derechos de propiedad. Desde esta perspectiva, el perfilamiento algorítmico sin consentimiento violaría los principios lockeanos al usurpar la propiedad privada (los datos personales) sin el acuerdo del individuo.

Thomas Hobbes, al haber vivido la Guerra Civil Inglesa, busca enunciar los principios racionales para fortalecer un gobierno que prevenga su autodestrucción[53]. Con su visión de la naturaleza humana y su énfasis en la necesidad de un poder soberano absoluto para mantener el orden, podría ofrecer una perspectiva diferente. Podría argumentarse que, en el contexto del perfilamiento algorítmico, un estado basado en la visión de Hobbes, justificaría la vigilancia y el control algorítmico como medios para prevenir el caos y proteger a la sociedad de sus peores impulsos. Sin embargo, esto también plantea preocupaciones sobre la erosión de la libertad individual y la autonomía, elementos que Hobbes estaba dispuesto a sacrificar por la seguridad y el orden.

Hobbes y Locke mantienen que la voluntad para mantener la cohesión social y política es el interés propio. Por eso surgen las teorías individualistas que satisfacían el interés individual. Es entonces la vida política el mejor medio para proteger los intereses individuales. Las ideas liberales derivadas de estas teorías individualistas establecen una jerarquía de responsabilidad política, pero un gran problema surge a partir de su posición. Será el Estado el depositario de la voluntad individual y él deberá proteger la privacidad

[52] Aludido por Nucci, Hilda. *Op. Cit*. p. 185
[53] *Supra*, Nucci p. 185 y sigs.

del ciudadano, o por lo menos deberá darle un sentido negativo; es decir, no molestar esa privacidad a no ser que haya un interés jurídico mayor necesario para que la propia convivencia continúe. Locke fue todavía más claro que Hobbes al relacionar la vida pública con el interés privado. Para él, una persona es lo que posee -desde su cuerpo- y lo que hace. El rol del estado es proteger esos bienes. Así la vida pública debe reconocer un ámbito mínimo de libertad personal a aquélla. El derecho a no ser molestado.

Marx sostiene que el Estado es enajenante y arrasa con los intereses privados, dejando sin oxígeno la privacidad del ciudadano[54]. Aconseja combinar la libertad individual con la participación social, pero para ello el Estado liberal requeriría ciertos cambios referidos al espíritu de solidaridad revolucionario, el cual la propia historia nos ha demostrado que ahogó aún más la libertad individual.

Con su enfoque en las relaciones de poder económico y la lucha de clases, ofrecería una crítica del perfilamiento algorítmico centrada en cómo estas prácticas refuerzan las estructuras de poder capitalistas. Desde una perspectiva marxista, el perfilamiento algorítmico podría verse como una herramienta de explotación que permite a las corporaciones y al estado capitalista monitorear, manipular y controlar a los trabajadores y consumidores, al maximizar las ganancias a expensas de la privacidad y la autonomía individual. Además, la acumulación de datos personales se convierte en una forma de capital, con corporaciones que extraen valor de este nuevo "recurso" en un proceso reminiscente de la acumulación primitiva descrita por Marx.

1.0.3. Habermas y el Perfilamiento Algoritmo

[54] Karl Marx, *Early Writings*. New York, NY: Mc Graw Hill, 1964, (Originalmente publicada en 1844.) p. 1-31.

Jurgen Habermas en su libro Historia y Crítica de la Opinión Pública previene de la confusión que las palabras y su manipulación representa para la comprensión exacta de la esfera pública y privada. Destaca que "la ciencia jurídica, la politología y la sociología son manifestaciones incapaces de sustituir categorías tradicionales como público y privado por conceptos más precisos[55]". Esta advertencia de Habermas anticipa la problemática causada por el desarrollo de las nuevas tecnologías para delimitar el concepto público y privado a partir de las ciencias sociales. Previene el peligro que esto conlleva, pues al no tener un concepto preciso, no podemos proteger lo ambiguo. Nos podemos preguntar si el internet es un espacio público al ser accesible a todos con acceso a una terminal. Parece anticipar el problema cuando señala "..en el ámbito de los medios de comunicación de masas la notoriedad pública ha variado evidentemente su significación. De una función de la opinión pública ha pasado a ser un atributo de aquello que precisamente atrae a la opinión pública hacia sí[56]". La obra de Jürgen Habermas, especialmente su análisis de la esfera pública y la acción comunicativa, ofrece un marco crítico para evaluar el impacto del perfilamiento algorítmico en la sociedad contemporánea. Habermas concibe la esfera pública como un dominio de discusión racional donde los ciudadanos pueden participar en el debate y la deliberación sobre asuntos de interés común, libres de coacción tanto del estado como de intereses privados. La integridad de este espacio es fundamental para el funcionamiento de la democracia, ya que permite la formación de una opinión pública que es esencial para la legitimidad democrática y la toma de decisiones políticas.

[55] Habermas, Jürgen. Historia y Crítica De La Opinión Pública. Barcelona: Gili, 1981. p. 41.
[56] Habermas*, Supra* p. 41

Desde la perspectiva de Habermas, el perfilamiento algorítmico presenta desafíos significativos a este ideal de la esfera pública por varias razones:

a) Manipulación de la opinión pública: El perfilamiento algorítmico permite una segmentación fina de la población y la entrega personalizada de contenido, incluyendo noticias y publicidad política, que puede ser diseñada para manipular opiniones y comportamientos. Esto puede debilitar el proceso democrático al distorsionar la formación de una opinión pública informada, al reemplazarla por un eco de preferencias y prejuicios individuales manipulados por entidades con acceso a grandes conjuntos de datos.
b) Privatización de la esfera pública: Habermas ya criticaba la transformación de la esfera pública, que se veía comprometida por la creciente influencia de intereses comerciales y la mercantilización de la comunicación. El perfilamiento algorítmico, al ser una herramienta principalmente en manos de corporaciones tecnológicas y otros actores privados con fines de lucro, intensifica este proceso al convertir la información y la comunicación en bienes comercializables y segmentar el espacio público en nichos de mercado.
c) Erosión del discurso racional: La idealización del debate público por Habermas presupone un intercambio de argumentos racionales que permite a los participantes llegar a un entendimiento mutuo. Sin embargo, el perfilamiento algorítmico puede contribuir a la formación de cámaras de eco y la polarización, donde la exposición a puntos de vista contrapuestos es limitada. Esto erosiona la base del discurso racional y crítico necesario para la deliberación democrática.

Para confrontar estos desafíos desde la perspectiva de Habermas, sería esencial promover regulaciones y políticas que aseguren transparencia y responsabilidad en el uso de algoritmos, especialmente aquellos que influyen en el flujo de información y la formación de opinión pública. Además, sería crucial fomentar espacios de comunicación que estén protegidos de la manipulación comercial y algorítmica, posiblemente a través del fortalecimiento de plataformas de medios públicos y el apoyo a iniciativas que promuevan el debate y la deliberación racional.

En última instancia, el pensamiento de Habermas nos insta a reconsiderar cómo las tecnologías de información y comunicación pueden ser diseñadas y reguladas de manera que fortalezcan la esfera pública democrática, en lugar de disminuirla. Esto implica no solo una reflexión crítica sobre el papel de la tecnología en la sociedad, sino también un compromiso activo para moldear ese papel de manera que promueva la democracia, la participación y el entendimiento mutuo.

1.0.4. Contraste entre las posiciones de Arendt y Habermas

Arendt y Habermas brindan perspectivas distintas pero complementarias que son especialmente relevantes en la era del perfilamiento algorítmico y la transformación digital de la sociedad. Arendt, como hemos discutido, distingue claramente entre la esfera pública y la privada, enfatiza la importancia de ambas para el funcionamiento de una sociedad libre y democrática. Habermas, por otro lado, se centra en el concepto de la esfera pública desde una perspectiva ligeramente diferente. Habermas describe la esfera pública como un foro de debate racional donde los ciudadanos participan en discusiones libres y abiertas sobre asuntos de interés común, idealmente libres de coacción tanto del Estado como de intereses privados. Para Habermas, esta esfera es fundamental para la

democracia, ya que facilita la formación de una opinión pública ilustrada y crítica que puede influir en la toma de decisiones políticas.

La confrontación entre Arendt y Habermas sobre la esfera pública y privada se hace particularmente relevante en el contexto del perfilamiento algorítmico. Mientras Arendt subraya la importancia de mantener separadas las esferas para proteger la individualidad y permitir la acción política genuina, Habermas pone énfasis en la necesidad de una esfera pública vibrante y crítica para el ejercicio de la democracia. El perfilamiento algorítmico, al erosionar las fronteras entre lo público y lo privado, plantea desafíos significativos a ambas visiones: compromete la autonomía individual al exponer la vida privada al escrutinio y la manipulación, y al mismo tiempo, puede distorsionar el proceso democrático al influir en la formación de la opinión pública a través de la selección y presentación de información. Desde la perspectiva de Arendt, la incursión de tecnologías de perfilamiento en la esfera privada podría amenazar la capacidad de los individuos para actuar y presentarse auténticamente en el espacio público. Para Habermas, la manipulación de la opinión a través del control de la información y la comunicación en la esfera pública por medio de algoritmos compromete la calidad del debate democrático y la formación de una voluntad pública genuina.

La confrontación de estas dos teorías destaca la importancia de salvaguardar tanto la integridad de la esfera privada como la calidad del discurso en la esfera pública. En la práctica, esto puede requerir políticas y regulaciones que aseguren la transparencia y la equidad en el uso de tecnologías de información, así como mecanismos para proteger la privacidad y promover un espacio público donde el debate racional y crítico pueda florecer.

En conclusión, la interacción entre las ideas de Arendt y Habermas nos ayuda a examinar y responder a los desafíos planteados por el perfilamiento algorítmico y otras tecnologías emergentes, enfatizando la necesidad de proteger los espacios privados y públicos para preservar la democracia y la libertad individual.

1.0.5. Crítica de Fraser a Habermas y el perfilamiento algorítmico

Nancy Fraser ofrece una crítica sustancial a la noción de esfera pública de Habermas que tiene implicaciones importantes para comprender los desafíos del perfilamiento algorítmico en la sociedad contemporánea. Fraser[57] califica de idealista la descripción de Habermas del ámbito público como un grupo de personas privado que se reúne para para hablar de asuntos de interés público o bien común y que funciona como interlocutor entre el poder público y la ciudadanía burguesa que tenía la fuerza del mercado privatizado al dejar fuera a otros sectores de la población más allá de la sociedad burguesa. Los medios que se usan para garantizar tal comunicación son la libertad de acceso a la información, la libertad de expresión, asociación o reunión entre otras, mismos que se quedan cortos o limitados siempre por el poder público. Fraser cita a Joan Landes quien destaca que hay una exclusión clara de género que influyó en las construcciones masculinistas que llevaron a la exclusión de la mujer del ámbito público. Fraser narra cómo la mujer fue participando en la vida pública de manera creativa a través de fundaciones creadas por sus padres o abuelos e incluso al participar en manifestaciones públicas de otros sectores de la sociedad como los obreros. Fraser resume que la historiografía revisionista destaca cuatro supuestos específicos del ámbito público burgués y excluyente del género

[57] Fraser, Nancy. *Rethinking the Public Sphere: A contribution to the Critique of Actually Existing Democracy.* Ensayo que aparece en Calhoun, Craig. *Habermas and the Public Sphere*, Cambridge MA: MIT Press 1991, p. 28

femenino. La autora argumenta contra estos 4 supuestos. El primero es el acceso abierto a todos y a todas las personas en un ambiente de equidad y paridad. La autora destaca que, si bien la ley puede redactar dicha paridad, la vida pública -de facto- excluía a mujeres y a personas por motivos raciales o étnicos. Y aún cuando se alcance esa paridad, en el debate se tiende a poner más atención a lo que dicen los hombres e ignorar las aportaciones de las mujeres. Este poner entre paréntesis las desigualdades no ayuda a la vida pública porque es una hipocresía para legitimar a la clase o partido dominante. La desigualdad social contamina la equidad política hasta que no sea reconocida. El segundo supuesto afirma que el convocar a muchos públicos y ponerlos a competir aleja a la democracia, es preferible, un ámbito público único. La autora crítica que, en la burguesía, la pluralidad de grupos se vea como sinónimo de decadencia, cuando la existencia de lo que llama contra-públicos alternos[58] siempre beneficiará el ámbito discursivo. El tercer supuesto del masculinismo burgués es que el terreno público es aquél donde se discurre sobre el bien común, de la autoridad estatal, accesible para todos como lo constatamos con las leyes relativas al acceso de la información. En este supuesto, los asuntos privados son de dos tipos, los primeros son aquellos que pertenecen a la propiedad privada dentro de una economía de libre mercado, aquí se le llama privacidad económica y, los segundos aquellos que tienen que ver con la vida íntima o personal que incluye la propia imagen - llamada privacidad doméstica. Este supuesto se pone en entredicho porque sus fronteras no son claras, temas como la violencia intrafamiliar puede ser dejado como un tema de la vida íntima de una pareja, pero necesariamente es un tema de interés común el prevenirlo

[58] Fraser, *Supra* p. 41

y sancionarlo. Fraser aconseja que la teoría crítica eche una mirada a los términos público y privado pues no son palabras refiriéndose a un ámbito social, sino cultural y retórico[59].

El cuarto supuesto de la concepción burguesa del ámbito público es que éste requiere una separación clara y específica entre la sociedad civil y el estado. El liberalismo exige que la actividad económica sea considerada como privada y dentro de la llamada sociedad civil. La consecuencia de tal concepción es la gran desigualdad económica que produce. Las audiencias de la sociedad civil sólo producen opiniones que no entran al ámbito público en su expresión más amplia como es la toma de decisiones.

Fraser plantea la necesidad de romper los límites señalados en estos supuestos al destruir cualquier indicio de desigualdad, es preferible tener múltiples públicos, pero todos iguales ante la ley; además de que es necesario incluir ciertos temas privados, así llega a lo que llama la concepción postburguesa alternativa del ámbito público para cubrir las necesidades de la teoría crítica actual. Habermas se queda corto para explicar los nuevos segmentos de la sociedad que exigen ser escuchados y tomados en cuenta en el debate público. Fraser explica que al surgir la democracia de masas del estado benefactor, "la sociedad y el estado se entrelazaron mutuamente; lo público, en el sentido de escrutinio crítico del estado, dio paso a las relaciones públicas, a los despliegues escénicos de los medios masivos y a la manufactura y manipulación de la opinión pública[60]". Para Fraser el argumento de la privacidad ya doméstica (como en el caso del maltrato a la mujer en el hogar) o privacidad económica (como el caso de una empresa que paga menos a las mujeres por el mismo trabajo que hacen los hombres) estos temas son sacados del ámbito público y, por ende, hacen que se mantenga la opresión y desigualdad bajo el argumento

[59] Fraser, *Supra* p. 51
[60] Fraser, *Supra* p. 28

del respeto a la privacidad[61]. La crítica de Fraser destaca dos aspectos principales que son especialmente relevantes en el contexto del perfilamiento algorítmico:

1. Exclusión y Marginalización: Fraser señala que la esfera pública definida por Habermass, en su idealización, tiende a excluir o marginalizar voces y perspectivas de grupos menos poderosos o minoritarios. De manera similar, el perfilamiento algorítmico puede exacerbar estas exclusiones al reforzar sesgos existentes en los datos y algoritmos. Los sistemas de perfilamiento, al depender de patrones de datos históricos, pueden perpetuar y amplificar prejuicios y discriminaciones existentes, al marginar aún más a aquellos que ya están en desventaja dentro de la sociedad.
2. Pluralidad de Esferas Públicas: La visión de Fraser sobre la existencia de múltiples esferas públicas subalternas sugiere una complejidad en la formación de opinión pública y deliberación democrática que es opacada por la uniformidad del perfilamiento algorítmico. Este último tiende a homogeneizar la experiencia del usuario a través de la personalización, reduciendo la exposición a perspectivas diversas y limitando las oportunidades para el encuentro y el diálogo entre grupos diferentes. Esta dinámica puede debilitar la capacidad de las esferas públicas subalternas para formar contrapúblicos y ejercer influencia sobre el discurso más amplio, algo que Fraser considera esencial para la justicia democrática.

Al relacionar la crítica de Fraser con el perfilamiento algorítmico, se destaca la necesidad de tecnologías de información y comunicación que no solo respeten la pluralidad de voces y perspectivas, sino que también promuevan la inclusión y la equidad. Esto implica diseñar sistemas algorítmicos que sean transparentes, responsables y sensibles a los

[61] Fraser, *Supra* p. 51

sesgos y discriminaciones. Además, sería esencial apoyar la creación y sostenimiento de espacios digitales que faciliten la formación de esferas públicas subalternas, donde grupos marginados puedan expresarse y participar en la deliberación democrática en igualdad de condiciones. La digitalización de la esfera pública debe fomentar la pluralidad, inclusión y equidad democrática.

1.0.6. La Teoría del *The Right to Privacy* y el perfilamiento algorítmico

Warren y Brandeis en su obra *The Right to Privacy*[62] aportan su capacidad sintética para enunciar el famoso derecho a la privacidad que intenta salvaguardar nuestra informacion de la intrusión de los otros, su mérito es que concretaron las doctrinas existentes y los diversos casos del derecho norteamericano para generar un nuevo derecho a la privacidad que se constituyó como: *the right to be alone*[63]*,* basado en un principio de la personalidad inviolable ante la tecnología de la época, a saber, la fotografía.

William Prosser dividió el derecho a la privacidad descrito por Warren y Brandeis en 4 tipos de daño civil: l) contra la intrusión en la soledad, o en los asuntos privados de uno; 2) contra la revelación de actos privados embarazosos; 3) contra la publicidad que coloca a uno en una falsa imagen ante el público; y 4) contra la apropiación del nombre de uno en beneficio de otro[64]. El mérito de Prosser es que ordenó cientos de tipos de casos que afectaban la privacidad en 4 grupos, muy apropiado para 1960; sin embargo, no ha podido ser adaptado a la era de la información porque no enunció una teoría coherente del derecho a la privacidad que se pudiera adaptar a la época del internet[65].

---

[62] Warren, Samuel, *and* Louis Brandeis. "*The Right to Privacy*" Harvard Law Review Volume 4, no. No. 5 (December 15, 1890): 193–220.
[63] *Op. Cit.*
[64] Prosser, William. *Privacy*. *California Law Review*, vol. 48, num. 3, 1960, pp. 383-423.
[65] Solove, Daniel. *Prosser´s Privacy Law: A Mixed Legacy*. 98 Cal. L. Rev. 1887 (2010).

Alan F. Westin escribió uno de los primeros libros con un estudio profundo de la Privacidad al definirla como el control sobre la información personal, es el derecho a decidir el momento, la forma y la cantidad de información personal comunicada a otros. A esto le llama la autodeterminación informativa. "Proceso de autodeterminación personal que ha de integrarse asimismo en los procesos comunicativos y participativos en los que interviene el individuo"[66].

Si relacionamos la teoría de Warren & Brandeis con el concepto de perfilado algorítmico, emergen varios aspectos clave:

1. Aplicación Amplia de los Principios de Privacidad: Warren y Brandeis proponen un derecho a la privacidad que pudiera adaptarse a nuevas circunstancias y tecnologías[67]. Enfatizaron que la ley debe progresar con los avances tecnológicos para proteger lo que denominaron "el derecho a estar solo". En el contexto del perfilado algorítmico, esto sugiere una necesidad de que las leyes de protección a la privacidad evolucionen para abordar las complejidades introducidas por el análisis de datos, el aprendizaje automático, denominado *machine learning* y la inteligencia artificial.
2. Respuestas Legales Proactivas: Al igual que Warren y Brandeis respondieron a los desafíos planteados por las tecnologías relacionadas con los medios de comunicación, emergentes de su tiempo[68], hoy hay una necesidad similar de abordar proactivamente los desafíos planteados por el perfilado algorítmico. Esto implica crear y hacer cumplir regulaciones que gobiernen la recopilación, uso y

[66] Aludido por Saldaña, María Nieves. La protección de la privacidad en la sociedad tecnológica. Ed. Araucaria, Revista Iberoamericana de Filosofía, Política y Humanidades, vol. 9, núm. 18, 2007, pp. 99.
[67] Warren, S. D., & Brandeis, L. D. (1890). *The right to privacy*. Harvard Law Review, 4(5), 193–220.
[68] *Supra,* Warren*, etal.* p. 195

transparencia de datos, asegurando que los individuos retengan el control sobre su información personal.

3. Privacidad como Derecho Defensivo: El artículo enmarca la privacidad como un derecho que destaca la defensa de la autonomía personal y la protección contra intrusiones injustificadas[69]. En la era del perfilado algorítmico, este derecho defensivo se traduce en protecciones contra el uso no sancionado de datos personales y el derecho a impugnar y corregir inexactitudes en perfiles basados en datos.
4. Consideraciones Morales y Éticas: Warren y Brandeis estaban preocupados por las implicaciones morales y éticas de la invasión a la privacidad. Señalan: "It is a **violation of moral and social duties** that is the essence of the wrong committed, and not the breach of a legal contract or trust[70]" .De manera similar, las consideraciones éticas son de suma importancia en la implementación del perfilado algorítmico, particularmente en lo que respecta al consentimiento, la mitigación de sesgos que pueden causar discriminación y las posibles consecuencias de la toma de decisiones automatizada en la vida de las personas.
5. Neutralidad Tecnológica de los Derechos: Aunque la tecnología ha cambiado, el principio subyacente de proteger la privacidad de los individuos sigue siendo pertinente. El derecho a la privacidad, tal como lo concibieron Warren y Brandeis, debería aplicarse independientemente de la tecnología involucrada, asegurando que se mantengan la dignidad personal y la autonomía incluso en contextos altamente digitalizados y basados en datos. Así se infiere en su escrito *"The*

[69] *Supra* Warren*, etal*, p. 205
[70] *Supra* Warren*, etal*, p. 196

> *principle which protects personal writings and all other productions of the intellect or of the emotions, is the right to privacy, and* ***the law has no new principle to formulate when it extends this protection to the person and to the affairs of private life****.*[71]**"**

El concepto del derecho a la privacidad por parte de Warren y Brandeis proporciona un marco amplio para comprender y abordar las implicaciones del perfilado algorítmico hoy en día. La analogía es que el perfilamiento algorítmico es una tecnología que usa información de las personas que ignoran dicho hecho, para intereses que son ajenos al titular del derecho a la privacidad. Destaca la importancia de adaptar las protecciones legales para asegurar que los derechos de privacidad se protejan incluso frente a la tecnología que avanza a pasos más rápidos que el derecho objetivo.

1.0.7. Perspectiva interdisciplinaria de la Privacidad con el perfilamiento algorítmico

La relación entre la privacidad y el perfilamiento algorítmico se examina mejor a través de una visión interdisciplinaria, considerando las contribuciones de diversos campos académicos y profesionales a esta problemática. El perfilamiento algorítmico, que implica el uso de algoritmos para analizar datos personales y predecir comportamientos, preferencias y capacidades individuales, plantea importantes preguntas sobre la privacidad desde varias perspectivas.

El Derecho se preocupa por la forma en que el perfilamiento algorítmico puede chocar con las leyes de protección de datos y privacidad, como el GDPR[72] en Europa, que exige

[71] *Supra* p. 205
[72] Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo (GDRP). EUR-Lex https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa

transparencia, consentimiento informado y la posibilidad de optar por no participar en el procesamiento de datos personales. Los desafíos legales incluyen cómo garantizar que los individuos mantengan el control sobre sus datos y cómo se utilizan en el perfilamiento algorítmico. Ahora bien, el GDPR[73], por mucho la más completa regulación jurídica de protección de datos, tan solo aborda unos pocos temas de la inteligencia artificial en su artículo 22, sobre todo el perfilamiento algorítmico y la toma de decisiones con base en ellos.

Desde la Sociología y Psicología se explora el impacto del perfilamiento algorítmico en la sociedad y la psique individual. Se cuestiona cómo la segmentación y personalización basadas en el perfilamiento pueden influir en la identidad personal, las relaciones sociales y la cohesión social, y cómo la vigilancia algorítmica puede afectar la percepción de la privacidad y la autonomía personal. Altman[74] define la privacidad como el control selectivo del acceso a uno mismo o a su grupo (a saber, espacios de trabajo o multitudes). En el contexto del perfilamiento algorítmico, esto resalta la preocupación sobre quién tiene acceso a los datos personales y cómo se utilizan estos datos para formar perfiles de usuarios. La capacidad de controlar este acceso es fundamental para mantener la autonomía personal y la privacidad en la era digital.

Antropología de la Privacidad (Sjaak van der Geest) [75]: Los antropólogos estudian a las personas, sus prácticas, tradiciones, palabras en su contexto. En su campo, la privacidad importa por su naturaleza cultural que surge en el contexto real de la vida de las personas.

---

[73] Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo (GDRP). EUR-Lex https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa. Artículo 22 del "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar".

[74] Altman, Irwin. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding.* Monterey, CA: Brooks/Cole Publishing Company, 1975.

[75] Van der Sloot, Bart. *Op. Cit.* p. 416

Desde una perspectiva antropológica, la privacidad se considera como una condición en la que las personas se sienten cómodas, seguras y protegidas. El perfilamiento algorítmico puede amenazar esta sensación de seguridad al exponer o malinterpretar contextos culturales y prácticas personales, lo que puede llevar a decisiones y acciones basadas en datos que no respetan la diversidad cultural o el contexto de las personas.

Desde la tecnología, el desafío radica en desarrollar algoritmos y sistemas de datos que sean seguros, transparentes y que respeten la privacidad de los usuarios. Esto incluye la implementación de prácticas de privacidad desde el diseño y por defecto, así como el desarrollo de tecnologías que permitan a los usuarios tener un mayor control sobre sus datos. La filosofía y la ética interrogan los fundamentos morales del perfilamiento algorítmico, especialmente en términos de consentimiento, autonomía, justicia y equidad. Se reflexiona sobre si es ético usar algoritmos para tomar decisiones que afectan significativamente la vida de las personas, a menudo sin su conocimiento o consentimiento explícito. En el ámbito económico y empresarial, el perfilamiento algorítmico se valora por su capacidad para dirigir la publicidad y personalizar servicios, mejorando la eficiencia del mercado. Sin embargo, también plantea preguntas sobre la equidad del mercado, la discriminación y la manipulación del consumidor basada en datos personales.

Privacidad en la Política: Desde la perspectiva de las ciencias políticas, el perfilamiento algorítmico suscita preocupaciones sobre la vigilancia gubernamental y corporativa, la democracia y la libertad de expresión. La información privada es vista como un instrumento de poder y control sobre las masas. Los datos personales pueden ser utilizados para influir o manipular comportamientos y decisiones políticas, al plantear

preguntas sobre la manipulación electoral y la autonomía política. En este contexto, resalta el caso de Cambridge Analytica, donde Christopher Wylie[76], empleado de la compañía, filtró documentos que detallaban el proceso de perfilado utilizado para identificar tendencias de voto y dirigir anuncios específicos con el fin de influir en las decisiones de las personas.

Los estudios de comunicación examinan cómo el perfilamiento algorítmico afecta la autenticidad de las interacciones en línea, la privacidad en las redes sociales y la dinámica del espacio público y privado en el entorno digital.

Medicina y Privacidad de la Información:

En salud y bioética, el perfilamiento algorítmico plantea preguntas sobre la privacidad de los datos médicos y genéticos, el consentimiento para su uso en investigación y práctica médica, así como las implicaciones éticas de la predicción de enfermedades y condiciones sobre todo en el ámbito de los seguros médicos. Los sistemas que emplean perfilamiento algorítmico para mejorar la atención médica deben garantizar que esta información se maneje con los más altos estándares de seguridad y privacidad.

Esto subraya la necesidad de que los ingenieros y desarrolladores de sistemas pongan un énfasis particular en la protección de la información contra ataques cibernéticos.

Desafíos Normativos y Descriptivos: El análisis conceptual tanto descriptivo como normativo de la privacidad subraya la necesidad de entender cómo se aplica y se debe regular la privacidad en la era del perfilamiento algorítmico. Las leyes y regulaciones existentes pueden necesitar adaptarse para abordar mejor los nuevos desafíos que presentan las tecnologías emergentes, evaluando los límites y el alcance real de nuestra

[76] Friedman, Vanessa & Engel Bromwich, Jonah. *Cambridge Analytica Used Fashion Tastes to Identify Right-Wing Voters*, *New York Times*, 29 de Noviembre, 2018.

privacidad cuando navegamos en internet e interactuamos con sistemas basados en algoritmos. La relación entre el perfilamiento algorítmico y la privacidad es compleja y multidimensional. Requiere un enfoque holístico que considere aspectos psicológicos, culturales, políticos, médicos y éticos para garantizar que se protejan los derechos individuales y se mantenga la dignidad en un mundo cada vez más digitalizado y controlado por datos.

1.0.8. El perfilamiento algorítmico en la información pública

El acceso a la información pública es un derecho protegido por el derecho objetivo, sin embargo, nos preguntamos cuáles son los límites para proteger las bases de datos que se tienen de particulares.

El perfilamiento algorítmico es una práctica que utiliza datos personales para crear perfiles detallados de individuos a través de algoritmos. En 1997 surgió Choice Point[77] una empresa creada para proveer el servicio de verificación de datos. En un principio, su servicio se limitó a atender aseguradoras interesadas en las comprobaciones de datos proporcionados por sus asegurados, pero su ámbito se ha ampliado a niveles de seguridad estatal. Paradójicamente, señalaba en su página que proteger la privacidad es su prioridad. Incluso presumía ser miembro de Truste[78] una organización que protege la privacidad mientras los usuarios navegamos en sitios web. Esta empresa compró la base de datos del IFE (Instituto Federal Electoral) y licencias de conducir de mexicanos en abril del 2003[79]. James Lee, jefe de mercadotecnia de Choice Point, defendió a su

[77] Adquirida por LexisNexis en 2008, https://hpccsystems.com/case-studies/choicepoint-migration
[78] "*Truste Privacy Certification Standards*" TrustArc *The Leader in Privacy Management Software*. Consultado el 23 de febrero de 2023. https://trustarc.com/consumer-info/privacy-certification-standards.
[79] Ver López, Mayolo. *Adquiere EU listas del IFE,* Portada Periódico Reforma. Domingo 13 de abril de 2003.

empresa bajo el argumento de que "...*nuestro único propósito en la vida es vender información para hacer que el mundo sea más seguro*..."[80]. Esta empresa fue comprada por LexisNexis en 2008. Sin embargo, esta actividad planteó serias preocupaciones sobre la privacidad y la protección de datos, especialmente cuando se accedió a bases de datos de ciudadanos mexicanos sin un consentimiento informado ni un objetivo claro.

Es decir, los datos del IFE debieron estar siempre protegidos y nunca ser enajenados. Fue una violación fragante al derecho a la privacidad de los ciudadanos mexicanos. Respecto a la legislación que protege los datos personales de los electores el INE publica ahora un aviso de privacidad del Registro Federal de Electores[81]. En él destaca la protección que da el derecho objetivo a los datos personales en el Registro Federal Electoral. Asimismo, enumera los datos personales que obran en el sistema, destaca que los datos de contacto como número telefónico o correo electrónico no son parte del Padrón Electoral y señala como datos sensibles la fotografía, la firma y la huella dactilar[82].

Al respecto la Organización para la Cooperación y Desarrollo Económico (OCDE) que agrupa 37 países y marca directrices a seguir para enfrentar los retos económicos que conlleva la globalización, define ciertos principios básicos para proteger la privacidad[83]. Estos principios han sido llevados a la legislación en materia de datos tanto en México como en Europa. La protección a la privacidad enfrenta nuevos retos con el comercio electrónico potenciado por la pandemia COVID19. Con base en sus principios la OCDE

[80] López, Mayolo, *Supra.*
[81] "Manifestación De Protección De Datos Personales Del Registro Federal De Electores," Instituto Nacional Electoral, March 31, 2021, https://www.ine.mx/credencial/manifestacion-proteccion-datos-personales-del-registro-federal-electores/.
[82] Acuerdo del Consejo General del Instituto Nacional Electoral por el que se aprueban las adecuaciones para ampliar y fortalecer el servicio de verificación de datos de la credencial para votar. "Instituto Nacional Electoral," repositoriodocumental.ine.mx (INE, 2020), https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113983/CGex202005-15-ap-2-Gaceta.pdf.
[83] "*Why Privacy Matters*," OECD, 2022, https://www.oecd.org/digital/privacy/.

se compromete a proteger la privacidad sin inhibir con los negocios, corporaciones, industrias, asociaciones civiles. Esto sólo se logra a partir de principios y políticas claras. El primer principio es el que limita la recolección de datos a sólo aquellos que sean obtenidos a través de medios legales y siempre con el conocimiento de la persona cuyos datos son recogidos. Es común que la tecnología digital permite recolectar más datos de los que estamos dispuestos a dar, aquella puede invadir nuestra privacidad sin nosotros darnos cuenta. Es curioso que ahora podemos leer las políticas de privacidad de las empresas, pero muchas veces las aceptamos sin leerlas. Por ello, la OCDE insiste en este principio con el objeto de protegernos, aún cuando aceptaramos -sin leer- dar datos que no son necesarios para las operaciones electrónicas.

El segundo principio se refiere a la calidad de los datos. Sólo los datos esenciales para el objetivo de la operación que se lleva a cabo serán recolectados. Este principio exige que los datos sean exactos, completos y actuales.

El tercer principio apela a la especificación del propósito. La institución o corporación que recoge nuestros datos nos debe informar cuál es el fin por el que los recoge. El momento para hacerlo es precisamente cuando los recolectan. Si hubiera un cambio de objetivo se le impone la obligación de informarlo.

El cuarto principio limita el uso de nuestros datos. Prohíbe divulgar nuestros datos salvo nuestro consentimiento u orden legal. Incluso el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) mexicana exige en su párrafo segundo la cancelación de los datos cuando hayan dejado de ser necesarios para el cumplimiento del objetivo por el que fueron recolectados.

El quinto principio denominado salvaguardia de la seguridad obliga a contar con medidas de seguridad que dificulten el acceso indebido a datos. Algunos de ellos es el cifrado de los mismos, la seudonimización que consiste en cambiar los datos del particular por un seudónimo. Este proceso exige información adicional para relaciones los datos recogidos con el particular que los provee. Es importante distinguir la pseudonimización de la anonimización, pues la primera es reversible, la segunda no. Este principio es fundamental para proteger los datos, pues se ha puesto de moda el secuestro de la información de las instituciones a través del *hacking*, la ciberseguridad es un tema esencial para las empresas u organizaciones que manejan datos personales de particulares. Es principio también impone la obligación a las instituciones de disponer de medios para recuperar la información perdida en caso de ataque o incidente técnico o físico a sus servidores. Este principio se registra en el artículo 19 de nuestra LFPDPPP que detalla en su primer párrafo los tipos de medidas de seguridad, a saber: administrativas -como niveles de autorización y acceso a la información a partir de los puestos y funciones; físicas, como bóvedas de seguridad para proteger los servidores o puertas electrónicas; o técnicas, como puede ser el cifrado de los datos. El artículo 20 de nuestra LFPDPPP exige informar al particular -persona física o moral- cuando sus datos han sido vulnerados en posible detrimento de sus derechos patrimoniales o morales.

El sexto principio se refiere a la transparencia que exige a las organizaciones una política sobre la transparencia de los datos, sobre todo para acceder rápidamente a los servidores o lugares de almacenamiento de datos para determinar su existencia y alcance de los datos personales. Este principio incluye determinar el próposito del uso así como la identidad y lugar físico de residencia de quien los controla.

El séptimo principio es el de participación individual, se refiere a que la persona física o moral siempre tendrá el derecho a que la institución o persona que maneje sus datos le confirme que tiene datos sobre él o ella. Esto debe hacerse en un plazo, precio, forma razonable e inteligible. En caso de negarse el acceso a nuestros datos, nos deben dar una explicación razonada del porqué y la posibilidad de rectificarlos o elminarlos.

El octavo principio se denomina de Responsabilidad que exige a todas las instituciones o personas en posesión de datos personales de particulares señalar expresamente el controlador de los datos quien será el responsable de aplicar todos los principios explicados anteriormente.

Los principios de la OCDE que se mencionan –como la recolección limitada de datos, la transparencia, la especificación del propósito, y la responsabilidad– se aplican en gran medida para controlar el perfilamiento algorítmico, buscando evitar que se recopilen datos innecesarios o se empleen sin el conocimiento y el consentimiento de las personas. Sin embargo, el perfilamiento algorítmico tiende a sobrepasar estos principios debido a la capacidad de los algoritmos para inferir información adicional a partir de los datos recolectados, creando riesgos adicionales de invasión de la privacidad y explotación de información personal.

II. Naturaleza Jurídica de la Privacidad

2.0. Concepto General

La naturaleza jurídica de la privacidad se refiere a la esencia y categoría normativa que define este derecho dentro del marco legal. Estudia dónde se clasifica y caracteriza jurídicamente como derecho a proteger para establecer los criterios normativos y las

disposiciones legales aplicables. La naturaleza jurídica de la privacidad resulta fundamental en la interpretación y aplicación de las normas, ya que determina cómo debe ser protegida, los límites de su tutela y las obligaciones del Estado y los particulares en su salvaguarda. El perfilamiento algorítmico que implica el uso de grandes cantidades de datos para realizar perfiles de las personas que hacen uso del mismo por necesidad o placer debe incluirse en la esencia de la privacidad. Pasquale[84] reconoce que las prácticas de las empresas líderes en internet y finanzas usan sus tecnologías patentadas para construir y mantener su imagen, facilitar la búsqueda de información relevante para los usuarios y pero siempre con un enfoque de ganar más dinero. Nos preguntamos cuál es esa tecnología patentada y siempre llegamos a algoritmos avanzados para clasificar, filtrar información y usar sistemas que manejan datos financieros complejos, lo que siempre implica una ventaja a la hora de tomar decisiones en medio de un flujo constante de información que puede ser difícil de interpretar.

2.1. Análisis morfológico y semántico.

La naturaleza jurídica de la privacidad, el perfilamiento algorítmico y la distinción entre análisis morfológico y semántico de la privacidad están intrincadamente relacionados; ya que dicho análisis morfológico se refiere a la forma y estructura de la privacidad como estructura legal para proteger los derechos subjetivos de las personas; así como sus fuentes como las constituciones, los tratados, reglamentos, jurisprudencia. En dicha estructura cabrán las diversas dimensiones de la privacidad incluido el perfilamiento algorítmico y sus riesgos.

[84] Pasquale, Frank author. *The Black Box Society : the Secret Algorithms That Control Money and Information.* Cambridge, Massachusetts*;* Londres, Inglaterra *:Harvard University Press, 2015, p. 14*

El análisis semántico se enfoca en el **significado** y la **interpretación** de la privacidad en diferentes contextos, la forma en que se **aplica** el derecho a la privacidad en diversas situaciones, particularmente en el perfilamiento algorítmico. El análisis semántico implica el estudio profundo de los **valores** y **principios** que subyacen a la privacidad, como la dignidad, la autonomía y la autodeterminación.

La aceptación del término privacidad es ampliamente discutida. Morfológicamente, privacidad tiene su origen en el inglés *privacy*. Este término toma fuerza a partir de uno de los ensayos jurídicos más importantes en la historia del Derecho escrito por Samuel Warren y Louis Brandeis en 1890[85] que define a la privacidad como el derecho a estar solo ("*the right to be let alone*"[86]). Este ensayo marca un parteaguas en la protección de la libertad individual en la era moderna y surge como una reacción a la actividad invasiva del gobierno, la prensa y algunas instituciones a invadir ámbitos previamente inalcanzables. Es la primera vez que se da reconocimiento legal a la privacidad como entidad propia, derecho que había sido reconocido implicitamente por el *Common Law,* como ellos mismos señalan[87].

El argumento es que el derecho debe modernizarse para proteger a la persona ante cualquier dispositivo nuevo, en el caso, la cámara fotográfica, una grabadora; ahora el internet. Destacan que el derecho siempre ha reconocido la importancia de las necesidades intelectuales y espirituales del hombre que, al ser atacadas, pueden doler más que heridas al cuerpo al disminuir el prestigio de la persona en la sociedad por la tendencia natural del hombre a transmitir información amarillista[88].

[85] *Op. Cit*.
[86] *Op. Cit.*
[87] *Op. Cit.*
[88] *Op. Cit.*

Si bien el artículo se publicó en 1890, no fue sino hasta 1902 que fue llevado a prueba en la Corte de Apelaciones de Nueva York cuando una persona se quejó de que su fotografía había sido puesta en unas bolsas de harina que el demandado vendía (caso Abigail M. Roberson v. Rochester Folding Box Co.[89]). Tres de los cuatro miembros de la Corte rechazaron la tesis de Warren and Brandeis bajo los siguientes argumentos: a) la falta de precedentes, tan importante para el derecho norteamericano b) la infinidad de casos que podría desatar aceptar tal derecho c) lo difícil que es poner una línea divisoria de lo que transgrede y lo que no al derecho[90]. Sin embargo, el Juez Gray disintió al declarar que el quejoso tiene un derecho a ser protegido contra el uso de su imagen ante la ventaja comercial del demandado y que "cualquier otro principio de decisión… es tan repugnante a la equidad como impactante a la razón"[91]. Si bien fue criticada tanto la quejosa Abigail M. Robertson como el Juez Gray, un año después, Nueva York fue el primer estado americano en publicar un Estatuto que enarbolara la protección al derecho a la privacidad en 1903 (ver Kessler), en él se menciona que el estatuto fue creado para proteger los sentimientos, pensamientos y otros sentimientos que el individuo pudiera sufrir por la apropiación comercial de su nombre o derechos de la personalidad[92]. La mayoría de los estados americanos siguió esa tendencia de proteger el derecho a la privacidad. Es paradójico que Inglaterra no haya seguido esa tendencia, no obstante haber dado los antecedentes en sus cortes para tan importante artículo.

[89] Kessler, Frederick R. *A Common Law for the Statutory Era: The Right of Publicity and New York's Right of Privacy Statute*, 15 Fordham Urb. L.J. 951 y siguientes (1987). Disponible en: https://ir.lawnet.fordham.edu/ulj/vol15/iss4/3/ consultado el 6 de febrero 2023
[90] *Supra* p. 959
[91] Wacks, Raymond. *Privacy, a very short introduction,* Ed. Oxford, 2010, p. 55
[92] *Op. Cit*. p. 959

Analicemos la traducción literal de *privacy,* sería privacía, quizá el sufijo –idad- fue tomado del francés *privacité.* Desde el punto de vista morfológico se forma con la raíz: priva; una consonante infijada: -c-; y el sufijo –idad-[93]. En la doctrina y legislación se usa intimidad como sinónimo de privacidad. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares vigente usa la palabra privacidad desde su artículo 1 cuando menciona el objeto de la ley "…garantizar la **privacidad** y el derecho a la autodeterminación informativa de las personas…[94]"

La palabra privacidad es un anglicismo de *privacy*[95] su uso se ha extendido en varios países hispanoamericanos. La misma Real Academia Española lo ha aceptado desde el 2001 como un neologismo tolerable, ante la crítica de los protectores del idioma[96] y lo define como 'ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión'[97]. De la misma manera que otras palabras anglosajonas pueden tener varios significados en castellano, la palabra privacy puede significar según el Libro de Estilo de El País: "intimidad, confidencialidad, soledad, aislamiento, vida privada[98]". Incluso señala un ámbito más al público y privado, precisamente el íntimo. La Real Academia

[93] Una primera anomalía, aunque encontrada en el castellano (abogado, abogacía; atender, atención) es que –c- la consonante intermedia no está en el adjetivo: privado. La mayoría de las palabras terminadas en -cidad, toman la -c- de la –z- de la palabra base como en capaz, capacidad; o de –co, con omisión de la o- como en caduco, caducidad. Aceptamos que existe un tercer grupo de palabras que aparentemente no siguen estas reglas como multiplicidad (de múltiple), pero el sufijo se justifica por ser tomado del latín multiplicitas. La explicación a esta excepción se encuentra en la evolución de las palabras por su uso y la inclusión de derivaciones de cultismos latinos o extranjerismos. El hecho de encontrar palabras que siguen reglas semejantes como *animacidad - animado-*, del inglés *animacity*, hace que la consideremos aceptable.
[94] Alberto Enrique Nava Garcés, "Art. 1," in *Ley Federal De Protección De Datos Personales En posesión De Los Particulares: Y Su Reglamento: Con Comentarios* (México, CDMX: Editorial Porrúa, 2012).
[95] Díaz Rojo, José Antonio. *Privacidad: ¿neologismo o barbarismo?* Revista de Estudios Literarios, Num. 21 p. 46
[96] Ver El País, *El País: Libro De Estilo* (España, Madrid: Aguilar, 2021), p. 809
[97] Real Academia Española, "Diccionario De La Lengua Española," Real Academia Española, 2001, https://www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-espanola.
[98] *Supra* p. 809/1118

Española define intimidad como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia[99]"

Semánticamente, en castellano el término correcto es intimidad o vida privada.

En general, nuestro término privacidad es encontrado en los diccionarios de castellano o español como un ámbito protegido contra cualquier invasión; cualidad referida a lo personal-familiar, no público; o propiedad referida a la vida privada de la persona[100].

El perfilamiento algorítmico nos demuestra que la privacidad es un concepto dinámico y que el Derecho debe evolucionar a partir del análisis tanto morfológico como semántico al responder a las preguntas: ¿Qué dimensiones de la privacidad se ven afectadas por el perfilamiento algorítmico? ¿Cómo se pueden reconfigurar las leyes y regulaciones para abordar estos desafíos? ¿Cómo se interpreta el derecho a la privacidad en el contexto de los algoritmos? ¿Cómo se pueden equilibrar los valores de la privacidad con otros intereses, como la innovación y la seguridad?

La protección del derecho a la privacidad versus los algoritmos exige un marco legal adecuado (análisis morfológico) y un debate profundo que potencie la comprensión (análisis semántico) de cómo la tecnología afecta no sólo el derecho a la privacidad, sino la vida de las personas al predecir sus comportamientos.

2.2. Privacidad y confidencialidad

Es común la confusión entre estos dos términos, tan es así que en varias ocasiones se usan como sinónimos; sin embargo, sí existen diferencias sustanciales que llevan a

[99] Rae - Asale, "Intimidad: Diccionario De La Lengua Española," "Diccionario de la lengua española" - Edición del Tricentenario, 2022, https://dle.rae.es/intimidad.
[100] Ver Moliner, María, *Diccionario de uso del español*, Madrid, Gredos, 1999. Seco, M., O. Ándres, G. Ramos, *Diccionario del español actual*, Madrid, Aguilar, 2016.

diferentes consecuencias jurídicas. Confidencialidad nos refiere a la calidad de confidencial, adjetivo de confidencia (del latín *confidentia*), noticia reservada que se dice en un ambiente de confianza[101]. En nuestro ámbito jurídico, implica secrecía, es decir, tener restringida la diseminación de cierta información[102]. No sólo se refiere a datos personales, pueden ser datos de la empresa, secretos profesionales, fórmulas, patentes o marcas como en un acuerdo de confidencialidad[103]. Cuando esos datos se procesan con algoritmos al procesar información confidencial, como datos médicos o financieros invariablemente se logra un perfilamiento algorítmico para los fines de aquella persona física o moral que creó el algoritmo. Si estos datos no se protegen adecuadamente, se puede violar la confidencialidad y causar daño a los individuos. La seguridad mide el grado de confidencialidad, integridad, confianza y disponibilidad de la información. En el universo de internet, como usuarios de sitios web, otorgamos nuestros datos a una compañía a través del *website*, le tenemos la confianza para dárselos, esto se procesa a través de las *cookies* que registran información nuestra, este tema lo explicaremos a detalle en el apartado 4.3. Sin embargo, esa información es susceptible de ser vendida a un tercero interesado en nuestro perfil en un término que se ha denominado *market matching*, que afirma la eficacia de la venta cuando se ofrece al mejor perfil de comprador (persona, lugar y tiempo adecuado a la oferta).

Desde el 1 de julio de 1997, un año antes del nacimiento de Google, el presidente norteamericano Bill Clinton publicó *The Framework for Global Electronic Commerce*[104]

---

[101] Rae - Asale, "Confidencia: Diccionario De La Lengua Española," "Diccionario de la lengua española" - Edición del Tricentenario, 2022, https://dle.rae.es/confidencia.
[102] Garner, Brian A. *Black Law´s Dictionary*, 9th edition, p. 339
[103] *Supra* p. 349
[104] Bill Clinton, "*Framework for Global Electronic Commerce ," National Archives and Records Administration (National Archives and Records Administration)*, consultada el 18 de noviembre de 2024, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

para potenciar la confianza y el uso del comercio electrónico, así como para establecer una agenda de discusión internacional respecto al tema. En ese documento se establecieron 5 principios:

1. El sector privado debe liderar y autoregularse.
2. El gobierno debe dejar hacer y dejar pasar con base en el viejo adagio *pactas suum servanda*.
3. El gobierno sólo debe proveer la ley para protección de la propiedad intelectual y un ecosistema legal para las transacciones.
4. El gobierno debe reconocer la naturaleza global de internet y adecuar las leyes a tal contexto.
5. El comercio electrónico global debe facilitarse en cuanto a su consistencia a pesar de los posibles problemas que surjan por la jurisdicción.

También dio 9 recomendaciones desde impuestos en internet hasta la privacidad (recomendación 5) donde asegura que es esencial asegurar la privacidad personal en el ecosistema de la red… los recolectores de datos deben informar al consumidor qué información están recogiendo y cómo intentan usarla. Los consumidores deben tener la posibilidad de decisión respecto a cómo se usarán o reusarán sus datos. De igual manera, los papás podrán decidir si se recoge información o no respecto a sus hijos menores de edad. También recomienda que los consumidores siempre tengan la capacidad de corregir sus datos.

El 27 de enero de 1998, la *National Telecommunications and Information Association y el Department of Commerce* norteamericanos publicaron un esbozo de discusión denominado "*Elements of Effective Self-Regulation for Protection of Privacy*[105]." En este

[105] NTIA *and Department of Commerce*, *Elements of Effective Self-Regulation for Protection of Privacy - Discussion Draft | National Telecommunications and Information Administration, January* 27, 1998, https://www.ntia.doc.gov/report/1998/elements-effective-self-regulation-protection-privacy-discussion-draft.

document se incluyen los Principios de Prácticas de Información Justa -*Principles of Fair Information Practices*-:

A. Conciencia –incluye políticas de privacidad, notificación y educación al cliente-,

B. Elección al cliente respecto a qué hacer con su información.

C. Seguridad de los datos obtenidos.

D. Acceso del cliente a la información[106].

2.3. Privacidad e intimidad

En la nueva sociedad de la información uno de los bienes jurídicos más susceptibles de ser quebrantados es la intimidad, sin la plena conciencia del afectado.

Marc Carrillo define "La intimidad es el derecho de la persona a impedir cualquier intromisión sobre aquel ámbito de su vida privada, que considera vedado a los demás, salvo que medie su consentimiento[107]". Garzón Valdés considera que "lo íntimo es, por lo pronto, el ámbito de los pensamientos de cada cual, de la formación de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no sólo porque no se desea expresarlo sino porque es inexpresable[108]". Íntimo, del latín *íntimus* -situado en lo más interno-, variación de *intumus*, superlativo del adverbio intus que significa interior o dentro. *Íntimo* expresa lo más profundo e interior de una persona tanto física como espiritualmente, reservado únicamente a aquellos que la persona elige. Es aquella esfera donde somos lo que somos. San Agustín dice que la intimidad es allí donde nadie puede penetrar ni con el oido, ni

[106] *Supra*
[107] Carrillo, Marc. *La intimidad, las celebridades y el derecho a la información*. Diario La Ley, Nº 6979, Sección Doctrina, 1 Jul. 2008, Año XXIX, Editorial LA LEY p. 1. Disponible en: https://www.uv.es/limprot/boletin5/bicarrillo.pdf consultado el 6 de febrero de 2023.
[108] Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, México, ed. IFAI, 2005, Colección: Cuadernos de Transparencia, p. 17.

con la vista, ni con la mente[109]. La privacidad, señala Garzón, se refiere más a relaciones interpersonales en donde la selección de los participantes depende de la libre decisión de cada individuo. La palabra clave, entonces, es **control** que cada persona tenga sobre su intimidad y en la interacción con los demás. Alan F. Westin[110] al reconocer las diferencias culturales y políticas en las naciones democráticas occidentales menciona cuatro estados de privacidad: la **soledad**, donde el individuo se separa del grupo y se libera de la observación de otras personas. En este estado la persona puede dialogar con algún familiar o su conciencia; es en la soledad donde se puede vivir el más amplio sentido de la privacidad. La **intimidad** es otro estado de la privacidad -según Westin, aquí el individuo actúa como parte de una pequeña unidad que reclama y se le permite ejercer aislamiento que se puede dar en una relación cercana y relajada entre dos o más individuos como en el caso de un matrimonio, familia, amigos y hasta compañeros de trabajo. Burgoon[111] distingue privacidad informática (control de información de datos), privacidad interactiva (control sobre la interacción de datos) y privacidad psicológica (control sobre con quién compartimos los datos). También consideró la privacidad física como aquella libertad sobre la vigilancia y la intrusión de las nuevas tecnologías como las *spy-cams, cookies*, así como virus informáticos. Aunque debemos reconocer que, si bien las tecnologías de la información han facilitado la invasión a la privacidad a través de la intrusión, vigilancia, destrucción del anonimato y la invasión a la autonomía; también es cierto que han desarrollado protecciones a tales violaciones. En general, los diversos tipos

[109] Citado por Garzón Valdés, *Op. Cit*. p. 17-18
[110] Westin, Alan F. *Privacy and Freedom*, *Chapter Two -Privacy in the Modern Democratic State*, IG Publishing, NY USA 1967, p. 16, ebook
[111] Aludido por Thomas Lee, Laurie. *Defining Privacy: Freedom in a Democratic Constitutional State*. *Journal of Broadcasting & Electronic Media*, Dec2002, Vol. 46 Issue 4, p. 646, 5p AN: 8735532 ISSN: 0883-8151 *Database: Academic Search Elite*.

de privacidad están ampliamente relacionados entre sí, pero debemos reconocer que seguirá evolucionando la manera en que nuestra privacidad pueda ser invadida, así como la incapacidad del derecho para protegerla oportunamente.

El quebranto a la privacidad o la intimidad es irreversible, es decir, una vez que alguien ha violado nuestra privacidad o intimidad, sólo queda al derecho imponer sanciones civiles o penales.

Intimidad entonces alude a algo más profundo que privado, es decir, no sólo aquello oculto o secreto que envuelve la actuación de todo ser humano; sino a características internas, de la naturaleza del individuo y esenciales para él. Privado sonaría a algo que el individuo quiere proteger de lo público, íntimo implica la propia autonomía del ser humano que mantiene a salvaguarda su individualidad sagrada[112]. Intimidad implica una situación entre dos o más personas que permite la validación de todos los componentes de la valía personal; esta situación permite la colaboración donde una de las personas ajusta su conducta a partir de las necesidades de la otra, Sullivan diferencia entre cooperación que es una relación de tomar y dar a colaboración que es descubir el nosotros en la intimidad[113]. En España, se usa la expresión intimidad cuando se implica un contenido jurídico, como derecho a la intimidad y violación de la intimidad[114]. Nucci señala que "la intimidad se infiere a lo interno del individuo, es decir se da en función de las preferencias de un sujeto, mientras que la vida privada procede del tratamiento de la información.[115]" Carbonell distingue dos tipos de privacidad: la "privacidad territorial" y la "privacidad de la información". La privacidad territorial alude a las interferencias en

[112] Westin, Alan F. *Op. Cit*. Chapter Two -*The Functions of Individual Privacy*, p. 17, *ebook*
[113] Sullivan, Harry. *The interpersonal theory of Psychiatry*, Routledge, NY 1982, p. 246
[114] Constitución Española Artículo 18. Numeral 1.
[115] Nucci, Hilda. *Op. Cit*. p. 197

nuestras propiedades o pertenencias, mientras que la privacidad de la información se relaciona con el acceso indebido a los denominados datos personales[116].

En México se ha protegido la indemnidad de la privacidad de los menores en la Reforma de 2018 al adicionar un capítulo al Código Penal Federal para proteger Delitos contra la Indemnidad de Privacidad de la Información Sexual. Sanciona al que use tecnología digital para contactar menores de edad o incapaces y requerirles imágenes sexuales o imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual[117]. También identificamos el bien jurídico de la intimidad en el artículo 259 bis del CPF mexicano al sancionar el hostigamiento a persona de cualquier sexo por su posición jerárquica a partir de sus relaciones laborales, docentes, domésticas o cualquiera otra que implique subordinación[118].

En el inglés, los términos *intimity* e *intimacy* significa el estado de tener una relación cercana con alguien[119]. Curiosamente, tanto en inglés como en español *intimacy* resulta más amplio que *privacy*; La primera, se refiere a lo más profundo del sujeto. La segunda, a los diversos aspectos e implicaciones de nuestra vida que no son públicas. Estos términos fueron los elegidos para el significado propio de lo no público, pero desde aquel artículo de 27 páginas de Warren and Brandeis "*The right to privacy*"[120], se ha impuesto *privacy* que significa el estado de permitir a alguien estar solo y no ser observado o molestado por otro. Ha sido sinónimo de protección a nosotros los ciudadanos comunes y no comunes al restringir el acceso a otros de lo nuestro. Nucci destaca que con la

[116] Aludido por Nucci, Hilda. *Op. Cit*. p. 189
[117] Art. 199 septies, Código Penal Federal, 2023, https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf.
[118] Art. 159 bis, Código Penal Federal, 2023, https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf.
[119] Westin, Alan F. *Op. Cit*. *Chapter Two -Privacy and Individual Life in Western Democracies*, p. 16, *ebook*
[120] Warren & Brandeis, *The right to privacy*, *Harvard Law Review*, Vol. IV December 15, 1890 No. 5 https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, consultado el 6 de febrero de 2023.

publicación del artículo de Warren y Brandeis se garantiza la protección a la vida privada de las personas y la intimidad es designado como *privacy-personality*, que implica la protección de la persona, un concepto más amplio del *privacy-property* referida a una protección otorgada a la propiedad privada[121]. Warren y Brandeis argumentaron a favor de un derecho a la privacidad basado en el principio de "inviolabilidad de la persona[122]", extendiendo la protección legal más allá de los daños físicos para incluir los psíquicos y emocionales provocados por intrusiones en la vida privada de las personas. Este fundamento teórico se puede aplicar al perfilado algorítmico de varias maneras:

Autonomía personal: El artículo destaca la importancia de la autonomía personal y el derecho a ser dejado en paz. El perfilado algorítmico, que implica recopilar, analizar y utilizar datos personales para crear perfiles detallados de individuos, puede verse como una invasión de esta autonomía personal, especialmente cuando se hace sin consentimiento explícito.

Intrusión en la privacidad: Warren y Brandeis abogaron por proteger contra la intrusión no deseada en la vida privada de las personas. El perfilado algorítmico, especialmente cuando se utiliza para publicidad dirigida, vigilancia o toma de decisiones automatizada, puede constituir una forma moderna de intrusión que ellos buscarían limitar.

Control sobre la información personal: Aunque Warren y Brandeis no pudieron prever el desarrollo de la tecnología de la información, su énfasis en el derecho a controlar la divulgación de información personal se aplica directamente a las preocupaciones sobre el perfilado algorítmico. La capacidad de controlar quién tiene acceso a nuestros datos personales y cómo se utilizan es central en la discusión sobre privacidad en la era digital.

[121] Nucci, Hilda. *Op. Cit.* p. 190
[122] *Supra* Nucci, p. 190

Consentimiento y transparencia: Un aspecto importante del derecho a la privacidad es que las intrusiones pueden ser permitidas si la persona afectada da su consentimiento. Esto resalta la importancia del consentimiento informado en el proceso de recopilación de datos, algo que es central en las discusiones sobre el uso ético del perfilado algorítmico.

En resumen, aunque el artículo de Warren y Brandeis no aborda específicamente el perfilado algorítmico, los principios que establece sobre la privacidad y la protección contra intrusiones no deseadas son altamente relevantes. Sirven como base ética y legal para abogar por una mayor regulación y control sobre las prácticas de perfilado algorítmico, asegurando que se respeten los derechos de privacidad de las personas en la era digital.

La expresión *privacy* ha adquirido la dimensión de **derecho subjetivo como facultad de protegernos de la intromisión de otros en una dimensión física y espiritual.**

En francés "*intimité*" se define como un carácter íntimo, interior y profundo; o bien, como un lazo estrecho y profundo; la vida íntima, privada[123].

El tercer estado de la privacidad para Westin[124] es el **anonimato** que ocurre cuando el individuo está en lugares públicos o realizando actos públicos pero busca estar libre de ser identificado o vigilado como podría ser en un estadio de futbol o en un medio de transporte público, incluso en las calles. El fundamento para proteger el anonimato es el miedo o ansiedad por sentirse vigilado en todo momento al estar en arenas públicas. En el anonimato Westin habla de la "privacidad pública[125]" que se da al publicar ideas anónimamente para evitar ser identificado sobretodo por la autoridad que le puede

[123] De Paul, Robert,. *Dictionnaire alphabétique de la Langue Francaise*, Paris, Societé du Noveau Littré, 1963, pags. 63-64
[124] Westin, Alan. *Privacy and Freedom*. IG *Publishing, New York*, 1967, *Chapter Two -Privacy and the Modern Democratic State, p.* 16 *ebook*
[125] Westin, *Supra* p. 16, *ebook*

perseguir por sus ideas. El anonimato es una forma de privacidad, sobretodo cuando se quiere emitir una opinión sin temor a represalias. En un mundo de tanta inseguridad, incluso las policías han puesto números de denuncias anónimas con garantía de no investigar más. Actualmente se considera el anonimato como una característica que promueve el progreso social y la creatividad[126]. Se requiere un equilibrio, pues el anonimato llevado al extremo y sin límites promueve la falta de responsabilidad por llamadas falsas o difamaciones que pueden transgredir el orden jurídico. Incluso algunas mujeres se han quejado que al dejar el hogar como el santuario de la privacidad se permite la violencia doméstica que no traspasa las fronteras legales. Incluso se han dado casos de hijos o mujeres enclaustrados en sus casas por diversas razones, nunca justificadas.

La cuarta forma de privacidad es la denominada **reserva[127]** que es la creación de una barrera psicológica ante una intrusión no deseada cuando una persona necesita limitar la comunicación acerca de él mismo por aquellos que le rodean, como en una boda que los invitados podrían obtener fotografías con su celular y publicarlas sin consentimiento de los novios que los invitaron. Es lo que Simmel llama la reserva recíproca e indiferencia, la relación que crea la "distancia mental"[128] como parte de la etiqueta social. En el caso mexicano destaca la Ley de Responsabilidad Civil para la Protección de la Vida Privada, Honor y Propia Imagen para la Ciudad de México publicada el 19 de mayo de 2006, cuyo objeto es "regular el daño al patrimonio moral derivado del abuso del derecho a la

[126] Brewster, Christopher, *etal*. *Legibility, Privacy and Creativity: Linked Data in a Surveillance Society*, *Aston Business School*, Birmingham, UK 2018. http://ceur-ws.org/Vol-1121/privon2013_paper6.pdf consultado el 6 de febrero de 2023.
[127] Westin, *Op. Cit*. *Privacy and Freedom*. IG *Publishing, New York*, 1967, *Chapter Two -Privacy and the Modern Democratic State, p.* 16 *ebook* p. 32
[128] Aludido por Westin, *Supra,* p. 32

información y de la libertad de expresión (art. 1, párrafo segundo)". Expresamente el artículo 15 de esta ley se refiere a la reserva al señalar que "..en ningún caso se considerará como ofensas al honor, los juicios desfavorables de la crítica literaria, artística, histórica, científica o profesional; el concepto desfavorable expresado en cumplimiento de un deber o ejerciendo un derecho siempre que el modo de proceder o la falta de **reserva**, cuando debió haberla, no demuestre un propósito ofensivo[129]".

Gutwirth define la privacidad como "el control de los individuos sobre lo que sucede con su información personal"[130], Dienheim sostiene que el derecho a la intimidad es la primer generación de los derechos humanos[131]. *Warren and Laslett* lo definen como un derecho acordado para mantener los límites personales[132]. La problemática sobre la naturaleza de la privacidad se complica porque las definiciones han girado sobre si es un derecho, una actitud o una meta. La doctrina germana con Hubmann[133] ha identificado 3 aspectos en cuanto los contenidos de la privacidad:

A) La esfera de lo secreto, aquello que debe permanecer ignorado.

B) Lo íntimo que forma parte de la vida privada y familiar.

C) Aquello que atañe a lo individual de la persona (honor, nombre, imagen).

---

[129] Gobierno de la Ciudad de México, "Art. 15 Ley De Responsabilidad Civil Para La Protección Del Derecho a La Vida ," Consejería Jurídica y de Servicios Legales, 2014, https://paot.org.mx/centro/leyes/df/pdf/2015/LEY_RESPONSABILIDAD_CIVIL_VIDA_HONOR__IMAGEN_28_11_2014.pdf, art. 15. Consultado el 14 de noviembre de 2025.

[130] Gutwirth, Serge. *Privacy and the information age*. Trad. R. Casert. Rowman and Littlefield Publishers, 144 pp. 2002.

[131] *Cfr*. Dienheim Barriguete. Aludido por Nucci, Hilda. *Op. Cit*. p. 189

[132] Warren, C. & Laslett, *Privacy and Secrecy: A conceptual comparison*. *Journal of Social Issues* 33 (3). pp. 43-51. 1977.

[133] Citado por Strömholm, S. (1967, mayo). *Right of privacy and rights of the personality: A comparative survey (Working Pape*r preparado para la *Nordic Conférence on Privacy organizado por la International Commission of Jurists*), p. 55. https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf

Eguiguren[134] añade al secreto de la vida privada, la dimensión de la libertad para tomar decisiones que tienen que ver con su vida privada.

Recientemente en la acción de inconstitucionalidad promovida por la presidenta de la Comisión Nacional de Derechos Humanos, María del Rosario Piedra Ibarra, el ministro Pardo Rebolledo declara la inconstitucionalidad de los artículos de las leyes de ingresos de 52 municipios de Zacatecas que intentaban cobrar por la realización de fiestas que no usaran la vía pública o bienes del dominio común, a saber: "…el hecho de que dichos preceptos no señalen de manera expresa la utilización de vías públicas u otros bienes de uso común que se aprovechen especialmente confirma la inconstitucionalidad de exigir un permiso, toda vez que ello hace suponer que los cobros y las anuencias municipales se realizarán por el simple hecho de llevar a cabo festejos o celebraciones particulares, cuestiones que pertenecen exclusivamente a la esfera privada de las personas[135]".

En la jurisprudencia argentina, la sentencia de la Corte Suprema de la Nación en el caso Ponzetti de Balbin c/Edit. Atlántida enunció el contenido del derecho a la intimidad o privacidad "comprende sentimientos, hábitos y costumbres, relaciones familiares, situación económica, creencias religiosas, salud mental y física y en suma las acciones, hechos o datos que … están reservadas al propio individuo…[136]".

Algunos ven a la privacidad como "necesidad innata y esencial del ser humano"[137], fuente esencial de otras libertades como la libertad de expresión, asociación,

---

[134] Eguiguren Praeli, La libertad de expresión, p. 105. Aludido por Nucci, Hilda. *Op. Cit*. p. 189

[135] Tribunal Pleno de la Suprema Corte de Justicia de la Nación, "Sentencia Dictada Por El Tribunal Pleno De La Suprema Corte De Justicia De La Nación En La Acción De Inconstitucionalidad 31/2021.," DOF, November 26, 2021, https://www.dof.gob.mx/nota_detalle.php?codigo=5636517&fecha=26%2F11%2F2021#gsc.tab=0.

[136] *Supra* p. 19

[137] Radwanski, George. *The Impact of the Different Regulatory Models in the World Scenario* Privacy Commissioner of Canada, Conference December 5, 2002 Rome, Italy. https://www.priv.gc.ca/en/opc-news/speeches/02_05_a_021205/ consultado el 6 de febrero 2023

pensamiento, trabajo; incluso necesaria para la dignidad o el honor del ser humano. Adelina Loianno sostiene dos facetas que definen la dignidad humana, una faz negativa conformada por todo aquello que es íntimo o secreto, es decir, la intimidad que guarda o reserva aquello; y la faz activa que se integra con las características del individuo que lo definen como tal y lo diferencian de otros tales como eel nombre, el honor, la imagen, etcétera[138]. El ministro canadiense Gérard La Forest afirma que la privacidad está en el corazón de la libertad en el estado moderno,[139] se cuestiona cómo ser libres si cada movimiento es monitoreado, vigilado y almacenado. En esta época tecnológica tenemos esa extraña sensación de que tanto el Estado como empresas e incluso otros individuos siempre están interesados en nuestra actividad laboral, profesional; pero también personal e íntima por la trascendencia que puede tener para el comercio, el gobierno y la seguridad. Sin embargo, sabemos que no es un derecho absoluto, sobretodo por los nuevos acontecimientos mundiales terroristas. La privacidad es un derecho subjetivo privado, luego individual, pero su protección es de interés público porque tienen un impacto directo en el bienestar de la sociedad; por ello la relevancia de su regulación.

En este contexto la privacidad se refiere al equilibrio entre dos valores: el derecho del individuo a mantener su intimidad intacta y el beneficio social derivado de compartir dicha información por cualquier motivo (seguridad, vigilancia, control fiscal, etcétera). Hacia donde se incline dicha balanza marcará los derechos que la legislación otorgue al individuo sobre su información.

[138] *Op. Cit*. p. 20
[139] *Ibidem*

En Canadá, por ejemplo, se ha legislado hacia el Estado con el *Privacy Act* de 1983 y hacia los particulares en la *Personal Information Protection and Electronic Documents Act*, de enero de 2001 y revisado en Mayo de 2019.

A continuación algunos argumentos respecto a la afirmación de que la privacidad expresa valores legítimamente buscados por todo individuo:

1. Todo individuo tiene derecho a pensar lo que le parezca sin que nadie se entere. Aquí nos preguntamos si, aun cuando suene a ciencia ficción, la tecnología diera la posibilidad de leer el pensamiento ¿que haría el derecho?, ¿cómo se legislaría?
2. El ser humano necesita privacidad en su relación con otros, de amistad, noviazgo. Perez Luño la presenta como "una condición de la existencia colectiva[140]" es decir, un derecho de la coexistencia.
3. La privacidad es necesaria para la competencia social, en la medida que yo no dé a conocer mi estrategia habrá lugar a la creatividad y competencia.
4. El sector de la salud enfrenta un proceso acelerado de digitalización, impulsado por la incorporación de registros médicos electrónicos, herramientas de monitoreo remoto y aplicaciones móviles de salud. Este desarrollo plantea desafíos éticos y de seguridad, especialmente en relación con el perfilamiento algorítmico. Entre las propuestas para manejar estos datos sensibles destaca el uso de tecnologías como blockchain. La digitalización ha permitido la generación y el intercambio masivo de datos médicos sensibles entre actores públicos y privados, lo que abre la posibilidad de identificar patrones, predecir comportamientos y personalizar tratamientos. No obstante, estas capacidades, aunque prometedoras, también conllevan riesgos significativos relacionados con la privacidad y la potencial

[140] Citado por Loianno, Adelina. *Op. Cit.* p. 19.

discriminación algorítmica. Los algoritmos, al procesar esta información, pueden tomar decisiones automatizadas que impacten directamente en los pacientes, desde diagnósticos hasta la disponibilidad de servicios. Esto evidencia la necesidad de un marco jurídico sólido que concilie la innovación tecnológica con la protección de los derechos individuales. Adicionalmente, la exposición de datos personales sensibles, como condiciones médicas específicas (por ejemplo, el VIH), podría reforzar estigmas sociales y afectar negativamente el desarrollo social de los individuos afectados. Esto subraya la importancia de abordar tanto los aspectos técnicos como las implicaciones éticas y sociales de la digitalización en la salud.

5. El sector de la salud vive un proceso de digitalización acelerada, con la adopción de registros médicos electrónicos, herramientas de monitoreo remoto y aplicaciones móviles de salud. Este flujo de información plantea desafíos éticos y de seguridad, particularmente en relación con el perfilamiento algorítmico[141]. Incluso hoy hay propuesta del uso de blockchain para manejar estos datos sensibles[142]. La digitalización ha facilitado la generación y transferencia grandes cantidades de datos médicos sensibles entre diversos actores del sector salud, tanto públicos como privados; esto permite identificar patrones, predecir comportamientos y personalizar tratamientos. Sin embargo, aunque estas capacidades ofrecen oportunidades para mejorar la atención médica, también presentan riesgos significativos en términos de privacidad y discriminación

[141] Thantharate, *A. ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain*. Big Data Cogn. Comput. 2023, 7, 165. https://doi.org/10.3390/bdcc7040165
[142] *Supra* p. 3

algorítmica. La capacidad de los algoritmos para procesar datos sensibles puede derivar en decisiones automatizadas que impacten directamente en los pacientes, desde diagnósticos hasta acceso a servicios, lo que subraya la necesidad de de derecho objetivo que equilibre la innovación tecnológica con la protección de los derechos individuales. Otros prejuicios sociales pueden inhibir mi desarrollo social si la información personal es conocida, como la revelación de condiciones médicas como el VIH.

6. El argumento quizá más importante es la seguridad; en la medida en que me conozcan más, soy vulnerable. Al respecto, muchas legislaciones penales del mundo sancionan la conducta delictiva de apoderarse de datos personales de otros sin su consentimiento. En México, el artículo 109 de la Ley Federal de Derechos de Autor protege las bases de datos personales[143] y los delitos informáticos están regulados en el Código Penal Federal[144].

2.4. El concepto de privacidad en la legislación internacional.

La disparidad en la protección de la privacidad dentro de las diversas legislaciones del mundo puede entorpecer el libre flujo de información. En la Declaración de Derechos Humanos, artículo doce se usa la expresión "…vida privada…" para proteger tal derecho humano esencial[145]. La Convención Europea de Derechos Humanos de 1950 en su artículo 8 -basada en la Declaración Universal de Derechos Humanos, proclamada por la

[143] Congreso de la Unión, "Ley Federal Del Derecho Del Autor - Honorable Cámara De Diputados," Ley Federal del Derecho del Autor, Art. 109, July 1, 2020, https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf.
[144]Código Penal Federal, TITULO NOVENO, *Revelación de secretos y acceso ilícito a sistemas y equipos de informática*. Artículos 210, 211 y 211bis 1-72023. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf.
[145] Declaración Universal de Derechos Humanos. Artículo 12, United Nations, accessed March 20, 2023, https://www.un.org/es/about-us/universal-declaration-of-human-rights.

Asamblea General de las Naciones Unidas el 10 de diciembre de 1948-, protege "el derecho al respeto a la vida familiar y privada, así como protección de datos[146]. El nuevo capítulo de Derechos Humanos de la Unión Europea agrega "la protección a los datos personales" [147], señala en su artículo 8 que los datos personales sólo deben ser procesados para propósitos específicos y sobre la base del consentimiento u otra base legítima por el derecho. Toda persona tiene el derecho a acceder a los datos que han sido recogidos sobre él o ella, y el derecho a hacer que se rectifiquen. En 1966, como parte de la Organización de Estados Americanos -OEA- se redactó el Pacto Internacional de Derechos Civiles y Políticos en Nueva York, entró en vigor hasta el 23 de marzo de 1976. En su artículo 14-I se protege de la prensa y del público a los juicios por consideraciones de moral, orden público o seguridad nacional …. o cuando lo exija el interés de la vida privada de las partes… pero toda sentencia en materia penal o contenciosa será pública, excepto en los casos en que el interés de menores de edad exija lo contrario[148].

Es hasta mitad del siglo XX que nuestra habilidad para mantener fuera del alcance de otros nuestros datos cobra relevancia, sobre todo por la facilidad para almacenarlos. La vida que antes ocurría en lugares públicos como la plaza o la calle, se lleva a las oficinas o computadoras. Es a finales de los años 60´s que la convergencia entre dos corrientes: la revolución post industrial de la información y el incremento en el uso de datos personales

[146] Ver Convenio firmado en Roma, aunque el Tribunal de Justicia de la Unión Europea afirmó que la Comunidad Europea no podía adherirse al Tratado porque éste no incluía competencias para dictar normas internacionales en materia de derechos humanos. Este problema se solucionaría al dotar de personalidad jurídica a la Unión, figura contemplada en la nueva Constitución que está siendo ratificada. CNDH, "Entra En Vigor La Convención Europea De Los Derechos Humanos: Comisión Nacional De Los Derechos Humanos - México," Inicio, 2019, https://bit.ly/3dYLHIY.

[147] Diario Oficial de las Comunidades Europeas, "Carta De Los Derechos Fundamentales De La Unión Europea," Carta de los Derechos Fundamentales de la Unión Europea, December 18, 2000, https://www.europarl.europa.eu/charter/pdf/text_es.pdf. En sus artículos 7-8. Firmada y proclamada por los Presidentes del Parlamento Europeo, del Consejo y de la Comisión el 7 de diciembre de 2000 con ocasión del Consejo Europeo de Niza.

[148] OEA, "Relatoría Especial Para La Libertad De Expresión - OAS," Pacto Internacional de Derechos Civiles y Políticos, 1976, https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=189&lID=2.

por los gobiernos hacen necesario emitir leyes que protegieran a las personas y a sus datos personales[149].

En 1967 se constituyó una comisión consultiva para estudiar el impacto de las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, de dicha Convención surge la Resolución 506 de la Asamblea del Consejo de Europa ordenamiento que es considerado como cimiento del movimiento legislativo para la protección de datos personales. A partir de dicha resolución surge en el viejo mundo legislación que trata de inhibir el impacto de la tecnología en los derechos de privacidad de las personas. En 1972 se publica en el Reino Unido un reporte de 350 páginas respecto a la protección de las privacidad por Kenneth Younger[150]; 1976- La Constitución Portuguesa reconoce el derecho a la protección de datos en su artículo 35. En 1977 – Ley Alemana conocida como *Land of Hesse*; también en 1977, el Parlamento Europeo aprueba una resolución sobre la tutela de los derechos del individuo contra el creciente progreso tecnológico. En 1978 surge la Ley Francesa en Informática y Ficheros. Y en España la Constitución de 1978 en su artículo 18.4 que señala "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[151]. En Dinamarca, también en 1978 publica leyes para detener el ataque de la tecnología a la privacidad. Hacia los 80´s surge el Convenio del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal conocido como Convenio 108 que reconoce la protección de datos personales como un derecho humano a ser protegido en

[149] OECD, "*Thirty Years after the OECD Privacy Guidelines," The OECD Privacy Guidelines, 2011*, https://www.oecd.org/digital/ieconomy/49710223.pdf.
[150] *Supra* p. 15.
[151] *Council of Europe, "Council of Europe Data Protection Website - Data Protection* - Www.coe.int," 2021, https://www.coe.int/en/web/data-protection/home.

espacios tan diversos como las autoridades, el ámbito médico, compraventa de bienes o servicios, seguros médicos, bancos, justicia, empleo o, simplemente, al navegar por internet. Señala el derecho a la protección de datos personales como supuesto para otros derechos como los de libertad de expresión y libertad de consciencia. Este convenio fue abierto para que Estados no miembros de la Comunidad Europea pudieran adherirse en pro de la protección de datos personales[152]. Este convenio señala los principios fundamentales para una gestión adecuada de dichos datos:

• Los datos deberán obtenerse y utilizarse con una finalidad determinada y no deberán volver a utilizarse con un objetivo no relacionado;
• Sólo deberán ser almacenados y tratados los datos estrictamente necesarios para esta finalidad;
• Los datos tratados deberán ser exactos y estar actualizados;
• Los datos deberán conservarse únicamente por el tiempo necesario para cumplir la finalidad para la cual se hayan registrado[153].

El 23 de septiembre de 1980, la Organización para la Cooperación y Desarrollo Económico (que actualmente aglutina 37 países) se convirtió en el primer organismo internacional en emitir Directrices que rigieran la protección de la intimidad y la circulación transfronteriza de datos personales. Hacia 2013 la OCDE se actualizó con conceptos como principio de rendición de cuentas –*accountability*- que implica que los responsables del tratamiento de datos adopten programas de cumplimiento efectivo de dicha normativa de protección de datos personales, con énfasis en la importancia de establecer puertos seguros en las organizaciones; así como la notificación de la

[152] *Supra*
[153] *Supra*

vulneración de seguridad[154] y el establecimiento de puertos seguros. La OCDE ha establecido la llamada Red Global de Autoridades de Protección de Datos ("*Global Privacy Enforcement Network*[155]").

Y en la década de los 90, fue la Unión Europea la que adoptó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, misma que fue derogada y sustituida por el Reglamento de Protección de Datos (RGPD) conocido como Reglamento UE 2016/679, en vigor desde mayo de 2018[156].

2.5.1. La privacidad en el Derecho Norteamericano

En este apartado estudiaremos la evolución del concepto de privacidad en el derecho norteamericano por la influencia que tiene el manejo de datos en este país donde se asientan las grandes empresas que almacenan datos personales de los usuarios, así como los algoritmos de inteligencia de datos que tantas ganancias dan al oligopolio de datos y a las llamadas *Big Tech*. El primer antecedente se da en 1776 en la Constitución de Pensilvania, la Declaración del Buen Pueblo de Virginia, la Declaración de Derechos y las Normas fundamentales de Delaware y, la Constitución de Massachusetts en 1780; todas ellas lo reconocen como parte del derecho a la inviolabilidad del domicilio[157].

---

[154] OECD, "*Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013)," 2013, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
[155] *Global Privacy Enforcement Network* , 2013, https://www.privacyenforcement.net/content/home-public.
[156] Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo (GDRP). EUR-Lex https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa
[157] Nucci, Hilda, *Op. Cit*. p. 194

La Constitución de Estados Unidos de America no menciona explícitamente del derecho a la privacidad[158]. Es hasta 1928 en el caso Olmstead versus United States que el ministro Louis Brandeis afirma que el derecho a la privacidad es el derecho más valorado por el hombre. En aquél momento no todos sus compañeros estuvieron de acuerdo en tal afirmación y no es sino hasta 1960 que la Suprema Corte de Justicia declara que la Constitución sí protege el derecho a la privacidad en el caso Griswold versus Connecticut cuando la Suprema Corte invalidó una ley que prohibía los anticonceptivos bajo el argumento de que violaba el derecho a la privacidad, el Ministro de Justicia William O Douglas escribió que el derecho a la privacidad emanaba y era garantizado por la Primera, Tercera, Cuarta, Quinta y Novena Enmienda. En la Primera Enmienda se protege la libertad de religión y de expresión -incluye expresión de palabra, escrita, manifestación, prensa, reunión, asociación. La Tercer Enmienda protege la privacidad del hogar. La Cuarta Enmienda protege la privacidad tanto de las personas como sus posesiones, sin interferencia del gobierno; la Novena Enmienda protege los derechos no expresamente enumerados en la Constitución. La Décimo Cuarta Enmienda protege la privacidad en el debido proceso. La Novena Enmienda previene que la Constitución no niega otros derechos que no estén enumerados en ella y que se encuentran depositados en el pueblo.

De hecho, no obstante no aparecer en la Constitución de los Estados Unidos de America el derecho a la privacidad, hoy es considerado uno de los más importantes para la sociedad americana.

[158] Ver Anderson, David. *The failure of American Privacy Law*, en *Protecting Privacy: The Clifford Chance Lectures*, *Volume Four*, pp. 139 - 167. Ed. *Oxford University Press*. Nueva York, 1999.

En la legislación federal norteamericana ha habido varios intentos de redactar una protección a la privacidad integral, a saber:

1. *The Federal Trade Commission Act* (1914): protege la privacidad en las relaciones comerciales y otorga poderes a la *Federal Trade Commission* (FTC) para vigilar tales derechos.
2. *Freedom of Information Act (1960).* Hacia los años 60`s el gobierno americano comenzó a acumular datos de sus ciudadanos, quienes se preocuparon por ello y exigieron se les reconociera su derecho de acceso a sus propios datos. El año de 1966 se promulgó *Freedom of Information Act* que permitía a los ciudadanos requerir copia de los archivos que el gobierno tenía con sus datos.
3. *The Fair Credit Reporting Act* de 1970 asegura la privacidad, exactitud y claridad en la información crediticia de los consumidores en *bureaus* de crédito. Se regula la manera en que las agencias pueden acceder, recolectar, usar, compartir los datos que tienen sobre los consumidores.
4. *Privacy Act* de 1974 que registra una serie de principios de derecho denominado *Code of Fair Information* que regula la recolección, mantenimiento, uso, y diseminación de información personal recolectada por las agencias federales del gobierno.
5. *Family and Education Rights and Privacy Act* de 1974 limitó el acceso a evaluaciones y calificaciones almacenadas en las computadoras de las universidades tanto públicas como privadas. De hecho, recientemente el NYT

publicó que dos estudiantes obtuvieron toda la información de su proceso de admisión a Stanford con base en esta ley que les garantiza el acceso[159]

6. *Tax Reform Act* de 1976 preserva el derecho a la privacidad de la información financiera del ciudadano americano.
7. *The Right to Financial Privacy Act* de 1978 que prohíbe a las instituciones financieras entregar al gobierno federal archivos de clientes a menos que éstos lo consientan.
8. *The Electronic Communications Privacy Act* de 1986 protege la intercepción de información privada en los medios de comunicación electrónica al momento que la comunicación se lleva a cabo.
9. *The Driver´s Privacy Protection Act* de 1994 evita que los estados revelen información de sus conductores sin su consentimiento.
10. *The Children's Online Privacy Protection Act* (*COPPA*) de 1998 regula la recolección de datos en internet de información relativa a niños y su protección jurídica.
11. *The Health Insurance Portability and Accountability Act (HIPAA*) de 1996 señala las normas para almacenar, procesar y recolectar información médica al exigir a los proveedores de servicios médicos informar a los pacientes acerca de sus derechos a la privacidad y acerca de la forma en que su información será tratada.
12. *The Financial Services Modernization Act* de 1999 prohíbe la publicación de información personal no pública acerca de un cliente a una tercera parte no

[159] Richard Pérez-peña, *Students Gain Access to Files on Admission to Stanford*, The New York Times, *January* 17, 2015, https://nyti.ms/3Jvu8iw

afiliada a menos que el propio cliente lo acepte en formatos específicos dispuestos para ello.

13. *E-Government Act* de 2002 se obliga al gobierno a informar al ciudadano la información que se guardará de él en su visita a los sitios web del gobierno y los formatos electrónicos a ser llenados, así como en qué será usada.

14. *The Federal Information Security Management Act* de 2002 crea un Consejo para asuntos de Privacidad y Seguridad de la Información[160].

2.5.2. Estándares de Protección de Datos en Iberoamérica. Contexto, principios y alcances.

México pertenece a la Red Iberoamericana de Protección de Datos que han logrado acordar y firmar los Estándares de Protección de Datos para los Estados Iberoaméricanos el 20 de junio de 2017[161]. El documento busca consolidar un conjunto de principios y derechos homologados que los Estados firmantes integren en su legislación nacional para asegurar el flujo de transfronterizo de datos de manera segura sin inhibir el desarrollo económico y social. Se basa en modelos avanzados como los de la OCDE (2013), Convenio 108 del Consejo de Europa (1981), Marco de Privacidad de APEC (2017), el Reglamento General de Protección de Datos de la Unión Europea (2016), así como en las reuniones previas de la propia Red Iberoamericana de Protección de Datos; México fue sede del IV Encuentro Iberoamericano de Protección de Datos en 2005. A partir de las elecciones de 2000, México tuvo una transición a la democracia que llevó a resaltar el

[160] Para mayor información en el Derecho Estadounidense americano consultar: Leroy Miller, Roger. Jentz, A. Gaylor. *Business Law Today*, 10th edition. Mason, Ohio, USA, 2012. pp. 49 y sigs.
[161] Red Iberoamericana de Protección de Datos. (2017, 20 de junio). Estándares de protección de datos personales para los estados iberoamericanos. https://www.redipd.org/documento/estandares-iberoamericanos-2017.pdf

respeto a la dignidad de la persona, así como a la promoción de la protección de los derechos humanos. Pero ya en dicho Encuentro Iberoamericano de Protección de Datos (2005) se afirmó que "No podemos hablar de privacidad sin establecer una normatividad práctica que se haga cargo de la protección de personas en relación al tratamiento de sus datos[162]" y se vislumbró la necesidad de una ley federal de Protección de Datos para "*establecer un equilibrio justo entre los intereses individuales, las necesidades del Estado y las demandas, cada vez más acuciantes, de un mercado que aparece en eterna expansión*[163]". Proteger al individuo en su dimensión de persona física consumidor, paciente médico reconociendo que ya había para esos años un manejo de muchos datos personales sin regulación alguna, facilitado por las tecnologías de información a partir de su capacidad de almacenamiento de información y el desplome de precios de los servidores y darnos la capacidad de llevar los expedientes físicos a archivos digitales sujetos a una minería de datos para satisfacer los intereses no siempre éticos de otras instituciones. La entonces Comisionada Presidenta del IFAI, María Marván destacó "El objeto de la ley es la regulación del derecho a la autodeterminación informativa de las personas. Su ámbito de aplicación de ésta reside en las bases de datos, estén o no automatizadas. Por lo tanto, el legislador debe estar consciente de las distintas lógicas que imperan en la creación y manejo de las mismas, tanto en el sector privado como en el público[164]". Una afirmación muy fuerte de la Consejera Presidenta fue "la privacidad va de la mano de la libertad. Ambas son condiciones para la democracia[165]".

---

[162] Intervención de Marván Laborde, María en Agencia Española de Protección de Datos, "IV Encuentro Iberoamericano De Protección De Datos Personales Ciudad De ...," IV Encuentro Iberoamericano de Protección de Datos Personales Ciudad de México, 2005 http://www2.icai.org.mx/icainew_f/images/Biblioteca/Memorias/Memoria_Datos_Personales.pdf p. 14
[163] *Supra*, p. 14
[164] *Supra* p. 15
[165] *Supra* p. 16

Este documento de Estándares de Protección de Datos de Iberoamérica contiene los mismos principios rectores de tratamiento de datos que los modelos mencionados, los derechos ARCO, las garantías de protección a la transferencia de datos, así como la obligación para los Estados firmantes de contar con autoridades de control independientes para sanciones e imponer medidas correctivas. Su valor reside en la incorporación de buenas prácticas globales y en su llamado a la armonización jurídica en un mundo de expansión de la economía digital, de grandes contradicciones y paradojas persistentes acerca de la privacidad como menciona Nissenbaum quien afirma que "la privacidad se preserva cuando los flujos de información se ajustan a normas contextuales legítimas; se vulnera cuando no lo hacen[166]".

2.5.3. La evolución legislativa de la protección de datos en México

Reyes Krafft[167] explica que el primer instrumento legislativo sobre la protección de datos en México, con base en el Artículo 6 Constitucional, fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002, que contiene 33 veces la expresión datos personales. Esta ley fue abrogada por la nueva Ley Federal de Transparencia y Acceso a la Información Pública publicada el 9 de mayo de 2016 que, a su vez fue abrogada por la Ley General de Transparencia y Acceso a la Información Pública promulgada el 20 de marzo de 2025.

[166] Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, p. 104
[167]Tenorio, Guillermo. Los Datos Personales en México, Ed. Porrúa, México 2012, p. 27

Se creó también por decreto el Instituto Federal de Acceso a la Información Pública el 11 de junio de 2002[168] como un órgano de la Administración Pública Federal con autonomía operativa, presupuestaria y de operación. Es decir, organismo descentralizado no sectorizado, lo que evitaba cualquier vínculo jerárquico con alguna otra institución. Se señala también que sus resoluciones no estarían sujetas a autoridad alguna. En el artículo 2 del decreto se enfatizaba que el IFAI debería proteger los datos personales en poder de las dependencias y entidades. El IFAI fue disuelto por reforma constitucional del 20 de diciembre de 2024 y sus funciones se llevaron a la Secretaría de Anticorrupción y de Buen Gobierno.

Después de aprobada en el 2002 la LFTAIPG, se aprobaron 28 leyes estatales. Resultado de todos estos esfuerzos apartidistas para concientizar sobre la importancia de proteger los datos personales a nivel constitucional, el 20 de julio de 2007 el presidente Felipe Calderón -en pro de la transparencia y el acceso a la información- promulga la reforma constitucional del artículo 6 al adicionarle un párrafo con 7 fracciones.

Con este antecedente, el 1 de junio de 2009 se adicionó un párrafo relativo a la protección de datos personales al artículo 16 Constitucional dicho párrafo reza:

> 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.

Es bajo el gobierno del presidente Felipe Calderón, el 5 de julio de 2010 que se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[169], la cual

[168] Quijano, Camen. Derecho a la Privacidad en Internet, Ed. Tirant Lo Blanch, México, 2022 p. 108
[169] *Supra*, Quijano, *Op. Cit*. p. 97

es abrogada por la Nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares (NLFPDPPP) en vigencia desde el 21 de marzo de 2025.

2.5.4. Nueva Ley Federal de Protección de Datos Personales en Posesión de Particulares

El 20 de diciembre de 2024 se publicó el decreto de reforma a la Constitución para extinguir al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Es en marzo 20 del siguiente año cuando la presidenta de México publica el decreto para las 3 nuevas leyes:

Ley General de Transparencia y Acceso a la Información Pública

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Ley Federal de Protección de Datos Personales en Posesión de Particulares. Vigentes desde el 21 de marzo de 2025.

El objetivo de esta última ley es proteger los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (art. 1 NLFPDPPP). La ley define datos personales como cualquier información concerniente a una persona física identificada o identificable (art. 2 fr. V NLFPDPPP). Esta definición está en concordancia con Convenio 108[170] que en su inciso a) de su artículo 2 define el concepto de datos de carácter personal como: "cualquier información relativa a una persona física

[170] García Ricci. (n.d.). *La protección del derecho a la privacidad a través del modelo previsto en la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. *Derechos Humanos México. Revista del Centro Nacional de los Derechos Humanos, CNDH*. Retrieved from https://revistas-colaboracion.juridicas.unam.mx/index.php/derechos-humanos-cndh/article/view/5749 p. 145

identificada o identificable (persona concernida)"[171]. También con el Reglamento General de Protección de Datos (RGPD) 2016/679 en cuanto al concepto de datos personales de la siguiente manera: "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" [172]

La NLFPDPPP clasifica como datos sensibles a "aquellos datos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta". En particular, se consideran sensibles (artículo 2 fr. VI) aquellos que puedan "revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual". La ley otorga a los titulares de datos personales cuatro derechos esenciales, definidos como los derechos ARCO, a saber: acceso, rectificación, cancelación y oposición (Art. 21 NLFPDPPP). La autoridad que vigila el cumplimiento de esta ley es la Secretaría de Anticorrupción y Buen Gobierno, que desaparece al Instituto Federal de Acceso a la Información y Protección de Datos. Esta secretaría tendrá por objeto "difundir el conocimiento del derecho a la protección de datos

[171] Consejo de Europa. Convenio 108, de 28 de enero de 1981. Para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
[172] Unión Europea (2016). Reglamento (UE) 2016/679 del Parlamento Europeo (GDRP). EUR-Lex https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa

personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma"; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte delos sujetos regulados por este ordenamiento (art. 38 NLFPDPPP).

2.5.5. Principios de la Nueva Ley Federal de Protección de Datos Personales en Posesión de Particulares

Los principios de Licitud y Lealtad, de Consentimiento, de Información, de Proporcionalidad, de Finalidad, de Calidad y de Responsabilidad que rigen a la NLFPDPPP conllevan obligaciones para aquellas personas u organizaciones privadas que tratarán datos personales y se distingue haber tenido como modelo: los Lineamientos sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) emitidos por la OCDE en 1980 y revisados en 2013 por los nuevos retos que la tecnología ha presentado para la protección de los datos personales tales como la datos en la nube y la transferencia de datos a nivel internacional, lo que facilita el perfilamiento de datos[173]. También está conforme al Marco de Privacidad de la Asia Pacific Economic Cooperation[174] que no menciona explícitamente la frase perfilamiento algorítmico al ser creado en el 2015, antes que el término fuera usado de manera general. Sin embargo, sus principios de Limitación de la Recopilación, Uso de la Información Personal y Rendición de

[173] *Organisation for Economic Co-operation and Development*. (2013). *The OECD privacy framework*. OECD, Memorándum de Explicación a las Directrices. https://www.afapdp.org/wp-content/uploads/2018/06/oecd_privacy_framework.pdf
[174] *Asia-Pacific Economic Cooperation*. (2015). *APEC Privacy Framework*. APEC. https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf

Cuentas se relacionan directamente con el perfilamiento algorítmico por la recopilación de grandes cantidades de datos de diversas fuentes y el peligro de afectación de datos personales al no realizarse de manera transparente y justa; que dicha recopilación de datos tenga un fin específico y no otros para los que el aviso de privacidad no previno. La Rendición de Cuentas hace responsables a los Particulares que elaboren perfiles algorítmicos -normalmente para usos no contemplados en la fuente original de datos y sin especificar en el aviso de privacidad- para que demuestren cómo se alinean a estos principios. Es de distinguir que el artículo 6 de la ley incorpora la expectativa razonable de privacidad -inspiración de la jurisprudencia norteamericana-; ésta protege la filtración de datos personales[175]

2.5.6. Ley General de Protección de Datos en Posesión de Sujetos Obligados (LGPDPSO).

La publicación en el Diario Oficial de la Federación del paquete legislativo en materia de transparencia, acceso a la información pública, protección de datos personales y reorganización administrativa marca un cambio radical que faculta a la Secretaría Anticorrupción y Buen Gobierno para asumir las funciones previamente atribuidas al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Esta ley se publicó el 20 de marzo de 2025, abroga la anterior ley del 26 de enero de 2017 que fue el primer intento de regular la protección de datos en los tres niveles de gobierno a nivel federal, estatal o

[175] *Supra.* García Ricci, Op. Cit. p. 146

municipal; acorde al Convenio 108 al que México solicitó entrar en 2017[176] para potenciar la inversión extranjera que exigía la protección a los datos personales. Esta ley proporciona un marco legal para regular la recopilación, el procesamiento y el uso de datos personales en México por los sujetos obligados definidos en el fracción XXVII del artículo 3ro. En su artículo 10 marca los principios a partir de los cuales pueden elaborar perfiles algorítmicos, así como supervisar y gestionar su uso, ya que establece estándares para la transparencia, el consentimiento, la calidad de los datos, la seguridad y los derechos individuales. Sin embargo, la Ley Federal de Derechos de Autor reconoce a los programas de cómputo como obras protegidas -a saber, los algoritmos-.

La ley busca asegurar que la elaboración de perfiles algorítmicos se lleve a cabo de manera justa, ética y que proteja tanto la privacidad como los derechos de las personas pero los sujetos obligados pueden alegar que sus algoritmos tienen protección por la Ley Federal de Derechos de Autor, el riesgo del perfilamiento algorítmico puede tocar diversos ámbitos como el laboral[177]. De lo contrario, la elaboración de perfiles algorítmicos puede conducir a resultados discriminatorios, violaciones de la privacidad y otros daños. Destaca los requisitos para obtener el consentimiento (artículo 14 y 15) para el procesamiento de los datos, más aún de los datos sensibles. La ley enfatiza la importancia de mantener datos personales precisos y actualizados a partir del respeto de los derechos ARCO (artículos 37 y

[176] Mendoza Enríquez, Olivia Andrea. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291. Recuperado en 08 de septiembre de 2025, http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es

[177] Maldonado Smith, M. E. (2024). Discriminación algorítmica en el ámbito laboral. Quórum Legislativo, núm. 145, marzo 2024, 69-125

sigs), es decir, derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos de las personas, importantes en el contexto de la elaboración de perfiles algorítmicos, ya que las personas pueden exigir saber qué datos se utilizan para crear su perfil, corregir datos inexactos y oponerse al procesamiento. Si los perfiles algorítmicos se construyen con datos defectuosos, los perfiles y las predicciones resultantes serán poco confiables, injustos y potencialmente discriminatorios.

La transparencia, tratada en el artículo 79 de la LGPDPSO -con referencia a la Ley General de Transparencia y Acceso a la Información Pública publicada el 20 de marzo de 2025-, es particularmente importante en la elaboración de perfiles algorítmicos, ya que permite a las personas comprender cómo están siendo categorizadas, evaluadas y sus consecuencias.

Las Medidas de Seguridad definidas en la fracción XVIII a XXI del artículo 3 de la LGPDPSO exige que los sujetos obligados las implementen para proteger los datos personales del acceso, uso o divulgación no autorizados. Esto es esencial en la elaboración de perfiles algorítmicos, donde se procesan grandes cantidades de datos y el riesgo de violaciones de datos es alto. Hay 6 premisas que se desprenden de la ley para la protección de datos: la **seguridad administrativa** que implica instrumentar medidas y procedimientos por el sujeto obligado para llevar registros de documentos que permitan identificar y gestionar la información relativa de los servidores públicos responsables del manejo de datos, su nivel jerárquico, cargo y funciones; **física** como resguardo de equipos electrónicos o dispositivos de tecnologías de información; **técnicas**, a saber: *software, proxies, intranet, internet,*

wifi; **confidencialidad**, tales como encriptación de la información, constraseñas y limitantes para acceso a la información; **integridad**, que los datos no sean alterados es un parámetro para la seguridad informática[178] y **disponibilidad**, garantizar que los sistemas y los datos puedan ser accedidos por los sujetos obligados, aún en ataques o secuestro de datos.

2.6. Valores de la Privacidad

2.6.1. Dignidad humana y su implicación en el perfilamiento algorítmico

Al hablar de dignidad es frecuente quedarnos en la superficie al entenderse como vivir con un mínimo de decoro, bienes materiales esenciales. En otras ocasiones se pide el respeto a la dignidad, por ende, ésta sólo quedaría como un término que implica susceptible de ser lastimado. Carlos Llano explica que "el concepto de dignidad tiene una connotación más radical…trasciende los anécdotas.[179]". Toda ciencia se fundamenta en axiomas, entendidos como puntos de partida absolutos, a esto se le llama *dignitates*, éstas guían al intelecto para no equivocarse, están arraigadas en el ente (filosofía primera o metafísica) o en algún género de dicho ente (ciencias segundas), pero aparecen con la aprehensión inmediata del ente[180]. Llano explica que la palabra dignidad no sólo implica algo con mucho valor, "… sino que está más allá del valor, con este significado,: la dignidad de algo es lo que hace valiosas a las demás cosas por la relación que guardan con ese algo al que llamo digno"[181], pero Llano corrige inmediatamente al mencionar que es inapropiado hablar de algo digno, ya que la dignidad sólo puede aplicarse a la persona

[178] Bernard, G., Coudert, R., Chapuis, B., & Huguenin, K. (2023). *An empirical study of the usage of checksums for web downloads*. In *Proceedings of the ACM Web Conference 2023* (pp. 1234–1245)
[179] Llano, Carlos. *Los Fantasmas de la Sociedad Contemporánea*, Ed. Trillas, México, 1995, p. 47
[180] Mendoza, José (2017) *"Introducción a la noción de dignitates en orden a la comprensión de las ciencias según Tomás de Aquino* (Primera parte)", en Logos. Anales del Seminario de Metafísica 50, 149-163.
[181] Llano, *Op. Cit.* p. 48.

humana, critica que hablar de dignidad de la persona humana es pleonástico[182]. ¿Qué pasaría si no existiera el hombre en el universo? Es el hombre quien da sentido al universo, por eso se dice que el universo es antropocéntrico, "…el cual deriva no de que yo sea hombre, sino de que tengo dignidad, lo cual no engendra sólo derechos sino sobre todo deberes…[183]". Batista explica cómo el multiculturalismo relativista llama a los derechos humanos una consecuencia cultural que no tienen base en valores universales y menos morales por lo que no hay lugar a juicios de valor objetivos; esta posición está en contra de la base universal de los derechos humanos: la dignidad, preexistente al derecho objetivo, ontológica -es decir, tan solo por ser persona; por lo tanto erga omnes. La contrapone a la que llama dignidad bajo la concepción de autonomía personal y el derecho a la libre autodeterminación. Esta concepción está alejada de la ontológica[184].

Por ello, toda persona tiene derecho a su honra, buena imagen, nombre y reputación, todos podemos exigir que se nos respete, siendo un derecho único e irrenunciable propio de la dignidad de la persona, esto implicará la prohibición jurídica a toda invasión arbitraria en la vida privada, la de su familia, su domicilio o correspondencia. En contraste, los algoritmos de perfilamiento a menudo reducen al individuo a un conjunto de datos y patrones de comportamiento con fines comerciales o de control, sin considerar el valor inherente de la persona.

La doctrina italiana dice que es la dignidad personal reflejada en la consideración de los demás y en el sentimiento de la propia persona. Se refiere, entonces, al juicio de valor que la sociedad hace de nosotros mismos. En esta concepción de honor, éste se basa en la

[182] *Supra* p. 48
[183] *Supra*
[184] Batista, Fernando. Boletín Mexicano de Derecho Comparado, núm. 167, mayo-agosto de 2023, pp. 33-50ISSN: 2448-4873DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18535

sociedad en la misma proporción que en la misma persona. Por ende, si la sociedad considera que una persona no es digna de tener honor, faltaría esa otra mitad de tan importante derecho.

Westin afirma que hacia 1960 empieza la recolección de datos en el gobierno para bajo el argumento de buscar una mejor regulación económica, promover el bienestar y potenciar los derechos civiles, le llama a esto "computerized Big Brother" anticipa que las nuevas tecnologías pueden colisionar con los valores de la privacidad y la dignidad humana, destaca como función de la privacidad a la autonomía personal como un medio para salvaguardar su individualidad con dignidad y valor intrínseco[185]. Sin mencionar el perfilamiento algorítmico, Westin habla de la teoría de la información basado en el modelo predictivo de la conducta a partir de datos psicológicos, demográficos, de organizaciones para la toma de decisiones en las ciencias sociales, gobierno y hasta negocios.[186]

Daniel J. Solove[187] destaca el valor de la privacidad al preguntarse por qué vale la pena protegerla, qué valores persigue el respeto a la privacidad y su protección jurídica. Su enfoque es pragmático al abordar las actividades que impedirían la falta de respeto al derecho a la privacidad. Por ello, la privacidad no tiene un valor único, sus valores deben analizarse al compararlos con sus intereses opuestos (contra valores).

2.6.2. Bienestar psicológico o estabilidad emocional

La tecnología cada vez avanza más y su posibilidad de almacenar imágenes e información de las personas físicas se convierte en un riesgo por la facilidad con que

[185] Westin, *Op. Cit. Chapter Twelve -Pulling all the Facts Together*, p. 103 *ebook*
[186] Westin*, Supra, Chapter Twelve -Pulling all the Facts Together*, p. 103 *ebook*
[187] Solove, Daniel J. *Understanding Privacy, Harvard University Press*, Cambridge, MA, 2008, p.78

pueden ser compartidas. Si bien el ser humano tiene la necesidad de conectarse con otros para alcanzar su plenitud, lo que implica compartir datos personales, también existe la necesidad psicológica de protegerse, especialmente al sentir vulnerable su honor o intimidad tras haber compartido dicha información. El bienestar psicológico es un valor que aparece en varios autores a partir de un reporte del Departamento de Salud, Educación y Bienestar de Estados Unidos que apareció en 1973 donde se sostiene que "hay una creencia extendida que la privacidad personal es esencial a nuestro bienestar - físicamente, psicológicamente, socialmente y moralmente" [188]. Weinstein sostiene que la privacidad es valiosa al ser un intento por disminuir las tensiones personales derivadas de la conducta social de las personas[189]. La fama pública tiene todo que ver con el concepto de honor. Lucrecio Rebollo afirma que "el honor es la buena fama o reputación que una persona merece en el conjunto social"[190]. El honor tiene todo que ver con la auto estima, la autovalía, la percepción de sí mismo; la reputación con la opinión de los demás. El desarrollo de la personalidad se convierte en el porqué de la protección de los derechos fundamentales, entre ellos, la protección de datos personales. Se diferencia el honor de la fama en que el primero "…está referido al trato dado o recibido por los demás, y la fama es el rumor, voz pública"[191]. Por ello, la exposición de datos personales y el perfilamiento algorítmico puede producir un eco no deseado en la opinión pública referido a nosotros. El honor y la fama pública tienen que ver más con la dimensión espiritual de los derechos de la personalidad. Para Castán Tobeñas "…Es uno de los bienes jurídicos más preciados

[188] US Department of Health*, Education & Welfare. Records, Computers and and the Rights of Citizens. Chapter* III (Safewards of Privacy), 1973, DHEW Publication. p. 33
[189] Aludido por Solove, Daniel J. *Understanding Privacy, Harvard University Press*, Cambridge, MA, 2008, p. 79
[190] Rebollo Delgado, Lucrecio. Derechos de la personalidad y datos personales. En: Revista de Derecho Político, España, Nº 44, 1998. Pág. 149
[191] *Supra*

de la personalidad humana, que puede ser considerado como el primero y el más importante de aquel grupo de derechos que protegen los matices morales de esa personalidad[192]". La Suprema Corte de Justicia de la Nación ha señalado que este derecho tiene dos aspectos esenciales: la inmanencia que tiene que ver con el concepto y valoración de uno mismo y el de trascendencia que se relaciona con la fama pública o la forma en que los otros reconocen nuestra dignidad[193]. Existen 3 elementos del derecho al honor: A) Positivos que se refieren al sentir de la persona sobre su dignidad y de la impresión que los demás tienen de ella. La divulgación referida al momento en que los otros pueden atacar nuestra fama pública y lo que Callaghan[194] señala la diferencia entre expresión, información y opinión. Expresión son las palabras, insultos, que se separan de la idea objetiva que expresa. Opinión se refiere a un aspecto subjetivo que contiene el juicio de valor de quien la emite, afecta la fama pública cuando se basa en hechos falsos. De ahí la expresión denominada difamatoria, que afecta la fama pública. B) Negativos, se expresa una opinión basada en una mentira, o con imposibilidad de prueba; o bien no se tiene el consentimiento para compartir datos que afecten la fama pública, es decir, el honor. C. Jurídicos. Debe haber protección expresa al honor por la ley, en hipótesis concretas, así como sus excepciones por interés público.

2.6.3. Autodesarrollo

Otros autores sostienen que la privacidad es fundamental para el **autodesarrollo** al ser "…una cubierta para liberar las inhibiciones, para el auto-descubrimiento, autoconsciencia, autodirección, innovación, alimentación para un sentimiento de unicidad

[192] Castán Tobeñas, José. Derecho civil español, común y foral, t. l, 1984, vol.11, p. 398
[193] Sánchez Guzmán, Cecilia. Derecho al Honor. *Revista Praxis de los derechos de la personalidad,* Vlex México, 2017, p. 47 y 48.
[194] Aludido por Sánchez Guzmán, Cecilia, *Supra*, p. 49.

y un respiro a la opressión de la normalidad"[195]. Westin sostiene que la privacidad permite a las personas un respiro en la vorágine de la vida activa[196]. La privacidad, según Bensman y Lilienfeld, se requiere sencillamente porque la expresión de nuestro interior nos colocaría en desventaja con al ambiente cultural en el que vivimos"[197].

En este contexto, el avance tecnológico y el perfilamiento algorítmico cobran especial relevancia. Las técnicas de perfilamiento algorítmico empleadas actualmente recaban y analizan constantemente los datos personales, lo cual, al reducir el espacio privado disponible, limita significativamente la capacidad del individuo para desarrollar su identidad auténtica sin condicionamientos externos. Simmel sostiene que "en la privacidad podemos desarrollar, en el tiempo, una posición más firme y mejor construida e integrada en oposición a las presiones sociales dominantes" [198]. No obstante, el perfilamiento algorítmico corre el riesgo de erosionar estos espacios privados esenciales, volviéndonos vulnerables a influencias manipulativas y socavando la libertad necesaria para la autoformación y la autodeterminación. En nuestra opinión la privacidad está en nuestra naturaleza por lo que estamos de acuerdo en que es parte de la autorrrealización del ser humano el proteger ese derecho. De lo contrario, viviríamos una personalidad espejo, donde el espejo son los otros y daríamos lugar a la manipulación de la sociedad a las personas.

2.6.4. La democracia y el perfilamiento algorítmico

[195] Solove, *Op.Cit*. 79
[196] Citado por Solove, *Supra*. p. 79
[197] Citados por Solove, *Supra*.p. 79
[198] Citado por Solove, *Supra*. p. 79

El sistema político y jurídico de cada país determinará el grado de respeto a la privacidad de los datos de sus gobernados. No sólo temas de vigilancia, datos biométricos, exposición de datos personales por cuestiones de seguridad, sino también por el **perfilamiento algorítmico**: la aplicación de modelos predictivos que recopilan, cruzan y analizan información masiva (desde historiales de navegación hasta redes de contacto) para clasificar ciudadanos en función de sus características y comportamientos.

En general, encontramos que en los sistemas totalitarios la secrecía en cuanto a la actuación del estado es casi proporcional a la vigilancia secreta y exposición de datos personales de sus gobernados, así como la restricción a la libertad de expresión de sus ciudadanos. Esta dinámica se vuelve aún más opaca cuando los algoritmos deciden, por ejemplo, qué lugares "merecen" mayor patrullaje (policía predictiva) o qué contenidos políticos deben priorizarse o restringirse en redes sociales estatales.

La privacidad es esencial para un gobierno democrático porque potencia y promueve la autonomía moral del ciudadano, un requisito esencial para la democracia[199]. Como señala Gavison[200] la protección a la privacidad contribuye a una sociedad plural y tolerante, al permitir el espacio necesario para que cada individuo piense y decida sin sentirse permanentemente "visto" o perfilado. Sobre esa base se construye la deliberación pública y el voto secreto, auténticos pilares de un régimen democrático.

Sin embargo, la emergencia de sistemas algorítmicos introduce un nuevo choque de derechos: **privacidad versus interés público**, mediado por la opacidad y los sesgos de los algoritmos. Si bien el derecho a la privacidad no es absoluto, el perfilamiento algorítmico aplicado por gobiernos puede amplificar la diseminación de información

[199] Ruth Gavison, *Yale Law School Legal Scholarship Repository, January* 1980, https://digitalcommons.law.yale.edu/, p. 421-471
[200] *Supra*. p. 455

sesgada, estigmatizar grupos específicos y generar lo que la investigadora Shoshana Zuboff ha llamado "capitalismo de vigilancia estatal[201]", donde no solo las empresas tecnológicas, sino también los poderes públicos usan los datos para moldear la conducta ciudadana. En México es el artículo 6 de nuestra Constitución Política la que señala la libertad en la manifestación de ideas y su limitante al derecho a la privacidad de terceros. La vigilancia digital facilita la invasión a la privacidad de los particulares o a su manipulación como en el caso de la empresa Cambridge Analytica que compiló los perfiles personales de más de 50 millones de personas para usarlo a favor de la campaña de Donald Trump o el gran tema de Wikileaks de Snowden. Los algoritmos permiten que un cúmulo de noticias falsas se propaguen con extrema facilidad en grupos de personas, comunidades, familias para encontrar en ellos afinidad para manipularlos hacia una ideología u otra. Philip Howard[202] sostiene que las empresas tecnológicas asumen con un margen de laxitud sus obligaciones normativas respecto al uso de datos de particulares, incluso al mover sus bases de datos a jurisdicciones más permisivas; normalmente usan sus términos de servicio para protegerse de cualquier demanda un particular acerca del manejo de sus datos. Por ejemplo, las redes sociales contienen algoritmos para buscar las personas afines a ciertos mensajes y hacer que crezca una tendencia aún cuando no sea veraz. Ünver[203] señala que no sólo los ciudadanos han perdido privacidad frente a la tecnología, sino también los estados a partir de los servicios que ofrece la tecnología a ciudadanos comunes que pueden tener acceso a instalaciones secretas vía drones o

[201] Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, New York, NY, 2019.

[202] Howard, P. N. (2020). *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press.
[203] Ünver, H. Akın. "*Politics of Digital Surveillance, National Security and Privacy*." *Centre for Economics and Foreign Policy Studies*, 2018. http://www.jstor.org/stable/resrep17009.

recolectar meta datos en los teléfonos de las autoridades, entre muchas otras[204]. Podemos concluir este apartado al afirmar que el derecho a la privacidad debe ser protegida para perfeccionar la democracia.

2.6.5. Creatividad y perfilamiento algorítmico

La privacidad es un espacio vital para la creatividad, donde pueden darse expresiones artísticas auténticas libres del escrutinio constante de la crítica social inmediata y de algoritmos predictivos que podrían anticipar y juzgar negativamente obras aún en proceso. Muchos manuscritos valiosos han sido producidos en la intimidad y aislamiento de sus autores, protegidos por el derecho a la privacidad, lo cual permitió que desarrollaran ideas innovadoras sin las restricciones o presiones impuestas por la evaluación algorítmica o la crítica temprana de expertos. Es precisamente en estos contextos privados donde se han gestado obras maestras que, al ser eventualmente descubiertas, se han convertido en referencias fundamentales en diversas disciplinas científicas y artísticas. Por ello, proteger la privacidad ante el avance del perfilamiento algorítmico es esencial para preservar la libertad creativa y fomentar la innovación cultural y científica.

2.6.6. Legitimidad de la defensa de la privacidad y el perfilamiento algorítmico

Los alcances jurídicos de la defensa de nuestros datos como particulares deben estar claramente protegidos para dar certeza jurídica del acceso a nuestros datos, posibilidad de rectificarlos, cancelarlos u oponernos al uso de ellos. En la Constitución Política de la

[204] *Supra*, p. 3

Ciudad de México en su artículo 7, Inciso E[205]: El Derecho a la Privacidad y Protección de Datos Personales se establece el fundamento de los derechos ARCO en la ciudad de México con referencia a la Constitución Política de los Estados Unidos Mexicanos y las leyes relativas.

El aviso de privacidad debe garantizar nuestro control sobre la información personal que decidimos compartir, lo que adquiere mayor relevancia frente a las prácticas de perfilamiento algorítmico, que pueden capturar, analizar y utilizar información personal de manera invasiva. Reiteramos que el derecho a la privacidad no termina en sí mismo, aún con un recluso o ermitaño; tiene una trascendencia al ser un medio de auto realización. Por otro lado, las personas tenemos la necesidad de compartir nuestros pensamientos a la gente más cercana y con la que tenemos conexión emocional[206]. Esto nos hace vulnerables al proporcionar información personal en el plano físico o virtual, dicha información puede ser usada para hacer robo de identidad, fraude, o incluso secuestro. Debemos promover la cultura de proteger nuestra información personal de manera adecuada.

2.7. Contra valores de la Privacidad

Si bien algunos autores, como Arendt han analizado el valor de la esfera pública y la privacidad en términos de visibilidad y acción social, la era digital introduce una complejidad radicalmente nueva: la vigilancia algorítmica y el perfilado. Arendt describió la privacidad como "un estado de estar privado de algo[207]," específicamente de la realidad que deriva de ser visto y escuchado por otros en la

[205] Reforma publicada en la GOCDMX el 2 de Junio de 2022
[206] Ver Westin, *Op. Cit. Chapter Two, -The Individual Quest for Intra-Psychic Balance*, p. 18 *ebook*
[207] Arendt, Hannah. *The Human Condition*, 2nd Edition, The University of Chicago Press, 1958. p. 58

esfera pública. Sin embargo, en el contexto contemporáneo, la amenaza a la privacidad no proviene únicamente de la ausencia de otros, sino de la presencia omnipresente de sistemas automatizados que observan, registran y analizan el comportamiento para construir perfiles detallados de los individuos.

A grado tal que es como no existir. David Riesman escribe The Lonely Crowd[208] como un ensayo sociológico donde analiza la pérdida de autoridad y legitimidad de los adultos sobre los jóvenes, quienes desoyen a las generaciones mayores y buscan en la privacidad promover la anomia que se incrusta gradualmente en su personalidad y promueve la cultura de la soledad. Estudia cómo se forma la personalidad social en diversas regiones, eras y grupos. Una vez formada influye en la política, la educación, el trabajo y otras actividades sociales. En nuestra opinión los padres de familia cada vez menos asumen su rol de formadores de virtudes sociales y dejan que sean los medios masivos los que muestren los valores sociales a través de las series de Netflix, pero siempre en la soledad del adolescente. Sherry Turkle en su obra *Alone Together* [209] trata cómo el excesivo uso de la tecnología genera adolescentes que están en un grupo, pero siempre en su dispositivo móvil dentro de las redes sociales; es decir, están juntos, pero solos. Los niños y los jóvenes se proyectan en una figura lejana a la realidad sólo por encajar y el esquema de micro recompensas -como un *like* en un *post*- mantiene sus endorfinas al máximo con la consecuente adicción a ellas, un problema que Tim Cook detectó por lo que generó la *APP Screen Time* en todos los teléfonos Apple que nos permite no sólo ver el tiempo dedicado a descargas, *whatsapp* y *Apps* diversas, sino limitarlo; sobretodo en el caso de padres de familia. En estos autores detectamos a la privacidad como una amenaza a la

[208] Riesman, David. *The Lonely Crowd. A study of the changing American character*. Ed. Yale University Press, USA, 2000. p. xxv y p. 70
[209] Turkle, Sherry*, Alone Together*, Ed. *Basic Books*, 2011.

comunidad y a la solidaridad. En las sociedades comunistas, la privacidad es un antivalor que ataca el espíritu comunal. Tomás Moro en su obra Utopía (1516) describe una sociedad idílica con una vida comunal en la que nada se esconde y el orden social es lo fundamental al afirmar "…con los ojos de todos sobre ellos, la gente no tiene más elección que hacer el trabajo habitual o disfrutar del pasado que no sea deshonroso[210]". Solove sostiene que el respeto a la privacidad permite crear la contra cultura o crítica a la sociedad[211].

También la privacidad se ve como un antivalor para conseguir el control social[212], ya que puede encubrir actividades de terrorismo, espionaje y poner en peligro a la sociedad. Esto fue especialmente cuestionado después del ataque a las Torres Gemelas de Nueva York, el llamado 11/09 (*september eleven*). Joseph Pulitzer, en cuyo honor la Universidad de Columbia instauró el Premio Pulitzer, afirmó "no hay crimen, no hay estafa, no hay truco, no hay una evasión, no hay un vicio que no viva conforme a la secrecía"[213]. En 2007, Julian Assange da al mundo los *Wikileaks* que revelan documentos que demuestran invasión a la privacidad de las personas en aras de la seguridad nacional. Assange justificó esas acciones con la frase: "privacidad para los débiles, transparencia para los poderosos[214]". De acuerdo a Assange, Internet da poder sobre naciones enteras a agencias espías y a sus aliados. El sociólogo Steven Nock argumenta que "la confianza y la habilidad de creer en la palabra de los otros son ingredientes básicos en un orden

[210] Aludido por Solove, *Op. Cit*. p. 81
[211] *Supra.* p. 80
[212] *Supra* p. 81
[213] Aludido por Solove, p. 81
[214] Keulen, Sjoerd. Kroeze, Ronald. *The Handbook Privacy Studies*, Amsterdam University Press, 2018, p. 37.

social…la privacidad hace difícil conocer la reputación de otro"[215]lo que hace difícil determinar si son confiables.

Varias investigadoras, argumentan que la privacidad es problemática porque potencia el abuso y la opresión de las mujeres en el hogar[216]. Argumentan que la esfera pública siempre ha pertenecido al dominio de los hombres, y han dejado a las mujeres y familias la esfera privada; con ello, todos los temas relativos a la mujer. Esto lo podemos ver en el feminicidio de Abril Pérez Sagaón quien había acusado a su esposo de intento de homicidio, lo que hizo que lo detuvieran, un juez cambió la sentencia a violencia doméstica, lo que liberó a su esposo quien después fue el autor intelectual de su homicidio el 25 de noviembre de 2019[217]. Durante la pandemia de 2020, fue impresionante el aumento de la violencia en los hogares mexicanos al quedarnos en casa y vivir la privacidad no como un derecho, sino como un medio de prevención ante el virus. Catharine Mac-Kinnon completa la definición de privacidad "*the right to privacy is a right of men to be let alone to oppress women one at a time* (el derecho a la privacidad es el derecho de los hombres a estar solos para oprimir a las mujeres, una a la vez)"[218]. Carole Pateman afirma que la "dicotomía entre lo privado y lo público oscurece la

[215] *Supra*
[216] Para una visión feminista general crítica de la privacidad, ver Patricia Boling, *Privacy and the Politics of Intimate Life* (Ithaca, NY.: Cornell University Press, 1996). Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, NY.: Cornell University Press, 1997). pp. 81-94. Ruth Gavison. "*Feminism and the Public/Private Distinction*." *Stanford Law Review* 45, no. 1 (1992): 1–45. https://doi.org/10.2307/1228984. p. 327.
[217] BBC News, "El Asesinato De Abril Pérez, El Feminicidio Que Indignó a México," BBC News Mundo (BBC, 2020), https://www.bbc.com/mundo/noticias-america-latina-50603585.
[218] Mac Kinnon, *Catharine, Toward a Feminist Theory of the State*, Ed. Harvard University 1989, p. 191, 194.

sujeción de las mujeres a los hombres dentro un aparente orden universal, igualitario e individualista[219]".

Algunos ven la privacidad como un vestigio de la era gentil que ha pasado desde hace mucho tiempo. Westin argumenta que el ensayo *The Right to Privacy* de Brandeis fue esencialmente una protesta a favor de los valores patricios contra el ascenso de los valores culturales y políticos de la sociedad de las masas. Para los patricios, la prensa amarillista, los anuncios comerciales y la exposición de las actividades de los prominentes eran intrusiones injustificadas y agresivas de editores indulgentes ante la curiosidad y gustos de las masas[220]. Hoy un buen porcentaje de adolescentes no están interesados en la protección de su privacidad, publican todo aquello que nuestros padres reducían a su diario, en sus redes sociales al usarlas como catarsis en su periodos más tristes y solitarios; y mucho más en los felices[221]. Hoy los niños y adolescentes están acostumbrados a ventilar sus vidas en las diferentes redes sociales de las que son parte y donde buscan reconocimiento, consejo o empatía; aunque muchas veces encuentran lo contrario como el denominado *cyberbullying*. En Inglaterra se han establecido diversos mecanismos para prevenir el *bullying* online como la *Anti-Bullying Alliance* que define esta práctica como cualquier forma de *bullying* llevado a cabo por aparatos con tecnología de medios de comunicación, y se reconoce que afecta la vida social, escolar y personal[222].

---

[219] Pateman, Carol, *The Disorder of Women: Democracy, Feminism, and Political Theory*, Ed. Blackwell Publishers, Ltd. p. 121
[220] Westin, *Op. Cit. Chapter Thirteen -Common Law Attempts to Control Surveillance*, p. 110 *ebook*
[221] Mary Madden et al., "*Teens, Social Media, and Privacy*," *Pew Research Center: Internet, Science and Tech,* August 17, 2020, http://pewrsr.ch/1m8f24k.
[222] *Antibullying Alliance, "United Against Bullying (UAB) Programme*," Anti, 2022, https://anti-bullyingalliance.org.uk/.

La privacidad inhibe la eficiencia del mercado y sus ganancias. El mercado está ávido de tener más información y conocimiento acerca del cliente para atenderlo mejor, venderle más, aunque ello implique violar su derecho a la privacidad. Ahora se ha avanzado mucho en la protección de datos personales y se ha conseguido la obligación de la empresa de informar al cliente la forma en que será usada su información. Fred Cate escribe "la privacidad interfiere con la recolección, organización y almacenaje de la información en que los negocios y otros pueden atraer para hacer decisiones más rápidas, informadas, tales como otorgar un crédito o aceptar un cheque"[223]. Pensemos un escenario donde se puedan personalizar los precios con base en sus compras pasadas y ofertar sólo aquello que sea de interés para los posibles compradores de acuerdo con su capacidad de compra.

La privacidad también se conflictúa con el libre flujo de información, lo que impide la transparencia y apertura. Aquí encontramos un conflicto de bienes jurídicos, por un lado, el respeto a la privacidad y por otro la libertad de expresión de aquellos que quieren dar información privada de las personas. Eugene Volokh afirma que la privacidad interfiere el derecho de las personas de hablar de los otros[224]. Si alguien sabe algo acerca de ti, ¿tiene el derecho a comunicarlo? El filósofo periodista Sergio Sarmiento publicó un artículo que se denomina "Y la verdad..." donde narra la forma en que un político llamado Humberto Hernández Haddad lo denunció penalmente por difamación por publicar en su columna parte de una información que provenía de un documento de la Secretaría de Relaciones Exteriores (B094 del 25 de marzo de 1997) donde se aconsejaba

[223] Aludido por Solove, *Op. Cit*. p. 83
[224] Aludido por Solove, *Supra*. 83

destituir a dicho político por reiterado desacato a la autoridad[225]. El equilibrio de la ley indica que se deben sancionar las injurias, en un terreno civil más que penal. Pero, también debe protegerse el derecho de los periodistas éticos a informar.

En la medida en que el gobierno confía en los datos que proporcionamos, hay posibilidad de que resulte afectado. Existe la humana tendencia a sólo informar lo que nos conviene, esto que es un derecho nuestro puede afectar al bien común.

El derecho a la identidad como un derecho humano fundamental consagrado en el artículo 4 de nuestra Constitución Política (reconocido el 17 de junio de 2014). En México el 2 de diciembre de 2012 se firmó el Pacto por México[226] por los 3 principales partidos políticos de entonces: PAN, PRI y PRD. En el compromiso 33 se estableció: Una cédula de identidad Ciudadana y Registro Nacional de Población como parte del reconocimiento al derecho de identidad. Esta idea data del sexenio de Felipe Calderón para buscar la garantía de unicidad y con datos biométricos al encontrar muchas homonimias en las credenciales de elector expedidas por el entonces Instituto Federal Electoral. El fundamento constitucional yace en el Decreto del 6 de abril de 1990 que destaca que el artículo 36 constitucional indica que los ciudadanos tienen la obligación de inscribirse en el Registro Nacional de Ciudadanos y expedir el documento que acredite la ciudadanía mexicana bajo la responsabilidad del Estado[227]. Sin embargo, no se ha logrado esta cédula de identidad única con tecnología biométrica. En 2015 la Auditoría Superior de la Federación determinó que la Secretaría de Gobernación carece de información

---

[225] Sarmiento, Sergio, Columna Editorial Jaque Mate: *Y la verdad*, Periódico Reforma, México, D. F., 28 de Abril de 2006.
[226] Guerrero, Francisco. Amador, Juan Carlos. *La Concertación Política en Contextos de Democracias Fragmentadas el caso de Pacto por México*, D3 Ediciones SA de CV, 2016. http://biblioteca.diputados.gob.mx/janium/bv/lxiii/PactoxMexico.pdf consultado el 17 de febrero de 2023.
[227] Dirección General de Análisis Legislativo, "Cédula De Identidad Ciudadana y Registro Nacional De Población," Mirada Legislativa, 2014, http://bibliodigitalibd.senado.gob.mx/.

certera para expedir dicha cédula de identidad única lo que inhibe a los ciudadanos de hacer trámites básicos con la certeza de que nadie les haya robado su identidad. En 2015 había un sobreregistro de 46.4% de registros de la población estimada en México. Las ventajas de la identidad única son muchas tales como eliminar la duplicidad de identidades, identificación inmediata de víctimas en accidentes, registros de salud para mejor atención, en fallecimientos o cuerpos desaparecidos la identificación podría ser inmediata[228].

Es importante destacar que el derecho a la privacidad puede ser afectado al contar con toda nuestra información biométrica por parte del Estado. Quizá sea el inicio para una estrategia de vigilancia y cruce de información para fines políticos o en pro de las corporaciones de seguros. Es algo muy parecido a lo que hace Google con nuestra información al crear un perfil de identidad para fines comerciales a partir del uso de *big data e* inteligencia artificial.

III. Ámbitos de la privacidad

Tradicionalmente al pensar en la privacidad se piensa en un ámbito que pertenece a una persona y es invadida con una ruptura de su derecho subjetivo a la privacidad. Lo anterior se entiende porque es aquella la más vulnerable. Sin embargo la privacidad tiene varios ámbitos. En la era digital, de la inteligencia artificial, *deep learning* y *machine learning*, a estos ámbitos tradicionales se suma una nueva dimensión esencial: la privacidad algorítmica, la cual se refiere a la protección de la autonomía individual y la no-discriminación frente a los procesos de recolección masiva de datos, análisis

[228] Jorge Monroy, "Ni Cédula, Ni Clave Única Son Una Realidad En México," El Economista, 2017, https://www.eleconomista.com.mx/politica/Ni-Cedula-ni-Clave-Unica-son-una-realidad-en-Mexico-20170703-0020.html.

automatizado y toma de decisiones predichas o inferidas por algoritmos, que, a menudo, operan sin transparencia respecto a la recolección y uso de nuestros datos. A diferencia de las intrusiones tradicionales, el perfilamiento algorítmico no necesariamente requiere una "invasión" física o el acceso explícito a un espacio privado, sino que opera sobre la base de la información que los individuos generan digitalmente, configurando perfiles predictivos que pueden afectar el acceso a servicios, oportunidades e incluso influir en el comportamiento.

3.1. Privacidad física

Es la primera, se relaciona al ámbito estrictamente espacial, sus orígenes se remontan al origen del hombre. Edward T. Hall[229] lo explica detalladamente en su obra *The Hidden Dimension*, señala que las aves y mamíferos no sólo tienen territorios que ocupan y defienden incluso contra los de su propia especie; sino que también mantienen distancias uniformes entre uno y otro. *Hall* acuñó el término *proxemics* que se refiere a dicho espacio y que forma parte de cada cultura. La privacidad es un valor que la propiedad privada protege, para Locke una persona es lo que hace y lo que posee, comenzando con su propio cuerpo y el Estado es un instrumento para asegurar dicha propiedad y los límites de esa autoridad estatal están puestos por el propio interés del gobernado[230]. Westin afirma que la Constitución de Estados Unidos de América yace en los principios de la filosofía de John Locke, sobre todo en lo que se refiere a la privacidad. Primero por el individualismo con sus ideas del valor de cada persona, el juicio religioso privado, los motivos económicos y los derechos para los individuos. Segundo, el principio de

[229] Edward T. Hall. *The Hidden Dimension*, *Anchor Books Doubleday*, NY 1966. P. 111 y sigs.
[230] Neville, Robert C., "*Various Meanings of Privacy- A Philosophical Analysis*," in *Privacy: A Vanishing Value?* ed. William C. Bier (New York: Fordham University Press, 1980), 24.

gobierno limitado -*limited government*- con su corolario de limitaciones legales a la autoridad ejecutiva, la regla del derecho y la primacía moral de lo privado sobre la esfera pública de la sociedad. Tercero, el concepto esencial de la propiedad privada y su enlace con el ejercicio individual de la libertad. Estos conceptos requerían amplia inmunidad de la intrusión y interferencia con las posesiones personales. Cada una de estas ideas -sostiene Locke- tenían un propósito común: liberar a los ciudadanos de la vigilancia ilimitada y el control que habían ejercido sobre los sujetos tanto reyes como *Lords*, municipalidades, gremios de la sociedad europea[231]. La privacidad física sobreentiende una base de espacio y territorio como un requisito *sine qua non*. Según Bier[232], la tradición del hogar europeo como santuario inviolable data muy probablemente de la Edad de Bronce, desde entonces se destaca la relación entre casa y propietario como una forma territorial de la identidad y por su valor como un modelo en que la privacidad se concibe en términos espaciales. De hecho, aún subsisten comunidades que tienen el nombre de la familia en un mosaico, así como el año en que fue construida[233]. Es aquí donde encontramos el enlace entre la identidad de un hombre con su propiedad con base en el cual el hombre ha construido el concepto de vida personal para concebir a la privacidad en términos de territorio e inevitablemente ser considerado como un derecho subjetivo y una especie del género derecho de propiedad. Ésta fue la base para el gran ensayo *The Right to Privacy* de Warren y Brandeis (1890) fundamento para un derecho de la personalidad inviolable y la percepción del derecho a la privacidad como un tipo de derecho de propiedad[234]. Su gran aportación fue despertar la tradición del *Common Law*

[231] Westin, Alan, *Op. Cit. Part Two - The New Tools for Invading Privacy* p. 26 *ebook*
[232] Bier, William C., *Privacy: A Vanishing Value*? (New York: Fordham University Press, 1980), p.6
[233] *Supra* p. 7
[234] *Supra* p. 7

que destaca la protección del individuo, de su propiedad, de ser invadido, así como extender esa protección al ámbito moral y emocional. Gisela Pérez Fuentes indica precisamente que el derecho a la intimidad nace al ámbito jurídico como un derecho subjetivo de la persona física que se constituye como un derecho de la personalidad para que alcance "su realización social y psicológica"[235].

Por otro lado, Locke[236] destaca que la educación privada, entendida como aquella dada en casa, es el lugar donde se pueden formar las virtudes y los vicios como hábitos operativos privados que se forman más por la práctica que por las reglas, vicios tan fuertes como la falta de carácter y la ignorancia son una consecuencia del ámbito privado de la educación.

3.2. Privacidad algorítmica

A partir de la digitalización de los datos y las telecomunicaciones la privacidad física centrada en el espacio y propiedad privada deja de ser la única amenazada por la invasión a ella. La facilidad para crear algoritmos para el perfilamiento amenaza con extender la invasión a la esfera de los datos y las consecuentes inferencias sobre la persona. La tecnología de geolocalización y el análisis de patrones de movimiento a través de dispositivos móviles pueden crear un "mapa" detallado de la vida privada de un individuo, perfilando sus hábitos, preferencias e incluso su identidad, sin que exista una intrusión física directa.

De esta manera, el territorio de la privacidad se expande más allá de lo tangible, adentrándose en el territorio digital y los modelos predictivos que se construyen sobre los datos personales. La nueva Ley en Materia de Telecomunicaciones y Radiodifusión

[235] Aludida por Nucci, Hilda, *Op. Cit*. p. 187
[236] Locke, John. *Some Thoughts Concerning Education*. Numeral 82 *in Complete Works of John Locke*, Delphi *Series*, UK, 2017.

publicada en el Diario Oficial de la Federación el 16 de julio de 2025 señala en su artículo 131 que los proveedores de servicios de acceso a Internet, ya sean concesionarios o autorizados, están obligados a cumplir con las directrices generales -respetando los principios de libertad de elección, no discriminación, protección de la privacidad, transparencia y los derechos previstos en la Constitución, la legislación vigente, las sugerencias de organismos internacionales especializados, así como los tratados y convenios internacionales ratificados por México, en lo que sea pertinente- que emita la Comisión correspondiente.

Dwork y Roth[237] hablan de la Privacidad Diferencial, no como un algoritmo sino como una propiedad que los mismos algoritmos deben satisfacer, dicha promesa se basa en un aparente oxímoron donde la persona que posee datos de otra, le promete que el algoritmo no aprenderá nada sobre ella, mientras obtiene información útil sobre un grupo de la población. Esta solución matemática se logra al introducir la aleatoriedad en el perfilamiento algorítmico y con ello se alinea con los principios de la Estadística, entendida como la "ciencia que trata con datos sobre la condición de un estado o comunidad"238. La solución matemática que implica la privacidad diferencial garantizaría que el análisis y cruce de datos no describa a un individuo sino a una comunidad en su conjunto alinéandose con los principios legales y éticos en la recopilación, análisis y uso de datos.

[237] Dwork, Cynthia & Roth, Aaron. *The Algorithmic Foundations of Differential Privacy*, *Foundations and Trends in Theoretical Computer Science* 9, nos. 3–4 (2014): 211–407, https://doi.org/10.1561/0400000042
[238] *Supra*, Dwork, Cynthia & Roth, Aaron. p. 258

3.3. Privacidad en la decisión y el perfilamiento algorítmico

El derecho a la privacidad protege la capacidad de decisión que tiene una persona respecto a sus acciones privadas que no afecten derechos de tercero. La privacidad entendida como el derecho a decidir libremente está íntimamente relacionada con el perfilamiento algorítmico que da la capacidad de vulnerar la autonomía de las personas porque puede recolectar, procesar, discriminar al utilizar datos personales sin el conocimiento pleno y menos el consentimiento informado, como se defiende en el derecho objetivo.

En México es reconocido el derecho a la privacidad como derecho de decisión con base en el libre desarrollo de la personalidad con base en el Artículo 4to párrafo segundo constitucional respecto a decidir el número y espaciamiento de hijos, el Artículo 16 constitucional a Suprema Corte de Justicia de la Nación al revisar la constitucionalidad de las reformas al Código Penal de Coahuila en 2017 -impugnadas por la entonces Procuraduría General de la República-, que señalaban como delito el aborto. El ministro Luis María Aguilar en su proyecto de sentencia que fue avalado por la mayoría de los ministros no reconoce el derecho a la vida a lo que llama "el producto de la concepción" al sostener que "escapa a la noción de persona como titular de derechos humanos, de modo que el ejercicio de éstos está determinado a partir de la existencia del individuo"[239]. También señala que "el derecho de la mujer a decidir es el resultado de una combinación de derechos y principios asociados a la libertad de autodeterminarse … conforme a sus convicciones[240]". Señala el artículo 1 y 4 constitucionales como fundamento. Es decir, no

[239] GIRE, "Caso Coahuila: La Marea Verde Llega a Pino Suarez 2," El Juego de la Suprema Corte, 2021, https://bit.ly/3aGXpcP.
[240] *Supra*

lo engloba como parte del derecho a la intimidad. Los 10 ministros que votaron unánimemente ignoraron el principio aristotélico de potencia y acto con el que podemos afirmar que los embriones y fetos poseen todos los atributos que tendrán como personas y, por lo tanto, deben ser protegidos por la ley. Y como sostiene John Finnis "para negar la fuerza racional u objetividad de este principio práctico, no es suficiente para los escépticos señalar la diversidad de opiniones morales[241]".

En el derecho norteamericano surge el argumento que el derecho a la privacidad comprende el derecho a decidir sobre abortar o no. El caso es *Roe vs Wade* en que la Suprema Corte dictaminó con una votación 7-2 que la Constitución protege a una mujer embarazada para escoger si abortar o no como parte de su derecho a la privacidad. Aunque este no es un ensayo de protección de la vida del feto, los argumentos de la Corte fueron muy criticados, a saber[242]:

1) tener una vida y un futuro estresado
2) causar daño psicológico
3) cuidar al niño puede causar a la madre alteraciones física o psicológicas.

Si bien limitó a 3 meses la posibilidad de abortar, el fallo recibió muchas críticas con base en los 2 ministros que argumentaron en contra al sostener que el fallo de la Corte rebasaba a la Constitución al dejar de proteger al feto y sostener que no es persona. Afirmamos que hay vida desde la concepción. El 24 de junio de 2022 la Suprema Corte dejó sin efecto este derecho, en el caso *Dobbs v. Jackson Women's Health Organization*, en el que se sostiene que no hay un derecho al aborto en la Constitución de los Estados

[241] Finnis, John. *Natural Law & Natural Rights*, Oxford University Press, 2011, p.73
[242] Chemerinsky Erwin, *Constitutional Law Principles and Policies*, Ed. Wolters Kluwer, NY 2015, p. 1201.

Unidos de América; por lo tanto, la decisión para definir los derechos al aborto o sus restricciones regresan a los estados.

El derecho a la privacidad en la decisión también se protegió en la educación de los hijos como en *Meyer v. Nebraska* en 1923 donde la Suprema Corte declaró inconstitucional una ley estatal que prohibía la enseñanza en la escuela de otro idioma que no fuera el idioma inglés. La Corte dijo:

> "Sin duda, libertad denota no sólo libertad de limitación corporal, sino también el derecho del individuo a dedicarse a cualquier ocupación en la vida, adquirir conocimiento útil, casarse, establecer una casa y criar sus hijos para adorar a Dios de acuerdo los dictados de su propia conciencia …esenciales para buscar la felicidad por los hombres libres[243]".

Si bien la Constitución de los Estados Unidos de América no contiene la palabra privacidad, la Corte se fundamenta en la Novena Enmienda que dice:

"La enumeración en la Constitución de ciertos derechos no ha de interpretarse como que niega o menosprecia otros que retiene el pueblo[244]". Así como en la Decimocuarta Enmienda primera sección que dice:

> Toda persona nacida o naturalizada en los Estados Unidos, y sujeta a su jurisdicción, es ciudadana de los Estados Unidos y del Estado en que resida. Ningún Estado podrá crear o implementar leyes que limiten los privilegios o inmunidades de los ciudadanos de los Estados Unidos; tampoco podrá ningún Estado privar a una persona de su vida, libertad o propiedad, sin un debido proceso legal; ni negar a persona alguna dentro de su jurisdicción la protección legal igualitaria[245].

En EUA, la Suprema Corte de Justicia se ha pronunciado sobre los derechos constitucionales que el individuo tiene en cuanto al derecho a la privacidad. Se protege:

- La detención, búsqueda e inspección ilegal de personas y casas.
- Intervención de medios de comunicación.

[243] *Supra* p. 1176
[244] *Supra* p. 1895
[245] *Supra* p. 1896

- Contaminación de ruido
- Interferencia gubernamental en el ámbito de la decisión personal en cuanto al aborto[246]
- Derecho a morir naturalmente.

En el aspecto de derecho privado, la invasión a la privacidad en EU es considerado un daño (*tort*) en casi todos sus estados. Esto significa que la persona que considere su privacidad invadida puede demandar por daños[247]. La fórmula aceptada parece subjetiva y ambigua. "Aquél que invada la privacidad de otro será sujeto a responsabilidad por el daño resultante a los intereses de la otra parte[248]".

En el *Restatement (second) of torts*, donde se plasman los principios del *Common Law*, encontramos 4 tipos de daño, cada uno ofrece un remedio para su tipo de invasión. El **primero** se dirige al descubrimiento público de hechos privados a través de medios no gubernamentales. El problema aquí es cuando se descubre información cierta, pero privada; el conflicto de intereses se presenta entre la libertad de expresión y la privacidad. El **segundo** protege la intervención de medios de comunicación para invadir el espacio privado. Un **tercero** protege sobre la tergiversación de datos para ofender a una persona. En estas dos figuras, el conflicto es la comercialización de la información privada de celebridades y la privacidad. El amarillismo de algunos periódicos que son capaces de pagar miles de dólares para obtener una fotografía del bebé de una actriz de moda o de una persona de la nobleza en una fiesta. Es un hecho que todas las noticias giran en torno a las personas, mismas que pueden considerar invadida su privacidad al verse en medios.

[246] Aquí observamos la paradoja del Derecho, se desprotege la nueva vida en aras del derecho a la privacidad. Si una Constitución no está hecha para proteger la vida, entonces para qué está hecha.
[247] *Protecting Privacy*: *The Clifford Chance Lectures*. *Op. Cit*. p. 140
[248] *Restatement (Second) of Torts* §§ 652A-E

Entonces la libertad de prensa y la privacidad parecen contrapuestas. La manera más adecuada de apoyar una noticia son las imágenes y videos obtenidos normalmente sin consentimiento del sujeto grabado. El **cuarto** prohíbe la explotación comercial de personas. Aquí podemos encontrar el famoso caso del programa *Big Brother*, patrocinado por la empresa Endemol, donde un cierto número de personas o artistas renuncian totalmente a su privacidad con el objeto de ganar un premio en dinero al evitar ser sacados de la casa con los votos del público, cuyas llamadas tienen un costo en beneficio de Endemol. La cultura de los medios de cada país o lugar pone su presión para vencer a la privacidad. Esto se retroalimenta porque un asunto es resuelto por el gobierno cuando los medios le ponen atención. Las escuelas y la academia no quedan fuera de esto, pues la manera en que despliegan su información en los medios puede hacerles llegar más recursos. Normalmente, los medios toman la información sin compensar a la persona afectada en su privacidad.

3.4. Privacidad en la información

En el derecho a la privacidad, el bien jurídico protegido es nuestra información. Nucci destaca que "los datos personales se han entendido como una prolongación del derecho a la vida privada[249]". Es el ámbito que más trasciende hacia las esferas pública y económica por el uso que los demás hagan de ella. Esta información puede estar en físico o digital, en nuestra oficina o en la *web*; y en este último caso, en nuestro servidor o en ajeno, en nuestro país o el extranjero. El modelo de negocios de las grandes empresas que explotan internet para dar servicios gratuitos como Google, Meta y últimamente TikTok es utilizar nuestra información, perfilarnos, rastrear nuestro compartmiento, nuestras

[249] Nucci, Hilda. *Op. Cit*. p. 77

búsquedas e incluso nuestras conversaciones; todo ello para vender publicidad que nos induzca a la compra de productos o servicios. Recientemente el Tribunal de Apelación de Bruselas[250] dictó una resolución que aborda el perfilamiento algorítmico del llamado *Real Time Biding* o sistema de subastas online para la compra y venta de anuncios a partir de la información recolectada del usuario. En ella, el Tribunal afirma que el consentimiento en el que se basa el RFT por parte de las cuatro grandes empresas tecnológicas que venden publicidad online, a saber: Google, Microsoft, Amazon y X (antes Twitter) no cumple con la legislación de protección de datos de la Unión Europea. Bélgica cuenta con la GBA (Autoridad de Protección de Datos) que argumentó ante el tribunal belga que los datos recogidos con base en la Cadena de de Transparencia y Consentimiento (*TC String*) -que aunque no contenga datos de identificación, al combinarla con otros datos como el IP- se convierten en datos personales. El Tribunal estuvo de acuerdo en que se violan los principios sobre la transparencia, consentimiento, rendición de cuentas y seguridad en el procesamiento de datos personales con fines de publicidad del Reglamento General de Protección de Datos de la comunidad europea (2016)[251].

Alan Westin ha definido a la privacidad en la información como "la petición de individuos, grupos, o instituciones de determinar para sí mismos cómo, cuánto, y hasta qué grado de información acerca de ellos se comunica a otros[252]". Al leer esta definición

[250] Amnistía Internacional España, "Una gran victoria para el derecho a la privacidad en Europa", Amnistía Internacional España, 16 de mayo de 2025, https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/europa-la-resolucion-de-un-tribunal-de-bruselas-sobre-la-publicidad-basada-en-el-seguimiento-una-gran-victoria-para-el-derecho-a-la-privacidad/.
[251] Hof van beroep Brussel, Marktenhof. (2025, 14 de mayo). *Interactive Advertising Bureau Europe IVZW (IAB Europe*) contra *Gegevensbeschermingsautoriteit*, Rolnummer 2022/AR/292 https://www.iccl.ie/wp-content/uploads/2025/05/Arrest-Marktenhof-14-05-2025.pdf
[252] Westin, Alan. *Privacy and Freedom*. *Op. Cit. Part One -The Functions of Privacy and Surveillance in Society, p.* 9*, ebook.*

nos preguntamos si la privacidad es un derecho renunciable, es decir, si el sujeto renuncia a ella, ¿puede ser invadida[253]?

En nuestra vida social, el mundo recolecta información de nosotros; pensemos en una persona que acude a una cita al médico. Desde que sale toma su auto, los otros ven físicamente el tamaño de su auto, calculan para no golpearlo, inclusive en un tope puede voltear a ver al otro conductor que también se detiene. Al llegar al consultorio, estaciona su vehículo y toma un ticket para pagarlo en una máquina a la salida. No obstante, al llegar a la consulta, le pedirán su nombre, incluso si es primera vez le pedirán dirección, teléfono, quién la recomendó, antecedentes médicos familiares, entre otras cosas –ahí hay una recolección de datos, pero que fue una sola en su visita al médico-. En cambio, en el mundo virtual de internet, la excepción se convierte en regla, pues desde que ingresamos a la web todos nuestros datos serán guardados, nuestro IP, el nombre de nuestra computadora, sitios visitados, palabras escritas en el teclado, entre muchos otros datos y microprogramas instalados en nuestra computadora aun sin nuestro consentimiento. Un problema ha sido que la tecnología ha facilitado cada vez más la captura de información del ciudadano común. De hecho, bajo el pretexto de seguridad, muchas empresas han colocado cámaras ocultas para monitorear a sus empleados. Hoy se trabaja en varios países en realizar una base de datos nacional de ciudadanos con huella digital, muestra de DNA, el futuro es la pérdida del anonimato, en cualquier lugar seremos localizados con dispositivos GPS que pueden contener también información médica nuestra en caso de accidente y que puede colocarse vía subcutánea. Además, el almacenaje de información es cada vez más barato y más pequeño.

[253] Como en el caso *Big Brother* o la casa de vidrio en Chile.

Debemos preguntarnos qué sucede a la privacidad cuando toda nuestra información depende de algoritmos.

En 2004, el periódico Iltalehti y su editor en jefe el señor Karhuvaara[254] publicaron varios artículos acerca del juicio acerca del esposo de una miembro del Parlamento Finlandés, ilustrando las notas con detalles relevantes de su vida como su adicción al alcohol. La miembro del parlamento finlandés demandó al periódico y su editor por invasión a su privacidad. El editor fue condenado por invasión a la privacidad con circunstancias agravadas y se le ordenó pagar daños y perjuicios. Éste alegó ante la Corte Europea de Derechos Humanos una violación a su libertad de expresión. Ésta señaló que los límites de crítica son más amplios en los políticos y que la miembro del parlamento finlandés debía tolerar más de la prensa que el ciudadano común; esto, aún cuando el fondo del asunto no tenía que ver con temas políticos o el rol de la miembro del parlamento. Pero la Corte señaló que el derecho del público a ser informado se extiende aún a aspectos de la vida privada de figuras públicas. Asimismo, destacó que los artículos periodísticos no se referían a la miembro del parlamento, sino a su esposo. Ni siquiera hacían mención de la vida privada de la miembro del parlamento, excepto que era esposa del convicto, lo cual era ya del conocimiento general y tampoco encontró falsedades en los hechos que describían o mala fe de los demandados.

En el juicio Lindon, Otchakovsky-Laurens y July vs Francia[255] la Corte Europea de Derechos Humanos sostuvo la condena de la Corte francesa en el juicio de difamación contra y el autor y la casa editorial de una novela llamada *Jean Marie Le Penn en Juicio* -

[254] European Court of Human Rights. "Karhuvaara and Iltalehti v. Finland." Human Rights Guide, 2004. https://www.zmogausteisiugidas.lt/en/case-law/karhuvaara-and-iltalehti-v-finland.
[255] *Global Freedon of Expression*, "Lindon, Otchakovsky-Laurens and July v. France," July 12, 2022, https://globalfreedomofexpression.columbia.edu/cases/lindon-and-others-v-france/.

publicada en agosto de 1998- donde el autor mezcla personajes ficticios con una figura de la vida real: Jean Marie Le Penn y su partido, el Frente Nacional. En el reverso del libro hacía una pregunta: *¿Cómo puede Jean Marie Le Penn ser vencida eficazmente?* Y en las primeras líneas hace otra pregunta más acusadora: *¿Acaso no es el presidente del Frente Nacional responsable del asesinato cometido por uno de sus jóvenes militantes motivado por su retórica*? Inmediatamente el lector sabe la línea crítica de la novela contra la persona Le Penn y su partido. La Corte europea señaló que la condena a 6 extractos de la novela considerados difamatorios no constituía una violación a la libertad de expresión del autor y sí constituía un daño a la imagen de la persona aludida y su partido. Dichos extractos pintaban a Le Penn como la jefa de una pandilla de asesinos que cometen asesinatos raciales inspirados por la ideología del partido derechista, incluso en un extracto es llamada vampira. La CEDH (Corte Europea de Derechos Humanos) reconoció que estaba consciente de la amplitud aplicada a la libertad de expresión en el caso de políticos, pero que dichos extractos sí constituían mala fe del autor. La decisión fue dividida por 13 a 4 votos[256].

En otro caso *Avgi Publishing and Press Agency S.A*. & Karis vs Grecia la Corte Europea de Derechos Humanos resolvió el 5 de junio de 2008 que se habían violado los derechos de libertad de religión, conciencia y pensamiento de los demandados (artículo 9 de la Convención Europea de Derechos Humanos; así como su libertad de expresión (artículo 10 de la misma Convención). Al amparo del artículo 41 de la propia Convención se condenó al pago de 60,000 euros por daño pecuniario.

Los hechos son que el periódico patrocinado por los demandados, así como el griego Constantinos Karis editor del mismo publicaron un artículo referido a un periodista K.V.

[256] *Supra*

que escribía libros políticos e incluso tenía un programa en la televisión local. K.V. eventualmente ganó un puesto en el parlamento griego en 2007 como miembro del partido Alerta Ortodoxa Popular. El artículo periodístico en cuestión mencionaba a K.V. como el organizador de ciertas reuniones contra una decisión de la Autoridad de Protección de Datos en la que dicha autoridad señalaba que destacar la religión de una persona o su carta de identidad era contrario a derecho. En el artículo lo llamaron "loco nacionalista notorio"[257]. Por ello, K.V. demandó al periódico en 2000 y la casa editorial responsable, así como a su editor en jefe. La Corte de Atenas resolvió en 2001 que el artículo no era difamatorio, pero en mayo de 2003 la Corte de Apelaciones de Salonika resolvió que la frase "nacionalista loco notorio" sí era difamatoria y que el objetivo del periodista era mostrar a K.V. como mental y psicológicamente desequilibrado. Ese argumento fue sostenido por la Corte de Casación Griega y condenaron al periódico a pagar 58,000 euros por daños y perjuicios. El periódico y su casa editorial, así como el editor en jefe acudieron a la Corte Europea de Derechos Humanos alegando violación a su libertad de expresión. La corte declaró que la prensa era el perro guardián (*watchdog*) en cualquier sociedad democrática y consideraba que la libertad periodística incluía un poco de exageración o, incluso provocación.

Una antecedente importante para el derecho al respeto a la vida privada y familiar que protege el artículo 8 del Convenio Europeo de Derechos Humanos es el caso López Ostra contra España y de los recursos jurídicos interpuestos ante el municipio, el Estado y finalmente ante el Tribunal Europeo de Derechos Humanos, que emitió sentencia el 9 de diciembre de 1994.

[257] *Editors Human Rights Case Digest*, "*I Avgi Publishing Press Agency S.A. and Karis V. Greece*," Brill (Brill Nijhoff, October 3, 2008), https://brill.com/view/journals/hudi/18/9-10/article-p929.xml.

En julio de 1988 se construye, con financiamiento público, una planta de tratamiento de residuos en Lorca, Murcia, a poca distancia de la casa de la familia de Gregoria López Ostra quien, ante los gases y malos olores comienza con problemas de salud. Dicha planta comienza a funcionar sin licencia y con emisiones de sulfato de hidrógeno fuera de los límites. La Sra. López Ostra acudió al proceso de protección de derechos fundamentales**.** Esta vía fue desestimada por la sentencia de la Audiencia Territorial de Murcia de 31 de enero de 1989, y posteriormente por el Tribunal Supremo mediante sentencia de 27 de julio de 1989. El Ayuntamiento ordena limitar el funcionamiento de la planta a sólo el tratamiento de aguas residuales; los daños a la salud de varias personas, incluyendo la familia de la actora. Finalmente el Ayuntamiento proveyó de medios económicos para reubicar a la familia en el centro de Lorca de octubre de 1992 a febrero de 1993, fecha en que deciden comprar otra casa ante subsistencia de la planta que, finalmente es cerrada el 27 de octubre de 1993 por una denuncia por delito ecológico realizada por la cuñada de la actora. El Tribunal Constitucional declaró inadmisible el recurso de amparo interpuesto, considerándolo manifiestamente infundado. La actora acude el Tribunal Europeo de los Derechos Humanos y argumenta que las autoridades españolas tuvieron una **actitud pasiva** frente a los olores, ruido y humos contaminantes, lo que constituía una violación del Artículo 8 del Convenio Europeo de los Derechos Humanos referido al respeto a la vida privada y familiar de las personas; así como a su domicilio, su alegato fue más allá cuando reclama la violación del Artículo 3 de dicho Convenio referido a la prohibición de someter a una persona a tortura o tratamientos inhumanos o degradantes. El gobierno español se defendió con dos excepciones: una formal, bajo el argumento de que la actora no agotó los recursos internos; el TEDH

desestimó dicha excepción al considerar que la actora interpuso el recurso adecuado ante la Audiencia Territorial de Murcia por ser efectivo y rápido. La segunda excepción fue de fondo al sostener que la actora perdió la condición de víctima al ser reubicada, con cargo al Ayuntamiento, más aún, con la misma clausura definitiva de la planta. El TEDH también consideró sin fundamento dicha excepción al sostener que haber sido obligada a abandonar su hogar por razones medio ambientales sí la hace víctima; en todo caso, la clausura de la planta y el regreso a su hogar puede disminuir el monto de la indeminización. El fondo de la resolución del TEDH protege el derecho a la privacidad que tutela el Artículo 8 de la CEDH al considerar que una grave contaminación del ambiente puede afectar el bienestar del individuo e impedirle disfrutas de su hogar de tal modo que se ataca su vida privada y familiar, aun cuando no ponga en peligro su salud resuelve que las sentencias del Estado español no lograron el equilibrio justo entre los intereses de la persona y de la comunidad y ordenó al Estado español a pagar a la recurrente 4,000,000 (cuatro millones) de pesetas por daños y 1,500,000 (un milln quinentas mil) pesetas, menos 9,700 (nueve mil setecientos) francos franceses a convertir a pesetas al tipo de cambio aplicable en la fecha de pronunciamiento de l asentencia, por costas y gastos.[258]. El último caso que queremos mencionar en este apartado es Moreno Gómez vs. Reino de España en que la Corte Europea de Derechos Humanos da el derecho al silencio a una española que había perdido ante la corte de ese país su apelación que la condenaba porque no había acreditado el daño causado por el ruido generado por las cantinas que habían autorizado las autoridades de Valencia a pesar de que la propia

[258] Tribunal Europeo de Derechos Humanos. (1994, 9 de diciembre). Caso López Ostra vs. España (Demanda núm. 16798/1990), Sentencia Nº 22.

legislación local había reconocido el problema y había señalado como límite los 45 decibelios entre las 22 horas y las 8 horas. La corte europea señaló que el ruido afecta a la vida privada y al derecho a la inviolabilidad del domicilio protegidos por la Convención Europea de Derechos Humanos, dejando sin efecto la sentencia de la Corte Española que argumentaba que las afectaciones eran causadas por negocios particulares y que no se había probado el daño causado por el ruido a la ciudadana española. La corte europea señaló que no puede invertirse la carga de la prueba en el caso de derechos fundamentales. Condenó al Estado español al pago de una indemnización de 8,384 euros.

IV. Privacidad en la era digital

Cuando usamos la expresión privacidad en la era digital. ¿Significa acaso que debemos encriptar nuestra información en nuestra computadora o teléfono inteligente? ¿O acaso que debemos tener un respaldo de toda la información que servidores tienen de nosotros? ¿La información que subimos a las redes es nuestra, está protegida?

En la era digital se tiende a pensar en la privacidad como una recolección de datos para diversos fines y los riesgos que ello envuelve a partir de la facilidad que ofrece la tecnología para recopilar datos. Esta evolución tiene una parte positiva, como poder realizar pagos en línea, hacer pedidos de bienes y servicios tan sólo con acceder a nuestro perfil de cualquier app o sitio web que nos reconozca a través de su tecnología y que incluso nos sugiere productos o servicios con base en lo que hemos comprado. Pero hay una parte negativa, la evolución de la tecnología para invadir la privacidad amenaza seriamente con hacer el concepto obsoleto. La tecnología facilita al gobierno y a empresas privadas o incluso personas como en el caso de los hackers mantenernos en su vista digital, nuestros movimientos, nuestra interacción con otros e incluso de nuestra ideología o estado de ánimo. A esto se le llama la paradoja de la privacidad[259], por un lado nos beneficiamos; por otro, cedemos control sobre nuestra información. Algunos ámbitos incluyen el internet y la recolección de datos, las cámaras que abundan en las calles y comercios, las tecnologías de reconocimiento facial, tecnologías biométricas, rastreo vía GPS, satelital, vigilancia en el trabajo física y digital, y más[260]. La tecnología que nos garantice el anonimato será muy valorada en los siguientes años. Internet nos da

[259] Anglim, Christopher T., *Privacy in the Digital Age*, First Edition, Ed. Grey House Publishing, NY 2015, p. xxi
[260] Véase el artículo Michael Froomkin, "(PDF) the Death of Privacy? ," ResearchGate, 2000, https://www.researchgate.net/publication/228711041_The_Death_of_Privacy.

la apariencia de facilitarnos la comunicación anónima. Como usuarios somos capaces de ingresar a la *web* a través de nuestro servicio de internet y tener interacción en las redes sociales, *blogs*, *chatrooms*; podemos fabricar una personalidad artificial al usar nombres ficticios y no revelar nuestra verdadera identidad. Algunos consideran que el anonimato potencia y democratiza la comunicación, en la web todos somos editores y tenemos la capacidad de atraer seguidores a nuestras ideas. La liberdad de expresión alcanza su mejor versión. Otros, consideran que el anonimato en la web resulta en discursos de odio que desconectan al autor del daño emocional que pueda causar, esto sin dejar a un lado que el anonimato es la máscara de lo ilegal[261]. Es fundamental saber que nada es anónimo en internet, los proveedores del servicio tienen el IP (*internet protocol*) que se compone de cuatro números: el primero es el país, el segundo el proveedor de internet, el tercero es la red y el cuarto es el usuario. Si quieres saber cuál es tu IP accede al sitio https://who.is/. Los proveedores de servicios de internet están obligados a develar la identidad del usuario a través de una orden judicial. Hay 2 formas de hacer más difícil el rastreo:

1. *Networked anonymizers* que transfieren la comunicación del usuarrio a través de una red de servidores antes de llegar a su destino. Éste regresa los resultados de búsqueda a través de la misma intrincación de servidores. De esta manera, se aparenta que el usuario no ha visitado el sitio cuya búsqueda intenta ocultar.

2. *Single Point Anonymizers* es un sitio *web* a través del cual se hace la búsqueda, los resultados regresan al sitio web que encripta la comunicación y la provee al usuario[262].

[261] Anglim, Christopher T., *Privacy in the Digital Age, First Edition*, Ed. Grey House Publishing, NY 2015, p. 15
[262] *Supra* p. 16

La llamada revolución de la información apenas nos da tiempo para comprender sus implicaciones en muchos ámbitos de la sociedad y la vida personal, por supuesto, en la privacidad. Aquellos días donde la información se almacenaba en folders o los llamados diskettes parecen muy lejanos. Hoy toda operación en línea, las tarjetas que almacenamos en nuestra cartera y los teléfonos inteligentes están diseñados para almacenar nuestros datos. La capacidad de almacenar información y el bajo costo que ello implica facilita recolectar datos que pueden ser intrascendentes como los sitios visitados en internet, los productos que nos gustan y los que no, quiénes somos y qué poseemos. Todo esto puede dar lugar a que tengamos nuestra huella digital lo que Solove llama persona digital[263]. Toda la teoría de la privacidad que hemos estudiado en los capítulos previos es muy importante, pero internet ha venido a ser un disruptor en la privacidad y debemos usar este conocimiento en el ámbito digital. A diferencia del libro *Big Brother* de George Orwell que destaca un gobierno totalitario que controla todo a partir de la vigilancia, en la actualidad no sólo es el gobierno quien tiene acceso a nuestros datos. El flujo de nuestra información entre instituciones públicas y privadas, pero sobretodo nuestra ignorancia acerca de dicho flujo y qué se hace con nuestra información es verdaderamente lo que amenaza nuestra privacidad.

El paradigma de la secrecía es roto por la tecnología y somos invadidos en aquello que antes estaba escondido del mundo al hacer accesible nuestra información[264]. El daño que esto causa va desde inhibirnos a entrar a dichas tecnologías, auto censurarnos, y hasta dañar nuestra reputación como en el caso del llamado *cyberbullying*. Sin embargo, para el derecho en general aquello que no es secreto, puede ser público. Hoy es virtualmente

[263] Solove, Daniel. *The Digital Person, Technology and Privacy in the Information Age*, New York University Press, 2004, p.1
[264] *Supra* p. 8

imposible vivir como un fantasma en la era de la información[265]. Debemos repensar el concepto de invasión, en la postura tradicional la privacidad se violaba por una persona en particular y causaba un daño directo a la víctima. En la era digital normalmente no éramos conscientes cuando nuestros datos eran recolectados o transferidos de una empresa a otra hasta que se obligó jurídicamente a las empresas a dar su aviso de privacidad. La biometría es el uso de la unicidad biológica del ser humano para fines de seguridad o sencillamente de autentificación. La huella dactilar, el iris, el adn, la voz, las medidas de esqueletos, y toda una base de datos biométricos se utilizará para diversos fines en la industria o en el estado, sobretodo para evitar ataques terroristas, el peligro es que haya un estado totalitario que use esos datos para represión. Hoy se menciona la posibilidad de incrustar chips en las personas con información biométrica y con capacidad para transmitirla con uso de las tecnologías de información[266]. Los datos biométricos constituyen datos personales porque éstos se definen como cualquier información concerniente a una persona física identificada o identificable[267] y, por ende, deben ser tratados bajo las leyes que protegen nuestra privacidad contra particulares o los llamados sujetos obligados.

El otrora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales conocido como INAI -desaparecido por la llamada reforma de simplificación orgánica aprobada por el senado el 28 de noviembre de 2024 que trasladó sus funciones a la secretaría de la Función Pública, ahora llamada de Anticorrupción y de Buen Gobierno- publicó una guía dirigida a los responsables del manejo de datos

[265] *Supra* p.8
[266] Wacks, Raymond, *Privacy*. *A very short introduction*, Oxford University Press, 2010, p. 11
[267] Tanto en la LFPDPPP Art. 3 fr. V, así como en la LGPDPPSO Art. 3 fr. IX

biométricos de particulares[268]. Esta guía toma como base el Grupo de Trabajo del Artículo 29 de la *European Data Protection Board* [269]. Es importante destacar que un dato biométrico aislado que no pueda ser usado en el sistema tecnológico para asociarlo a una persona particular no constituye un dato personal. Asimismo, los datos biométricos asociados a persona particular que haga identificar las hipótesis de datos sensibles como la salud del paciente -como el caso del iris- o acceso a bienes patrimoniales -como el caso de banca patrimonial- podrán ser considerados sensibles y protegidos por las leyes relativas.

Robo de Identidad. "..el robo de identidad implica la obtención y uso NO autorizado e ilegal de datos personales[270]". El objetivo es asumir la identidad del sujeto particular afectado frente a terceros públicos o privados para beneficiarse con su nombre o identidad. De acuerdo a la CONDUCEF, México se ubica en el 8vo país del mundo y 2do de Latinoamérica con más número de robos de identidad[271]. El robo de identidad no sólo afecta el patrimonio de particular afectado, sino otros fines como su reputación.

Lawrence Lessig llama a internet *the new society*, a la que también llama *cyberspace*, lugar donde investigadores, universidades, inventores y toda la sociedad, buscaron una nueva utopía libertaria más allá de los reyes y presidentes. Nacida del propio departamento de Defensa americano, internet nace de la propia arquitectura de control[272]. Sin embargo, Internet y nuestra actividad en ella nos hace especialmente vulnerables, la

[268] INAI, "Inai – Instituto Nacional De Transparencia, Acceso a La Información y ...," 2018, https://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf
[269] *EDPB, "Grupo De Trabajo Del Artículo 29," Grupo de Trabajo del artículo 29 | European Data Protection Board, 2018, https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es.*
[270] INAI, "Guía Para Prevenir El Robo De Identidad," INAI, accessed March 21, 2023, https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/Guía_Prevenir_RI.pdf Se advierte que tras la extinción del INAI, la información que aloja este sitio web se mantiene como fue publicada por el Instituto hasta el 20 de marzo de 2025, la cual será migrada al sitio de https://transparencia.gob.mx
[271] *Supra*, INAI, "Guía Para Prevenir El Robo De Identidad".
[272] Lessig, Lawrence, *Code* v.2.0 Basic Books, NY 2006, p. 2

artillerría se despliega con *software* malicioso denominado *malware* tales como virus, trojanos, *horses*, *spyware*, *phishing*, *bots*, *zombies*, *bugs*, entre otros[273]. Un virus es un bloque de código que introduce copias de sí mismo en otros programas, normalmente incluye una carga de instrucciones. El más peligroso es un programa denominado *trojan horse* que es capaz de grabar golpes de tecla y enviarlo a su creador. El *spyware* es un software que normalmente llega por correo electrónico y que ejecuta instrucciones para recolectar datos como hábitos de búsqueda en internet, passwords a determinados sitios, entre otros. Imaginemos lo peligroso que puede ser acceder a nuestra cuenta bancaria en un dispositivo que contenga estos virus. El *phishing* llega vía correo electrónico simulando ser de alguna institución confiable con el objeto de generar confianza al receptor de dicho correo para que despliegue información confidencial y ser sujeto de fraude. Algún tipo de malware se instala en tu dispositivo y lo convierte en un *bot* controlado por un tercero eso normalmente sucede en los *torrents* (sitios de piratería de *software*, películas, libros y revistas). Estos *bots* son usados para recolectar correos electrónicos, enviar publicidad *spam*, o incluso montar ataques a corporativos para pedir rescate para liberarlos de dichos *bots*. Los *bugs* son errores de *software* que nos hace vulnerables a ataques de terceros.

Normalmente descuidamos los aspectos de control de nuestra información en las relaciones externas tales como el anonimato en transacciones y el control sobre el *spam* que llega a nuestro correo electrónico.

[273] *Supra* Lessig p. 12

Para comprender la invasión a la privacidad en internet es necesario comprender cómo funciona esa maravilla tecnológica que es internet, más allá de usar sus instrumentos como un correo electrónico, consultas a la *web*, transferencia de archivos, entre otras.

La palabra internet proviene de *interconnected network* –red de computadoras interconectadas-. Nos preguntamos si internet depende de una o varias computadoras en algún lugar del mundo, si alguien puede bajar el *switch* de internet y dejarnos sin acceso a la *web*. Cómo sería nuestra vida sin internet.

La construcción de internet comienza con *intranets,* es decir, grupos de computadoras llamadas *LANs* (*Local Area Networks*) enlazadas en una red local, cada una de estas redes internas son autosuficientes y trabajan con otras redes internas para transmitir la información. Cada universidad, empresa, oficina u hogares tienen sus propias *LANs*. El conjunto de estas *LANs* forma lo que denominamos internet.

Internet, como su nombre lo indica, es una red global de computadoras interconectadas con una infraestructura física como cables de fibra óptica, ruteadores, satélites; así como protocolos desarrollados por diversas organizaciones como el IETF (Internet Engineering Task Force)[274], gobernada por el *Internet Engineering Steering Group* (IESG).

. La *World Wide Web Consortium* (W3C)[275]es un consorcio que desarrolla y estandariza los protocolos de la llamada web, tales como HTML, CSS, XML y HTTP. Otras organizaciones como IETF (*Internet Engineering Task Force*), ICANN (*Internet Corporation for Assigned Names and Numbers*), IEEE (*Institute of Electrical and*

[274] El Consejo de Arquitectura de Internet es auditor tanto del Comité de la *Internet Engineering Task Force* (IETF) y de la *Internet Society* (ISOC). Ver en Posted On and Cindy Morgan, Internet architecture board, May 23, 2016, https://www.iab.org/.
[275] *World Wide Web Consortium., "W3C," W3C, 2022, http://www.w3.org/.*

Electronic Engineers), ISOC (*Internet Society*), entre otras trabajan en conjunto para asegurar el funcionamiento seguro de internet a nivel mundial.

Ahora entendamos la mecánica de internet, cada vez que hacemos una consulta a la web o enviamos un correo electrónico nuestra información se empaqueta en *datagrams*, esto paquetes tendrán una dirección IP, misma que le ayudará a cruzar las redes y llegar a su destino. Este *datagram* al dejar la intranet, un *router* le ayudará a entrar a la gran red regional –que es un conjunto de redes locales-. Ahora el paquete irá a la verdadera carretera de la información denominada *Network Access Point* (NAP) que se asemejan a una estación de trenes donde los *datagrams* o paquetes tomarán el tren adecuado que los acerque a su LAN destino. Estos trenes son denominados *Backbones* que llegan a transmitir hasta a 155 millones de *bits*[276] por segundo. Un elemento esencial de la red de redes es el repeater (repetidor) que fortalece la señal de paquetes que vienen desde muy lejos. En estos cruces o NAPs se facilita la interceptación de datos por parte de proveedores de internet, gobiernos o incluso terceros. Un ejemplo es el caso de Edward Snowden (ex contratista de la Agencia de Seguridad Nacional de Estados Unidos (NSA) que en 2013 filtró documentos sobre la vigilancia masiva del gobierno norteamericano, por supuesto sin consentimiento de los perfilados. Snowden utilizó los NAPs para capturar metadatos (tales como dirección -denominadas IPs- tiempos de conexión y volúmentes gigantes de datos que se usan para construir perfiles algorítmicos y determinar patrones de conducta que construyen huellas digitales únicas para cada persona que accede a internet[277]. Esto puede estar pasando dentro de los algoritmos de

[276] Un *bit* es la abreviación de *binary digit* que es la unidad de dato más pequeña en una computadora. Ocho *bits* equivalen a un *byte*. Un *kbyte* equivale a 1000 *bytes*.
[277] Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books

Google, Meta o TikTok, pero al ser secretos no se pueden sacarlo a la luz. Snowden probó cómo el perfilamiento se puede convertir en vigilancia masiva con todos los riesgos éticos que conlleva (sesgo, privacidad, autonomía).

Un tema aparte son las direcciones de internet y los dominios (*domain names*). Toda computadora, incluidos los servidores[278], tiene una dirección IP (*Internet Protocol*) que son identificadores para repartir la información en internet. La IP no revela la identidad, pero sí la ubicación geográfica. Estos servidores y nuestras propias computadoras están siendo rastreadas por programas específicos transgrediendo nuestro derecho a la privacidad.

4.1. IPs y Perfilamiento Algorítmico

Los algoritmos de perfilamiento usan las direcciones IP como una pieza clave para identificar y rastrear a los usarios, dichos algoritmos permite a las empresas o inclusos autoridades vincular la actividad en línea del sujeto, sitios visitados, guardar un historial de navegación y asociarlo con conductas e interacciones con diversas páginas *web* a una única persona o perfil algorítmico. La segmentación para anuncios se base en dichas direcciones IP[279]. La creación de perfiles de usuario combinan los IPs con cookies, historiales de búsqueda, hábitos de consumo y preferencias respecto al momento de adquisición o tipos de anuncios que detonen la compra.

La problemática de identificar y memorizar sitios a través de números fue resuelta por una de las grandes compañías de tecnología Sun Microsystems al crear el *Domain System*

[278] Recordemos que el término servidor se utiliza para una computadora en una red que maneja información y responde a las peticiones de información desde la red. También denomina los programas que se usan para tal efecto.
[279] Leick, Alfred, *etal. GPS satellite surveying* / 4th *Edition*. Wisley, USA 2015

Name (DNS) a los principios de los 80's, en dicho sistema dos números son separados por el símbolo @ que significa en (*at*) por ejemplo en rmeneses @up.edu.mx rmeneses es el usuario, up.edu es el *hostname* y mx es el *domain name*. El *hostname* identifica al servidor de la organización que hospeda toda la información. El *domain name* es mucho más amplio[280]. En general los dominios utilizados son *.com* (empresas comerciales), .biz (negocios), *.info* (información), *.gov* (gobierno de EUA), *.org* (organizaciones no lucrativas), *.net* (*networks*), y las iniciales de los países con excepción de EUA por haber sido el país creador de internet[281]. Paradójicamente la extensión .eu se usará para la Unión Europea (*european union*).

Eso sucede en los correos electrónicos, lo mismo sucede en las direcciones de internet (*Uniform Resource Locator –URL*) que escribimos y las que deben llegar al sitio-servidor requerido que nos enviará un paquete de información. Aquí se traducirá el URL a un IP requerido formado por los cuatro números ya mencionados. Esto se lleva a cabo en pocos segundos.

Esta explicación ha sido necesaria para entender precisamente como en ese trayecto que recorre nuestra información y la información que nos es enviada pueden ocurrir invasiones a la privacidad, así como la apropiación de nuestra información por terceros que desconocemos.

También la tecnología dota de instrumentos para prevenir los ataques de terceros, uno de ellos el *firewall* que denomina un conjunto de programas que protegen las redes de ataques de intrusos a través de dos instrumentos específicos: 1. Al bloquear el ingreso de

[280] Incluso el buscador Google ofrece búsqueda específica a través de domain names. Al escribir en la caja de búsqueda la palabra site:mx arrojará el número de sitios con el dominio mx. Es decir, ubicados en México.
[281] Véase *Domain*. "*Every Successful Business Needs a Strong Online Presence*." Accessed March 21, 2023. http://www.101domain.com/. Sitio que provee dominios por país o área de interés.

paquetes no deseados y 2. Autorizar los paquetes de información que, conforme a su programación, son apropiados.

El impacto de internet en la vida actual hace que se descubra la vida privada de muchas personas en sitios como *youtube.com* u otros. En el derecho norteamericano cuando hay un conflicto de intereses con la privacidad, normalmente es la privacidad la que se sacrifica y cuando gana, es por el impacto comercial que pudiera tener tal invasión.

4.2. Cookies o rastreo en línea

La facilidad de consulta en internet se basa en una tecnología tan inteligente como simplista. En realidad, descubriremos que la tecnología que más facilita el rastreo es en realidad una tecnología necesaria para el funcionamiento adecuado de la red de redes. Hemos analizado que al dar clic a un enlace en internet es enviar una petición de información a una dirección específica (IP) para ello se usa un navegador[282] el cual facilita la visita a sitios que devolverán la interfase requerida con un clic. Lawrence Lessig[283] señala

> "El ciberespacio presenta algo nuevo para aquellos que piensan sobre regulación y libertad. Demanda un nuevo entendimiento de cómo trabaja la regulación y de lo que verdaderamente regula la vida ahí. Nos obliga a ver más allá del ámbito que el abogado tradicional ve -más allá de leyes, regulaciones y normas".

La riqueza de internet comenzó siendo precisamente la falta de regulación y límites a la circulación de información que constituyó el medio de comunicación más poderoso de la historia de la humanidad. Precisamente esta falta de regulación impulsó la creación de la tecnología para facilitar el uso de internet.

[282] El navegador más común es Google Chrome, pero existen muchos otros tales como Safari, Mozilla, Opera, Firefox.
[283] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999) pag. 6

Cuando una persona entra a internet, lo hace a través de un navegador que como configuración predeterminada acepta un tipo de *software* pequeño denominado cookie que consiste en archivos de texto (cuyo tamaño oscila entre 50 y 150 *bytes* o hasta un máximo de 4kb). El navegador baja estos archivos ubicados en el sitio web que visitamos y son salvados en una carpeta de nuestro disco duro, incluso cuando después de salir de internet y apagar nuestra computadora. El objetivo de estos archivos es que cuando abrimos una nueva ventana el sitio nos siga identificando como el receptor de su información; esto es esencial en servicios a los que nos suscribimos, ya que al introducir nuestra contraseña la *cookie* informa al sitio que somos nosotros los que navegaremos en el sitio *web*[284]. Sin embargo, desde el punto de vista de la privacidad, estos archivos tienen la posibilidad de escribir en el disco duro del usuario –muchas veces sin saberlo. Además, en cada visita al sitio, nuestro URL (dirección en internet) es almacenada en un servidor para conocer la frecuencia y el interés del usuario en el sitio; más aún, si hice una consulta en un servidor, dicha consulta es almacenada y relacionada a mi URL. Esta información incluye el día y hora de la visita. La tecnología *cookie* es originalmente para el beneficio del usuario al facilitar su navegación en el sitio, sus preferencias, su historial, sus consultas y hasta sus comentarios. Jerry Kang explica:

> Una *cookie* es una pieza de información enviada por el servidor a la computadora, teléfono o tableta del cliente para almacenar información y personalizar la experiencia de búsqueda. Por ejemplo, varios servidores de la *web* proveen listados de películas de acuerdo con el código postal. Debido a que es ineficiente pedir al usuario volver a ingresar su código postal en cada visita, el servidor salva el código postal y otra información en el disco duro del cliente en la forma de una *cookie*[285].

[284] Quijano*, Op. Cit*., p. 36
[285] Kang, Jerry. *Information Privacy in Cyberspace Transactions*, Stanford Law Review, vol. 50: pp. 1193 a 1227.

El verdadero problema es que toda esta información no es visible al usuario, queda sólo en la parte del servidor, quien podrá utilizar esta información a su conveniencia y ética. Sandra Davidson de la Universidad de Missouri las llama "migajas de *software* almacenadas en la computadora del visitante de un sitio *web*. El sitio *web* provee la *cookie*, y el navegador del visitante instala la *cookie* en el disco duro del visitante. La *cookie* permite al operador del sitio web rastrear los movimientos del visitante en el sitio *web* del operador[286]". Las *cookies* se alimentarán del sitio web con información del usuario hasta crear su perfil. Éstas son llamadas *cookies* de primera parte o benignas para recordar las preferencias del usuario y facilitarle la experiencia de navegación, versus las llamas cookies de terceros, colocadas por empresas para rastrear, almacenar y vender información de hábitos de navegación de usuarios, por supuesto, sin su consentimiento[287]. También podemos clasificar las *cookies* en temporales y permanentes. Las primeras sólo permanecen en el sitio duro durante la sesión; las segundas permanecen aún después de apagada la computadora.

4.3. Las cookies ¿son buenas o malas?

Las cookies no tienen naturaleza negativa *per se*. En realidad, su primer uso fue siempre positivo; algunas ventajas son: a) Almacena *passwords* y nombres de usuarios; b) Elimina la necesidad de volver a proporcionar datos al navegador en un sitio; c) Almacena información sobre preferencias del usuario[288]. Somos las personas los que les ponemos cierta maldad a la naturaleza de las cookies al almacenar información que

[286] Davidson, Sandra. Capítulo 14 *Cyber-Cookies: How Much Should The Public Swallow? Advertising and the World Wide Web*, ed. David W. Schumann and Esther Thorson (Mahwah, NJ: Lawrence Erlbaum Associates, 1999) 219.
[287] Hu, X., Sastry, N.R., & Mondal, M. (2021). CCCC: Corralling Cookies into Categories with CookieMonster. *Proceedings of the 13th ACM Web Science Conference 2021*.
[288] *Op. Cit*. Davidson, Sandra, p. 220

conviene al administrador del sitio web al seguir los movimientos del usuario en la web y determinarle un perfil de ventas.

Las *cookies* pueden presentar varias complicaciones al derecho a la privacidad. Como usuarios frecuentemente proporcionamos información confidencial, tales como teléfonos, correos electrónicos y, en ocasiones, hasta direcciones. Todo esto puede ser almacenado en una *cookie*[289]. El límite para invadir nuestra privacidad lo ponen los técnicos y la cultura que el usuario tenga para protegerse de ellas.

En el espacio virtual, los usuarios creen estar en el anonimato, cuando en realidad sus clics son rastreados por infinidad de genios informáticos con el objetivo de sacar provecho a dicha información. Este problema se incrementa con la mayor demanda de comercio electrónico, que va más allá de una simple compra. Almacena la información, los sitios visitados previamente, cuántos clics tardó en realizar la compra, cuáles sitios comparó, entre otras cosas que ayuda a determinar el perfil de un comprador potencial.

Doubleclick es una empresa americana que se especializa en mercadotecnia digital y cuyas cookies se especializan en asignar un identificador único a cada usuario y rastrear sus clics en la web. "Se trata de entregar el mensaje correcto al cliente correcto en el tiempo correcto" dijo Kevin O'Connor[290], Presidente de DoubleClick. Dicha empresa adquirió Abacus[291] que ofrecía un manejo de los datos de clientes que compren en nuestros sitios. Hoy mantienen datos de miles de millones de transacciones. Su tecnología

[289] *Supra*. p. 221
[290] Véase Paul M. Schwartz, "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy and Fair Information Practices," *SSRN Electronic Journal*, 2001, https://doi.org/10.2139/ssrn.254849, p. 773
[291] CNET, "DoubleClick, Abacus Merge in $1.7 Billion Deal," CNET (CNET, January 3, 2002), https://www.cnet.com/tech/services-and-software/doubleclick-abacus-merge-in-1-7-billion-deal/.

denominada DART tiene la capacidad de dirigir *banners*[292] específicos a visitantes cuyo perfil sea idóneo a la publicidad. Jason Catlett[293] presidente de una organización no lucrativa que protege la privacidad denominada JunkBusters afirmó que "esto es potencialmente el fin del anonimato en internet", Catlett y otros promotores de la privacidad amenazaron con pedir a la Comisión Federal de Comercio americana que vigile esta combinación. Ante ello, Kevin Ryan presidente de DoubleClick aseguró que los usuarios serán informados y podrán eliminar la cookie. Parece ser insuficiente en un mundo donde el usuario tiene prisa por navegar y poco tiempo para leer las letras pequeñas. Finalmente, Google adquirió DoubleClick en 2007 por 3,100 millones de dólares[294], el doble de lo que pagó por YouTube un año antes. La visión de Google y la publicidad digital anticipaba lo que sucedió en 2019: 130,000 millones de dólares gastados en publicidad digital del total de 240,000 millones en publicidad total en EUA.[295]

Debemos dar crédito al inventor de las cookies: Louis J. Montulli[296] quien además inventó uno de los primeros navegadores denominado Lynx (1991) y luego contribuyó a crear el esquema de *cookies* en Netscape (1994). Este invento ha dado paso a que muy pronto haya un software capaz de invadir nuestro disco duro y transmitir datos a partir de él, sin percibirlo.

---

[292] Baron, David P., *DoubleClick and Internet Privacy*, Graduate School of Business, Stanford, Case number P-32, August 2000, p. 5. https://www.gsb.stanford.edu/gsb-box/route-download/353221 Consultado el 17 de febrero de 2023.
[293] *Supra*, p. 5
[294] Louise Story and Miguel Helft, "Google Buys DoubleClick for $3.1 Billion," The New York Times (The New York Times, April 14, 2007), https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html.
[295] Tony Yiu, "Why Did Google Buy Doubleclick?," Medium (Towards Data Science, May 6, 2020), https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.
[296] Norman Jeremy, *Louis Montulli II Invents the HTTP Cookie : History of Information,* 1996, https://www.historyofinformation.com/detail.php?id=2102.

4.4. Segmentación Algorítmica

Hoy la tecnología digital permite establecer correlaciones de datos entre bases que pueden ser utilizadas para identificar o representar un sujeto humano o no humano (individual o grupal) y/o la aplicación de perfiles -es decir, conjuntos de datos relacionados para personalizar y representar a un sujeto o identificarlo como miembro de un grupo o categoría, esto es el perfilamiento[297].

El doctor Guillermo Tenorio reconoce la necesidad de la tecnología en nuestra vida, pero hace la reflexión hacia una vida libre de algoritmos que violen nuestros derechos humanos al invadir nuestra privacidad[298]. Menciona el sistema de decisión automatizado que Canadá instrumentó en 2013 para manejar cientos de miles de solicitudes de migración al país y el impacto que éste tuvo en una posible violación de derechos humanos al reemplazar a las personas del gobierno que pudieran tener una visión más amplia como la migración por peligro a la vida de los solicitantes[299]. La Universidad de Toronto publicó un estudio completo acerca de estos algoritmos que el gobierno de Canadá ha establecido como un análisis predictivo de las decisiones a tomar en el ámbito administrativo. El estudio liderado por Petra Molnar recomienda que el gobierno canadiense publique todos los sistemas de decisión automatizada relacionados con la inmigración y refugiados al probarse, después de un análisis minucioso, la violación de derechos humanos como el derecho a la no discriminación, derecho a la igualdad,

[297] Hildebrandt, Mireille. *Profiling the European Citizen*, Ed. Springer, 2008, p. 19
[298] Tenorio Cueto, Guillermo Antonio. (2021). *El derecho a una vida libre de algoritmos*. Revista IUS, 15(48), 115-135. Epub 14 de marzo de 2022.https://doi.org/10.35487/rius.v15i48.2021.708
[299] *Supra*

derecho la libertad de movimiento, derecho a la libertad de expresión, religión y asociación, derecho a la privacidad, a la vida, la libertad y la seguridad de las personas[300]. Los algoritmos son entendidos como procedimientos codificados[301] o como una serie lógica de pasos para organizar y actuar sobre un cuerpo de datos y conseguir el resultado deseado rápidamente[302]. Vivimos rodeados de ellos, en el aspecto de negocios, Spotify, Waze, Netflix, Amazon, entre muchos otros nos hacen la vida más fácil. En el ámbito público, varios gobiernos han usados las grandes bases de datos para mejorar su toma de decisiones, su sistema de salud (*Event and Pattern Detection Lab* -India, Sri Lanka), disminuir la corrupción, mejorar la seguridad (*Crime Radar* en Brasil), la impartición de justicia o la educación (Microsoft-Andhra Pradesh State -India)[303]. Hacia el 28 aniversario del nacimiento de la *World Wide Web*, su creador Tim Bernard Lee, previno acerca de 3 grandes riesgos en que la WWW ha resultado: 1. Hemos perdido control de nuestros datos que rondan en la *web*. 2. La desinformación se esparce muy fácilmente. 3. Necesitamos más transparencia y entendimiento de la publicidad política digital[304]. Claramente el primer riesgo que vislumbró Bernard-Lee fue la invasión a la privacidad por las tecnologías digitales. Gillespie[305] habla de los algoritmos de relevancia pública e identifica seis: 1. Patrones de inclusión. Al ser los algoritmos inertes toman significado cuando son cruzados con bases de datos, es decir, son dos conceptos separados, la base de

[300] Molnar, Petra y Gill, Lex. *Bots at the Gate. A human-rights analysis of automated decision-making systems in Canada´s immigration and refugee systems*. Citizen Lab, University of Toronto, 2018. Disponible en: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf , última fecha de consulta el 24 de septiembre de 2022.
[301] Gillespie. Tallerton. *The Relevance of Algorithms, Media Technologies: Essays on Communication, materiality and society,* Cambridge, Massachusetts, MIT Press, 2014, p. 167
[302] *Supra*
[303] Sangokoya, David, *Data-Pop Alliance, Algorithmic Accountability*, *World Wide Web Foundation*, 2017, p.7
[304] *Supra*, p. 3
[305] *Op. Cit*. p. 168

datos y el algoritmo; ambos, normalmente son usados por una sola entidad o persona que tiene un interés económico o político; por ello, debe ahondarse en un estudio sociológico. El ejemplo es Google Maps que fotografía una calle determinada al considerarla pública, pero que puede molestar a quien vive en dicha calle. 2. Ciclos de Anticipación como los algoritmos de búsqueda que pueden arrojar distintos resultados ante la misma búsqueda cuando es hecha por diferentes usuarios con diversos hábitos de internet. Zimmer[306] afirma que los buscadores aspiran no sólo a indexar la web sino a recordar todo lo posible acerca del usuario, con el complemento de sus perfiles sociales, geolocalización, clics a enlaces, plataforma usada, amigos, hábitos de búsqueda. 3. La evaluación de relevancia, como al usar Netflix o Amazon que nos recomienda productos que podemos consumir con base en nuestras elecciones previas. Google confiesa tener más de 200 criterios para identificar el resultado más relevante a cierta búsqueda[307]. 4. La promesa de la objetividad algorítmica. Gillespie[308] los llama estabilizadores de la confianza, y tiene razón, ya que si hacemos una búsqueda en Google damos por hecho que el primer resultado natural -es decir, no promovido por anuncios- debe ser el más idóneo y objetivo a nuestra necesidad de información; sin tomar en cuenta que detrás puede haber un interés económico. 5. Entrelazamiento con práctica, aquí el algoritmo se desarrolla con base en criterios puestos con cierta intención de los usuarios como los *hashtags* que, en ocasiones, se usan para ser encontrados por el algoritmos -como en Twitter-. En el caso de Napster los usuarios colocaban los nombres de artistas incorrectamente para que la industria discográfica no los encontrará, pero sí los usuarios que querían bajar dicha música. Toda la industria del SEO - *Search Engine Optimization* - surge a partir de este

[306] Aludido por Gillespie, *Op. Cit.* p. 173
[307] *Supra* p. 175
[308] *Supra* p. 179

entrelazamiento y que los productores de contenido intentan empatar para salir en los primeros lugares de las búsquedas importantes para su industria. 6. La producción de los públicos calculados. En este caso, los algoritmos tienden a ordena el caos de información que existe en internet y agrupar públicos que pueden estar interesado en diversos tópicos. Así lo hace Google, Facebook y Twitter[309].

En el Reglamento de Protección de Datos de la Unión Europea o GDPR, en su recital 30 habla de los identificadores en línea para perfilar e identificar usuarios y describe:

> las personas naturales pueden ser asociadas a identificadores en línea provistos por sus aparatos, aplicaciones, herramientas y protocolos, tales como las direcciones *IP*, *cookies* u otros identificadores como etiquetas de radio frecuencia. Esto puede dejar huellas digitales, sobre todo al combinarse con identificadores únicos y otra información recibida por los servidores, todo lo cual puede ser usada para crear perfiles de las personas naturales e identificarlas[310].

Y el recital 38[311] del GDPR ofrece una protección específica para los niños que no son siquiera conscientes de que sus datos personales pueden ser usados para perfilamiento con efectos de venta. El propio reglamento exige el principio de transparencia en el recital 60[312] para informar al interesado la forma y los fines del tratamiento de sus datos, así como la elaboración de perfiles con sus datos. El recital 70[313] del mismo Reglamento da el derecho de oposición al interesado para oponerse al uso de sus datos para perfiles con fines de mercadotecnia.

---

[309] Birbak, Andreas, *etal*. *The Public and its Algorithms*, MIT Press, USA 2015, p. 23
[310] El Reglamento de Protección de Datos de la Unión Europea se compone de 173 Recitales y 99 Artículos. Los recitales proveen información adicional y contexto que es complementario a los artículos. Aquí el Recital 30: GDPR.eu, "Recital 30 - Online Identifiers for Profiling and Identification," GDPR.eu, July 23, 2020, https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/.
[311] *Supra* Recital 38 Reglamento de Protección de Datos de la Unión Europea
[312] *Supra* Recital 60 Reglamento de Protección de Datos de la Comunidad Europea
[313] *Supra* Recital 70 Reglamento de Protección de Datos de la Comunidad Europea

Hildebrandt[314] señala que perfilar implica el uso de un conjunto de tecnologías que comparten una misma característica: el uso de algoritmos u otras técnicas para crear, descubrir o construir conocimiento a partir de un conjunto masivo de datos. La práctica de perfilamiento se usa en diferentes ámbitos sociales con el objetivo de reconocer patrones desde la investigación criminal hasta el *marketing*, pero también en la ingeniería como en la cadena de suministro a través de la tecnología de etiquetado *RFID*. La elaboración de perfiles tiene por objeto la toma de decisiones, muchas veces automatizada, a partir de la comunicación de servidor a servidor. El perfilamiento usa un método inductivo porque se basa en las conductas pasadas de los usuarios en la *web*. Hildebrandt[315] menciona 3 elementos para el perfilamiento: a) el sujeto de los datos, uno o varios individuos, humanos o no; por ejemplo: mujeres de ojos azules y su predisposición al cáncer de seno b) el sujeto es el individuo humano o no del que se obtienen los datos para elaborar perfiles c) el controlador de los datos, entendido como la organización o persona que señala los propósitos del perfilamiento. El perfilamiento puede ser positivo en términos de prevención médica o individualización de ofertas en el mercado. Guillermo Tenorio[316] habla de 3 tipos de análisis a partir del perfilamiento: a) análisis descriptivo que consiste en acumular datos y visualizarlos de tal forma que puedan aportar datos acerca del comportamiento de una institución pública o privada. Este tipo de análisis difícilmente viola algún derecho humano. Un ejemplo de ello es el sitio llamado Google *Trends*; b) análisis predictivo se refiere a que usa algoritmos para aportar información que a simple vista no se identifica y que resulta del análisis de los datos, un ejemplo puede ser predecir valores o comportamientos futuros y aquí puede

[314] Hildebrandt, Mireille. *Profiling the European Citizen*, Ed. Springer, 2008, p. 17
[315] *Supra*, p. 19
[316] *Opus cit.,* p. 130

haber alguna violación a los derechos humanos de las personas al usar sus datos para predecir sus comportamientos e inducirlos a comportarse de una u otra manera. Un ejemplo de análisis predictivo fue el uso de Cambridge Anaytica para promover el voto a favor de un partido político en las elecciones presidenciales de EUA; por último c) el análisis prescriptivo es el más avanzado de los análisis pues recomienda a partir de los anteriores análisis acciones a tomar para la optimización de resultados. Esa prescripción puede consistir en recomendar dar o no dar un permiso de entrada a algún extranjero o recomendar un producto en términos de mercadotecnia.

En conclusión, hoy el mercado y el gobierno pretenden tener la suficiente justificación para invadir nuestra privacidad en internet, existe la tecnología para almacenar nuestros datos, combinarlos, crear perfiles, venderlos, procesarlos de manera eficaz; en suma, crearles valor, la pregunta es ¿valor? ¿para quién?. Tenorio, a partir del principio *pro homine*, recomienda conminar al Estado a respetar el principio de autodeterminación informativa y otorgar protección constitucional a todas aquellas personas que no desearan ser parte de estos algoritmos que relacionan sus datos con otros para la creación de perfiles[317]. Destaca también el derecho que tenemos al olvido digital cuando se trata de nuestros datos. Esto se regula en el Reglamento Europeo de Protección de Datos Personales en el Recital 59 que recomienda instrumentos que permitan a la persona acceder, rectificar y oponerse a la recolección de datos o pedir la supresión de los mismo[318].

[317] *Supra* p. 132
[318] Se puede consultar en EUR-lex, "Lex - 32016R0679 - En - EUR-Lex," EUR, 2016, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679.

4.5. Derecho a la vida privada ante una sentencia judicial

Cifuentes afirma que la privacidad es un valor esencial y constitutivo de la persona al integrarse como un elemento propio de su identidad y su esfera moral. La construcción y desarrollo de la personalidad psicológica sólo se podrá alcanzar cuando la persona tiene la capacidad de preservar determinados aspectos, circunstancias y experiencias de su vida fuera del escrutinio del entorno social[319]. Tenorio aborda el derecho a la información y su relación con el espacio público, critica la concentración de medios informativos y la que llama justicia mediática a grado tal que los comunicadores asumen roles judiciales con afectación al honor y la reputación[320]. Existe una línea muy tenue entre el derecho a la privacidad y el derecho a la información en un estado democrático como el mexicano. El derecho a la vida privada se regula en el primer párrafo del artículo 16 de nuestra Constitución Política; la protección de datos personales y los derechos ARCO -acceso, rectificación, corrección y oposición- en el segundo que también ordena a la ley secundaria establecer los supuestos de excepción a dichos principios, "… por razón de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."[321]. Sin embargo, nuestro artículo 6to. Constitucional que regula la libertad de expresión y el derecho a la información dispone que toda la información de los poderes ejecutivo, legislativo y judicial, así como de órganos autónomos, partidos políticos y fondos públicos, así como de toda persona que reciba o disponga de recursos del estado será información pública[322]. La pregunta que debemos

[319] Aludido por Quijano, Carmen. Derecho a la Privacidad en Internet, Colección Tirant 4.0, CDMX 2022, p. 54.
[320] Tenorio, Guillermo. El Derecho a la Información, Ed. Porrúa, CDMX México, 2009, p. 39.
[321] Artículo 16 de la *Constitución De Los Estados Unidos Mexicanos: Expedida Por El Congreso General Constituyente El Día 5 De Febrero De 1857 Con Sus Adiciones y Reformas: Leyes orgánicas Y Reglamentarias: Texto Vigente De La constitución* (México, CDMX: Gobierno Federal, 1905).
[322] Artículo 6to, Apartado A, fracción I de la Constitución Política de los Estados Unidos Mexicanos.

hacer es hasta dónde llegan los alcances del derecho a la vida privada cuando se ha cumplido alguna sentencia. La fracción II del mismo apartado A del artículo 6to constitucional señala que "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes"[323]. También el Reglamento para la Protección de Datos de la Unión Europea regula en sus recitales 65 y 66, así como en su artículo 17 al establecer en su apartado 1, el derecho a ser borrado vía la petición a las organizaciones para borrar datos personales con seis requisitos: 1. Que los datos personales ya no sean necesarios para el fin que fueron recolectados. 2. Que se retire, por parte del titular de los datos, el consentimiento para su tratamiento. 3. Que el interesado se oponga al tratamiento de sus datos sin haber motivos legítimos para hacerlo. 4. Que sus datos hayan sido usados ilícitamente. 5. Los datos personales deben suprimirse inmediatamente con base en el derecho de los estados miembros. 6. Que los datos personales del titular hayan sido obtenidos con oferta de servicios. Pero el propio artículo 17 en su apartado 3 señala que los datos personales no serán borrados cuando su uso sea necesario por: 1. Ejercer el derecho a la información o libertad de expresión 2. Por disposición legal de acuerdo al derecho de la Unión. 3. Por razones de salud pública por interés público 4. Por tener fines de interés público, de archivo histórico, investigación científica y 5. Cuando dichos datos personales sean necesarios para el ejercicio de reclamaciones[324].

El grupo más vulnerable a esta actividad son la gente pública; a saber, políticos, empresarios, artistas, deportistas, quienes se vuelven vulnerables ante medios sin

[323] *Supra*, apartado A, fracción II.
[324] Nicholas Vollmer, "Artículo 17 UE Reglamento General De Protección De Datos," Artículo 17 UE Reglamento general de protección de datos. *Privacy/Privazy according to plan*. (SecureDataService, August 22, 2022), https://www.privacy-regulation.eu/es/17.htm.

escrúpulos capaces incluso de comprar noticias que invaden la privacidad. Existen dos casos famosos, la persecución de Ralph Nader por General Motors en 1965 ante la publicación de su libro *Unsafe at any speed* donde demostró la inseguridad de Corvair un auto fabricado por General Motors. GM contrató detectives privados para investigar su vida privada y chantajearlo; intervinieron su teléfono, contrataron mujeres para seducirlo, entre otras cosas que invadían su privacidad. Nader demandó y llegó a un arreglo con GM para que se disculpara y le pagara $ 284,000 dólares[325].

4.6. Privacidad o Seguridad Nacional

Incluso antes de los atentados del 11 de septiembre del 2001, el gobierno americano sugirió al Congreso se autorizaran varias leyes para reforzar la seguridad nacional. Una de ellas fue la *Cyberspace Electronic Security Act Bill* del 4 de agosto de 1999 donde se sugería usar la tecnología *back door*[326] que se define como un hueco en la seguridad de un sistema o de un software con el objetivo de que el gobierno americano pudiera rastrear cualquier golpe de tecla, *passwords* y archivos encriptados. Nunca floreció por protestas de grupos de libertades civiles.

Hacia octubre del 2000 se dio un caso que marcó el camino de la privacidad en Estados Unidos: Kyllo vs. USA donde la policía sospechaba que en la casa de Kyllo se sembraba marihuana y los agentes usaron un aparato de imagen térmica para determinar si la cantidad de calor emanada se parecía a las lámparas de alta intensidad usadas típicamente para el cultivo de marihuana en interiores. El aparato arrojó que el garaje de Kyllo estaba

[325] Lexis Nexis, "Nader v. General Motors Corp. - 25 N.y.2d 560, 307 N.y.s.2d 647, 255 N.e.2d 765 (1970)," Community, visitado Marzo 21, 2023, https://www.lexisnexis.com/community/casebrief/p/casebrief-nader-v-general-motors-corp.
[326] Véase FOLDOC, "*Online AI Legal Research Tools: Lexis+,"* LexisNexis, 1995, https://www.lexisnexis.com/en-us/products/lexis-plus.page.

más caliente que el resto de la casa y casas circundantes. A partir de esta prueba un Juez Federal otorgó una orden de cateo en la casa de Kyllo, donde los agentes efectivamente encontraron cultivo de marihuana. Kyllo fue acusado con cargos federales por cultivo de droga, inútilmente trató de eliminar la prueba tomada con dicho aparato sobre su garaje y no tuvo otra opción que aceptar una culpabilidad condicionada. El Noveno Circuito afirmó basado en la evidencia térmica que Kyllo no había mostrado expectativa de privacidad al no haber intentado esconder el calor que escapaba de su garaje. Y aún si lo hubiese hecho, dijo la corte, no había expectativa razonada de privacidad porque el detector térmico no exponía detalles íntimos de la vida de Kyllo, sino sólo puntos calientes en el exterior de su casa. Además, en algunos casos antecedentes se había aprobado el vigilar una casa en su exterior.[327]Asimismo, se ha sostenido que lo que una persona no cuida como privado no es garantizado por el derecho a la privacidad. Aquí podemos discutir el tema de si el bien protegido es público o privado, al ser público aún cuando la persona no lo protegiese sería considerado un bien a proteger por la Constitución y el Derecho. Es claro que la Cuarta Enmienda norteamericana protege la privacidad como un derecho privado. En el caso, el calor hubiera sido notorio incluso por vecinos sensibles al mismo. Se sostuvo en el caso que las ondas de calor, al igual que los olores generados en una cocina o en un laboratorio pasan a ser del dominio público. El pensar que quieren conservarse como privados pasa a ser no razonable. Se señala que las inferencias a las que los policías llegaron fueron indirectas, derivadas de su observación y sospechas previas. Tan indirectas como pudieron haberlo hecho a partir del análisis de la basura de la propia casa de Kyllo. Este caso dejó un precedente claro sobretodo para las tecnologías por venir, incluido el internet con *surveillance* cámaras. El principio dice:

[327] "California v. Ciraolo." Oyez. Accessed March 21, 2023. https://www.oyez.org/cases/1985/84-1513.

"No se instituirá un impedimento constitucional –a partir de la Cuarta Enmienda norteamericana- a las nuevas tecnologías a menos que provea al usuario información con el equivalente funcional de presencia real en el área inspeccionada"[328].

Ante el nuevo principio nos preguntamos qué pasará cuando la tecnología proporcione imágenes del interior de las casas con un simple aparato disponible a cualquier persona; al igual que ha sucedido con las grabadoras de voz. Esto implica que las amenazas a la privacidad continuarán proporcionalmente al desarrollo de las nuevas tecnologías. La regla es sumamente amplia, podemos pensar en aparatos que sustituyan el olfato de los perros entrenados para detectar droga. Nos preguntamos qué sucedería si dicho aparato detectara sustancias destinadas a hacer explosivos y que no fueran detectables al exterior por ningún tipo de aparato normal. Claramente los límites del principio de la Corte quedarían poco claros. Podría haber ministros que señalaran que si el olor es detectado desde el exterior –aún por máquinas avanzadas- se ha obtenido de manera constitucional.

El caso Kyllo vs USA, Danny Kyllo sospechoso de sembrar mariguana es detectado por un agente usando monitoreo térmico para identificar a Kyllo a través de las paredes, así como las lámparas para sembrar la droga en interiores; el caso fue 5-4 a favor de Kyllo.

El viejo aforismo "el hecho siempre antecede al derecho" se torna en "la tecnología siempre antecede al derecho". Es decir, la tecnología nos permite hacer cosas que el derecho no ha alcanzado a regular.

4.7. Nuevas tecnologías que amenazan la privacidad

Es frecuente escuchar que al vivir en este mundo tecnológico debemos estar dispuestos a renunciar en cierta manera a nuestra privacidad[329]. Los bienes a cambio, la rapidez de la

[328] *Supra* p. 7

información, el pago en línea, la consulta de nuestra propia información en cualquier momento parece valer la pena. Sin embargo, tal afirmación nos llevaría a justificar la frase maquiavélica de que el fin justifica los medios, qué podríamos entonces decir sobre la terrible contaminación y daño al planeta a cambio de la evolución comercial e industrial. De la misma manera que no podemos decir que progreso es igual a contaminación, desdeñamos la idea de que tecnología avanzada es igual a pérdida de privacidad. *Clearview AI* fundada por Hoan Ton-That y Richard Schwartz —quien fue asistente de Rudolph W. Giuliani cuando fue alcalde de Nueva York— y respaldada financieramente por Peter Thiel, el inversionista de capital de riesgo detrás de *Facebook* y *Palantir*, es una APP de reconocimiento facial que, al cargar una fotografía de una persona, arroja fotografías públicas de dicha persona con las ligas a los sitios que las contienen. Su sistema tiene una base de datos de 3,000 millones de imágenes.

"Es espeluznante lo que están haciendo, pero habrá muchas más de estas empresas. No hay un monopolio sobre las matemáticas… a falta de una ley federal de privacidad muy fuerte, todos estamos arruinados", dijo Al Gidari, profesor de privacidad en la Facultad de Derecho de la Universidad de Stanford, en California[330]. Apps como *Clearview AI* parecen ser el fin del anonimato público.

Hace algún tiempo no nos preocupaba el tema de la invasión a nuestra privacidad más allá del terreno físico el cual protegíamos con bardas, cortinas, vidrios polarizados y otras soluciones más. Sin embargo, la tecnología hoy permite invadir nuestra intimidad sin siquiera estar conscientes. Cuando alguien nos menciona el tema nos preguntamos por

---

[329] Polly Sprenger, "*Sun On Privacy: 'Get over It',*" *Wired* (Conde Nast, January 26, 1999), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

[330] Hill, K. *Amenaza una App Idea de Privacidad*. New York Times, International Weekly, Suplemento del Diario Reforma del 25 de enero de 2020.

qué a alguien le interesa almacenar nuestros datos de por vida. Los *feel data*, concepto creado por la empresa Datakalab[331] usan algoritmos para analizar emociones al grabar a las personas en video para aumentar el vínculo entre las personas y las marcas. La idea es analizar las emociones a partir de las expresiones de las personas o, incluso un análisis de la dilatación de su pupila para ver si le agrada o no un producto. Hoy con los avances de la neurociencia aplicada al marketing se crean algoritmos que pueden arrojar conclusiones útiles para la creación o mejora de productos y servicios comerciales. Meta lo usa al utilizar diversos tipos de íconos con diversas expresiones de me gusta, me enoja, me entristece, entre otras. El concepto de neuro derechos fue creado por Marcelo Ienca, un profesor de Ética de la Inteligencia Artificial y Neurociencias de la Universidad Técnica de Múnich; con la colaboración de Roberto Andorno un abogado especializado en Bioética en su artículo *Towards new human rights in the age of neuroscience and neurotechnology*[332]. Los neuro derechos toman en cuenta Las Cuatro Prioridades Éticas de las Neurociencias y la Inteligencia Artificial artículo escrito por Rafael Yuste y otros autores, a saber: "la privacidad mental, la identidad personal, el libre albedrío, el acceso equitativo entendida como la no discriminación en el acceso a las neuro tecnologías[333]" Google ha desarrollado FaceNet[334] que puede reconocer un rostro entre millones, otro sistema de inteligencia artificial de Google puede reconocer una escena y proponer sitios

[331] Datakalab, "*Computer Vision on the Edge*," Datakalab, accessed March 21, 2023, https://datakalab.com/.
[332] Ienca M., Andorno R. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sci. Soc. Policy 13:5. 10.1186/s40504-017-0050-1, 2017. [PMC free article] [PubMed] [CrossRef] [Google Scholar]
[333] Maldonado, Pedro "Neuroderechos: La Discusión Por La Privacidad Mental y El Control Del Cerebro Ya Está Aquí," Universidad de Chile, August 5, 2019, https://www.uchile.cl/noticias/156392/neuroderechos-la-discusion-por-la-privacidad-mental.
[334] Yuste, R., Goering, S., Arcas, B. et al. *Four ethical priorities for neurotechnologies and AI*. *Nature* 551, 159–163 (2017). https://doi.org/10.1038/551159a

donde debió haberse tomado, muy útil para los viajeros que quieren reconocer alguna escultura o calle.

De alguna u otra manera nos sentimos invadidos y nace un interés natural de protección a nuestra intimidad que conlleva, primero, una conciencia de esta invasión para tener ciertas precauciones; luego, un razonamiento lógico, si la tecnología facilita la invasión a la privacidad, debe haber tecnología que la proteja; y, por último, nos preguntamos ¿dónde está el Derecho Objetivo?, ¿cuál es su papel? ¿es él quien debe ordenar a la tecnología proteger nuestra privacidad? ¿Es suficiente el derecho que ahora tenemos para nuestra protección básica? ¿debemos renunciar a ese derecho básico[335]?. Desde 1964 en Helsinki se firma la Declaración de Principios Éticos para la Investigación Médica que envuelva seres humanos y en el principio 11 dice: "Es deber de los médicos que participen en investigación médica proteger la vida, salud, dignidad, integridad, derecho a la autodeterminación, privacidad y confidencialidad de la información personal de los seres humanos que intervengan en dicha investigación"[336]. En 1979 el Reporte Belmont[337] producto de la Comisión Norteamericana de Protección de Sujetos Humanos de Investigación Biomédica y Comportamiento que señala 3 principios éticos básicos: 1. Respeto a las Personas 2. Beneficiencia entendido como el juramento socrático de "no hacer daño" y 3. Justicia para equilibrar los beneficios con la responsabilidad de la

[335] *Declaración de los Derechos Humanos*. Artículo 12: 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. Naciones Unidas, "La Declaración Universal De Derechos Humanos | Naciones Unidas," United Nations (United Nations), accessed March 21, 2023, https://www.un.org/es/about-us/universal-declaration-of-human-rights.
[336] *The World Medical Association, Inc.Declaration of Helsinki. "World Medical Association Declaration of Helsinki Ethical ...* - WMA." *Declaration of Helsinki*, 2008. https://www.wma.net/wp-content/uploads/2016/11/DoH-Oct2000.pdf.
[337] Departamento de Salud, Educación, y Bienestar. , "*The Belmont Report* - Hhs.gov," Principios Éticos y Directrices para la Protección de Sujetos Humanos de Investigación, 1979, https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.

investigación[338]. Por ultimo, el *Asilomar artificial intelligence (AI) statement of cautionary principles*, publicado en 2017 y firmado por investigadores de Inteligencia Artificial y empresarios -incluidos Google (Peter Norvig) y OpenAI (Elon Musk y Sam Altman) que se benefician de ella. Después de un profundo trabajo se concluyeron 23 principios divididos en 3 grandes grupos: I. Investigación II. Ética y Valores, aquí destacan el principio doce: Privacidad Personal: "Las personas deben tener el derecho al acceso, manejo y control de los datos que generen, dado el poder de los sistemas de Inteligencia Artificial para analizar y utilizar esos datos; principio trece: Libertad y Privacidad: La aplicación de la inteligencia artificial a datos personales no debe razonablemente limitar la libertad real o percibida de las personas"[339].

La discusión sobre la privacidad y la tecnología viene desde hace más de 100 años con la declaración de Thomas McIntyre Cooler que en 1888 declaró "*The Right to be alone*[340]", el derecho a ser dejado en paz y poder disfrutar libremente de la privacidad o el derecho a la soledad. Dos años después, sale a la luz el famoso artículo de 27 páginas de la Universidad de Harvard por Louis Brandeis y Samuel Warren *The Right to Privacy* en el invierno de 1890 a 1891. En él se alega un derecho al pago de daños por la invasión a un nuevo derecho redefinido como privacidad para seguir protegiendo la esfera jurídica del individuo pero alcanzando las demandas de la sociedad moderna. Warren y Brandeis definen la privacidad como "el derecho a estar sólo". Previenen la amenaza de que la privacidad está en peligro debido a "inventos recientes y métodos de negocios"[341].

---

[338] *Supra*
[339] *Future of Life Institute, "Ai Principles," Future of Life Institute*, March 15, 2023, https://futureoflife.org/open-letter/ai-principles/.
[340] Cooley McIntyre, Thomas. *A Treatise on the Law of Torts*, Callaghan and Company, Chicago 1907, p. 192.
[341] Warren, Samuel D. and Brandeis, Louis D.*The Right to Privacy*, Harvard Law Review Vol. 4, No. Dec.15, 1890.

La tecnología amenaza la privacidad en dos vertientes: aquella que facilita la adquisición de datos personales y aquélla que permite a alguien reunir, procesar y filtrar datos para su beneficio.

Es paradójico que la inversión es tan alta en la evolución tecnológica, pero mínima en desarrollo de tecnología que proteja la privacidad. Es un tema que no deja dinero. Actualmente, software relativamente sencillo permite monitorear y clasificar correos electrónicos, cualquier palabra escrita –aún siendo borrada- hábitos y sitios visitados en la web[342].

4.8. Privacidad en el aspecto laboral.

Un aspecto relevante de productividad es el uso eficaz de internet en la oficina, se sostiene que la industria americana pierde mil millones de dólares por el hecho de que los empleados naveguen en internet en las horas de trabajo. La natural inocencia de los empleados puede hacerlos perder de vista el riesgo de ser monitoreados[343]. La pandemia de Covid19 llevó a las empresas a exigir webcams en las casas o rastreo vía GPS para garantizar que los trabajadores estuviesen laborando dentro del horario de trabajo. Esto llevó a un estrés laboral por el peligro de perder el trabajo con la consecuente inequidad con aquellos trabajadores de la base de la pirámide[344]. Amazon, por ejemplo, instrumentó el consentimiento biométrico para sus repartidores con cámaras con inteligencia artificial

[342] Ver Content Audit https://www.contentwatch.com/ que es una herramienta gratuita que audita los contenidos de su computadora a partir de un servidor en internet sin alterar la configuración de la PC. Despliega el tipo de archivo, incluyendo páginas web, documentos, textos.
[343] Michelle Masterson, "*Cybersurveillance at Work*," CNNMoney (Cable News Network, 2000), https://money.cnn.com/2000/01/04/technology/webspy/.
[344] Kathryn Zickuhr, *Equitable Growth,* March 16, 2021, https://equitablegrowth.org/.

para acceder a su ubicación, movimiento y datos biométricos[345]. En nuestro país, esta acción podría estar dentro de las causas de rescisión laboral ubicadas en la fracción II del artículo 47 de la Ley Federal del Trabajo que dice: Son causas de rescisión de la relación de trabajo, sin responsabilidad para el patrón: II. Incurrir el trabajador, durante sus labores, en faltas de probidad u honradez, ... [346]

Muchos trabajadores mexicanos no tienen acceso a internet en sus casas y es más probable que naveguen en internet para contestar correos electrónicos, realizar tareas de los hijos, entre otros hábitos. En México, la privacidad de los empleados no está protegida contra sus patrones. Es más, en Estados Unidos de América, la última ley aprobada al respecto es *The Electronic Communication Privacy Act* de 1986 que prohíbe a los patrones intervenir las conversaciones telefónicas de sus empleados, aún no se había popularizado el correo electrónico y el internet. La tecnología se perfecciona para dicha invasión y monitoreo[347]. El software *forcepoint* ofrece informes sobre las tendencias en el uso de internet de cada empleado, actividad en línea de cada uno.

4.9. Internet of Things

El internet de las cosas define aparatos físicos -tales como lentes, marcapasos, relojes, medidores de glucosa hasta dispositivos en edificios como elevadores, luces, procesos de manufactura entre otros- conectados a internet para recolectar, compartir o usar datos; en principio, es para el beneficio del usuario y de la comunidad, como en el caso de que los

[345] Lauren Kaori Gurley, "Amazon Delivery Drivers Forced to *Sign 'Biometric Consent' Form or Lose Job*," VICE, March 23, 2021, https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job.
[346] Congreso de la Unión. "Leyes Federales De México - Honorable Cámara De Diputados," 202AD. https://www.diputados.gob.mx/LeyesBiblio/index.htm.
[347] Ver Forcepoint. Accessed March 21, 2023. https://www.forcepoint.com/.

botes de basura avisaran que están a su tope a los camiones recolectores. Sin embargo, representan un peligro si no cuidan el derecho a la privacidad de los datos de los usuarios. Es obligatorio para las empresas que producen internet de las cosas cumplir las leyes de privacidad vigentes en cada país[348].

Hoy la vida de más de 3,000 millones de personas en el planeta[349] transcurre en medio de redes digitales con dispositivos como Alexa o Apple HomePod, Hue de Phillips, Refrigeradores con inteligencia artificial; el Apple Watch contiende datos sobre nuestra salud que podría afectarnos al contratar una póliza de seguro si se hicieran públicos del conocimiento de las aseguradoras. Dejamos rastros de información por doquier. Esta información está siendo almacenada en lo que se conoce como *Reality Mining* a partir de análisis estadísticos e inteligencia artificial basada en algoritmos. El MIT Technology Review consideró el *Reality Mining* como una de las 10 tecnologías emergentes que transformarán al mundo[350]. El *Reality Mining* se entiende como poner atención a patrones en la vida diaria y usar esa información para ayudar en cosas como políticas de privacidad, compartir intereses con personas, notificar personas acerca de sus patrones de conducta o incluso su salud; todo ello, para mejorar nuestras vidas. Esta tendencia para recoger datos ya se vivía, pero los datos recolectados eran impersonales, tales como el número de autos que circulan en una carretera en horas pico, o el número de productos que una máquina fabrica antes de fallar. El cambio radica en que ahora la recolección de datos es acerca de personas. La proliferación del mundo móvil con conexión a internet

[348] Interesante artículo sobre *Internet de las Cosas y la Privacidad* el que ofrece el Comisionado de la Información en Victoria, Australia. *Freedom of Information | Privacy | Data Protection Version*: April 2021 – D19/8046

[349] 4,300 millones de personas todavía no tienen acceso a internet, 90% de ellos en países subdesarrollados. Ver "Measuring the Information Society Report," ITU, 2014, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

[350] Greene, Kate. *TR10 Reality Mining*. MIT Technology Review, March-April 2008, http://www2.technologyreview.com/article/409598/tr10-reality-mining/

potencia la posibilidad de recolectar más datos de más actividades humanas. Un ejemplo concreto es la aplicación *ihealth* del Iphone[351]

El internet de las cosas es un término acuñado en 1999 por Kevin Ashton al trabajar en el Media Center del MIT, con esta expresión se refería al concepto de computadoras y máquinas con sensores que se conectan a internet para transferir datos y aceptar comandos de control. Toda esta información se conoce como big data que ha generado un cambio revolucionario tanto en la sociedad como en la manera de dirigir una empresa.

Sin embargo, el éxito de los big data parte de una presunción no del todo legítima, que los datos recolectados por los aparatos y las cosas con sensores son de la organización o empresa que los recolecta. A partir de la legislación mundial, los propietarios de los datos son los titulares de los derechos ARCO.

4.10. Enemigos de la privacidad

Podemos plantear algunas causas por las que la privacidad es más sensible. Una de ellas es la miopía de los individuos que vamos repartiendo datos sin control tanto al policía de tránsito como a la persona que se nos acerca a realizar una encuesta. Otro es el derecho a la información y libertad de expresión mal entendidos. El tercero es la seguridad del Estado, sobre todo después de los hechos del 11 de septiembre del 2001 y las bombas en España e Inglaterra. Ante el conflicto de bienes jurídicos predomina el bien público sobre el privado por lo menos así lo afirman los jefes de seguridad nacional. Es menester desarrollar una cultura de protección de datos personales por los grandes peligros de robo de identidad, o tergiversación de los mismos en beneficio de particulares o corporaciones.

[351] Apple. "*Ios - Health*." Apple. Accessed March 21, 2023. https://www.apple.com/ios/health/.

Ya hemos tocado en otro apartado el tema del conflicto de bienes jurídicos entre la libertad de expresión y la privacidad de nuestros datos.

4.11. Formas de invasión de la privacidad

Surveillance: De acuerdo a una nota periodística[352], el gobierno de los Estados Unidos de América usó cámaras para registrar las caras de los casi 50,000 asistentes al estadio Raymond James, todo ello sin su consentimiento. Pero la tecnología no se detuvo ahí, las caras fueron inmediatamente comparadas con la base de datos de la policía a través de un software específico de reconocimiento de cara. Esto cada vez es más frecuente para evitar un ataque terrorista o sencillamente para vigilar barrios o lugares peligrosos donde se registra tu cara y es comparada con la base de datos de delincuentes prófugos con orden de aprehensión. El software hace un mapa de la cara con 80 puntos de referencia para ser comparados. Si el sistema encuentra más de doce referencias un oficial de policía detendrá al sospechoso para investigaciones más profundas[353]. Parece que el libro de George Owell está haciéndose realidad. No obstante, la información que reporta EPIC es que dicho software no tiene la precisión que la autoridad requiere y no ha rendido el potencial que originalmente se pensó[354]. Sin embargo, ahora se usa para la seguridad de las fronteras con México a través del programa United States *Visitor and Immigrant Status Indicator Technology* (US-VISIT) que obliga a los visitantes a dejar su huella y fotografía digital al momento de entrar. Este sistema cruza datos con un sistema biométrico para detectar si el visitante es peligroso.

---

[352] *"Super Bowl Snooping,"* The New York Times, February 4, 2001, https://www.nytimes.com/2001/02/04/opinion/super-bowl-snooping.html.
[353] Thales Group, "*Facial Recognition: Top 7 Trends (Tech, Vendors, Use Cases*)," visitado en marzo 21, 2023, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.
[354] EPIC, "*Face Surveillance and Biometrics*," EPIC, visitado en marzo 21, 2023, http://www.epic.org/privacy/facerecognition/.

Nos hemos acostumbrado a las cámaras de monitoreo, sobre todo en tiendas, casas, farmacias, tiendas de discos, supermercados, bancos, cajeros automáticos, aeropuertos y hoteles. Incluso se ha comenzado a usar esta técnica, cada vez más barata, para monitorear empleados. Incluso el *surveillance* no sólo ha sido formal para efectos de seguridad, sino ha invadido baños, hoteles, bares, vestidores, clubes privados para subir dichas imágenes a la *web* y vender el acceso a usuarios sin escrúpulos.

4.12. Carnivore. Tecnología *Packet Sniffer*.

El FBI desarrolló este programa para intervenir proveedores de internet (*IPS*[355]*),* por cuestiones de seguridad nacional, pero no sólo intervino, sino filtraba los correos electrónicos con palabras que sugirieran actividades sospechosas –bajo una orden de la Corte-. El problema es que la herramienta está diseñada para capturar la totalidad de la información de nuestros correos electrónicos y, sólo luego, con orden judicial, desecha lo demás para tomar sólo lo que le interesa. Es decir, primero invade nuestra privacidad y luego filtra para obtener seguridad nacional. Esto nos permite ver que la actividad de monitoreo no sólo está a un nivel físico de lugares públicos y privados.

Carnivore tuvo su origen en un programa ahora comercial llamado *Etherpeek*, más adelante en 1997 el *FBI* utilizó un segundo programa llamado *Omnivore* para finalmente llegar a la *DragonWare Suite* que le permitió descifrar correos electrónicos, copiar archivos bajados e incluso reconstruir páginas web visitadas. Esta suite se componía de tres elementos: *Carnivore*, herramienta para capturar la información; *Packeteer*, herramienta para armar los paquetes de información –que sabemos son desarmados al

[355] *Internet Service Provider*

entrar a la *web*- y *Coolminer* una herramienta para relacionar los contenidos con palabras clave y relacionarlas con actividades peligrosas.

4.13. *Packet Sniffing*

Tecnología utilizada con fines de monitoreo de red, sobre todo para detectar problemas y optimizarlas. En general estos programas pueden ver toda la información que viaja a través de las redes a las que está conectado.

La tecnología es tan diversa y rica en la invasión a la privacidad física en lugares públicos o privados que se ha acuñado el término *surveillance* que define el monitoreo de la conducta.

- Monitoreo en lugares públicos o privados (empresa, casa, escuela).
- Tecnología de reconocimiento facial o dactilar, DNA, y otras. (biometría).
- Invasión de llamadas telefónicas.
- Monitoreo de vehículos o personas (para evitar secuestros).
- Monitoreo vía internet a través de los cookies, kazaa, clictrails, identificadores de equipos de cómputo, snitchware (protección de la propiedad).
- Visión a través de paredes y ropa.

4.14. Software espía

Después de explicar el concepto de cookies y entender su importante función de rastrear la navegación de un usuario, es relevante hablar del spyware que mantiene el registro de los hábitos en línea de los usuarios de manera normalmente imperceptible. Estos registros se guardan en la mayoría de los proveedores de internet y pueden ser usados para rastrear

cualquier movimiento en la web. También es posible que empresas o gobierno pongan software específico a través de los proveedores de internet para inhibir el ingreso a ciertos sitios en la web.

La distinción entre lo público y lo privado surge históricamente desde el advenimiento de la cosa pública como interés del Estado hacia un bien común dando privilegios a la autoridad en una relación de supra a subordinación con los particulares. Las prácticas para respetar la privacidad nuestra y de los otros son de la vida diaria.

El problema de la solución es que nosotros los individuos no confiamos ni en la esfera pública, ni privada; por ende, deseamos ser nosotros quienes definamos la extensión de la protección de nuestros datos.

4.15. Tecnología GPS y la invasión a la Privacidad

El Sistema de Posicionamiento Global está basado en aproximadamente 31 satélites propiedad del Fuerza Aérea norteamericana. Esta tecnología permite determinar la ubicación exacta, con una posibilidad de error de 5 a 10 metros, de cualquier persona con un dispositivo. Su finalidad es facilitar la navegación, seguimiento de paquetes o personas y mapeo para diversos usos.

La tecnología funciona a partir de señales enviadas desde los dispositivos en la tierra a los satélites, éstos devuelven la señal que permite calcular la ubicación precisa. La descripción de la tecnología del Sistema de Posicionamiento Global (GPS) para efectos jurídicos debe centrarse tanto en su capacidad de proporcionar datos precisos de ubicación como en las implicaciones que tiene su uso no autorizado, especialmente en el contexto de la privacidad. Esta tecnología requiere por lo menos 4 satélites ya que el proceso triangula la posición a partir de mediciones de distancia. El avance de la

tecnología ha mejorado la precisión a partir del GPS diferencial que usa puntos terrestres para corregir las señales satelitales. Otra ventaja de esta tecnología es que puede funcionar aún cuando el dispositivo no tenga conexión a internet. Dicha tecnología tiene varias implicaciones jurídicas como la posible violación del derecho a la privacidad de las personas cuando se les rastrea sin su consentimiento. También la posibilidad del GPS de localizar a una persona en tiempo real es fundamental para investigaciones, evidencias forenses. Inclusive ya hay empresas que ofrecen instalar uno de esos chips en nuestro cuerpo e incluir información de antecedentes médicos, tipo de sangre, medicinas prescritas, entre otras[356]. Definitivamente puede ser positivo el uso de esta tecnología bien usada. Pero, la pregunta al derecho es si debiera o no proteger el mal uso de tan valiosa información personal. Por ejemplo, los laboratorios farmacéuticos podrían estar interesados en comprar una base de datos de diabéticos que hubiesen comprado dicho chip para venderles la más nueva medicina para dicha enfermedad. Parece que no somos más anónimos para el estado o para las empresas. Incluso en la mayoría de los países se trabaja en sistemas para tener una base de datos nacional ya sea a través de la seguridad social, credencial para votar, licencias de conducir o un ID nacional. El futuro puede ser una base de datos mundial de individuos con el DNA de cada uno y otras características biométricas de identificación. ¿Qué hacer con esa información? Sólo las potencias mundiales lo saben. Pero el peligro del mal manejo de dicha información puede causar una crisis mundial. Es paradójico que mientras las corporaciones, los bancos y demás instituciones financieras, así como los organismos del Estados ocultan sus actuaciones por diversos acuerdos legales de confidencialidad, patentes y otros instrumentos

[356] Janice Hopkins Tanne, "*FDA Approves Implantable Chip to Access Medical Records*," PubMed Central (PMC), November 11, 2004, https://bit.ly/2TIInLf.

jurídicos; las vidas de las personas físicas comunes y corrientes son libros abiertos para ellos con el fin de recolectar información a partir de algoritmos para diversos fines, en el mejor de los casos legales. El software de anonimización denominado Red Privada Virtual (VPN, por sus siglas en inglés) provee de un acceso cifrado para ocultar nuestra dirección virtual, los sitios a los que accedemos y la información que proveemos. Sin embargo, esa misma tecnología puede constituir una amenaza a nuestros datos. La privacidad de nuestra información en internet es un derecho que difícilmente podemos exigir pues la arquitectura de la *web* está diseñada de tal manera que es relativamente sencillo y barato recolectar nuestra información. Una vez teniendo la base de datos, también es extremadamente fácil filtrarlos, clasificarlos conforme a criterios de interés, ingresos, sitios visitados con el objeto de crear lo que se ha dado en llamar perfiles cuyo contenido determina los hábitos de una persona en internet, así como el mercado al cual pueden ser vendidos sus datos.

Varios protectores de los derechos de la privacidad han exigido desarrollar tecnologías, si no para evitar la colección de datos, por lo menos dar la posibilidad al usuario de conocer qué datos son recopilados y tener la oportunidad de corregirlos o limitarlos.

Sin embargo, debemos reconocer que los intereses mercantilistas han vencido ampliamente a estas asociaciones desinteresadas y, en ocasiones sin muchos recursos para defender a usuarios que parecen no estar siquiera conscientes de los riesgos que la invasión a su privacidad conlleva.

Son varios los argumentos que una empresa puede esgrimir para recolectar base de datos de sus clientes, todos ellos –dirán- encaminados a mejorar el servicio que podamos recibir. Negarán, sin embargo, que muchas de estas empresas hacen negocio con nuestros

datos y son vendidos a terceros sin muchos escrúpulos. La empresa que vende estos datos no sufre ningún menoscabo en su patrimonio, pues los clientes nunca se enteran de dónde provino su información a aquel tercero que la explota. Amazon.com es uno de los negocios que más ha crecido con base en la recolección de datos para conocer y servir mejor a sus clientes usando tecnología para combinar los servicios con los perfiles de clientes desarrollados a partir de sus hábitos de visita y compra. Los expertos de Amazon usan la tecnología para predecir qué libros o bienes nos gustarán. Como toda empresa seria, Amazon tenía su política de privacidad que prometía no vender la información de los usuarios a terceros, por lo menos si tenía tal petición a través de un correo electrónico del usuario. Varias personas escribieron tal correo electrónico confiando en Amazon, ésta recolectó datos de sus usuarios por años en beneficio de ellos. Sin embargo, a finales del 2000, Amazon anunció un cambio en sus políticas de privacidad aclarando que, de esa fecha en adelante, Amazon podría vender datos de sus usuarios a personas externas. Hubo una aclaración peligrosa, dicha información podría ser incluso de aquellos usuarios que hubieran escrito el correo electrónico para ser excluidos de tal práctica. Es decir, aplicaba una política retroactivamente que traicionaba la confianza de sus usuarios. Se basó en una frase de la anterior política de privacidad que indicaba que dichas políticas podían ser cambiadas en cualquier momento. Amazon rechazó incluso borrar información de usuarios que lo requirieron. Esta preocupación se acentuó al anunciar su navegador Silk en su tableta Kindle Fire –lanzada en septiembre de 2011-, la tecnología de este navegador se basa en *Amazon Elastic Compute Cloud* que actúa como un proxy o filtro para conocer los hábitos de búsqueda de sus usuarios al mantener en sus servidores las páginas web precargadas y hacer más rápida la visita del usuario a dichos sitios. El

hecho es que siempre que te conectas a internet con Kindle Fire lo haces a través del sitio Amazon[357].

El desarrollo del comercio electrónico ha sido un riesgo, pero también una oportunidad para la protección a la privacidad en internet. Han existido diversos esfuerzos por regular jurídicamente las transacciones sobretodo para evitar riesgos de fraudes en la web. La administración del presidente Clinton promovió la regulación a estas operaciones[358]. Sin embargo, son pequeños esfuerzos ante el impulso avasallador del mercado. El consentimiento en la era digital ha perdido mucho de su brillo pues en el comercio electrónico ha sido suplantado por un pseudo-consentimiento y principios de consentimiento tácito envueltos en la propia navegación del usuario para completar la operación de comercio electrónico con simples contratos de adhesión escritos por el vendedor, sin oportunidad de negociarlos por el comprador.

Es el reto del Derecho suplir la deficiente regulación de la protección de datos personales ante el ataque de los intereses comerciales y estatales.

Nuestro interés jurídico radica en que no deben ser utilizados para beneficios de otros, sino sólo para el nuestro. Sugiero llamar a esto el ***Principio Positivo de la Privacidad para la Persona*** (PPPP) como una guía que pueda ser llevada a ámbitos constitucionales como aquél ámbito protegido aún contra el Estado.

[357] Para más detalle de su política de privacidad consultar: Amazon, "GP," Amazon (Goettsche Partners, 2011), https://www.amazon.com/gp/help/customer/display.html/?nodeId=200775270.
[358] John Woolley and Peters Gerhard, "Executive Order 13133-Working Group on Unlawful Conduct on the Internet," *Executive Order 13133-Working Group on Unlawful Conduct on the Internet* | The American Presidency Project, August 5, 1999, https://www.presidency.ucsb.edu/documents/executive-order-13133-working-group-unlawful-conduct-the-internet.

V. Conclusiones

1. El perfilamiento algorítmico tiene varios aspectos positivos como la personalización en los servicios con base en la experiencia de la persona. También permite al Gobierno la toma de decisiones eficiente para hacer llegar las ayudas a las personas que realmente lo necesitan para efectos de salud o economía, efectos estadísticos. También es positivo para la detección de fraudes. Es fundamental para identificar patrones que indican actividades fraudulentas, mejorando así la seguridad en transacciones financieras e interacciones en línea. Contribuye a campos de investigación analizando grandes conjuntos de datos, lo que lleva a nuevos conocimientos y descubrimientos.
2. Distinguimos el régimen utilitarista de los Estados Unidos de América que da preferencia a los intereses del mercado sobre el régimen sobreprotector de Europa que enfatiza el interés del individuo a la dignidad, autonomía y libertad lo que se conseguirá sólo con una adecuada protección a la privacidad de la información. Los riesgos de una legislación inapropiada son muchos, el robo de identidad, acoso, amenazas anónimas, entre otros.
3. La protección al derecho a la privacidad es también cultural, pues dependerá de los antecedentes históricos que cada país haya tenido en cuanto a la protección que dará y en dónde la fundamentará, donde el punto común es el deseo de protegerlo.
4. El origen del derecho a la privacidad en los Estados Unidos de América encuentra su fundamento en la vieja Europa que evocan los mismos principios de protección al derecho a la privacidad.

5. En un principio, las discusiones se basaban en si alguien podía mostrar su intimidad públicamente o descubrir la intimidad de otro. Sin embargo, como vimos en los capítulos anteriores, ahora la discusión se basa en la protección de datos personales en las operaciones de comercio electrónico, o el espionaje de la web por intereses comerciales o políticos.
6. Nos podemos plantear si existen principios universales bajo los cuales podemos fundamentar el derecho a la privacidad; o bien, si la protección al derecho a la privacidad debe ser cultural, acorde a las circunstancias históricas de cada pueblo. El derecho europeo basa su protección a la privacidad en las ideas franco-germanas sobre el honor con una fuerte influencia de haber padecido la 2ª guerra mundial –recordemos que se persiguió a los judíos con base en los censos-; el derecho estadounidense la fundamenta en el concepto de libertad privilegiando la actividad económica sobre el derecho individual de la privacidad. Sobretodo la información crediticia fluye de manera tal que sería imposible en Europa.
7. Los autores están lejos de ponerse de acuerdo acerca del bien jurídico protegido por el derecho a la privacidad, parece variar de cultura a cultura. ¿Es acaso el honor?, o ¿la libertad? Los franceses odian decir su salario, pero aceptan playas nudistas. En la antigua Grecia, particularmente en Efeso, era costumbre dialogar sobre asuntos políticos sentados en letrinas.
8. Solamente si la privacidad es una necesidad humana básica dará lugar a un derecho fundamental. Muchos juristas lo asocian a los derechos de la personalidad al fundarla en argumentos intuitivos, como los filósofos *ius* naturalistas que sostienen que todos tenemos una consciencia de lo correcto e incorrecto, guía de

la toma de decisiones éticas. Este argumento, nos llevaría a fundar un caso de privacidad en las intuiciones que tienen nuestros clientes sobre las violaciones a la privacidad. Dicho fundamento teórico sólo será válido si todos los seres humanos compartiéramos esas intuiciones sobre la privacidad. Sin embargo, la realidad nos muestra que hay mucho debate sobre aquello que debemos mantener privado.

9. Hay un choque continental acerca de la manera de abordar la defensa a la privacidad. Si bien partimos de que en cada rincón del mundo occidental hay un clamor por considerar a la privacidad como un bien jurídico, encontramos que los europeos consideran a los americanos como carentes de una etiqueta de privacidad al preguntar naturalmente cuánto ganamos o dar información crediticia a cualquier comerciante sobre sus clientes. Por el otro, el derecho europeo protege fuertemente varias áreas de nuestra privacidad, desde los datos de crédito, privacidad laboral, asuntos jurídicos, médicos, hasta la distribución de imágenes en la web. Un tema como la privacidad de los clientes ante los comerciantes ha sido motivo de debate entre el derecho europeo y norteamericano. Esto es importante cuando se desea realizar contratos intercontinentales. Dichos conflictos se vieron resueltos con la firma del Safe Harbour en el año 2000[359] por el que se permite a las empresas americanas auto certificar que cumplen con los estándares de respeto a la privacidad europeos. Estos últimos se quejan de que el norteamericano constantemente viola estos acuerdos en aras del mercantilismo. Por ejemplo, el derecho norteamericano permite investigar a su contraparte y sacar a juicio antecedentes privados que puedan ayudar a ganar el mismo, algo

[359] Ita, "Join Us Today," Export.gov, accessed March 21, 2023, https://2016.export.gov/safeharbor/eg_main_018238.asp.

inusual para el derecho europeo. La cultura americana tiene una tendencia a hablar mucho sobre el término privacidad. Invierten muchos dólares para asegurarse de que la tienen y que está protegida. Esto evoluciona a grado extremo cada vez más, por ejemplo, en estos tiempos es mal visto preguntar "¿cuál es tu religión?", "¿es tu esposa? Esto incluye preguntas que podrían ser trascendentes para el empleador como "¿planea casarse y tener hijos?", "¿está embarazada? Preguntas que en otras culturas serían totalmente válidas, en EUA parecen estar sobreprotegidas por la privacidad.

10. Una tesis doctoral es inacabada y vienen temas muy interesantes para complementar esta investigación. La eliminación de las cookies, la protección de la privacidad no sólo contra la sociedad, sino contra el estado, las tecnologías para quebrar la regulación y el derecho. La privacidad en temas de salud, un análisis comparativo de protección de datos en las diferentes sociedades, entre muchos otros. El uso de la inteligencia artificial para el perfilado algorítmico, entre muchos otros. La legislación parece quedarse corta ante los desafíos de la tecnología, sólo una participación activa de la sociedad, investigadores, filósofos, juristas e ingenieros pueden luchar porque la tecnología sirva a la persona humana y no al revés.

VI. Bibliografía

Agencia Española de Protección de Datos. “IV Encuentro Iberoamericano De Protección De Datos Personales Ciudad De ...” IV Encuentro Iberoamericano de Protección de Datos Personales Ciudad de México, 2005. https://www.redipd.org/sites/default/files/inline-files/nota_prensa_nov_2005.pdf.

Altman, Irwin. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA: Brooks/Cole Publishing Company, 1975.

Amazon. “GP.” Amazon. Goettsche Partners, 2011. https://www.amazon.com/gp/help/customer/display.html/?nodeId=200775270.

Anderson, David. *The failure of American Privacy Law*, en *Protecting Privacy: The Clifford Chance Lectures*, *Volume Four*, pp. 139 - 167. Ed. Oxford University Press. Nueva York, 1999.

Anglim, Christopher T., *Privacy in the Digital Age*, First Edition, Ed. Grey House Publishing, NY 2015,

Antibullying Alliance. “United Against Bullying (UAB) Programme.” Anti, 2022. https://anti-bullyingalliance.org.uk/.

Apple. “Ios - Health.” Apple. Accessed March 21, 2023. https://www.apple.com/ios/health/.

Arendt, Hannah. *La Condición Humana*. Argentina: Paidós, 2003.

Asale, Rae -. “Intimidad: Diccionario De La Lengua Española.” "Diccionario de la lengua española" - Edición del Tricentenario, 2022. https://dle.rae.es/intimidad.

Barfiel, Woodrow. *The Cambridge Handbook of the Law of Algorithms*, Cambridge, UK 2021: Ed. Cambridge University Press:, p. 3.

Baron, David P., *DoubleClick and Internet Privacy*, Graduate School of Business, Stanford, Case number P-32, August 2000,

Batista, Fernando. Boletín Mexicano de Derecho Comparado, núm. 167, mayo-agosto de 2023, pp. 33-50ISSN: 2448-4873DOI: https://doi.org/10.22201/iij.24484873e.2023.167.18535

BBC News. "El Asesinato De Abril Pérez, El Feminicidio Que Indignó a México." BBC News Mundo. BBC, 2020. https://www.bbc.com/mundo/noticias-america-latina-50603585.

Bentham, Jeremy. *Panopticon*, 1787.

Bier, William Christian. *Privacy, a Vanishing Value?* Fordham University Press, 1980.
Birbak, Andreas, *etal*. *The Public and its Algorithms*, MIT Press, USA 2015,

Boling, Patricia. *Privacy and the Politics of Intimate Life*. Ithaca, NY.: Cornell University Press, 1996.

Brewster, Christopher. "Legibility, Privacy and Creativity: Linked Data in a Surveillance Society." *Aston Business School*, Privon, Vol 1121 (2018).
Calhoun, Craig. *Habermas and the Public Sphere (Studies in Contemporary German Social Thought)*. Massachusetts: MIT Press, 1991.

"California v. Ciraolo." Oyez. Accessed March 21, 2023. https://www.oyez.org/cases/1985/84-1513.

Carrillo, Marc. *El Derecho a No Ser Molestado: (Información y Vida Privada)*. Pamplona: Aranzadi, 2003.

Carrillo, Marc. "La Intimidad, Las Celebridades y El Derecho a La Intimidad." *Diario La Ley* XXIX, no. 6979 (July 1, 2008).

Castán Tobeñas, José. *Derecho civil español, común y foral*, t. l, 1984, vol.11, p. 398

Chemerinsky, Erwin. *Constitutional Law: Principles and Policies*. Frederick: Aspen Publishing, 2023.

Cladis, Mark Sydney. *Public Vision, Private Lives: Rousseau, Religion, and 21st-Century Democracy*. Oxford: Oxford University Press, 2003.

Clinton, Bill. "Framework for Global Electronic Commerce ." National Archives and Records Administration. National Archives and Records Administration. Accessed February 6, 2023. https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

CNDH. "Entra En Vigor La Convención Europea De Los Derechos Humanos: Comisión Nacional De Los Derechos Humanos - México." Inicio, 2019. https://bit.ly/3dYLHIY.

CNET. "DoubleClick, Abacus Merge in $1.7 Billion Deal." CNET. CNET, January 3, 2002. https://www.cnet.com/tech/services-and-software/doubleclick-abacus-merge-in-1-7-billion-deal/.

Código Penal Federal, Art. 199, 2023. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf.

Council of Europe. "Council of Europe Data Protection Website - Data Protection - Www.coe.int." Data Protection, 2021. https://www.coe.int/en/web/data-protection/home.

Congreso de la Unión. "Ley Federal Del Derecho De Autor - Honorable Cámara De Diputados." Diario Oficial de la Federación, July 1, 2020. https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf.

Congreso de la Unión. "Ley Federal De Transparencia y Acceso a La Información Pública." Diario Oficial de la Federación, 2015. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_200521.pdf.

Congreso de la Unión. "Ley General De Protección De Datos Personales En Posesión De Sujetos ..." Nueva Ley, 2017. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

Congreso de la Unión. "Leyes Federales De México - Honorable Cámara De Diputados," 202AD. https://www.diputados.gob.mx/LeyesBiblio/index.htm.

Constitución De Los Estados Unidos Mexicanos: Expedida Por El Congreso General Constituyente El Día 5 De Febrero De 1857 Con Sus Adiciones y Reformas: Leyes orgánicas Y Reglamentarias: Texto Vigente De La constitución. México, CDMX: Gobierno Federal, 1905.

Cookie Central. "Cookie Central." Cookie Central, 1996. http://www.cookiecentral.com/.

Cooley McIntyre, Thomas. *A Treatise on the Law of Torts*, Callaghan and Company, Chicago 1907.

Corte Interamericana de Derechos Humanos. "Fontevecchia y D'Amico Vs. Argentina." Corteidh.or.cr, 2011. https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191.

Corte Interamericana de Derechos Humanos. "Técnica: Kimel Vs. Argentina." Corteidh.or.cr, 2006. https://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=291.

Corte Interamericana de Derechos Humanos. "Tristán Donoso Vs. Panamá." Corteidh.or.cr, 2008. https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253.

Davidson, Sandra. Capítulo 14 *Cyber-Cookies: How Much Should The Public Swallow? Advertising and the World Wide Web*, ed. David W. Schumann and Esther Thorson (Mahwah, NJ: Lawrence Erlbaum Associates, 1999)

Datakalab. "Computer Vision on the Edge." Datakalab. Accessed March 21, 2023. https://datakalab.com/.

De Paul, Robert. *Dictionnaire Alphabetique De La Langue Francaise*. Paris: Societe du nouveau Littre, 1963.

DeCew, Judith. "Privacy." Stanford Encyclopedia of Philosophy. Stanford University, January 18, 2018. https://plato.stanford.edu/archives/spr2018/entries/privacy/.

DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY.: Cornell University Press, 1997.

Departamento de Salud, Educación, y Bienestar. "The Belmont Report - Hhs.gov." Principios Éticos y Directrices para la Protección de Sujetos Humanos de Investigación, 1979. https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf.

Diccionario De La Lengua Española. Madrid: Real Academia Española, 2001.

Diario Oficial de las Comunidades Europeas. "Carta De Los Derechos Fundamentales De La Unión Europea." Carta de los Derechos Fundamentales de la Unión Europea, December 18, 2000. https://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Diario Oficial de la Federación. "Ley Federal De Protección De Datos Personales En Posesión De Los ..." Decreto, 2007. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

Díaz Rojo, José Antonio. "Privacidad: ¿Neologismo o Barbarismo? ." *Revista de Estudios Literarios*, no. 21 (n.d.): 46.

Digest, Editors Human Rights Case. "I Avgi Publishing Press Agency S.A. and Karis V. Greece." Brill. Brill Nijhoff, October 3, 2008. https://brill.com/view/journals/hudi/18/9-10/article-p929.xml.

Dirección General de Análisis Legislativo. "Cédula De Identidad Ciudadana y Registro Nacional De Población." Mirada Legislativa, 2014. http://bibliodigitalibd.senado.gob.mx/.

Domain, "Every Successful Business Needs a Strong Online Presence.," 101domain, accessed March 21, 2023, http://www.101domain.com/.

Domingos, Pedro, *The Master Algorithm: How the Quest for the Ultimate Learning Machine will Remake our World*, New York, NY 2018: Ed. Basic Books.

EDPB. "Grupo De Trabajo Del Artículo 29." Grupo de Trabajo del artículo 29 | European Data Protection Board, 2018. https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es.

Educativo, Consejo Nacional de Fomento. "Ley General De Protección De Datos Personales En Posesión De Sujetos Obligados." gob.mx, January 26, 2017. https://www.gob.mx/conafe/documentos/ley-general-de-proteccion-de-datos-personales-en-posesion-de-sujetos-obligados-289438.

El País. *El País: Libro De Estilo*. España, Madrid: Aguilar, 2021.

EPIC. "Face Surveillance and Biometrics." EPIC. Accessed March 21, 2023. http://www.epic.org/privacy/facerecognition/.

Esteve, Asunción. "Análisis Legal Del Proyecto Google Books Desde La Perspectiva De Los Derechos De Propiedad Intelectual." Textos universitaris de biblioteconomia i documentació. Universidad de Barcelona, 2010. https://bid.ub.edu/24/esteve2.htm.

EUR-lex. "Lex - 32016R0679 - En - EUR-Lex." EUR, 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679.

European Court of Human Rights. Case of Juppala vs. Finland, 2008. https://www.stradalex.com/en/sl_src_publ_jur_int/document/echr_18620-03.

European Court of Human Rights. "Karhuvaara and Iltalehti v. Finland." Human Rights Guide, 2004. https://www.zmogausteisiugidas.lt/en/case-law/karhuvaara-and-iltalehti-v-finland.

European Court of Human Rights. Case of Thorgeir Thorgeirson vs. Iceland, 1992. https://www.humanrights.is/static/files/Itarefni/torgeir_torgeirson_gegn_islandi.pdf .

Fariñas, Luis. *El Derecho a La Intimidad*. Madrid: Ed. Trivium, 1984.

Finnis, John. *Natural Law & Natural Rights*, Oxford University Press, 2011

FOLDOC. "Online AI Legal Research Tools: Lexis+." LexisNexis, 1995. https://www.lexisnexis.com/en-us/products/lexis-plus.page.

Forcepoint. Accessed March 21, 2023. https://www.forcepoint.com/.

Foucault, Michel. *Power / Knowledge: Selected Interviews An*. Brighton, Sussex: The Harvester press, 1980.

Friedman, Vanessa & Engel Bromwich, Jonah. *Cambridge Analytica Used Fashion Tastes to Identify Right-Wing Voters*, *New York Times*, 29 de Noviembre, 2018.

Froomkin, Michael. "(PDF) the Death of Privacy? ." ResearchGate, 2000. https://www.researchgate.net/publication/228711041_The_Death_of_Privacy.

Fustel de Coulanges, Numa Denis. *The Ancient City*. Ontario, Canada: Batoche Books, 2001.

Future of Life Institute. "Ai Principles." Future of Life Institute, March 15, 2023. https://futureoflife.org/open-letter/ai-principles/.

Gaceta del Semanario Judicial de la Federación, Décima Época, Tomo III, Libro 42, mayo de 2017, Tribunales Colegiados de Circuito, p. 1900, Tesis: (VIII Región) 2o.6 K (10a.), Registro: 2014250.

Gannes, Liz. "Four Years Later, Obama Will Start Tweeting Himself." AllThingsD. Accessed March 15, 2023. https://allthingsd.com/20110617/four-years-later-obama-will-start-tweeting-himself/.

Garner, Brian A. *Black Law's Dictionary*. 9th ed., n.d.

Garzón Valdés Ernesto. *Lo íntimo, Lo Privado y Lo Público*. México, D.F.: IFAI Instituto Federal de Acceso a la Información Pública, 2005.

Gavison, Ruth. Yale Law School Legal Scholarship Repository, January 1980. https://digitalcommons.law.yale.edu/.

Gavison, Ruth. "Feminism and the Public/Private Distinction." *Stanford Law Review* 45, no. 1 (1992): 1–45. https://doi.org/10.2307/1228984.

GDPR.eu. "Recital 30 - Online Identifiers for Profiling and Identification." GDPR.eu, July 23, 2020. https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/.

Gillespie. Tallerton. *The Relevance of Algorithms, Media Technologies: Essays on Communication, materiality and society,* Cambridge, Massachusetts, MIT Press, 2014

GIRE. "Caso Coahuila: La Marea Verde Llega a Pino Suarez 2." El Juego de la Suprema Corte, 2021. https://bit.ly/3aGXpcP.

Global Freedon of Expression. "Lindon, Otchakovsky-Laurens and July v. France." Global Freedom of Expression, July 12, 2022. https://globalfreedomofexpression.columbia.edu/cases/lindon-and-others-v-france/.

Global Privacy Enforcement Network . "Home (Public): Global Privacy Enforcement Network." Home (public) | Global Privacy Enforcement Network, 2013. https://www.privacyenforcement.net/content/home-public.

Gobierno de España. "Agencia Estatal Boletín Oficial Del Estado." Ir a la página de inicio, 1995. https://bit.ly/3LFWObu

Gobierno de la Ciudad de México. "Art. 15 Ley De Responsabilidad Civil Para La Protección Del Derecho a La Vida ." Consejería Jurídica y de Servicios Legales, 2014. http://www.aldf.gob.mx/archivo-f1622931dc0f6677e86f68ef7b9b2270.pdf.

Gobierno de la Ciudad de México. "Ley De Responsabilidad Civil Para La Protección Del Derecho a La Vida." Gaceta Oficial del gobierno federal, 2014. http://aldf.gob.mx/archivo-bf7113fe54a3042531735d5b5d7eb27a.pdf.

Greene, Kate. *TR10 Reality Mining*. MIT Technology Review, March-April 2008

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. Metropolitan Books.

Guerrero, Francisco. Amador, Juan Carlos. *La Concertación Política en Contextos de Democracias Fragmentadas el caso de Pacto por México*, D3 Ediciones SA de CV, 2016.

Gurley, Lauren Kaori. "Amazon Delivery Drivers Forced to Sign 'Biometric Consent' Form or Lose Job." VICE, March 23, 2021. https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job.

Gutwirth, Serge, and Raf Casert. *Privacy and the Information Age*. Lanham Md.: Rowman & Littlefield Publishers, 2002.

Habermas Jürgen. *Historia y Crítica De La Opinión Pública*. Barcelona: Gili, 1981.

Hall, Edward T. *The Hidden Dimension*, *Anchor Books Doubleday*, NY 1966

Hastie, Circuit Judge., and Chief Judge (dissenting). BIGGS. "Jenkins v. Dell Publishing Company." Legal research tools from Casetext, January 13, 1958. https://casetext.com/case/jenkins-v-dell-publishing-company-2/.

Hildebrandt, Mireille. *Profiling the European Citizen*, Ed. Springer, 2008

Hu, X., Sastry, N.R., & Mondal, M. (2021). CCCC: Corralling Cookies into Categories with CookieMonster. *Proceedings of the 13th ACM Web Science Conference 2021*.

Ienca M., Andorno R. *Towards new human rights in the age of neuroscience and neurotechnology*. Life Sci. Soc. Policy 13:5. 10.1186/s40504-017-0050-1, 2017. [PMC free article] [PubMed] [CrossRef] [Google Scholar]

INAI. Generadores de Avisos de Privacidad. Accessed March 20, 2023. https://generador-avisos-privacidad.inai.org.mx/.

INAI. "Guía Para Prevenir El Robo De Identidad." INAI. Accessed March 21, 2023. https://home.inai.org.mx/.

INAI. "Instituto Nacional De Transparencia, Acceso a La Información y ...," 2018. https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf.

Indos Media, "Presentación De La Declaración De Lima Del Observatorio Iberoamericano De Protección De Datos," RS Privacidad, November 6, 2019, https://www.rsprivacidad.es/presentacion-de-la-declaracion-de-lima-del-observatorio-iberoamericano-de-proteccion-de-datos/. p.1

"Instituto Nacional Electoral." repositoriodocumental.ine.mx. INE, 2020. https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/113983/CGex202005-15-ap-2-Gaceta.pdf.

Ita. "Join Us Today." Export.gov. Accessed March 21, 2023. https://2016.export.gov/safeharbor/eg_main_018238.asp.

Jeremy, Norman. "Louis Montulli II Invents The Http Cookie." Louis Montulli II Invents the HTTP Cookie : History of Information, 1996. https://www.historyofinformation.com/detail.php?id=2102.

Kang, Jerry. *Information Privacy in Cyberspace Transactions*, Stanford Law Review, vol. 50

Kessler, Frederick R. "A Common Law for the Statutory Era: The Right of Publicity and New York's Right of Privacy Statute." *Fordham Urban Law Journal* , 03, 15, no. 04 (1987): 951-siguientes.

Keulen, Sjoerd. Kroeze, Ronald. *The Handbook Privacy Studies*, Amsterdam University Press, 2018.

Korzybski, Alfred. *Selections from Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics*. NY, NY: Institute of General Semantics, 1998.

Leick, A., Rapoport, L., & Tatarnikov, D. (2015). GPS satellite surveying (4th ed.)

John Wiley & Sons.

Leroy Miller, Roger. Jentz, A. Gaylor. *Business Law Today*, 10th edition. Mason, Ohio, USA, 2012.

Lessig, Lawrence. *Code*. New York: Basic Books, 2006.

Lexis Nexis. "Nader v. General Motors Corp. - 25 N.y.2d 560, 307 N.y.s.2d 647, 255 N.e.2d 765 (1970)." Community. Accessed March 21, 2023. https://www.lexisnexis.com/community/casebrief/p/casebrief-nader-v-general-motors-corp.

Lexis Nexis. "Onassis v. Christian Dior-New York, Inc. - 122 Misc. 2d 603, 472 N.y.s.2d 254 (Sup. Ct. 1984)." Community. Accessed March 21, 2023. https://www.lexisnexis.com/community/casebrief/p/casebrief-onassis-v-christian-dior-new-york-inc.

Llano, Carlos. *Los Fantasmas de la Sociedad Contemporánea*, Ed. Trillas, México, 1995, p. 47

Locke, John. *Some Thoughts Concerning Education*. Numeral 82 *in Complete Works of John Locke*, Delphi *Series*, UK, 2017.

Loianno, Adelina. *La Defensa De La Intimidad y De Los Datos Personales A Traves Del Habeas Data*. Argentina: Ediar, 2001.

López, Mayolo. "Adquiere EU Listas Del IFE." *Reforma*. April 13, 2003, Impresa edition, sec. Primera Plana.

Maldonado, Pedro. "Neuroderechos: La Discusión Por La Privacidad Mental y El Control Del Cerebro Ya Está Aquí." Portada Universidad de Chile, August 5, 2019. https://www.uchile.cl/noticias/156392/neuroderechos-la-discusion-por-la-privacidad-mental.

Maldonado Smith, M. E. (2024). Discriminación algorítmica en el ámbito laboral. Quórum Legislativo, núm. 145, marzo 2024.

"Manifestación De Protección De Datos Personales Del Registro Federal De Electores." Instituto Nacional Electoral, March 31, 2021. https://www.ine.mx/credencial/manifestacion-proteccion-datos-personales-del-registro-federal-electores/.

Madden, Mary, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaten. "Teens, Social Media, and Privacy." Pew Research Center: Internet, Science & Tech, August 17, 2020. http://pewrsr.ch/1m8f24k.

Marx, Karl. *Early Writings*. New York, NY: Mc Graw Hill, 1964.

Masterson, Michelle. "Cybersurveillance at Work." CNNMoney. Cable News Network, 2000. https://money.cnn.com/2000/01/04/technology/webspy/.

Media, Indos. "Presentación De La Declaración De Lima Del Observatorio Iberoamericano De Protección De Datos." RS Privacidad, November 6, 2019. https://www.rsprivacidad.es/presentacion-de-la-declaracion-de-lima-del-observatorio-iberoamericano-de-proteccion-de-datos/.

Mendoza, José (2017) *"Introducción a la noción de dignitates en orden a la comprensión de las ciencias según Tomás de Aquino* (Primera parte)", en Logos. Anales del Seminario de Metafísica 50, 149-163.

Mendoza Enríquez, Olivia Andrea. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291. Recuperado en 08 de septiembre de 2025, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es.

Measuring the Information Society Report. ITU, 2014. https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

Mill, Stuart. *On liberty*. Yale University Press, NY 2003, p. 84

Moliner María. *Diccionario De Uso Del Español*. Madrid: Gredos, 2016.

Molnar, Petra y Gill, Lex. *Bots at the Gate. A human-rights analysis of automated decision-making systems in Canada´s immigration and refugee systems*. Citizen Lab, University of Toronto, 2018.

Monroy, Jorge. "Ni Cédula, Ni Clave Única Son Una Realidad En México." El Economista, 2017. https://www.eleconomista.com.mx/politica/Ni-Cedula-ni-Clave-Unica-son-una-realidad-en-Mexico-20170703-0020.html.

Muñoz, Ana F, *etal* . Revolución Digital, Derecho Mercantil y Token Economía, Ed. Tecnos, España 2019

Muñozcano Eternod, A. (2010). *El derecho a la intimidad frente al derecho a la información*. Editorial Porrúa. México 2010.

Naciones Unidas. "La Declaración Universal De Derechos Humanos | Naciones Unidas." United Nations. Accessed March 20, 2023. https://www.un.org/es/about-us/universal-declaration-of-human-rights.

Nagle, Brendan D. *The Household as the Foundation of Aristotle's Polis*. Cambridge, UK: Cambridge university press, 2006.

Nava Garcés, Alberto Enrique. "Artículo 1."In *Ley Federal De Protección De Datos Personales En posesión De Los Particulares: Y Su Reglamento: Con Comentarios*. México, CDMX: Editorial Porrúa, 2012.

Neville, Robert C. *Various Meanings of Privacy: A Philosophical Analysis, in Privacy: A Vanishing Value?* . New York, New York: Fordham University Press, 1980.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, California, USA.

"No, Tom Cruise Isn't on TikTok. It's a Deepfake | CNN Business." CNN. Cable News Network, August 6, 2021. https://edition.cnn.com/videos/business/2021/03/02/tom-cruise-tiktok-deepfake-orig.cnn-business.

NTIA , and Department of Commerce. "Elements of Effective Self-Regulation for Protection of Privacy - Discussion Draft." Elements of Effective Self-Regulation for Protection of Privacy - Discussion Draft | National Telecommunications and Information Administration, January 27, 1998. https://www.ntia.doc.gov/report/1998/elements-effective-self-regulation-protection-privacy-discussion-draft.

Nucci, Hilda. Los derechos de la personalidad en el internet y las redes sociales: propuesta de regulación, Conacyt , México CDMX, 2022.

Obama, Barak. Accessed March 15, 2023. . https://twitter.com/BarackObama.

OEA. "Relatoría Especial Para La Libertad De Expresión - OAS." Pacto Internacional de Derechos Civiles y Políticos, 1976. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=189&lID=2.

OECD. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)," 2013. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

OECD. "Thirty Years after the OECD Privacy Guidelines." The OECD Privacy Guidelines, 2011. https://www.oecd.org/digital/ieconomy/49710223.pdf.

On, Posted, and Cindy Morgan. "Internet Architecture Board." Internet architecture board, May 23, 2016. https://www.iab.org/.

Orwell, George. *Nineteen Eighty Four*. Burwood, N.S.W.: Royal Blind Society of New South Wales, 1963.

Parliamentary Assembly. PACE website, 1998. https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang+=en#:~:text=The%20Assembly%20reaffirms%20the%20importance,they%20are%20of%20equal%20value.

Partridge, Eric. *Origins: A Short Etymological Dictionary of Modern English*. London: Routledge, 2006.

Pateman, Carol, *The Disorder of Women: Democracy, Feminism, and Political Theory*, Ed. Blackwell Publishers, Ltd.

Pérez-peña, Richard. "Students Gain Access to Files on Admission to Stanford." The New York Times. The New York Times, January 17, 2015. https://www.nytimes.com/2015/01/17/us/students-gain-access-to-files-on-admission-to-stanford.html?_r=0.

Prastien, L. (2019, 28 de agosto). Rayid Ghani, pioneer in applying AI to social issues, joins Carnegie Mellon. Carnegie Mellon University.

Quijano, Camen. Derecho a la Privacidad en Internet, Ed. Tirant Lo Blanch, México, 2022

Radwanski, George. "The Impact of the Different Regulatory Models in the World Scenario." Rome: Privacy Commissioner of Canada, 2002.

Real Academia Española. "Diccionario De La Lengua Española." Real Academia Española, 2001. https://www.rae.es/obras-academicas/diccionarios/diccionario-de-la-lengua-espanola.

Rebollo Delgado, Lucrecio. Derechos de la personalidad y datos personales. En: *Revista de Derecho Político*, España, Nº 44, 1998

Reglamento General de Protección de Datos, (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Recio, Miguel. "La OCDE Actualiza Sus Directrices Sobre Protección De Datos." La OCDE actualiza sus directrices sobre proteccin de Datos, 2013. https://www.lawyerpress.com/news/2013_09/1209_13_005.html.

"Recurso de revisión del procedimiento especial sancionador." Rap, 2015. https://www.te.gob.mx/sentenciasHTML/convertir/expediente/SUP-REP-00055-2015.

Richard Pérez-peña, "Students Gain Access to Files on Admission to Stanford," The New York Times (The New York Times, January 17, 2015), https://nyti.ms/3Jvu8iw

Riesman, David. *The Lonely Crowd. A study of the changing American character*. Ed. Yale University Press, USA, 2000.

Rotenberg, Marc. "Privacy and Security for Medical Information Systems." Epic Review of Medical Privacy, October 1994. https://archive.epic.org/privacy/medical/epic_review.html.

Saldaña, María Nieves. "La Protección De La Privacidad En La Sociedad Tecnológica: El Derecho Constitucional a La Privacidad De La Información Personal En Los Estados Unidos." *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades* 09, no. 18 (2007): 85–115.

Samuelson, Pamela. "Privacy as Intellectual Property? ." Privacy As Intellectual Property? Accessed March 21, 2023. https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf.

Sánchez Guzmán, Cecilia. Derecho al Honor. *Revista Praxis de los derechos de la personalidad,* Vlex México, 2017, p. 47 y 48.

Sangokoya, David, *Data-Pop Alliance, Algorithmic Accountability*, *World Wide Web Foundation*, 2017

Sarmiento, Sergio, Columna Editorial Jaque Mate: Y la verdad, Periódico Reforma, México, D. F., 28 de Abril de 2006.

Secretaría de Gobernación. "Diario Oficial De La Federación." DOF, 2007. https://www.dof.gob.mx/nota_detalle.php?codigo=4994148&fecha=20%2F07%2F2007.

Secretaría de Gobernación. "Diario Oficial De La Federación." DOF, December 24, 2012. https://www.dof.gob.mx/nota_detalle.php?codigo=716452&fecha=24%2F12%2F2002#gsc.tab=0.

Semanario Judicial de la Federación. "Tesis Relevantes De La Primera Sala De La Suprema Corte De Justicia De ..." Tesis relevantes de la primera sala de la suprema corte de justicia de la nación, publicadas en el semanario judicial de la federación del 20 de septiembre al 11 de octubre DE 2019, 2019.

https://www.scjn.gob.mx/sites/default/files/comunicacion_digital/2019-10/TesisPrimeraSaladel20deseptiembreal11deoctubrede2019.pdf.

Serrano, Antonio en Muñoz, Ana, *etal*. Revolución Digital, Derecho Mercantil y Token Economía, Ed. Tecnos, España 2019

Solove, Daniel. *The Digital Person, Technology and Privacy in the Information Age*, New York University Press, 2004

Solove, Daniel J. *Understanding Privacy, Harvard University Press*, Cambridge, MA, 2008

Sommermann, Karl-Peter, and Ricardo García Macho, trans. "Ley Fundamental De La República Federal De Alemania." Deutscher Bundestag, 2020. https://www.btg-bestellservice.de/pdf/80206000.pdf.

Sprenger, Polly. "Sun On Privacy: 'Get over It'." Wired. Conde Nast, January 26, 1999. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

Story, Louise, and Miguel Helft. "Google Buys DoubleClick for $3.1 Billion." The New York Times. The New York Times, April 14, 2007. https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html.

Strömholm, S. (1967, mayo). *Right of privacy and rights of the personality: A comparative survey (Working Pape*r preparado para la *Nordic Conférence on Privacy organizado por la International Commission of Jurists*). https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf

"Super Bowl Snooping." The New York Times. The New York Times, February 4, 2001. https://www.nytimes.com/2001/02/04/opinion/super-bowl-snooping.html.

Suprema Corte de Justicia de la Nación. "Secretaría General De Acuerdos: Sentencias y Datos De Expedientes: Suprema Corte De Justicia De La Nación." Secretaría General de Acuerdos | Sentencias y Datos de Expedientes | Suprema Corte de Justicia de la Nación, 2012. https://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=142105.

Supreme Court of the United States. "U.S. Reports: New York Times Co. v. Sullivan, 376 U.S. 254 (1964)." The Library of Congress, 1964. https://www.loc.gov/item/usrep376254/.

Sullivan, Harry. *The Interpersonal Theory of Psychiatry*. NY: Routledge, 1982.

Schwartz, Paul M. "*Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices*." *SSRN Electronic Journal*, 2001. https://doi.org/10.2139/ssrn.254849.

Shin, Donghee, Kerk F. Kee, and Emily Y. Shin. "*Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms?" International Journal of Information Management* 65 (2022): 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494

Tenorio, Guillermo. *El Derecho a La Información*. México, CDMX: Porrúa, 2009.

Tenorio Cueto, Guillermo Antonio. (2021). *El derecho a una vida libre de algoritmos*. Revista IUS, 15(48), 115-135. Epub 14 de marzo de 2022. https://doi.org/10.35487/rius.v15i48.2021.708

Tenorio, Guillermo. Los Datos Personales en México, Ed. Porrúa, México, 2012

Thantharate, A. *ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. Big Data Cogn. Comput*. 2023, 7, 165.

"Thirty Years after the OECD Privacy Guidelines." Accessed February 25, 2023. https://www.oecd.org/digital/ieconomy/49710223.pdf.

T. Hall, Edward. *The Hidden Dimension*, *Anchor Books Doubleday*, NY 1966

Tanne, Janice Hopkins. "FDA Approves Implantable Chip to Access Medical Records." PubMed Central (PMC), November 11, 2004. https://bit.ly/2TIInLf.

Thales Group. "Facial Recognition: Top 7 Trends (Tech, Vendors, Use Cases)." Thales Group. Accessed March 21, 2023. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.

Thomas Lee, Laurie. "Defining Privacy: Freedom in a Democratic Constitutional State." *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002): 646–50. https://doi.org/10.1207/s15506878jobem4604_10.

Tony, Blair. "Tony Blair Félicite Nicolas Sarkozy (En Français)." 10 Downing Street 10 Downing Street. YouTube, May 7, 2007. https://www.youtube.com/watch?v=P6Cu9187tCY.

Tribunal Constitucional de España. "Sentencia 20/1992, De 14 De Febrero." Sistema HJ - Resolución: Sentencia 20/1992, 1992. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1907.

Tribunal Pleno de la Suprema Corte de Justicia de la Nación. "Sentencia Dictada Por El Tribunal Pleno De La Suprema Corte De Justicia De La Nación En La Acción De Inconstitucionalidad 31/2021." DOF, November 26, 2021. https://www.dof.gob.mx/nota_detalle.php?codigo=5636517&fecha=26%2F11%2F2021#gsc.tab=0.

"Truste Privacy Certification Standards." TrustArc The Leader in Privacy Management Software. Accessed February 23, 2023. https://trustarc.com/consumer-info/privacy-certification-standards.

Turkle, Sherry, Alone Together, Ed. Basic Books, 2011.

Tutt, Andrew, *An FDA for Algorithms* (Marzo 15, 2016). Administrative Law Review, Vol. 69, No. 1 (Winter 2017), pp. 83-123 (41 pages)

Ünver, H. Akın. "Politics of Digital Surveillance, National Security and Privacy." Centre for Economics and Foreign Policy Studies, 2018. http://www.jstor.org/stable/resrep17009.

Van Der, Sloot Bart. *The Handbook of Privacy Studies: An Interdisciplinary Introduction*. Amsterdam: Amsterdam University Press, 2019.

US Department of Health, Education & Welfare. *Records, Computers and and the Rights of Citizens. Chapter* III (Safewards of Privacy), 1973, DHEW Publication

Vollmer, Nicholas. "Artículo 17 UE Reglamento General De Protección De Datos." Artículo 17 UE Reglamento general de protección de datos. Privacy/Privazy according to plan. SecureDataService, August 22, 2022. https://www.privacy-regulation.eu/es/17.htm.

Wacks, Raymond. *Privacy: A Very Short Introduction*. Oxford: Oxford University Press, 2010.

Warren, Carol, and Barbara Laslett. "Privacy and Secrecy: A Conceptual Comparison." *Journal of Social Issues* 33, no. 3 (1977): 43–51. https://doi.org/10.1111/j.1540-4560.1977.tb01881.x.

Warren, Samuel, and Louis Brandeis. "The Right to Privacy." *Harvard Law Review* Volume 4, no. No. 5 (December 15, 1890): 193–220.

Westin, Alan Furman. *Privacy and Freedom*. New York: IG Publishing, 1967*, ebook* .

"Why Privacy Matters." OECD, 2022. https://www.oecd.org/digital/privacy/.

The World Medical Association, Inc.Declaration of Helsinki. "World Medical Association Declaration of Helsinki Ethical ... - WMA." Declaration of Helsinki, 2008. https://www.wma.net/wp-content/uploads/2016/11/DoH-Oct2000.pdf.

Woolley, John, and Peters Gerhard. "Executive Order 13133-Working Group on Unlawful Conduct on the Internet." Executive Order 13133-Working Group on Unlawful Conduct on the Internet | The American Presidency Project, August 5, 1999. https://www.presidency.ucsb.edu/documents/executive-order-13133-working-group-unlawful-conduct-the-internet.

World Wide Web Consortium. W3C, 2022. http://www.w3.org/.

Yiu, Tony. "Why Did Google Buy Doubleclick?" Medium. Towards Data Science, May 6, 2020. https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.

Yuste, R., Goering, S., Arcas, B. et al. *Four ethical priorities for neurotechnologies and AI*. *Nature* 551, 159–163 (2017). https://doi.org/10.1038/551159a

Zickuhr, Kathryn. "Home." Equitable Growth, March 16, 2021. https://equitablegrowth.org/.

Zuboff, S. (2019). *La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós, Barcelona.