Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: La protección de los datos personales y el derecho a la privacidad: tensiones y desafíos en los casos Edward Snowden y Christopher Wylie (2013-2018)

Autores (en el caso de tesistas y directores):

Mercedes Báez Rinaudo

Sergio Arribá, dir.

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2021

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS SOCIALES

La Protección de los Datos Personales y el Derecho a la Privacidad

Tensiones y desafíos en los casos
Edward Snowden y Christopher Wylie (2013-2018)

Mayo de 2021

Estudiante: Mercedes Báez Rinaudo

DNI: 26.746.487

Teléfono: + (1) 917-332-8520

E-mail: mercedes@bookgild.com

Tutor:

Sergio Arribá

Legajo UBA N° 146.984

Índice

Capítulo IV

Marco Jurídico: La Evolución de los Acuerdos

Capítulo V

El caso Edward Snowden y el Caso Christopher Wylie

Capítulo VI

Tensiones y desafíos en la protección de datos personales y el derecho a la privacidad

INTRODUCCIÓN

La revolución tecnológica que estamos presenciando y participando en el siglo XXI tiene como actor protagónico a Internet, que se comporta como la herramienta central de la vida cotidiana de la mayoría de los ciudadanos del planeta.

En este contexto hablamos de una vida tecnológica basada fundamentalmente en cuatro dimensiones: 1) gobierno electrónico (gobierno), 2) comercio electrónico (economía), 3) redes sociales (sociedad) y 4) juegos en redes (entretenimientos).

Estas cuatro dimensiones han conformado un nuevo paradigma y un fenómeno sin precedentes que consiste en la generación y transferencia de datos personales y datos sensibles, que los ciudadanos aceptan difundir con consentimiento (a través de la aceptación contractual "I agree") en innumerables plataformas electrónicas y redes sociales. Es decir, que los ciudadanos aceptan dar a conocer imágenes, sonidos, voces y datos personales a otras personas jurídicas (empresas de Internet) y personas físicas ("amigos" que no conocen, en el ciberespacio).

Históricamente el Estado era el sujeto del derecho responsable de poseer, resguardar y controlar los datos personales de los ciudadanos: a través del número de documento de identidad, de la atención en los hospitales, de los registros y desempeños escolares, de la participación en el mercado laboral, en los impuestos, en la seguridad social y en la emisión del voto, principalmente. El Estado era el único depositario del saber ciudadano desde la partida de nacimiento hasta el acta de defunción.

Pero la tecnología, específicamente en el siglo XXI a partir de la consolidación de Internet, de la conectividad, de la evolución de los teléfonos celulares y de las cámaras de vigilancia, permitió que no sólo los Estados sino las personas jurídicas y personas físicas pudieran tener acceso, conocimiento y transferencia de los datos personales y de los datos sensibles de la mayoría de los ciudadanos del mundo.

Actualmente, los datos personales y los datos sensibles circulan en el universo por lugares y por actores desconocidos donde los propios ciudadanos afectados por sus datos carecen de la totalidad

de esta información. Nadie sabe con precisión quién o quiénes tienen, conocen y transfieren los datos de los ciudadanos. ¿Por qué? ¿Para qué? ¿Desde cuándo y hasta cuándo sucederá este fenómeno? ¿A los ciudadanos les importa? ¿Cuáles son los riesgos y los daños causados? ¿Quién o quiénes son los responsables?

Los datos personales son informaciones que se relacionan con la identificación de los ciudadanos: el número de documento de identidad, dirección, teléfono, situación crediticia e imagen, entre otros.

Por su parte, se considera que los datos sensibles son aquellos que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

El Estado –en el escenario internacional-, por acción u omisión, ha delegado en este siglo en otros actores la protección de los datos personales y de los datos sensibles.

Hoy, ¿dónde está el Estado? ¿Es un nuevo Estado con nuevas funciones y nuevas responsabilidades? ¿Cuál es el marco jurídico para proteger los datos personales y los datos sensibles? ¿Es un marco jurídico real o formal? ¿Los ciudadanos conocen sus derechos? ¿Alguien protege a los ciudadanos o están totalmente desprotegidos en esta nueva realidad del mundo?

La elaboración masiva y descontrolada de datos personales y datos sensibles –que se produce segundo a segundo-, expone y transfiere la vida pública y privada de todos los ciudadanos del mundo. Esta exposición ha generado impactos, riesgos y nuevos delitos (informáticos, económicos, penales y civiles). Hay una nueva vida a partir y a través de Internet. Y parecería ser que hay un nuevo Estado.

Se estima que estamos ante la presencia de un Zettabyte de información, una unidad de almacenamiento de información impensada décadas atrás y que sigue creciendo progresivamente. Presenciamos la generación de información sin límites de tiempo y espacio.

Esta nueva realidad tensiona permanentemente no sólo el derecho a la protección de los datos personales y los datos sensibles, sino también el derecho a la intimidad de los ciudadanos.

El derecho a la intimidad es una facultad subjetiva de las personas que no permite la intromisión de extraños, en lo que respecta al ámbito de su reserva individual, sin perjuicio de las limitaciones normativas que de manera expresa se establezcan o de costumbres y usos sociales prevalecientes

en una época y lugares determinados. Entonces el derecho a la intimidad o la vida privada quedaría configurado como aquel ámbito de libertad necesario para el pleno desarrollo de la personalidad, espacio que debe estar libre de intromisiones ilegítimas y que constituye el presupuesto necesario para el ejercicio de otros derechos (Muñoz de Alba Medrano y Cano Valle, 2002: 38). El derecho a la intimidad puede ser configurado como aquel que garantiza a su titular el desenvolvimiento de su vida y de su conducta dentro de aquel ámbito privado, sin injerencias ni intromisiones que puedan provenir de las autoridades ni de terceros, en tanto dicha conducta no ofenda al orden público, a la moral y a las buenas costumbres ni perjudique los derechos de los demás (Scalvini y Leyva, 2002: 238).

Este panorama internacional -sobre la protección y la transferencia de datos personales y datos sensibles y, el derecho a la intimidad- ha sido develado por dos casos extraordinarios que han tenido una repercusión mundial: el caso Edward Snowden (2013) y el caso Christopher Wylie (2016).

En el 2013 Snowden, ex empleado de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos, divulgó a través de los diarios *The Washington Post* y *The Guardian* que este organismo estatal tenía registros de conversaciones telefónicas de millones de ciudadanos y, además difundió que tenían acceso a los servidores de las principales empresas de Internet (*Microsoft*, *Yahoo*, *Google*, *Facebook*, *PalTalk*, *AOL*, *Skype*, *YouTube* y *Apple*). El argumento que justificaba este primer espionaje mundial a los ciudadanos se amparaba en el combate del terrorismo internacional.

Snowden puso al descubierto información que demuestra la existencia de varios programas de vigilancia masiva de la NSA. Dentro de estos programas se destacan la existencia de: *PRIS* y *Xkeyscore*, que Estados Unidos utilizaban como herramientas para indagar todas las comunicaciones y datos personales y datos sensibles de usuarios en Internet a través de empresas como *Google*. Estas acciones realizadas por estos programas se encontrarían amparadas por la enmienda a la Ley de Vigilancia de la inteligencia Extranjera FISA.

Por otra parte, en el 2016, Wylie, empleado de la empresa Cambridge Analytica[1], divulgó a través de los diarios *The New York Times* y *The Guardian* que esta empresa accedió y utilizó de *Facebook* datos personales de 50 (cincuenta) millones ciudadanos. El argumento que justificaba este segundo espionaje mundial a los ciudadanos se amparaba en la generación de avisos personalizados con finalidad política, específicamente para influir en la intención del votante.

Wylie describió las operaciones secretas que Cambridge Analytica llevo a cabo para apoderarse de información no autorizada de millones de cuentas de *Facebook* con el propósito de crear campañas políticas, basadas en perfiles psicológicos y de personalidad, para influenciar la votación de estos usuarios en las elecciones presidenciales de Estados Unidos del 2016.

Es decir, que estos dos casos darían cuenta que fueron vulnerados el derecho a la protección de datos personales y el derecho a la intimidad de más de 50 (cincuenta) millones de ciudadanos.

Esta tesina analizará el fenómeno de la protección de los datos personales y el derecho a la intimidad en relación con los dos casos de estudio seleccionados: Edward Snowden (2013) y Christopher Wylie (2016).

El problema fundamental que considera esta tesina es la ausencia del Estado en la revolución tecnológica, que históricamente ha cumplido el rol de protección a la sociedad y control a las empresas privadas. Y parecería –porque los Estados actúan de forma tardía, débil o posterior al hecho consolidado- que se ha producido un fenómeno inverso: actualmente se protegería a las empresas y se controlaría a la sociedad.

Es importante destacar que, para el estudio, análisis, e investigación de esta tesina de graduación resulto necesario e imprescindible acceder a libros, publicaciones, informes y notas de

[1] Cambridge Analytica (CA) fue una compañía privada que combinaba la minería de datos y el análisis de datos con la comunicación estratégica para el proceso electoral. La empresa fue creada en 2013 como una rama de la casa matriz *Strategic Communication Laboratories* (SCL), para participar en la política estadounidense. La consultora estaba especializada en la recopilación y en el análisis de datos para la creación de campañas publicitarias y políticas. En el 2014, CA estuvo implicada en 44 campañas políticas estadounidenses. La compañía es en parte, propiedad de la familia de Robert Mercer, un administrador estadounidense de fondos de cobertura, quien respalda varias causas políticas de carácter conservador. Cuenta con oficinas en Londres, Nueva York, y Washington D. C. El papel de CA en esas campañas generó controversias, por lo que actualmente la empresa se enfrentó a investigaciones en diferentes países. El 2 de mayo de 2018 la empresa anunció su cierre tras el escándalo de filtración de datos personales.

diarios y periódicos que estuvieran en idioma inglés, sumado al hecho de encontrarme residiendo en Estados Unidos. Estos acontecimientos implicaron un valor y un esfuerzo complementario por mi parte para traducir al español no solo artículos periodísticos y de análisis sino también textos académicos, utilizando las palabras adecuadas en las distintas informaciones adquiridas y analizadas.

Estamos ante un Estado ausente y expectante que observa la evolución social y el desarrollo tecnológico, pero, al mismo tiempo, se posicionaría de manera neutral entre la sociedad y las empresas generadoras y transportadoras de contenidos en Internet (imágenes, sonidos, voces y datos).

Diversos autores confirman que el derecho a la protección de datos personales es el derecho ciudadano del siglo XXI, pero este derecho estaría siendo lesionado juntamente con el derecho a la intimidad en el escenario internacional.

Por su parte, las empresas, se encontrarían en una posición tecnológica de avanzada con respecto al Estado, y este nuevo escenario significaría que las empresas tienen mayor acceso, control y decisión de los datos personales y los datos sensibles que el propio Estado o los propios ciudadanos poseen.

En el problema destacado en este trabajo se visualiza que la pérdida de control y protección del Estado vislumbra ocho aristas o "caras geométricas" de un mismo problema, a saber: 1) El Estado no protegería y controlaría los datos personales y los datos sensibles de los ciudadanos, 2) El Estado no protegería el derecho a la intimidad de los ciudadanos, 3) El Estado no generaría un marco jurídico real y sencillo que pueda ser conocido y utilizado por los ciudadanos, 4) Los ciudadanos aceptarían dar y transferir (están de acuerdo) sus datos personales y datos sensibles a las empresas, 5) Existiría un desconocimiento de los riesgos y de los impactos de las transferencias y utilizaciones de los datos personales y los datos sensibles de los ciudadanos, 6) Existiría un desconocimiento de quién o quiénes poseen las bases de datos personales y de datos sensibles de

los ciudadanos, 7) La revolución tecnológica[2], que trae aparejado el desarrollo de Internet y de los dispositivos celulares, sería irreversible, y 8) Internet, en el territorio del ciberespacio, presentaría dos características fundamentales: hostilidad y vulnerabilidad.

Considerando lo dicho previamente la presente investigación plantea la siguiente hipótesis: *La ausencia del Estado y la carencia de un marco jurídico real y simple para proteger los datos personales y el derecho a la intimidad en la revolución tecnológica fortalecería a las empresas de Internet y debilitaría el ejercicio del derecho de los ciudadanos.*

Esta hipótesis se desarrollará en el marco de la realización de una tesina de grado de la Licenciatura en Ciencias de la Comunicación, mediante un trabajo que tendrá los siguientes capítulos: El capítulo I "Marco Metodológico: Lineamientos Teóricos y de Planificación" hace referencia a las diversas herramientas metodológicas utilizadas, y se explica el procedimiento y las fuentes para abordar el problema de la investigación. Luego en el capítulo II "Marco Teórico: Los Principales Conceptos del Problema de Investigación" se despliega el marco conceptual, donde se expone las nociones fundamentales que aborda el trabajo. Para completar esta primera parte teórica, el capítulo III "Marco Histórico: La Revolución Tecnológica" realiza un análisis del contexto socio-económico, tecnológico y educativo, y de los principales antecedentes históricos en la aparición de las Tecnologías de la Información y la Comunicación (TIC´s), Internet, el ciberespacio y las redes sociales.

[2] La revolución tecnológica da cuenta de un proceso dentro de la historia donde ocurre un cambio importante al introducirse una o varias tecnologías nuevas. Su implementación, es decir, su puesta en marcha, marca una época de progreso, desarrollo, e innovación, en una serie de aspectos de la sociedad. Un concepto similar y complementario es el de la evolución tecnológica, cuyo autor es el filósofo checo Radovan Richta. Este consiste principalmente en describir el desarrollo histórico de la tecnología, y por lo tanto desarrolla las distintas revoluciones tecnológicas que han existido en el desarrollo de la sociedad humana. A diferencia de los cambios tecnológicos, la revolución tecnológica comprende un período en donde se desarrollan e introducen casi simultáneamente más de una tecnología en la sociedad, produciendo cambios profundos dentro de la vida humana. Estos cambios producen una serie de revoluciones (transformaciones importantes) ya sea en materia científica, económica, y técnica, como en relación con el trabajo, y a los sistemas de dirección y organización de la producción, sin dejar de lado tampoco lo referente a la ecología y a la educación, así como lo vinculado a los sistemas de salud, de alimentación, y de comunicaciones.

El capítulo IV “Marco Jurídico: La Evolución de los Acuerdos” describe el pasaje evolutivo de Safe Harbour a Privacy Shield, y finalmente al Reglamento General de la Protección de Datos Europeo (GDPR), el capítulo V “El caso Edward Snowden y el caso Christopher Wylie”, desarrollan los hechos de estos dos acontecimientos que tuvieron un impacto internacional y el capítulo VI “Tensiones y desafíos en la protección de datos personales y el derecho a la privacidad” desarrollan las principales connotaciones y consecuencias que incidieron en el rol, los deberes, funciones y responsabilidades del Estado, las empresas privadas y los ciudadanos.

En la parte final, en las “Conclusiones” se hace un cierre reflexivo y se responden las preguntas de investigación planteadas.

La elección de la temática fue producto de los contenidos aprendidos principalmente en las siguientes materias: Derecho a la Información (Cátedra Luis Alén), Políticas y Planificación de la Comunicación” (Cátedra Glenn Postolski) y Teorías del Estado y la Planificación (Cátedra Gustavo Bulla). Y al mismo tiempo, se realizó por motivos personales, porque siempre me atrajo la atención la gravitación y la importancia de la protección de los datos personales como fenómeno impactante en el derecho a la intimidad en la utilización de las TIC´s y las redes sociales.

Es importante destacar que si bien la problemática de la protección de los datos personales y el derecho a la intimidad son temática que han sido abordadas en la Facultad de Ciencias Sociales, no se ha hallado ningún trabajo de investigación, con formato de Tesina de Grado, que se refiera, específicamente, a los casos reconocidos a través de la figuras de Edward Snowden y Christopher Wylie. Sin embargo, por aproximación y cierta afinidad al tema abordado, se puede hacer referencia a las siguientes tesinas, las cuales lamentablemente no pudieron ser consultadas por no encontrarse estos textos digitalizados y de acceso libre.

- “Google adsense y la protección de datos personales. El conflicto del modelo de la publicidad digital dentro de la normativa argentina”, autora: Julieta Lezcano (Tutor: Federico Corbiere, 2012).

- “Protección de Datos Personales en redes sociales y webs 2.0”, autor: Ezequiel Passeron. (Tutor: Damián Loreti, 2012).
- “Derecho a la intimidad en la sociedad de la información”, autora: Daniela Chiaeppe (Tutor: A. Alem, 1998).

Finalmente, se destaca que se procura iniciar un camino de investigación en esta Alta Casa de Estudios sobre casos emblemáticos y críticos que impactaron en el escenario internacional del derecho a la protección de datos personales y en el derecho a la intimidad, con el deseo de que otros textos futuros e investigaciones académicas profundicen los aportes presentados.

CAPITULO I. MARCO METODOLÓGICO:

LINEAMIENTOS TEÓRICOS Y DE PLANIFICACIÓN

"No estoy aquí para decir la Verdad.
Estoy aquí sólo para darte un método para percibirla"

Sadhguru Jaggi Vasudev[3]

[3] Es un yogui indio y creador de la Fundación "Isha". Autor de numerosos libros considerados *best sellers*, entre los que se destaca "Ingeniería interior: guía yogui para alcanzar la alegría y el gozo" (2020, Madrid: Gaia) y "Adiyogi: the source of Yoga (2017, India: Harper Collins).

1.1. Aproximaciones metodológicas

En primer lugar, resulta importante definir el concepto de metodología. Dentro de las diferentes ciencias, la metodología es lo que se llama al conjunto de técnicas y métodos de estudio a nivel científico, que se aplican sistemáticamente durante un proceso de investigación y se utilizan como guía con el objetivo de producir un conocimiento nuevo y deducciones válidas. Bourdieu, sostiene que el hecho científico se conquista, se construye y se comprueba. Esta posición del autor implica rechazar al mismo tiempo el empirismo que reduce el acto científico a una confrontación y el convencionalismo que solo le opone los preámbulos de la construcción. (…) la jerarquía epistemológica de los actos científicos que subordina la confrontación a la construcción y la construcción a la ruptura… (Bourdieu et al., 2004 [1972]: 25).

Bourdieu define la construcción del objeto de estudio como la más importante de la investigación, pero sin embargo la más ignorada por encontrarse la atención del investigador usualmente enfocada en la oposición entre "teoría" y "metodología" (Cerón-Martinez, 2011). Según el autor: "un objeto de investigación, por más parcial y parcelario que sea, no puede ser definido y construido sino en función de una problemática teórica que permita someter a un sistemático examen todos los aspectos de la realidad puestos en relación por los problemas que le son planteados" (Bourdieu, Chamboderon y Passeron 2002:54).

Dentro de las ciencias sociales se reconocen mayormente dos tipos de metodologías para analizar los problemas y los diversos temas de investigación: **la cualitativa y la cuantitativa**. Cada uno de estos métodos utiliza herramientas, procedimientos y fuentes de investigación para indagar los diferentes objetos de estudio.

Bonilla y Rodríguez (1997) explican que la investigación **cuantitativa**, utiliza como herramienta principal la medición de fenómenos sociales, lo cual supone derivar de un marco conceptual, pertinente al problema analizado y una serie de hipótesis que expresan relaciones esperadas entre las variables formuladas de forma deductiva. En la metodología cuantitativa se busca un dato para poder tabularlo y analizarlo a través de instrumentos.

Por otro lado, los Bonilla y Rodriguez (1997) consideran la visión del mundo social por parte de la investigación **cualitativa** como un orden dinámico creado por la acción de los participantes cuyas significaciones e interpretaciones personales guían sus acciones y los hallazgos derivan en interpretaciones de la realidad social estudiaba en su forma natural y según el dinamismo de la vida socia.

Tanto la metodología cualitativa como la cuantitativa son válidas como método de estudio y ninguna es superior a la otra ni tampoco son contrapuestas. Ambas proporcionan ventajas y limitaciones, así como información heterogénea y hasta pueden utilizarse de manera complementaria como si fueran dos puertas de entrada para abordar un mismo objeto de estudio. Desde el punto de vista del investigador, es importante penetrar el contexto con el objetivo de entender la realidad de lo que rodea al objeto de estudio y así adquirir una comprensión global de su realidad y en consecuencia generar un conocimiento fehaciente.

Como ya hemos mencionado en la introducción, para esta tesina hemos descripto y analizado el caso de Edward Snowden en el año 2013, así como el caso Christopher Wylie en el año 2018. Para este objeto de estudio es necesaria una preeminencia de la metodología cualitativa. Consistió en una serie de actividades interpretativas y materiales que hicieron al mundo visible desde mi lugar de observadora enmarcándolo dentro de un cierto lugar y tiempo, analizando y recolectando información de estos dos casos particulares.

Mi investigación ha requerido el uso de una variedad de técnicas de recolección de datos y registros de materiales empíricos, producciones culturales y textos observacionales. Como resultado, he desplegado un amplio rango de prácticas interpretativas interconectadas con el objetivo de lograr un superior entendimiento de los casos estudiados y de sus consecuencias en los procesos sociales, políticos, económicos, jurídicos y culturales. El estudio implicó la descripción, análisis, el contraste y la generación de conclusiones respecto a la protección de datos personales y al derecho a la privacidad, utilizando fuentes primarias y contrastándolas con diferentes fuentes secundarias.

En cuanto al uso de **fuentes primarias**, o aquellas que no han sido interpretadas, que son originales y que se produjeron como resultado de un trabajo intelectual, he utilizado material bibliográfico tales como leyes, tratados, proyectos de ley, pactos internacionales, regulaciones,

normativas, reglamentaciones, declaraciones, trabajos de investigación, entre otras. En cuanto a las **fuentes secundarias** son aquellas consideradas interpretaciones y análisis de las fuentes primarias o de los hechos y declaraciones generadas por los actores involucrados en estos casos. Como tal, las fuentes secundarias conllevan una pérdida de la neutralidad característica de las primarias. En mi investigación fueron utilizados libros (de texto, de periodistas, analistas, profesores, investigadores entre otros), publicaciones en internet, periódicos, artículos en la web y aquellas que se consideran interpretaciones o comentarios acerca de los casos Snowden y Wylie.

Del mismo modo, he trabajado con diferentes interpretaciones y opiniones acerca del uso e implementación de las normativas jurídicas nacionales e internacionales dentro de cada caso y a nivel general, analizando publicaciones realizadas por organismos internacionales, regionales y nacionales, así como organizaciones no gubernamentales.

Cabe aclarar que al encontrarme residiendo en Estados Unidos, la mayoría de las fuentes consultadas estaban escritas en idioma inglés, lo cual generó la necesidad el esfuerzo adicional de traducir al español por mi parte.

Finalmente, quisiera agregar un párrafo escrito por Manuel Amezcua y Alberto Gálvez Toro (2002), los cuales sostienen que *"El análisis cualitativo es un proceso dinámico y creativo que se alimenta, fundamentalmente, de la experiencia directa de los investigadores en los escenarios estudiados, por lo que esta etapa no se puede delegar. Los datos son a menudo muy heterogéneos y provienen tanto de entrevistas (individuales y en grupo), como de observaciones directas, de documentos públicos o privados, de notas metodológicas, etc., cuya coherencia en la integración es indispensable para recomponer una visión de conjunto. Aunque todos los datos son importantes, se precisa de una cierta mirada crítica para distinguir los que van a constituir la fuente principal de la teorización (ej. un relato biográfico) de los que sólo aportan información complementaria o ilustran que cuando "y provienen de distintas fuentes [la] coherencia en la integración es indispensable para recomponer una visión de conjunto. Aunque todos los datos son importantes, se precisa de una cierta mirada crítica para distinguir los que van a constituir la fuente principal de la teorización (ej. un relato biográfico) de los que sólo aportan información complementaria o ilustran los primeros (ej. cartas, fotografías, etc.)". El estudio parte entonces de analizar diversos hechos en cada caso y contrastarlos con el objetivo de encontrar similitudes y diferencias en "un*

esquema en espiral que obliga a retroceder una y otra vez a los datos para incorporar los necesarios hasta dar consistencia a la teoría concluyente." (Amezcua, Galvez, 2002).

1.2. Hipótesis

La ausencia del Estado y la carencia de un marco jurídico real y simple para proteger los datos personales y el derecho a la intimidad en la revolución tecnológica fortalecería a las empresas de Internet y debilitaría el ejercicio del derecho de los ciudadanos.

1.3. Objetivo general

- Dar cuenta y analizar el rol del Estado y el marco jurídico generado en los casos Snowden (2013) y Wylie (2018).
- Presentar las principales tensiones y desafíos del derecho a la protección de datos personales y del derecho a la intimidad.

1.4. Objetivos específicos

- Definir los conceptos de Estado.
- Desarrollar el concepto de derecho a la comunicación.
- Dar cuenta del concepto del derecho a la intimidad.
- Describir el término de derecho a la protección de datos personales y datos sensibles.
- Analizar la Revolución Tecnológica.
- Indagar sobre el fenómeno conocido como "Internet de las Cosas".
- Presentar las principales características de la "Inteligencia Artificial".
- Examinar el "Capitalismo de Vigilancia".

- Analizar los acuerdos “Safe Harbour”, “Privacy Shield” y el “Reglamento General de la Protección de Datos Europeo (GDPR)”.

CAPÍTULO II. MARCO TEÓRICO:

LOS PRINCIPALES CONCEPTOS DEL PROBLEMA DE INVESTIGACIÓN

"Hablamos de ´software que se come el mundo´, ´Internet de las cosas´, y masificamos los ´datos´ declarándolos ´grandes´.
Pero estos conceptos siguen siendo en su mayor parte abstractos. Para muchos de nosotros es difícil comprender el impacto de la tecnología digital en el ´mundo real´ de cosas como rocas, casas, automóviles y árboles".

John Battelle[4]

[4] Es periodista y fundador de la Federated Media Publishing. Autor del libro "The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture" (La búsqueda: cómo Google y sus rivales reescribieron las reglas del negocio y transformaron nuestra cultura) -2006, Estados Unidos, Portfolio-.

2.1. El Estado

Guillermo O' Donnell (1984) define al Estado capitalista como el "componente específicamente político de la dominación en una sociedad territorialmente delimitada". El autor define dominación (o poder) como la capacidad de imponer la voluntad sobre otros, aun contra su resistencia. Esta dominación es relacional, por generar una vinculación entre sujetos sociales[5], desigual y asimétrica, al surgir del control diferencial de recursos tales como económicos, de información, científicos-tecnológicos e ideológicos, así como el control de los medios de coerción física. A esta relación desigual, el dominado la asume como justa y natural y no la cuestiona como dominación (O'Donnell, 1984:21). Resulta innecesario describir todos los recursos que el Estado posee en contraste con la sociedad para el propósito de esta tesina, pero si cabe mencionar la importancia del control de los recursos de información, especialmente aquellos programas y proyectos desarrollados sin el conocimiento o el consentimiento de la sociedad. Este secretismo es justificado detrás del concepto de "seguridad nacional", nuevamente esforzando la dominación por parte del Estado.

O' Donnell también sostiene que el Estado materializa y ejecuta la coerción mediante las instituciones estatales, generando una apariencia de agente externo al Estado pero esto solo es el una forma de encubrir la dominación (O'Donnell, 1984:13-15). Por otro lado, Bourdieu (2002) considera que el Estado es la manifestación resultante de diferentes especies de capital: el de la fuerza física que incluye los elementos de coerción, el económico y el cultural o informacional. En este sentido, el Estado está capacitado para ejercer la violencia simbólica y física pues la puede representar mediante la forma de estructuras.

En cuanto al concepto de Estado de derecho, O'Donnell (2001) considera que debería concebirse como una característica genérica del sistema legal y de la actuación de los tribunales, pero sobre todo como la norma basada en la legalidad de un estado democrático. Este sistema legal resulta democrático en tres sentidos:

[5] Cabe aclarar que no todas las relaciones sociales son asimétricas o de dominación, pero en aras de describir la relación Estado-Sociedad, es necesario hacerlo desde un lugar desigual.

- Uno, defiende las libertades políticas y las garantías de la democracia política.

- Dos, defiende los derechos civiles de todo el conjunto de la población.

- Tres, establece redes de responsabilidad y *accountability* que comportan que todos los agentes, privados y públicos, incluyendo los cargos más altos del régimen, estén sujetos a controles apropiados y legalmente establecidos sobre la legalidad de sus actos[6].

Esta legalidad se encuentra profundamente conectada con los atributos de la democracia política, o poliarquía, enunciados por Dahl (1989:221). A saber: 1) Cargos electos; 2) Elecciones libres y justas; 3) Sufragio universal; 4) El derecho de presentarse como candidato a un cargo; 5) Libertad de expresión; 6) Información alternativa; y 7) Autonomía asociacional. A estos atributos, O' Donnell (1996) añade: 8) Cargos electos (y algunos individuos nombrados, tales como jueces de tribunales supremos) no deberían ser cesados arbitrariamente antes de la finalización de su período de mandato constitucional; 9) Los cargos electos no deberían estar sujetos a restricciones severas, vetos, o exclusión por parte de otros de ciertos dominios políticos, actores no elegidos, especialmente las fuerzas armadas; y 10) Debería existir un territorio ganado sin oposición que definieran claramente los votantes. Al conjunto de estos diez atributos lo llamo democracia política, o poliarquía, o régimen democrático.

En otras palabras, el Estado de derecho consiste en la sujeción de la actividad estatal a la Constitución y a las normas aprobadas conforme a los procedimientos que ellas establecen con el objetivo de generar un funcionamiento responsable y controlado de los órganos de poder. Mann (1991) denomina al "poder del Estado" como poder infraestructural o su capacidad para penetrar la

[6] En este sentido O' Donnell describe el concepto de "accountability" como aquel en el cual el Estado debe dar cuenta de sus decisiones a la Sociedad. Veremos más adelante en esta tesina que Estados Unidos genera un proceso legal en contra de Snowden por haber denunciado programas de extremo secretismo y haber quebrado su responsabilidad como ciudadano a conservar esa información, pero falló en reconocer que la naturaleza de estos programas se encontraba en contra de los derechos a la privacidad por parte de la sociedad.

sociedad civil y poner en ejecución las decisiones políticas por todo el país. Por otro lado, Mann describe el "poder despótico" o "autonomía de poder" de la elite estatal, al abanico de acciones que la elite tiene facultad de emprender sin negociación rutinaria, institucional, con grupos de la sociedad civil. lo importante para Weber, es como valoran los seguidores al líder indistintamente de cuales sean sus características personales. La extraordinariedad se construye a través de la relación líder–adeptos (Deusdad: 2001).

Retomando las diferentes definiciones de Estado, Oszlak (1978) lo define como el resultado de un proceso de construcción social que supone la conformación de una instancia política que articula la dominación de la sociedad. Oslak denomina "estatidad" a la adquisición de una serie de propiedades que define la existencia del Estado y sus capacidades. A saber:

a) la capacidad de externalizar su poder, adquiriendo reconocimiento como unidad soberana dentro de un sistema de relaciones interestatales;

b) la capacidad de institucionalizar su autoridad al imponer un sistema de relaciones de poder donde ejerce el monopolio legítimo de la coerción;

c) la capacidad de diferenciar su control mediante la creación de un conjunto de instituciones públicas;

d) la capacidad de internalizar una identidad colectiva (por ejemplo, el patriotismo) mediante la emisión y transmisión de símbolos que refuerzan sentimientos de pertenencia y solidaridad social que aseguren el control ideológico como mecanismo de dominación. (Oszlak, 1978:19).

Dos años más tarde, Oslak afirmó que: "El Estado ya no puede concebirse como una entidad monolítica al servicio de un proyecto político invariable, sino que debe ser visualizado como un sistema en permanente flujo, internamente diferenciado, sobre el que repercuten también diferentes demandas y contradicciones de la sociedad civil" (Oszlak, 1980:12).

Por otro lado, Bourdieu (2002) considera que el Estado es la manifestación resultante de diferentes especies de capital: el de la fuerza física que incluye los elementos de coerción, el económico y el cultural o informacional. Para el autor, el Estado puede ejercer la fuerza física y la violencia simbólica a través de sus diferentes estructuras. O'Donnell coincide con Bourdieu en este punto. O'Donnell considera que el Estado ejecuta la coerción a través de ciertas instituciones estatales que él denomina como "tercer sujeto" y que se caracteriza por ejercer la supremacía de la coacción. El autor considera que la emergencia de un tercero (las instituciones sociales) pone en juego las relaciones capitalistas de producción que genera el Estado a través de una "difusa coerción económica". La considera difusa por que no puede ser imputada ni a los capitalistas concretos ni a las instituciones estatales, al no poder obligar a vender su fuerza de trabajo a ningún sujeto social concreto. Esta falta de coacción para vender la fuerza de trabajo es la condición necesaria para la apariencia, formal, de igualdad entre las partes.

Finalmente, me parece importante describir la postura de Ernesto Aldo Isuani (ver Isuani en Publicaciones, libros en línea e investigaciones académicas en Fuentes Consultadas) en cuanto al concepto del Estado pues analiza diferentes autores como Locke, Weber, Rousseau y Hobbes, entre otros, quienes fueron asimilados en varias materias durante la carrera de comunicación social. Isuani clasifica tres conceptos de Estado dentro de la teoría política: a) como una asociación o comunidad incluyendo una institución de gobierno; b) como una dimensión de la sociedad, cubriendo u oponiéndose a otras dimensiones sociales y c) como un aparato para el gobierno, la administración y la coerción.

a) *El Estado como una asociación o comunidad:* Esta es vista como desde "abajo"; el Estado emergiendo de un pacto entre los miembros de una comunidad humana determinada. Este enfoque adquirió su más pura formulación en las teorías del contrato social. Issuani describe cómo diferentes autores se refieren al Estado con diferentes nominaciones: Hobbes: "Estado civil" o "Commonwealth", Locke: "sociedad política" o "sociedad civil", "estado de paz", "comunidad" y "sociedad"; por su parte Rousseau usa la palabra "Estado civil", "Estado social" y "sociedad civil". Según Isuani resulta importante no confundir el Estado con el gobierno.

Dentro de las teorías del contrato social encontramos diferentes autores: para Hobbes "…(el bien común) (…)es una unidad real de individuos en una sola y misma persona, hecha por acuerdo entre todos los hombres, de manera tal, que un hombre debería decir a los otros: 'Yo autorizo y doy mi derecho de gobernar a este hombre o a esta asamblea de hombres, en la condición que de tú cedas al otro tu derecho y autorices todas sus acciones de esa manera'. Eso, la multitud unida en una persona sola es el llamado "Commonwealth" (ver Hobbes en Publicaciones, libros en línea e investigaciones académicas, en Fuentes Consultadas).

Las teorías de Locke (1690) se basan en la ley natural; "El Estado de naturaleza tiene una ley natural para gobernarlo y que obliga a todos. Es la razón, que es esa ley que enseña a toda la humanidad, que solamente a ella consultará, que siendo todos iguales e independientes, nadie deberá perjudicar al otro en su vida, salud, libertad o propiedad"[7]. Es la injusticia proveniente del hecho que el individuo es simultáneamente juez y acusador lo que torna al contrato social necesario". Así, cuando los individuos concuerdan en desistir de su derecho de castigar a los transgresores (un derecho que tienen en virtud de la ley natural) y establecen un tribunal, es cuando ellos crean una sociedad civil o un Estado.

En Rousseau (1936), la soberanía es del pueblo, siendo esta delegada a los funcionarios autorizados que son sujetos a la voluntad general: "Los miembros de ese cuerpo (gobierno) son llamados magistrados o reyes, es decir, gobernantes (...) y el cuerpo general lleva el nombre de príncipe. Tienen mucha razón aquellos que sostienen que no es un contrato en absoluto el acto por el cual un pueblo se somete a un príncipe. Es sola y simplemente una comisión, un empleo, en el cual los gobernantes, meros funcionarios del soberano, ejercen en su nombre el poder del que él los hizo depositarios. Ese poder puede ser limitado, modificado o recuperado cuando fuere aprobado, porque la alienación de tal derecho es incompatible con la naturaleza del cuerpo social y contraria al objetivo de la asociación". Según su teoría radical de la democracia directa, los delegados del pueblo poseen límites claros en sus actividades.

b) *El Estado como una dimensión de la sociedad, cubriendo u oponiéndose a otras dimensiones sociales:* Dentro de esta categoría se encuentra la teoría de Max Weber en la cual la asociación es vista como "desde arriba", o de dominación y en la cual ciertos grupos controlan otros grupos dentro de un territorio determinado.

Del mismo modo y desde un punto de vista marxista, Mabel Thwaites Rey (1999:4) considera que tanto el capital como el Estado son relaciones sociales. El Estado en particular es una relación de dominación: "(…) no es posible escindir Estado de Sociedad, como no es posible escindir lo económico de lo político, porque ambos son partes co-constitutivas de una única realidad: la relación social capitalista". De la misma manera que los trabajadores no poseen los medios de producción material, los capitalistas no poseen el uso de la fuerza física. Por lo cual el monopolio de la coerción se encuentra en manos del Estado.

2.2. Derecho a la Comunicación

La libertad de información puede definirse como el derecho a tener acceso a la información que está en manos de entidades públicas. Es parte integrante del derecho fundamental a la libertad de expresión, reconocido por la Resolución 59 de la Asamblea General de las Naciones Unidas, aprobada en 1946, así como por el Artículo 19 de la Declaración Universal de Derechos Humanos (1948), que dispone que el derecho fundamental a la libertad de expresión incluye el derecho de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

La legislación en materia de libertad de información refleja la premisa fundamental de que toda la información en poder de los gobiernos y las instituciones gubernamentales es, en principio, pública y solo podrá ser retenida si existen razones legítimas para no divulgarla, como suelen ser la privacidad y la seguridad.

En el artículo 19 de la Declaración Universal de los Derechos Humanos de 1948, todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser

molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. A su vez esta norma tenía como antecedente la resolución 59 del 14 de diciembre de 1946 en donde la ONU sostiene que: (...) la libertad de información es un derecho fundamental del hombre, y piedra de toque de todas las libertades a cuya defensa se consagran las Naciones Unidas... La libertad de información implica el derecho a recoger, transmitir y publicar noticias sin trabas en todos los lugares [...] constituye un elemento esencial de todo esfuerzo serio para favorecer la paz y el progreso en el mundo.

Por su parte, a nivel americano, el 22 de noviembre de 1969, la Convención Americana sobre Derechos Humanos (también denominada Pacto de San José de Costa Rica) pronunció en el artículo 13 y en el artículo 14 las siguientes expresiones: "1) Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2) El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. 3) No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. 4) Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2. 5) Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional".

En otro artículo del mismo pacto se refiere a lo que se conoce vulgarmente como el "derecho a réplica", en el cual la figura de "editor responsable" debe respetar el honor de las personas. Para

los intereses de esta tesina dejaremos fuera de la investigación los conceptos de libertad de prensa, aunque cabe aclarar que en la constitución argentina se excluye la censura previa, al menos que esta sea con el objetivo de proteger al estado en situación particulares como ser la de amenaza a la seguridad del Estado. Y se incluye la responsabilidad ulterior por cualquier ilícito penal o civil que pueda haberse cometido a través del ejercicio de esta libertad.

La evolución del concepto de libertades individuales hacia los derechos sociales se cristaliza cuando se reconocen los derechos humanos en todo el mundo por ser un derecho intrínseco de cada persona. Así, definimos que el derecho a la información implica la existencia de tres elementos principales: la búsqueda o investigación, la recepción y la difusión de la información.

Sin embargo, la concepción actual del derecho humano tiende a ampliarse al derecho a la comunicación. Por lo cual, consideramos que el concepto de comunicación abarca al concepto de información, el cual podría denominarse un antecedente del primero. El concepto de comunicación es más amplio. Duhalde y Alén (1980) llegan a considerar el término comunicación como más democrática y menos autoritaria pues no remite a quien es propietario del saber. La información tendría un carácter unidireccional, con un emisor y un receptor, ya sea individual o colectivo, y la comunicación, una acción dual, interactiva, con la existencia de un diálogo. Duhalde y Alén la definen como "el intercambio de significados entre individuos mediante un sistema común de símbolos, donde el lenguaje constituye el más importante medio de comunicación del hombre, el instrumento primordial que marca su diferencia con el resto de los animales". Sin embargo, el concepto de información no deja de ser importante, incluso nombrar que el mismo ha generado el nombre a la ciencia de la informática.

En 1974, en el informe provisional de la Comisión MacBride se indica: "Hoy en día, el concepto (esto es, el derecho a comunicar) con el cual engarza las nociones de libertad, responsabilidad, equilibrio, acceso y participación, tiende a sustituir el derecho a la información, relativamente reciente también, que abarcaba ya la libertad de información y la de prensa. A pesar de la ambigüedad del concepto, el derecho a comunicar presupone una comunicación de doble sentido y bilateral, una relación mutua. Implica varias libertades fundamentales que no afectan solamente a los individuos sino también a los grupos y las naciones. Sería muy oportuno estudiar el modo de reducir el abismo que media entre las especulaciones intelectuales sobre ese derecho y

las realidades concretas de las comunicaciones en el mundo actual. Lo que está en juego justifica ampliamente los esfuerzos necesarios para que el reconocimiento del derecho pueda constituir un progreso en el establecimiento de un nuevo orden mundial de la información.”.

Por su parte, Desmond Fisher en 1980 presentó el Informe “El Derecho a Comunicar, Hoy” (promovido por la UNESCO) considerando al derecho a la comunicación como un concepto es una idea y un ideal. Es una idea pues solo existe en forma teórica y no existe un acuerdo por el cual sobre sus elementos y cualquier relación entre ellos. Tampoco existe una expresión concreta en ningún convenio o tratado internacional o documentos jurídicos nacionales. Y es un ideal por el esfuerzo que los cultores del concepto tratan de que sea declarado y promulgado reconociendo su carácter de derecho humano básico. Sin embargo, Fisher señala que la razón de la falta de la formulación de este derecho es que se considera intrínseco y supuesto, similar al derecho a existir; el ser humano se representa como un comunicador natural por ser una necesidad humana el acto de comunicar. El principio de comunicación consiste en un intercambio interactivo de información y el fundamento ético es la responsabilidad de garantizar una distribución más justa mundial de los recursos que sean necesarios para que la comunicación sea posible.

En el Informe “El Derecho a Comunicar. Hoy”, Henry Hinley (jurista canadiense) y Aldo Armando Cocca (jurista argentino) (2014), enumeraron diferentes elementos del derecho a comunicar, entre ellos:

- El derecho a hablar.
- El derecho a ser oído.
- El derecho a recibir una respuesta.
- El derecho a contestar.
- El derecho a escuchar.
- El derecho a ver.
- El derecho a ser visto.
- El derecho a expresarse por escrito o en forma impresa.
- El derecho a expresarse por medio del arte.

- El derecho a ser selectivo o a no informar ni ser informado.

En este contexto, Duhalde y Alén distinguen también tres categorías básicas dentro del derecho a comunicar:

1. Derechos del individuo, con el siguiente contenido:

- Libertad de opinión y de expresión.
- Derecho a ser informado.
- Derecho a informar.
- Protección de la vida privada.
- Libertad de movimiento.
- Derecho a reunión.
- Acceso a las fuentes de información.

2. Derechos de los medios de comunicación y de los grupos profesionales interesados, con el siguiente contenido:

- Acceso a las fuentes de información.
- Libertad de opinión y de expresión.
- Derecho a informar.
- Derecho a publicar.
- Derecho al mantenimiento del secreto profesional.
- Libertad de movimiento.

3. Derechos de las comunidades locales, nacionales e internacionales, con el siguiente contenido:

- Derecho a informar.

- Circulación libre y equilibrada de la información.
- Protección de la integridad cultural.
- Libertad de opinión y de expresión.
- Derecho a ser informado.
- Derecho de rectificación.
- Derecho de respuesta.

Fisher (1984) considera que: "(...) el núcleo interior de una serie de libertades mutuamente relacionadas en el campo de la comunicación, rodeado por la libertad de opinión, la libertad de expresión y la libertad de información, las cuales no son absolutas en sí mismas, sino que constituyen los campos principales de la vida humana en los cuales se ejerce el derecho fundamental a comunicar".

Finalmente, y antes de introducir el concepto de tecnología y su influencia en la comunicación, quisiéramos agregar un párrafo del informe MacBride, donde se toma en cuenta la transnacionalización:

En el plano internacional, los modelos de comunicación se parecen mucho a los que se aplican en los demás sectores de la vida económica. La expansión general de las empresas trasnacionales en los sectores vitales es una tendencia reciente y significativa que incide en el mercado internacional, en los intercambios, en el empleo e incluso en la estabilidad y la independencia de ciertos países. El fenómeno conocido con el nombre de trasnacionalización o trasnacionalidad ha afectado prácticamente a todo el sector de la comunicación. Se puede hablar inclusive de un fenómeno trasnacional de la comunicación. Al igual que en otros sectores de la economía trasnacional, cabe distinguir, en las operaciones industriales y financieras de la comunicación de masas, los centros, que controlan la producción y los servicios, y los mercados periféricos que los absorben.

El Informe presidido por Sean MacBride (1980), titulado "Un solo mundo, voces múltiples. Información y Comunicación en Nuestro Tiempo" introduce la idea previamente mencionada de

ampliar el concepto de derecho a la información hacia el de derecho a la comunicación, entendido como un derecho fundamental del individuo como así también un derecho colectivo.

2.2.1. La comunicación y los avances tecnológicos

La comunicación y la tecnología han estado históricamente relacionadas e interconectadas de manera que una ha influido a la otra y viceversa generando a su vez crecimiento en otras áreas. A medida que el hombre adopta nuevas tecnologías, esto se hace aún más evidente. El poder de la comunicación social se encuentra cada vez más concentrado en los países centrales, en las grandes empresas de tecnología y sobre todo en quienes tienen capacidad financiera y los medios tecnológicos necesarios.

La tecnología influye en la creación, almacenamiento y transmisión de datos. Fraguas de Pablo sostiene al respecto:

> *Como todo adelanto tecnológico implica dos aspectos: La posibilidad por parte de la periferia más alejada de obtener una información inmediata y exhaustiva sobre cualquier tema y para aquellos en cuyas manos se encuentran o de cuyas manos han salido las memorias masivas, la de desinformar también masivamente. Se podría así preparar el advenimiento de una 'dictadura invisible que seguiría utilizando las formas de un gobierno democrático' (cita de la obra La persuasión clandestina, de V. Packard) (Fraguas, 1985).*

La informática deriva en una forma de poder al producir una realidad unidimensional donde el discurso de poder apunta a una unidad: una misma concepción del mundo que el gobernante y el gobernado viven como si fuera el mismo mundo. Lechner considera que la realidad social es formada y produce poder, al ser informada. Este poder genera un doble miedo: el miedo a perder los límites establecidos, el cual legitima el poder y los límites sociales, y el miedo al mismo poder,

el cual presenta sus propios peligros (Schmucler, 1989). Por otro lado, la información permite al Estado vigilar "invisiblemente" a través de la omnipresencia del control. Por este motivo, la informática deja de set una tecnología neutral e informar es uniformar al mismo tiempo. La función básica de la informática es almacenar datos y predecir o proyectar el futuro a nivel probabilidades numéricas y regulares, pero no puede dar cuenta de lo cualitativo.

La comunicación también forma parte de la llamada "aldea global" de la que se refería McLuhan. La globalización genera una especie de desaparición de las distancias geográficas, los diferentes idiomas, etnias, culturas e incluso fronteras estatales. Esta especie de "desaparición" da lugar a la creación de una nueva cultura "nacional" y un mercado único que arrasa todo lo que se le opone. Pareciera que la globalización, posibilitada por el ingreso de la tecnología, es el vehículo para "civilizar" a la población mundial. En palabras de Garcia Canclini (1999):

> *El relato más reiterado sobre la globalización es el que narra la expansión del capitalismo posindustrial y de las comunicaciones masivas como un proceso de unificación y/o articulación de empresas productivas, sistemas financieros, regímenes de información y entretenimiento [...] además la globalización –o más bien las estrategias globales de las corporaciones y de muchos Estados– configuran máquinas segregantes y dispersadoras: producen desafiliación a sindicatos, mercados informales conectados por redes de corrupción y lumpenización, culturas audiovisuales opuestas a la cultura letrada.*

Sin embargo, existe una paradoja: cuanto más comunicado e interconectado se encuentre el hombre, más lejos se encuentra de utilizar esas herramientas en pos del progreso social. La razón es que la integración y la comunicación operan sobre pautas impuestas por un poder económico y político que no está interesado en compartir ese poder ni sus logros (Duhalde, Alén, 1980). Por lo cual la tecnología sirve al propósito de sus dueños. Como afirma Emilio Caffasi (1998): "las redes computacionales son en sí mismas un instrumento de acción política y cultura.

Internet, como un producto del avance tecnológico, tiene algunas diferencias con la informática. La facilidad para acceder a la red, la explosión de la tecnología celular, y las grandes posibilidades de comunicación, así como la rapidez con la que los usuarios se convierten en

creadores de contenidos, entraña una nueva dificultad: la de controlar esos contenidos que circulan por la autopista informática. Ejemplos de esto es la invasión de la privacidad, pornografía, *fake news* o noticias falsas, y más. Lamentablemente la única forma de generar condiciones igualitarias tanto en países desarrollados como subdesarrollados es el generar una legislación internacional acorde. Duhalde y Alén consideran que para que esto sea posible, el NOMIC (el Nuevo Orden Mundial de la Información y la Comunicación), planteado desde el surgimiento del informe MacBride, y que generó gran oposición por parte de los países centrales, se tendría que transformar en realidad (Duhalde, Alén, 1980).

La UNESCO considera que este nuevo paisaje mediático ha generado la adopción de nuevas leyes y políticas, o la modificación y uso de las ya existentes, con el fin de limitar o castigar el acceso a los medios en línea, lo cual no muestra respeto por los estándares internacionales relativos a las limitaciones. A su vez, la UNESCO agrega que estos cambios han creado nuevos intermediarios en el sector privado cuyas decisiones impactan en los flujos de información y la privacidad y generan censura a través del bloqueo de usuarios y filtrado de contenidos (Esco, 2014).

Al respecto, la agencia *Associated Press* publicó un artículo recientemente donde algunos legisladores del partido republicano están promoviendo la generación de grandes multas y procesos legales en contra de las grandes empresas de medios sociales, como Facebook, por haber censurado cierta información con respecto a Donald Trump al final de su campaña política, o *Twitter* por haber bloqueado su cuenta en la plataforma[8]. Otro artículo en *The Wall Street Journal* explica como *Parler*, una aplicación mayormente utilizada por seguidores conservadores de Donald Trump, se encuentra en negociaciones con la empresa *Apple* y *Google*, luego de que ambas hayan prohibido la aplicación en sus plataformas por no haber tomado las precauciones necesarias

[8] https://apnews.com/article/donald-trump-legislature-media-lawsuits-social-media-848c0189ff498377fbfde3f6f5678397

a la proliferación de amenazas a la seguridad de las personas, incluido el ataque al *Capitolio* en Washington DC a principios de Enero del 2021[9].

Estos casos y situaciones también dan lugar a controlar las actividades y los contactos en línea como *bloggers* y registros de sitios en línea. Al respecto, otro estudio de la UNESCO afirmaba:

> *En algunas oportunidades se ha responsabilizado penalmente a los intermediarios por contenidos publicados por un usuario y que se consideran contrarias a las leyes de privacidad y difamación. Estos casos son señal de una tendencia emergente a la 'censura preventiva', por la cual las compañías llevan adelante su propio control y filtrado de contenidos a fin de evitar posibles repercusiones. A su vez, esto contribuye a la 'censura privatizada': a través de este proceso, algunos gobiernos se apoyan en las compañías privadas para regular los contenidos, por fuera de todo proceso legal y rendición de cuentas electoral* (UNESCO, 2014).

En el 2010, *Wikileaks* difundió una gran cantidad de información confidencial sobre asuntos diplomáticos. Tres años más tarde, en el 2013, Edward Snowden reveló acerca de los programas de vigilancia masiva llevada a cabo por varios gobiernos de América y Europa. Ambos casos causaron nuevos planteamientos en cuanto a la libertad de prensa y el interés publico. Al respecto la UNESCO agrega:

> *(…)A partir de las revelaciones de 2013 respecto de la vigilancia masiva, se ha convocado a los gobiernos que vigilan e intercambian información digital a introducir garantías contra la violación del derecho a la libertad de expresión y del derecho a la privacidad.* (UNESCO, 2014).

Como punto final nos gustaría agregar que desde 1993 y gracias a las innovaciones tecnológicas incluido el advenimiento de Internet, se han generado transmisiones de radio modo de *streaming* por parte de los usuarios "osados" de internet y de los medios sociales tocando

[9] https://www.wsj.com/articles/what-is-parler-app-apple-android-11610478890

diferentes temas de interés. Del mismo modo, a través de *YouTube* y otras plataformas similares como *Vimeo*, se han generado canales ya sean "caseros" con poca producción o con mayor inversión profesional. De la misma manera, plataformas como *Facebook*, *Instagram*, y *YouTube* permiten la posibilidad de transmitir en vivo, generando grandes posibilidades como nuevo modo de comunicación.

2.3. Derecho a la privacidad

Entre el siglo XII y el XVI surgieron en España y en otros países normas jurídicas relacionadas con el concepto de lo privado en relación con la protección a la inviolabilidad del domicilio. Entre estas se encuentran tres normas jurídicas: la Carta del Convenio entre el Rey Alfonso I de Aragón y los Moros de Tudela de 1119, los Decretos de la Curia de León de 1188 y el Decreto 11 firmado por Alfonso IX. Este último protegiendo a los dueños de casa en cuanto a daños y entradas sin invitación.

En la Carta Magna de 1215 se comienzan a sentar bases constitucionales en cuanto a los derechos pertenecientes al hombre como legítimos de cualquier ciudadano, dando comienzo a ciertos límites establecidos a los privilegios del Rey. Cientos de años más tarde, con la llegada de la independencia de los Estados Unidos, se generan ciertos textos de diferentes estados como Delaware y Virginia en concordancia con la Cuarta Enmienda de la Constitución de los Estados Unidos de América de 1787 que señala: "...el derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o promesa y describan específicamente el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

En el año 1890, un artículo titulado *"The right to privacy"* (El derecho a la privacidad), fue publicado en la revista *Harvard Law Review* de la Facultad de Derecho de la Universidad de Harvard donde los Dres. Samuel D. Warren y Louis D. Brandeis reaccionaban frente a la divulgación indiscriminada por la prensa de información privada y afirmaban que impedir su

publicación es un ejemplo del derecho más general del individuo a no ser molestado (Warren and Brandeis: 1890-2012).

Desde entonces, y a través del siglo XX, la protección de los derechos de la privacidad de los individuos en Estados Unidos ha pasado a la esfera de la máxima protección del derecho constitucional evolucionando desde la protección de la propiedad privada (*privacy-property*) a la protección de la dignidad de las personas.

La evolución política, económica y social trae aparejado la existencia y el reconocimiento de nuevos derechos en donde la necesidad de protección de las personas en el ámbito de la vida privada se separa del derecho de propiedad. Cabe aclarar que esta prerrogativa no prohíbe la publicación de material privado tales como fotos, videos y texto donde los individuos exponen voluntariamente su vida de forma cotidiana. Otra aclaración pertinente es la diferencia entre el derecho a la intimidad, también conocido como el derecho a la privacidad, del derecho al honor y del derecho a la imagen.

Por su parte, el Diccionario de la Lengua Española de la Real Academia de España define al concepto de vida privada como: "aquella parte de la vida humana que se desarrolla a la vista de pocos o que constituye la vida personal y particular" a la intimidad como: "la zona espiritual íntima y reservada de una persona o grupo, especialmente de una familia".

Ernesto Villanueva (2002), jurista mexicano, sostiene que: "el derecho fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente decide mantener fuera del conocimiento público". En otras palabras, se protege un bien jurídico que consiste en la necesidad social de manifestar la tranquilidad y la dignidad para desarrollar libremente la personalidad humana. Según Villanueva el derecho a la vida privada se cristaliza en el momento de proteger del conocimiento ajeno al hogar, la oficina o el ámbito laboral, los expedientes médicos, legales y personales, las conversaciones o reuniones privadas, la correspondencia por cualquier medio, la intimidad sexual, la convivencia familiar o afectiva y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público.

Para este autor el derecho a la privacidad posee las siguientes características:

- *Es un derecho esencial del individuo*: se trata de un derecho inherente a la persona con independencia del sistema jurídico particular o contenido normativo bajo el cual está tutelado por el derecho positivo.

- *Es un derecho extramatrimonial:* se trata de un derecho que no se puede comerciar o intercambiar como los derechos de crédito, habida cuenta que forma parte de la personalidad del individuo, razón por la cual es intransmisible e irrenunciable.

- *Es un derecho imprescriptible e inembargable*: el derecho a la privacidad ha dejado de ser un asunto doctrinal para convertirse en contenido de derecho positivo en virtud del desarrollo científico y tecnológico que ha experimentado el mundo moderno con el uso masivo de la informática que permite el acceso casi ilimitado a información personal por parte de instituciones públicas y privadas.

Por su parte, Novoa Monreal (1989) define al derecho a la intimidad como: el derecho del individuo de tener una esfera secreta de la vida, de la que tenga el poder de alejar a los demás y la vida privada como el retiro voluntario y temporal de una persona que se aísla de la sociedad por medios físicos o psicológicos sea para buscar la soledad o la intimidad de un pequeño grupo, sea porque ella se encuentre dentro de grupos más importantes, en situaciones de anonimato o de reserva. Se trataría de asegurar la integridad de la dignidad humana, por medio del amparo de una de las variadas manifestaciones de la personalidad".

En el artículo 8 del Convenio Europeo de Derechos Humanos, firmado en Roma el 4 de noviembre de 1950 se determina que: "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". Y agrega que: "el respeto a la vida privada debe también englobar el derecho del individuo a anudar y desarrollar relaciones con sus semejantes".

No obstante, los conceptos de intimidad y de privacidad parecían generar definiciones diferentes entre algunos de los autores analizados. Mientras que la intimidad estaría reservada a las

zonas más sensibles de la persona humana, la privacidad estaría comprendida en las zonas más exponenciales de la intimidad del individuo. Ambos son derechos fundamentales de cualquier individuo.

Alejandro Laje (2008) plantea que uno de los aspectos más controvertidos de la intimidad es su tratamiento como espectáculo lo cual deriva en una colisión de derechos. Por un lado, la intimidad se refiere a una zona reservada de la persona y por el otro el espectáculo a una zona publica donde se "expone" información abiertamente a la sociedad. Desde este punto de vista, el uso de las tecnologías de redes genera posibilidades de intromisión y de vigilancia que irrumpe en la privacidad de las personas. Laje sostiene que, de forma paradójica, se combinan en la sociedad tres elementos: "las nuevas tecnologías que comunican y exponen toda la vida de la persona, sus propios impulsos que la llevan a mostrarse a la vista no sólo de los que conforman su círculo próximo sino también de todo el mundo cibernético que lo ve todo desde todos los ángulos, y las necesidades de transparencia propias de la democracia".

En una de sus ponencias Laje explica también como las enseñanzas religiosas de San Agustín y de los evangélicos establecieron la importancia en occidente de identificar la importancia de la individualidad y de la subjetividad como un ámbito que merece protección. En la misma ponencia, Laje sostiene que el filósofo alemán Emanuel Kant, fue el precursor más importante de la historia al establecer los límites precisos de la individualidad considerando que esta es más como un fin en sí mismo que como un medio.

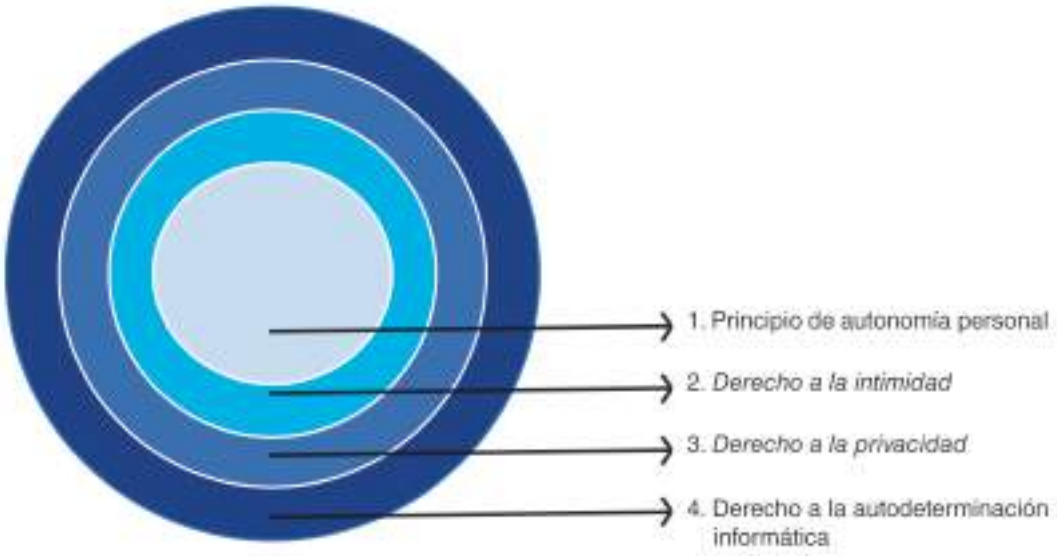
Por su parte, Julio César Rivera (1989) define los límites al derecho a la vida privada como: "la seguridad nacional, la seguridad pública y situaciones de emergencia en tiempos de paz, guerra o catástrofes naturales, el bienestar económico del país, la lucha contra el desorden y el crimen, la protección de la salud, la administración de la justicia civil, la libertad de expresión, información y deliberación".

En relación específicamente al caso Snowden que trabajamos en esta tesina, Damián Loretti (1995) resalta la Ley N° 1 de 1984 del Reino de España, que en el artículo 7° se considera intromisiones ilegítimas el emplazamiento de mecanismos de escucha o filmación para la grabación o reproducción de la vida íntima o manifestaciones de las personas o su correspondencia, no destinadas naturalmente al público, donde: "También son comprendidas en este marco las

divulgaciones sobre hechos relativos a la vida familiar de las personas, la reproducción de su voz o imagen y la profusión o reproducción de dichos difamantes. Del mismo modo también contempla la legislación argentina el derecho a que la imagen o figura de uno pueda ser explotada, salvo que se cuente con el consentimiento específico del interesado y para el fin determinado respecto del cual se solicitó la autorización". Queda claro que en el caso Snowden estos límites no son respetados.

Kemelmajer de Carlucci (2015) ejemplifica un caso donde las dimensiones de los derechos pueden confundirse: "puede ser lesionado el derecho a la imagen sin que haya sido atacada la intimidad, por ejemplo, si una modelo autorizó la toma de una fotografía, pero no su difusión publicitaria, o si se autorizó para publicitar un producto y se la utiliza indiscriminadamente para otros. El portador de su imagen no podría sostener que se ha lesionado su intimidad, puesto que ella estaba ya en la calle, había sido difundida al público, sin embargo, tiene el derecho a defender su propia imagen, impidiendo que ella sea más difundida que lo consentido".

De manera complementaria, la constitucionalista argentina, Marcela Basterra (2012) distingue cuatro tipos de límites o niveles de protección al derecho a la intimidad y los denomina esfera de protección:



Primera esfera de protección: el principio de autonomía personal

Según Basterra, el principio de autonomía de la persona humana "es uno de los ejes del sistema de derechos individuales y, por lo tanto, del Estado constitucional de Derecho, que tiene como fin esencial al ser humano". En su artículo 19, la Constitución Nacional Argentina, establece que: "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios y exentas de la autoridad de los magistrados". Este principio también se ha denominado como de reserva o autorreferencia y es el punto de partida de la protección del derecho a la intimidad y la privacidad.

El principio de autonomía implica que cada persona puede escoger el que considere el mejor plan de vida para sí misma aún así si esto implicara un daño personal. Solo un daño a terceros opera como límite. Al respecto, John Stuart Mill (2007) resalta: "El único fin por el cual la humanidad

tiene permitido, individual o colectivamente, interferir en la libertad de acción de cualquiera de sus miembros, es la autoprotección. El único propósito por el cual el poder puede ser concretamente ejercido sobre cualquier miembro de una sociedad civilizada, en contra de su voluntad, es prevenir el daño a otros. Su propio bien, sea físico o moral, no es justificación suficiente".

Basterra también define el principio de "perfeccionismo". Este concepto se presenta de manera antagónica al principio de autonomía y sostiene que "es misión del Estado hacer que los individuos adopten y lleven a cabo ciertos idea- les de excelencia homologados. En consecuencia, el Estado interviene en gran cantidad de aspectos de la intimidad de la persona humana. Para el Estado perfeccionista hay "buenos" y "malos" planes de vida, por eso el Estado elige los que considera buenos, y desalienta a los que entiende como malos.". Un ejemplo de esto es la situación de ciertos países de Medio Oriente como Irán, donde no se permite estudiar a las mujeres. En este ejemplo y otros similares, el principio de autonomía personal queda reducido a la nada.

Por último, el "paternalismo" es entendido como las medidas que toma el Estado, pero no pensando en modelos de vida a imponer o ideales de excelencia humana, sino basado por ejemplo en la preservación de la salud física y mental del individuo, desalentando decisiones de ellos mismos que pudieran poner en peligro a las personas.

Segunda esfera de protección: el derecho a la intimidad

Resulta difícil diferenciar entre el concepto de intimidad y de privacidad con un contraste casi nulo entre los dos. Según Basterra mientras el derecho a la privacidad o intimidad aparece como un reclamo de no exposición al público y a la sociedad; el principio de autonomía importa un reclamo al respeto más absoluto por las conductas "autorreferentes", o sea, a la no intervención estatal en los planes de vida que cada uno elige, reconociendo como único límite el de no dañar a otros.

Continuando la distinción entre el concepto de intimidad y el de privacidad, Carlos Nino (1992) distingue privacidad como todo aquello relacionado con las acciones voluntarias de los individuos que no afectan a terceros. Son privadas en el sentido de que, si violentan exigencias

morales, sólo lo hacen con las que derivan de una moral privada, personal o autorreferente. Tales exigencias no se refieren, como las derivadas de la moral pública o intersubjetiva, a las obligaciones que tenemos en relación con otras personas. Al contrario, alude al desarrollo o autodegradación del propio carácter moral del agente, reconociendo como único límite el daño que pueda provocarse a terceros. Para el autor son las "acciones privadas", la que se encuentran salvaguardadas por la normativa del artículo 19 constitucional.

Nino también agrega que la esfera de la persona que está exenta del conocimiento generalizado por parte de los demás. La intimidad de un individuo, o sea la exclusión potencial, de acuerdo con su voluntad del conocimiento y la intromisión de los demás se refiere, entre otros, a los siguientes aspectos: rasgos del cuerpo, imagen, pensamientos, emociones, circunstancias vividas, hechos pasados concretos, propios o de su vida familiar, escritos, pinturas, grabaciones y conversaciones.

Tercera esfera de protección: el derecho a la privacidad

Resulta ciertamente irónica la visión de Rodney Smolla (1992) cuando afirma: "si esperas protección legal para tu privacidad, deberías permanecer en tu casa con las persianas cerradas". En la película "Snowden", una de las escenas muestra como él se encuentra hablando muy bajo, y hasta había tapado la cámara de su computadora con una cinta. El advenimiento de las TIC´s o nuevas tecnologías de la información y la comunicación, incluidas las de los robots de inteligencia artificial como "*Siri*" en los celulares *IPhone* y *Alexa* en los hogares, cada vez más populares en todo el mundo. A esto se suma el uso masivo de las redes sociales, donde los usuarios se "exponen" al publicar su vida privada al mundo y donde su privacidad se encontraría también invadida, al estilo del "gran hermano". Un chiste que recorrió las redes sociales indica la nueva realidad de la privacidad dentro de los hogares: "Mi esposa me preguntó por qué yo estaba hablando tan suavemente en la casa. Le dije que tenía miedo de que Mark Zuckerberg (creador y dueño de *Facebook* e *Instagram*, entre otras) estuviera escuchando. Ella se río. Yo me reí. *Alexa* se río. *Siri* se rio".

A pesar de las posibles confusiones generadas entre los conceptos de privacidad e intimidad, la vida privada presenta una prerrogativa mayor que el derecho a la intimidad donde la intimidad es quizás más personal que la privacidad. En esta última influyen tanto la figura de persona (desconocida, pública o famosa), como el lugar (influyendo las TIC´s, redes sociales); en cuanto a la esfera de autonomía personal se podría afirmar que la intrusión más importante proviene del Estado, mientras que, en los derechos a la privacidad e intimidad, la intromisión más importante surge usualmente por parte de los medios de comunicación social y por terceros.

Cuarta esfera de protección: el derecho a la autodeterminación informática

En la Constitución Argentina se hace referencia al concepto de *Habeas Data*, aludiendo a la protección de datos personales almacenados en bancos de datos públicos y privados. El *Habeas Data* es considerado "una especie" de intimidad conocida como el derecho a la intimidad informática. Este derecho asegura: 1) El acceso al conocimiento de los datos personales y 2) La posibilidad de reclamar la supresión, rectificación, confidencialidad o actualización de esta información, ya sea que esta fuera falsa o utilizada con fines (posibles o actuales) discriminatorios.

En relación con el marco jurídico internacional e interamericano podemos destacar, según lo desarrollado hasta el presente, las siguientes normas que impactan el derecho a la privacidad e intimidad:

- En el Artículo 12 de la Declaración Universal de los Derechos Humanos se afirma: "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".

- En el Artículo 5° de la Declaración Americana de los Derechos y Deberes del Hombre, se establece que: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familia".

- En el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos se establecen dos principios: “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación y 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

- En el Artículo 11 de la Convención Americana sobre Derechos Humanos se protege el derecho a la intimidad cuando se establece que: “1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación, y 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques”.

- En México, la Constitución Nacional determina en su Artículo 16 que: “Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. (…) Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, 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”.

- En Perú, en el Artículo 200 de la Constitución Nacional, se protege el honor, la intimidad, la propia imagen, el derecho a la buena reputación y a la voz propia; y se menciona la figura de *Habeas Data*.

- En Colombia, en el Artículo 15 de la Constitución Nacional se establece que: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y

rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

- En Costa Rica en el Artículo 24 de la Constitución Nacional se determina que: "Son inviolables los documentos privados y las comunicaciones escritas y orales de los habitantes de la República".

- En Paraguay en el Artículo 33 de la Constitución Nacional se define al derecho a la intimidad de la siguiente forma: "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

Y finalmente mencionamos la situación jurídica de Chile:

- En Chile, en el Artículo 19, numeral 4to, la Constitución Nacional garantiza: "El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan."

2.4. Derecho a la protección de datos personales y datos sensibles

Banisar (2006) sostiene que el concepto de privacidad se puede dividir en 4 elementos: 1) *Privacidad informativa*: que involucra las reglas para gestionar los datos personales, 2) *Privacidad corporal*: vinculada a la protección de nuestra seguridad física frente a procedimientos invasivos, 3) *Privacidad comunicacional*: relativa a la seguridad y privacidad de la correspondencia y las comunicaciones telefónicas, 4) *Privacidad territorial*: que establece los límites a las intrusiones en los ambientes domésticos.

Natalia Torres sostiene que los datos personales se relacionan directamente con el primer punto, de privacidad informativa. Sin embargo, la protección de los datos personales no se limita exclusivamente a proteger la privacidad, sino que refiere a un universo de problemas:

> *"...el derecho a la protección de los datos personales garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada" (Silva, 2011: 171).*

La protección de datos personales se relaciona directamente con el concepto de protección de la privacidad en aquellos "datos personales de carácter sensible", definidos como:

> *"...aquellos datos que revelan información merecedora de especial resguardo por el mayor peligro que su tratamiento implica para las libertades y derechos ciudadanos...(...)...Entre estos se cuentan los datos relativos al origen racial o étnico de una personal, su color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo así como sobre la participación en una asociación o la afiliación a un sindicato. Algunos países, según su propia experiencia, agregan la información genética, la afiliación política u otros datos a este listado" (Silva, 2011: 171).*

A partir de 1960 y frente al avance de la tecnología, comenzaron a aparecer diferentes legislaciones con respecto a la protección de datos personales por el surgimiento de una gran cantidad de información y procesamiento de datos sobre las personas. La revolución tecnológica e informática ha generado una nueva preocupación en los gobiernos: la de proteger los datos personales. A su vez, pareciera que los usuarios no parecen reparar en los peligros de publicar sus datos privados en las redes sociales.

Banisar (2011) reseña varios principios generados con el fin de gestionar los datos personales:

- La recolección de datos personales debe ser limitada y los datos deben ser obtenidos a través de medios legales y, cuando sea necesario, bajo el consentimiento de los sujetos propietarios de los datos.

- Los datos personales recolectados deben servir exclusivamente para el objeto que guía e impulsa su recolección y deben ser precisos y actualizados.

- El objetivo de la recolección de la información debe ser determinado y explicitado al momento del relevamiento de los datos y debe orientar su uso posterior.

- Los datos personales no deben ser publicados o entregados por motivos ajenos a los especificados en el objeto de la recolección a menos que el titular de los datos otorgue consentimiento o mediante la autorización expresa de unos funcionarios legalmente autorizados a hacerlo.

- La información recolectada debe ser protegida frente a eventuales riesgos como pérdida, sabotajes, destrucción.

- Las políticas implementadas para la gestión de los datos personales deben ser públicas. La definición de lo que se considera datos personales, los objetivos de su recolección y uso,

el lugar en el que se almacena y el controlador de esa información deben ser publicados. Todo controlador de base de datos de información debe dar cuentas de las políticas implementadas y el cumplimiento de los principios de la gestión de la información.

- Todo individuo debe poder confirmar si el controlador de una base de datos posee o no datos personales suyos.

- Debe poder obtener esa información dentro de un tiempo razonable.

- Todo individuo debe recibir una explicación si la información se deniega.

- Todo individuo debe poder solicitar una corrección de la información contenida en la base, ya sea rectificándola, completándola, amentándola o borrándola.

Silva sostiene que "el derecho a la protección de los datos personales garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada, aspecto que, de hecho, se soslaya" (Silva, 2011: 171). Paterson (2011) se refiere al rol de control en la legislación de datos personales. Estas leyes permiten a los usuarios tener un mayor control sobre sus datos personales al regular la recolección, uso, almacenamiento y publicación de éstos. En este sentido, Paterson considera que este control es positivo pues contribuye a resguardar la privacidad.

2.4.1. Habeas Data

El concepto de *Habeas Data* está establecido en el artículo 43 de la Constitución de la Nación Argentina de la siguiente manera:

"Toda persona podrá interponer esta acción [se refiere a la de amparo] para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros y

bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.[10]

Desde el año 2000 se encuentra vigente en Argentina la Ley N° 25.326 (de Protección de Datos Personales) que fue modificada en varias circunstancias por decretos, leyes, y resoluciones, entre otros recursos legales. La ley tiene por objeto proteger los datos personales asentados en bancos de datos públicos o privados con el fin de garantizar el derecho al honor, y la intimidad de las personas y el acceso a la información sobre ellas mismas[11]. Esta ley establece que todo el que recabe datos personales deberá informar a sus titulares el objetivo para el que será tratados, donde serán registrados (archivos o bases de datos), las consecuencias de negarse a proporcionar datos o de hacerlo en forma errónea y la posibilidad de los interesados de ejercer los derechos de acceso, rectificación y supresión (Califano, 2021).

La Ley Modelo de Acceso a la información de la Organización de Estados Americanos (OEA) forma parte de un conjunto de herramientas de cooperación jurídica desarrolladas por la Secretaria General de la OEA[12], sobre este particular en su artículo 40, establece que el acceso a la información podrá restringirse cuando "Dañare los siguientes intereses privados: 1. el derecho a la privacidad, incluyendo privacidad relacionada a la vida, la salud o la seguridad. (…) las excepciones (...) no deberán aplicarse cuando el individuo ha consentido en la divulgación de sus datos personales o cuando de las circunstancias del caso surja con claridad que la información fue entregada a la autoridad pública como parte de aquella información que debe estar sujeta al régimen de publicidad" (OEA, 2010).

[10] Constitución de la Nación Argentina (1994), Artículo N° 43.
[11] Ley N° 25.326, art 1
[12] https://www.oas.org/juridico/english/ley_modelo_acceso.pdf

En cuanto las diferentes políticas promotoras del derecho y la resolución de controversias, Banisar (2006) y Torres (2009) distinguen las diferentes instancias institucionales:

- La revisión interna se utiliza en casos donde es denegado el pedido original de cierta información en donde el usuario desea apelar a una instancia superior la decisión de un organismo público. Las excepciones a este modelo son Bulgaria, Japón y Turquía que no cuentan con estos mecanismos. Otros países solo tienen este tipo de revisiones, a veces combinadas con la posibilidad de apelar a las cortes: Austria, Georgia, Holanda, Tajikistan, Ucrania y Estados Unidos (Banisar, 2006; Torres, 2009).

- La función del defensor del pueblo es la de defender el interés público frente a los posibles abusos de poder de los gobiernos. Así, poseen capacidad de revisión en la legislación sobre acceso a la información. Los defensores pueden revisar las decisiones de organismos públicos en Albania, Armenia, Australia, Azerbaijan, Belize, Bosnia y Herzegovina, Republica Checa, Dinamarca, Ecuador, Finlandia, Grecia, Kosovo, Moldova, Nueva Zelanda, Noruega, Pakistán, Perú, Filipinas, Polonia, Rumania, España, Suecia y Trinidad y Tobago (Banisar, 2006; Torres, 2009).

- En casi todos los países se puede apelar a las cortes para revisar decisiones en cuanto a acceso a información si este ha sido reconocido como derecho y si este ha sido vulnerado (Shapiro, 2002). Bulgaria, Israel, US y Uzbekistan poseen solo esta instancia institucional como revisora final (Banisar, 2006). Con la experiencia de la autora residiendo en US, esta posibilidad tiene sus desventajas en el hecho de que solo podrían recurrir a estos recursos aquellos individuos que poseen grandes recursos económicos, pues no existen recursos para el público en general en este sentido, quedando este desfasado por esta razón. Torres considera también la dificultad de modificar las prácticas en un sistema donde la cultura de secreto está fuertemente instalada a través de la administración de una acción de los jueces.

- En algunos países un solo legislador o partido regula tanto el acceso a la información como la protección de los datos personales. Según Banisar este sistema implican posibles desventajas: "...tener ambas funciones juntas puede engendrar confusión legislativa sobre el intento de las leyes y puede resultar en la oposición de algunos partidos que de otra manera apoyarían a un acto u otro. Una cuestión más práctica es la complejidad de la legislación, que puede resultar a los legisladores no dispuestos a revisarlo porque les falta el tiempo" (Banisar, 2011: 17).

- Existen ciertos organismos destinados a garantizar la protección de los datos personales, el diseño institucional sigue el modelo de comisión Banisar sostiene que este modelo puede traer ventajas: "... una comisión independiente para cada uno de los dos Derechos puede crear defensores específicos para tales Derechos, no limitados por la necesidad de equilibrar los intereses potencialmente competitivos" (Banisar, 2011: 23) y también desventajas: "... una preocupación principal de tener dos organismos en conflicto mutuo. También hay una preocupación de que los organismos públicos y el público mismo recibirán consejos contradictorios de los dos comisionados cuando éstos no estén de acuerdo" (Banisar, 2011: 24; Torres, 2009).

Específicamente relacionado con muestro objeto de estudio (Europa y Reino Unido, así como Estados Unidos), ciertos países como Reino Unido han regulado ambos derechos y han instituido un solo organismo para garantizar tanto el derecho a la información como a la protección de datos personales. Shoshana Zuboff (2019), considera que los legisladores y juristas de Estados Unidos están dándose cuenta de las falencias de la ley existente con respecto a las capacidades digitales. El foco se encuentra en la cuarta enmienda y a la necesidad de que la misma alcance a los avances del siglo XXI protegiendo a los individuos de la búsqueda y el apoderamiento de información privada de manera que refleje realidades contemporáneas de producción de datos. Asimismo, la Cuarta Enmienda determina la relación entre los individuos y el Estado. Para aclarar, la cuarta enmienda es el derecho de las personas a estar seguras en sus casas, papeles y objetos, sin ningún tipo de violación y en contra de búsquedas y capturas irracionales. Y ninguna entrada

a propiedad privada se puede llevar a cabo sin causa probable y permitida por alguna autoridad como ser la figura de un juez[13].

2.5. Ciudadanos en Internet

Los cambios tecnológicos en el marco de la información han generado a lo que algunos catedráticos llaman "ciberculturas" (Dery 1995, Castell 1996, Kerckhove 1997, Joyanes 1997, Tofts and McKeich 1998, Lévy 2001, Scolari 2008), lo cual ha generado cambios en las formas de comunicar e intercambiar información, o, en otras palabras, una serie de fenómenos sociales, artísticos, políticos y comunicativos y de interacción (Deusdad, 2001). El surgimiento y luego masificación de Internet ha generado un gran cambio en quienes poseen acceso a esta red, al poder opinar y organizarse de manera virtual de acuerdo con intereses comunes. A su vez surgen movimientos ciudadanos organizados a través de redes sociales.

Gracias a estas nuevas formas de comunicación, los hábitos sociales se van modificando y surge una nueva manera de organización y participación ciudadana en la que los individuos poseen acceso a la información en forma directa y constante pero también pueden participar del discurso público, el cual históricamente solo pertenecía a una elite. Deusdad se pregunta si este nuevo paradigma se trata de una utopía o si realmente se han generado cambios en la manera en cómo se desarrolla la política y la democracia. El concepto de tecnología se entiende como un conjunto d conocimientos específicos relacionados a una actividad, mientras que la técnica, se refiere a un conjunto de instrumentos y procedimientos. McLuhan, McQuail y Veblen se asocian a la hipótesis del determinismo tecnológico, donde la tecnología es vista como el principio motriz de la historia (Veblen, 1983).

[13] Descripción de la cuarta enmienda: https://www.govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf

A continuación, haremos un recuento de las distintas posiciones en cuanto al a influencia o falta de esta en las formas de la vida humana:

- Pinch y Bijker (1984 y 1989) defienden la idea de que la tecnología forma parte de las relaciones sociales e introducen el concepto de construcción social de la tecnología. La postura epistemológica critica esta perspectiva pero valida el abordaje del tema de la mediatización de la realidad a través de la tecnología digital.

- Williams considera que el determinismo tecnológico es una visión poderosa y al mismo tiempo ortodoxa de la naturaleza del cambio social. Asimismo, agrega que las nuevas tecnologías son descubiertas en un contexto de investigación y desarrollo, lo cual establece condiciones óptimas para el cambio social y el progreso (Williams 2000: 38).

- Según Lévy: "Una técnica se produce en una cultura, y una sociedad se encuentra condicionada por sus técnicas. Digo bien, condicionada y no determinada" (...) esto significa "que abre ciertas posibilidades, que ciertas opciones culturales o sociales no se podrían considerar en serio sin su presencia". (Lévy 2007: 9)

- Walter Benjamin se refería al cine y la fotografía en cuanto al cambio de percepción que producen las tecnologías y se refería al *sensorium* como una transformación del sistema de percepción sensorial (Benjamin 1973: 24). No solo los sentidos han cambiado con el advenimiento de la tecnología sino también la concepción de tiempo y espacio al poder estar en línea con personas a lo largo del planeta así como la rapidez en las conexiones.

- Para Heidegger (1954) el punto importante de la técnica es su capacidad de "develamiento" o de descubrir la "verdad".

- Marcuse sostiene que a pesar de todos los cambios, la tecnología es la continuidad histórica de la dominación del hombre por el hombre. La dependencia personal (del esclavo con su

dueño, del siervo con su señor) a una dependencia como "orden subjetivo de las cosas" ya sean las leyes económicas o los mercados. La dominación se hace más compleja pero "la sociedad mantiene una estructura jerárquica y explota más eficazmente los recursos mentales y naturales al distribuir los beneficios de la explotación en una escala más amplia" (Marcuse, 1993: 171)

- De Kerckhove sostiene que en la historia han existido tres etapas cognitivas que actualmente se encuentran entretejidas y sobrepuestas que se han basado en las relaciones entre tecnología y lenguaje: la oralidad, el alfabeto y la electricidad. Para el autor, la etapa digital es la segunda fase de la electricidad que es cognitiva. Según De Kerckhove actualmente nos encontramos en la tercera fase que es la condición inalámbrica, "donde todo el sistema electrónico sensorial, muscular y cognitivo regresa al cuerpo del usuario". También considera que algunos "sesgos" consecuencia de esta fase digital son: virtualidad, convergencia, conectividad, inmersión, hipertextualidad, acceso aleatorio, interactividad, movilidad, transparencia, ubicuidad, globalidad y tiempo real (De Kerkchove 2005: 3). Sesgo entendido como "una tendencia inherente de la tecnología a extender su influencia no solo directamente cuando se aplica, sino posteriormente, en los efectos que ejerce sobre el comportamiento social" (Innis, 1964).

- Deusdad Ayala finalmente aclara que, más allá de las diferentes posturas, vivimos en un ambiente tecnológico con dispositivos que pasan a ser parte de la vida diaria (*Ver y profundizar en el Capítulo III. Marco Histórico: "*Internet de las cosas *o Internet of things" e Inteligencia artificial")* y regulan la educación, las finanzas, la memoria, y la ciencia (Deusdad Ayala, 2001).

2.5.1. Las redes sociales

En los últimos años de avances digitales, la tecnología "de moda" ha ido evolucionando desde las páginas personales, pasando por los blogs de temas específicos hasta en nuestros días los "podcasts" que permiten generar diferentes "canales" virtuales de radio. A su vez, en cuanto al uso imagen, desde la época de *MySpace, Fotolog* creado en el 2002; *Flickr,* creado en el 2004, hasta *Instagram* creado en el 2010 y posteriormente adquirido por *Facebook*. También surgieron los foros como producto fundamental de la CMC (comunicación mediada por computadoras) donde se crean comunidades virtuales de acuerdo a temas comunes.

Años más tarde surgieron los sistemas de chat como *Messenger*, llamado *Windows Live Messenger*, donde millones de usuarios se conectaban diariamente durante horas de trabajo para "chatear" con amigos, familia y hasta compañeros de trabajo. No hay que olvidar también la explosión del email como herramienta de comunicación diaria en el trabajo, los espacios académicos y también los familiares y de amigos. Pero la verdadera revolución surgió con el nacimiento de *Facebook*, que fue creado en el 2004 y un año más tarde *YouTube* y la explosión de videos tanto caseros como profesionales. En el 2006 nació *Twitter* con una idea original de "microblogging" donde los "tweets" no podían superar los 140 caracteres, convirtiéndose en una de las aplicaciones más utilizadas. En el 2013, esta aplicación se cerró definitivamente pero dio lugar a otro tipo de chats como el de *Facebook* y el de *Instagram*, a los mensajes de textos a través de teléfonos celulares, *Skype,* con la "invención" de la videoconferencia, *WhatsApp* que fue creada en el 2009 y luego también adquirida por *Facebook*.

Boyd y Ellison definen las redes sociales como servicios basados en la *Web* que permiten a los individuos construir un perfil público o semipúblico dentro de un sistema limitado, articular una lista de otros usuarios con los que comparten una conexión y tanto ver como atravesar sus propias listas de conexiones como aquellas elaboradas por otros dentro del sistema (Boyd y Ellison, 2008). El grupo de personas en este sistema funciona como "reunión", ya sean conocidas o desconocidas, que interactúan entre sí. A su vez redefinen el grupo y lo retroalimentan (Caldevilla Dominguez, 2010), se centran en el contacto y la creación de amistades y las relaciones (Echeburúa y De Corral 2010). Area Moreira (2008) considera que el fenómeno de las redes

sociales y las comunidades virtuales, crecieron de forma paralela con los servicios y herramientas de la Web 2.0. La misma se define como "participativa" o aquellos sitios que se alimentan de contenido generado por el usuario, generando facilidad de uso y una cultura de participación convirtiéndose así los usuarios en creadores de contenidos en vez de consumidores del mismo. Las prácticas en este contexto son las de compartir opiniones (Mills, 2007).

Mientras que la Web 1.0 fue una plataforma estática de publicación de información sin la existencia de ninguna interacción con los usuarios que la recibían, Web 2.0 consiste casi exclusivamente por la alta participación de los usuarios donde algunas plataformas generan conocimientos a través de varios usuarios como el caso de *Wikipedia*, entre otros. La próxima fase de la evolución de la Web es la denominada Web 3.0 donde los contenidos de Internet se han convertido en más diversos y complejos por el gran aumento del volumen de datos, lo cual genera más crítico el manejo de esta información (Bergman, 2001). La web se convierte en una plataforma con "links" donde los datos se hacen disponibles hacia los consumidores y se generan conexiones que hacen a estos datos más valiosos. Wolgram (2010) define Web 3.0 donde las computadoras, más que los humanos, generan nueva información. Morris (2011) también afirma que la integración de los datos es la fundación básica de la Web 3.0 (Rudman and Bruwer, 2016).

Retomando el fenómeno de las redes sociales y las comunidades virtuales, Area Moreira (2008) considera que las mismas han ido creciendo de forma paralela al desarrollo de servicios y herramientas de la Web 2.0. Un primer grupo estaría formado por redes de propósito general o de masas como una megacomunidad en el caso de *Facebook, My Space* y *Twitter*. El segundo grupo se refiere a redes abiertas para compartir archivos como videos, presentaciones o fotografías (*YouTube, SlideShare, Snips o Flickr*). El tercer grupo alude a redes temáticas o microcomunidades como en el caso de *Facebook Groups* o *Ning.*

En cuanto a las comunidades locales, Campal García (ver Publicaciones, libros en línea e investigaciones académicas en Fuentes Consultadas) agrega que se las conoce por varios nombres: "*community networks*", "ciudades digitales", "telecentros", "*freenets*", "*civic networks*", "*Public Access Networks*", "redes comunitarias o de la comunidad", "redes de las libertades de los

ciudadanos" "*Community Tecnologic Centers*" "Centros comunitarios de tecnología" o "redes cívicas" o Redes Ciudadanas. En otras palabras, estas Redes Ciudadanas es el uso de las tecnologías de la información por actores locales con el objeto de generar cambios en la sociedad. Por ejemplo, instituciones gubernamentales, empresas privadas, asociaciones, vecinos, bibliotecas, nuevas organizaciones, movimientos de mujeres, ONG´s, se movilizan para potenciar el desarrollo local (a todos los niveles, social, económico y cultural), favorecer el renacimiento de la democracia fomentando la participación ciudadana, reducir la exclusión social. Al mismo tiempo abren la comunidad local hacia el mundo global a través de estas tecnologías y generan relaciones de solidaridad y cooperación incluidas las relaciones de comercio, trabajo, políticas, educativas, y más. A su vez el uso de las tecnologías de la información, generan nuevos vínculos económicos (*e-banking* y compras *online*), educativos (*e-learning*), hasta *e-dating* (búsqueda de relaciones amorosas online) lo cual genera transformaciones profundas en la vida urbana, generando nuevas formas de interacción humanas.

El espacio *Vircomm* define a las redes ciudadanas como “un grupo de personas que definen intereses y están dispuestos a interactuar, creando de esta manera nuevos contenidos”. Castells considera que las organizaciones locales que tenían acceso a internet mucho antes que los ciudadanos comunes, ayudaron a la expansión de las redes ciudadanas por generar acceso la red a través de bibliotecas, telecentros a estas personas que, por pobreza, desinformación y falta de educación, no tenían acceso a ellas o no poseían los medios para conectarse. (Castells 2001)

Artur Serra y Leandro Navaroo (ver Publicaciones, libros en línea e investigaciones académicas en Fuentes Consultadas) enumeran algunos de los objetivos de las redes ciudadanas son:

- Fomentar la creatividad y el dinamismo y la participación de la sociedad civil, en muchas ocasiones las redes ciudadanas se sostienen en gran medida sobre el trabajo y la colaboración voluntaria. Estas relaciones representan el lado humano de Internet, contribuyendo al nacimiento de otra sociedad alternativa, la *e-sociedad*.

- Facilitar el acceso y la formación de la ciudadanía a la naciente sociedad de la información, en este sentido, podrían considerarse como la escuela de la era digital.
- Democratizar el uso de Internet y evitar que se produzca una división entre los que tienen acceso a esta tecnología y los que no lo tienen (brecha o fractura digital).
- Desarrollar y aplicar soluciones telemáticas, de amplio espectro como comercio electrónico, teletrabajo, entre otras, tendentes a la creación de empleo, la democracia electrónica y la integración social.
- Promover y favorecer la comunicación, la cooperación y el desarrollo de servicios entre los ciudadanos, asociaciones, empresas y administraciones que constituyen una comunidad local (entendida esta en sentido amplio).
- Conseguir, en definitiva, una comunidad vertebrada, informada y organizada, ya que solo de esta forma se está en condiciones de garantizar una sociedad participativa, solidaria y tolerante.

A continuación, detallamos algunas características de las redes sociales:

- Son organizaciones comunitarias que usan TIC para comunicarse: ponen ordenadores e información electrónica a disposición los ciudadanos de manera gratuita o a bajo precio.
- Difunden información a los ciudadanos acerca de la historia y cultura de la localidad, de las normas legales, sucesos de actualidad, así como otros temas de interés, que les permitan participar de una manera eficiente en su devenir diario y en el quehacer de la sociedad.
- Son un medio de comunicación e intercambio de información interactivo y bidireccional, pero no simples tablones de anuncios, ya que ofrecen a los ciudadanos la posibilidad de disponer de cuentas gratuitas de correo y participar en fórums de discusión, por medio de los cuales comparten información acerca de bienes, servicios o cualquier tema de interés para la comunidad, bien entre si o entre ellos y las instituciones locales.
- Acercan a los ciudadanos entre sí, y también a los ciudadanos con sus gobernantes y legisladores, lo que favorece el renacimiento de la democracia participativa.

- Ayudan a reducir la exclusión social, creando lugares de encuentro e intercambio local de participación, de discusión colectiva y de toma de decisiones democráticas, bajo criterios de igualdad de acceso a la información y nuevas tecnologías para todos.
- Son gestionadas, organizados y/o moderados por los propios ciudadanos de forma voluntaria, a menudo y al menos inicialmente, lo que, en ocasiones, las lleva a su desaparición.
- Establecen alianzas estructurales o coyunturales con otras organizaciones, lo que tiene el doble objetivo de fortalecer el tejido asociativo de una comunidad concreta y de asegurarle la pervivencia a la propia red. Empieza a configurarse un nuevo tejido urbano, apoyado en la actividad virtual, donde los ciudadanos de una localidad establecen sus relaciones, aprovechando las nuevas formas de interrelación. Actores locales: asociaciones, ciudades, vecinos, bibliotecas, nuevas organizaciones, movimientos de mujeres, etc., intervienen con el propósito de la transformación social y del desarrollo local.

Este nuevo espacio socio comunicativo se caracteriza por la posibilidad de interactuar y relacionarse con otros usuarios, conocidos o no con los que se comparte alguna inquietud, motivación, o afición. La comunicación se convierte en un fin en si misma dando lugar al "comunicador permanente" que no requiere que los contactos sean necesariamente amigos o conocidos. Esto evidencia la profunda necesidad de millones de individuos de sentirse conectados con otros, aceptados, en compañía permanente y por tanto explorando nuevas formas de socialización.

Las comunidades virtuales implican un deseo para satisfacer necesidades o practicar roles específicos interactuando mediante herramientas tecnológicas que facilitan la cohesión entre las participantes sin importar la ubicación física. La fuerte cohesión que se genera en estos grupos da lugar a "*ciberbulling*", o sea cuando alguien opina de manera diferente y genera una gran cantidad de mensajes "atacando" y hasta amenazando a esa persona por sus ideas opuestas al grupo. McLuhan sostiene acerca de esto que "La pérdida del individualismo invita una vez más a la comodidad de las lealtades tribales" (McLuhan 1995:104). Como consecuencia, Castells sostiene que se debilitan los poderes simbólicos de aquellos sistemas tradicionales "que transmiten a través de las costumbres sociales codificadas por la historia: religión, moralidad, autoridad, valores tradicionales, ideología" (Castells 2006: 408).

Determinados fenómenos surgen como consecuencia del constante uso de las redes sociales. Uno de ellos es el llamado *FOMO* o "*Fear of Missing Out*" o el miedo a perderse algo, sucede frecuentemente entre los jóvenes que se caracteriza por el deseo o la necesidad de estar constantemente conectado a las redes sociales con el objetivo de saber constantemente que está haciendo el otro, lo cual esta facilitado por las redes sociales. Asimismo, surgen diferentes movimientos sociales en contra del poder establecido. Uno de ellos es el movimiento "*Anonymous*", donde se utiliza la máscara de Guy Fawkes (1570-1606), un católico inglés, quien planeó la "conspiración de la pólvora" con el objetivo de derribar el Parlamento con explosivos y asesinar al rey Jacobo I. Este personaje, quien inspiro la película *V of Vendetta* y de donde surge la máscara famosa fue el comienzo de este movimiento, surgió en el 2008 a nivel global a través

de acciones de protesta a favor de la libertad de expresión e independencia de Internet e incluyen ataques a sitios web de instituciones de gobierno y algunas privadas con el lema de "El conocimiento es libre. Somos Anonymous. Somos la Legión. No perdonamos. No olvidamos. ¡Espéranos!".

Las características de estos movimientos no podrían haberse dado en la realidad fuera de lo que llamamos cibercultura. El concepto de cibercultura podría contribuir a todos estos movimientos. Pierre Levy (2007) se refiere a este concepto como el conjunto de los sistemas culturales surgidos en conjunción con dichas tecnologías digitales.

De la misma forma se pueden utilizar los conceptos de cultura digital, cultura de la sociedad digital o sociedad digital como traducción de "*e-Society*" para designar la cultura característica de las sociedades en las que las tecnologías digitales configuran decisivamente las formas dominantes de información, comunicación y conocimiento como de investigación, producción, organización y administración. Según Levy, la cibercultura "se desarrolla conjuntamente con el crecimiento del ciberespacio" el cual se crea a partir de las infraestructuras materiales de ordenadores y otros materiales electrónicos, TICs (Tecnologías de la Información y la Comunicación) y las informaciones digitales contenidas y mediadas por dichos dispositivos. Otro rasgo importante es los problemas locales pasan a ser problemas globales por la transmisión viral a traves de las redes. Como indica Virilio (1995), el concepto de "*glocal*" une lo global y lo local pues lo local ha llegado a ser global y viceversa.

Ciertos casos hacen evidente el poder que poseen las "grandes tecnológicas" incluso sobre las comunidades digitales. Uno de ellos es el de Donald Trump quien fue "*banned*" o prohibido en *Facebook* y *Twitter* por considerar que éste sumó a las insurrecciones en el *capitolio* de Washington DC el 6 de enero del 2021, dos semanas antes de entregar el poder a Joe Biden, luego de haber perdido las elecciones, las que considero "fraudulentas". Los seguidores del partido conservador de Trump continuaron comunicándose a través de otra plataforma llamada *Parler*. Sin embargo, el *Apple* store para los teléfonos *iPhones* y *Google* store para los teléfonos Android

también prohibieron la aplicación. Esto llevó a una serie de discusiones acerca de "Free Speech" o libertad de prensa y el poder que poseen las gigantes tecnológicas.[14]

Howard Rheingold (2000) predijo la existencia de las "cibercomunidades" que darían a los ciudadanos el impulso para desafiar el control político y económico de las elites de poder detrás de los medios de comunicación. Así, muchos creyeron que la nueva era digital daría lugar a una era igualitaria o "republica electrónica" donde la el dialogo publico podría alterar la formación de la opinión pública y por lo tanto el comportamiento de los políticos, empoderando a los ciudadanos y profundizando la democracia. De alguna manera este fue el deseo de Edward Snowden (ver su caso en esta investigación) al denunciar públicamente la existencia de los sistemas de vigilancia creados por las agencias de inteligencia en Estados Unidos e Inglaterra. Ayala considera que "los optimistas siguen confiando en que la producción de información de bajo costo, conversaciones públicas igualitarias en el ciberespacio, nuevas oportunidades para la acción política y la relación interactiva entre los ciudadanos y los políticos transformarán la democracia" (Deusdad Ayala, 2001)

Para Patten, la gran mayoría de los ciudadanos no se comprometen como deberían políticamente e incluso no se informan lo suficiente (Patten 2013: 25). En consecuencia, el aumento en participación ciudadana no es suficiente para generar cambios en los asuntos de política tradicional.

En términos generales, la cibercultura ha generado comportamientos que se basan en la permanente conectividad, las comunicaciones se convierten en digitales y los dispositivos tecnológicos pasan a ser parte de nuestra vida diaria. En este nuevo paradigma, la comunicación se hace inmediata y se generan intereses en común y la posibilidad de expresar opiniones abiertamente. Por supuesto esto también implica consecuencias negativas como la falta de tolerancia y la agresividad en línea, la depresión que puede generar en los adolescentes o las

[14] https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/

personas con baja autoestima, y la falta de reflexión respecto de estos nuevos fenómenos y la necesidad de educar a la población sobre la necesidad del uso responsable de todo lo digital.

Sin embargo, las posibilidades que aportan las redes sociales como una activa participación ciudadana podría ser una de las características más importante de la cibercultura. Es tan rápido y grande el cambio generado por la cibercultura en las personas, que se vuelve importante que las instituciones educativas generen programas para educar a los niños desde una temprana edad, sobretodo a aceptar y respetar opiniones disimiles. En el caso de Estados Unidos, varias muertes generadas por tiroteos en las escuelas en varias ocasiones llevadas a cabo por estudiantes que generaron diversos tipos de obsesiones, depresiones y otros problemas emocionales a partir de la conexión en red. Muchos adolescentes y niños no están preparados para el mundo “agresivo de las redes sociales” y las instituciones educativas deberían formar parte de este proceso como forma de protección a las nuevas generaciones.

CAPÍTULO III.

MARCO HISTÓRICO: LA REVOLUCIÓN TECNOLÓGICA

"Hablamos de ´software que se come el mundo´, ´Internet de las cosas´, y masificamos los ´datos´ declarándolos ´grandes´.
Pero estos conceptos siguen siendo en su mayor parte abstractos. Para muchos de nosotros es difícil comprender el impacto de la tecnología digital en el ´mundo real´ de cosas como rocas, casas, automóviles y árboles".

John Batelle[15]

[15] Es periodista y fundador de la Federated Media Publishing. Autor del libro "The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture" (La búsqueda: cómo Google y sus rivales reescribieron las reglas del negocio y transformaron nuestra cultura) -2006, Estados Unidos, Portfolio.

3.1. Un nuevo modelo de sociedad

Los conocimientos científicos y tecnológicos requieren de esfuerzos en un complejo proceso que demanda la presencia de empresas, instituciones públicas y sociedad civil, institutos de investigación y universidades a lo que Henoch Aguiar (2007) llama Sistema Nacional de Innovación. A nivel internacional, existe una creciente importancia de las redes de conocimiento para crear ventajas competitivas.

La sociedad del conocimiento es considerada aquella en donde el principal generador de valor económico es el saber, lo cual genera un valor agregado intelectual. En la era industrial el valor consistía en la repetición para la producción en serie. En la era del conocimiento, el valor consiste en la innovación, la intelectualidad y la generación de ideas. La innovación pasa a ser el motor del crecimiento.

Aguiar sostiene que Internet funciona como proveedor potencial de conocimientos para todo el cerebro humano y generará una nueva economía que es basada en el conocimiento. La innovación, incluida la conexión y la informatización de los procesos, o lo que llaman Internet de las cosas (se profundizará al respecto en las próximas páginas), generados por otras actividades económicas, como por ejemplo la agropecuaria se encuentran empapando lo nuevo. A su vez, la informática y la economía de los contenidos, de nuevos servicios basados en las comunicaciones, ya se encuentran cumpliendo un papel más que importante. La informática se convierte en omnipresente, desde nuestros autos, hasta inteligencia artificial con la que convivimos en nuestras casas.

Resulta importante nombrar la importancia del concepto de las Tecnologías de la Información y la Comunicación (TIC´s) pues más allá de referirse a ciertas tecnologías en particular, han generado una revolución cultural muy profunda que, según Underwood (2009), cambia todos los modos y patrones y de nuestras vidas e incluso en la educación. A partir de finales de siglo pasado empezaron a surgir dispositivos de comunicación y almacenamiento tales como Correos electrónicos, *PDAs*, cámara de fotos, agendas electrónicas, *GPS*, así como teléfonos celulares, que en nuestros días realizan todo esto y mucho más (Flórez Romero, 2017).

El término TIC se utiliza para describir las tecnologías emergentes que han obligado a la sociedad a transformarse y se refiere al uso de los diversos medios informáticos que permiten el almacenamiento, procesamiento y difusión de los diferentes tipos de información. Según Depetris, "La transformación que están produciendo en nuestros modos de hacer –aún las actividades más cotidianas– y la magnitud en que han potenciado nuestras capacidades, las han convertido en un elemento indispensable para individuos y sociedades" (Depetris, et al., 2008). En el contexto actual económico y social, las TIC pasan a formar parte de todos los ámbitos y de la vida cotidiana tanto de ciudadanos como de las empresas, donde se los reconoce como pilares básicos para el desempeño normal de las actividades humanas.

Marques (2001) describe que las TIC tienen múltiples funciones ya sea en el campo social, económico, político o cultural. En relación con la producción de conocimiento se encuentran:

- Posibilitar la comunicación, la transmisión de la información y la construcción de comunidades de aprendizaje autónomo.

- Potencializar los procesos a nivel de pensamiento, permitiendo que las personas construyan estructuras mentales y nuevas formas de pensar.

- Organizar, clasificar y analizar la información en términos de eficiencia para mejor manejo y mayor acceso por parte de la sociedad.

- Crear nuevos espacios y metodologías para la enseñanza y el aprendizaje, como el campo del *e-learning*, fortaleciendo procesos metacognitivos.

- Generar nuevos modelos de aprendizaje para las comunidades.

Para adentrarnos al concepto de Sociedad del Conocimiento, nos gustaría hacer una distinción entre el concepto de Información y el de Conocimiento. Entendemos "Información" al "signo físico o simbólico, conservado o registrado cuyo propósito es representar, reconstruir o

demostrar un fenómeno físico o conceptual. La información tiene valor en sí misma al apoyar todo proceso interactivo. La información es la materia prima de la sociedad actual y se impone como un producto en sí. Es por naturaleza volátil, efímera y tiene una pronta obsolescencia. Su valor añadido, no está en su contenido sino en su posible explotación futura mediante el conocimiento. La información es pasiva pero también puede activar el saber. Representa una forma de transmisión de un conocimiento. (Romaní, 2005)

El conocimiento, por su parte, se asocia con la creación de nuevas ideas. El conocimiento es un acto humano que se basa en la interpretación de datos para actuar en un contexto determinado y reside fundamentalmente en las personas. (Romaní, 2005). Nonaka (1994) lo define como algo intangible que reside en un espacio común, que puede hacerse tangible y transferible pero cuando se separa de su contexto se convierte en información.

Los conceptos de información y conocimiento parecen difíciles de separar, pero existen diferencias que es importante no omitir. "La información es algo que la gente toma, posee, transmite, coloca en una base de datos, pierde, encuentra, escribe, acumula, cuenta, compara, etc. En cambio, el conocimiento no se adapta de igual manera a las ideas de enviar, recibir, y cuantificar. Resulta difícil tomarlo y transferirlo. (Romaní, 2005).

A continuación, enumeraremos algunas de las características de la sociedad de la información, basado en diversos autores y recopilado por Cobo Romaní. Estas características dan cuenta del rol protagónico de las tecnologías de la información y la telecomunicación y como estas penetran en los campos de la economía, la democracia, la guerra, la educación y las comunicaciones entre otras:

- *Procesual y flexible:* Becerra (2005) sostiene que "el rasgo procesual de las mutaciones y metamorfosis presentadas por la SI o Sociedad de la Información es una cualidad esencial que bien enfocada, permite aproximarse a los fenómenos contemporáneos ligados a la diseminación de la información y la comunicación". Algunas de las características de este rasgo procesual son: "liberación, desregulación y competitividad internacional". Como éstos son adoptados de manera desigual, en desiguales escenarios políticos y económicos, se podría decir que llevan a la coexistencia de varios modelos de SI, de la misma manera

que existen varios modelos de la sociedad industrial. Para Castells (2002: 89) la condición especifica de este rasgo procesual es la flexibilidad: "No solo los procesos son reversibles, sino que pueden modificarse las organizaciones (…) para reconfigurarse, un rasgo decisivo en una sociedad caracterizada por el cambio constante y la fluidez organizativa". Por su parte, Domínguez Sanchez-Pinilla (2003) sostiene que "La flexibilidad de las nuevas tecnologías implica que las mismas sean incorporadas a la organización de la empresa". Esto genera nuevas formas de trabajo que hemos visto explotar en torno de la Pandemia de Covid-19 en el año 2020 y 2021, donde la mayoría de las empresas continuaron funcionando a través del teletrabajo, telecompra y telebanco, entre otros. Este rasgo permite usos cada vez más "ad hoc" (adaptables) a las particularidades del que la necesite. Castells (2001) agrega que "La innovación tecnológica y el cambio organizativos, están centrados en la flexibilidad y la adaptabilidad"

- *Digitalidad:* La conversión de la información física (papel, pintura, fotografía) o analógica (audio, video), es un estándar universal susceptible de procesamiento por computadoras y transmisión de redes. En otras palabras, a un lenguaje binario de ceros y unos y susceptible de procesamiento de máquinas de cálculo. (Reusser, 2003). Entre otra característica es la de generar la compresión de datos en espacios muy pequeños que permite su acceso a alta velocidad. Un ejemplo es el Kindle o tableta electrónica de Amazon, donde una cantidad infinita de libros pueden ser almacenada en "la nube" y se pueden bajar cuando sean necesarios para luego borrar y reemplazarlo por otros libros. Estos son cambios sustanciales en la forma de producción, recepción, manipulación de contenidos gracias al uso de las TIC (Romaní, 2005).

- *Convergencia:* se refiere a la concentración, entrecruzamiento y vinculación tanto de medios como de organizaciones, sistemas y conjuntos de conocimientos. Cobo Romaní enumera dos tipos de convergencias: la primera es la puramente tecnológica en cuanto a la compatibilidad de diferentes TICs que resulta facilitada por la digitalización y otros avances

técnicos. El segundo tipo de convergencia es la relacionada con el conocimiento al tener acceso a información de otras disciplinas de saber, apoyada por el uso de las TICs, se potencian y complementan. Nos referimos a las diferentes practicas a las que se agrega el prefijo "e" como e-gobierno, e-aprendizaje o *e-learning*, además de otras disciplinas como la nanotecnología y la biotecnología. Otro concepto apropiado para describir la convergencia de las TICs es el de "multimedia", en la que diferentes medios confluyen para generar un producto multifuncional.

- *Reticularidad:* La estructura reticular de internet resulta similar a una tela de araña donde existen diversos "nodos" o puntos que concentran información y que poseen la capacidad de conectarse con otras redes de cualquier parte de la red, en este caso del planeta. La idea de millones de redes unidas presenta un modelo de interdependencia informacional. La estructura de "red de redes" se transfiere a otros fenómenos de la sociedad como la organización de un país, empresa o estructura social. Al respecto Whitaker (1999: 96 en Cobo Romaní, 2005) considera que Internet no es más que una encarnación particular de las posibilidades d las nuevas tecnologías de información en un momento determinado del desarrollo tecnológico (…). La Red deviene metáfora de una nueva forma de organización que las nuevas tecnologías hacen posible. Castells (2001: 43) agrega sobre esta estructura: "la arquitectura en red debe ser de carácter abierto, descentralizado, distribuido y multidireccional en su interactividad". En otras palabras, las redes telemáticas son configuradas por Internet, la telefonía inalámbrica y otras TICs. Esta configuración a su vez se transforma en redes sociales, comerciales y políticas, entre otras. Levis (1999: 111, en Cobo Romaní, 2005) considera que se genera un nuevo modelo de comunicación: "de muchos a muchos, que lo podemos denominar reticular, que no corresponde a los modelos tradicionales y que convierte a usuarios en el centro de la red".

- *Complejidad:* Burch et al. (2003: 5) sostiene que: "La Sociedad de la Información es una de esas expresiones que día a día gana mayores credenciales, más por tu efecto de impacto que por su claridad conceptual". Para Moragas (2001), los cambios en la comunicación moderna

generan un proceso complejo y por tanto analizable desde la teoría de la complejidad. Se generan "cambios tecnológicos, multiplicación de actores, y la convergencia y confluencia de distintos sectores que pierden su anterior autonomía". Una de las características de un sistema complejo es "aquello que está conformado por más de un elemento o, en consecuencia, tiene más de una sola forma, o se mueve en más de una dirección". (Font, 2000: 9, en Cobo Romaní, 2005). La complejidad resulta del exceso de información, interacción e interdependencia que se produce entre los individuos de la sociedad actual. Luhman (1990: 76) considera que "la complejidad es la información que le falta a un sistema para comprender y describir completamente su entorno (complejidad del entorno), o bien, así mismo (complejidad del sistema). Piscitelli (2002: 27) plantea que "el mundo se está volviendo cada vez más complejo a partir de la multiplicación de interacción de los hombres entre sí y con las maquinas. Finalmente, Cobo Romaní considera que las TIC´s generan un aumento en los canales de interacción, lo que se traduce en una sobreabundancia de relaciones, y ello influye en que resulte difícil entender los permanentes cambios que se producen en el entorno, generando mayor incertidumbre.

- *Incertidumbre:* Más de cuatro décadas después de la investigación llevada a cabo, sus palabras resultan aún vigentes en cuanto las transformaciones en la sociedad como consecuencia del desarrollo de las TIC´s: "los esquemas tradicionales para interpretar a la sociedad y prever su futuro, servirán muy poco. El nuevo desafío es el de la incertidumbre; no hay una previsión valida Algunos de los conceptos relacionados con la incertidumbre son: ambigüedad, confusión, duda, indecisión, irresolución, escepticismo, falta de confianza, estado de suspenso, impredictibilidad" (Nora, Minc, 1978).

Negroponte (1995, citado en Cuadra, 2003), sostiene que "estar digitalizados nos da muchos motivos para ser optimistas. Como fuerza natural, la era digital no puede ser ni negada, ni detenida". Según algunos autores, existe un determinismo tecnológico. Para Toffler, en su obra "La Tercera Ola" (1980, en Cobo Romaní, 2005), la informática y las telecomunicaciones son un vehículo del

progreso, democracia, cultura y libertad que conduce al aumento del tiempo libre y el mejoramiento en la calidad de vida. Este tipo de mirada de la tecnología es llamada determinismo tecnológico.

Castells considera que "La tecnología no es ni buena ni mala, ni tampoco neutral". Sin embargo, Blejman (2014) critica esta postura cuando sostiene: "Habitualmente suele decirse que las tecnologías no llevan en si una valoración axiológica ni positiva ni negativa y que el uso de estas no depende de lo que se desarrolle, sino como se aplique. Sin embargo, sería ingenuo quedarse con este planteamiento simplista y negar (…) que las tecnologías se insertan en el marco de un desarrollo mundial de telecomunicaciones y reproducen constantemente los modos de producción del sistema capitalista globalizado y transnacionalizado. (…) . Por lo tanto, creer que estas técnicas son solo van a utilizarse para obtener información que sirva a la navegación de una página Web es poco recomendable.

En una postura similar, Mattelart (2002), critica a una sociedad reducida al modelo tecnologizante, afirmando: "Es importante comprender que la noción de sociedad de la información (…) se refiere a un proyecto concreto, que no beneficia a la mayoría, sino que está construido, sobre el mito de que se va a beneficiar a la mayoría. Mattelart también introduce el concepto de "Sociedad del control" que proviene del modelo de fábrica postfordista. En este nuevo modelo de sociedad de la información, se multiplican los mecanismos sociotécnicos del control flexible. "Las virtudes cardinales de este modo de gestión-autonomía, creatividad, reactividad, adaptabilidad- se entrelazan con las exigencias de la "planilla de los objetivos" y de la "cultura del resultado". El mismo Mattelart cita a Gilles Deleuze cuando éste elabora el concepto de Pourparlers: "Es evidente que puede buscarse siempre la correspondencia entre un tipo de sociedad y un tipo de máquina: las máquinas simples o dinámicas de las sociedades de soberanía, las máquinas energéticas de las sociedades disciplinarias, las máquinas cibernéticas y los ordenadores de las sociedades de control. Pero las máquinas no explican nada, es preciso analizar los dispositivos colectivos de enunciación de los cuales las máquinas no son más que una parte".

Mattelart también menciona a Foucault en cuanto a sus estudios sobre los dispositivos panópticos. El panóptico es una forma de estructura arquitectónica, diseñada para cárceles y prisiones, que suponía una disposición circular de las celdas en torno a un punto central, sin comunicación entre ellas y pudiendo el recluso ser visto desde el exterior. A su vez, la torre era

construida con una estructura opaca de manera tal que no se pudiera ver hacia donde estaba mirando el vigilante. Por lo cual, el recluso podía ser vigilado constantemente y para no ser castigado debía controlar su comportamiento. Según Foucault, el tiempo ha provocado que nos sumerjamos en una sociedad disciplinaria, que controla el comportamiento de sus miembros mediante la imposición de vigilancia. "En el panóptico, cada uno según su puesto, está vigilado por todos los demás, o al menos por alguno de ellos; se está en presencia de un aparato de desconfianza total y circulante, porque carece de un punto absoluto" (Foucault, 1979: 20). La esencia del panóptico es sentirse controlado cada minuto del día, sin saber cuándo se está controlado. (González Santana, 2007).

Tiempo más tarde, Orwell escribió la novela 1984, presentando un protagonista que constantemente se encontraba vigilado: "A la espalda de Wiston, la voz de la telepantalla seguía murmurando (…). La pantalla recibía y transmitía simultáneamente. Cualquier sonido que hiciera Winston superior a un susurro, era captado por el aparato. Además, mientras permaneciera dentro del radio de visión de la placa de mental, podía ser visto a la vez que oído. (Orwell, 2003: 10). En una historia similar, Truman, el protagonista de "*The Truman Show"* o "El show de Truman", se subleva contra aquellos que ante la mirada constante de cámaras que transmiten sus vidas, haciendo de ellas un mero espectáculo de entretenimiento. A pesar de ser estos ejemplos de "ficciones", se muestra una sociedad que a nuestros días podría considerarse real, al encontrarse constantemente vigilada con cámaras en lugares públicos (metro, autobús, edificios púbicos), teléfonos móviles convertidos en pequeños ojos mediante sus cámaras integradas, webcams integradas en miles de hogares, tanto adentro como afuera, compañías y satélites que pueden captar lo más mínimo de los detalles.

Finalmente, quisiéramos incluir el concepto de Sociedad en Red introducido por Manuel Castells pues es un concepto que se sitúa entre el del Sociedad de Conocimiento y Sociedad de la información. Para Castells, información es comunicación del conocimiento y ha sido "fundamental en todas las sociedades (...) En contraste, el término informacional indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este periodo histórico" (Castells, 1996: 47; Krüger, 2015). El concepto de "sociedad red" sostiene que las transformaciones actuales en la sociedad

indican un cambio del modo de producción social con motivo de la creciente4 importancia de la información o del conocimiento para los procesos económicos y sociales. Información y conocimiento se convierten en los factores productivos más importantes.

3.2. La educación en la Sociedad del Conocimiento

Una vez expuestas las definiciones de la Sociedad del Conocimiento, ahora nos gustaría explicar qué papel debe jugar la educación en ésta. Desde la perspectiva de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2005) citada por Forero (2009), el acceso a la educación, información y la libertad de expresión son los pilares de la sociedad del conocimiento. La idea de educación en la sociedad de conocimiento es formar individuos que aporten al desarrollo económico político y social desde diferentes profesiones. A su vez, resulta importante cambiar los paradigmas tradicionales para dar lugar a otros paradigmas nuevos y pertinentes para la nueva sociedad del conocimiento.

Paur, Rosanigo y Bramati (2006: 45) sostienen que "El nuevo sistema de educación requiere nuevas metodologías, nuevos roles docentes, que se centran más en el diseño, gestión de actividades y medios de aprendizaje y que da lugar a nuevas metodologías y nuevos roles docentes, más centrados en el diseño y gestión de actividades y entornos de aprendizaje, en la investigación sobre la práctica, selección de contenido Profesor-Estudiante, recursos, en la orientación, asesoramiento y dinámica de grupos, en la evaluación formativa y en la motivación de los estudiantes".

Un punto crucial de la educación en la sociedad del conocimiento es que Internet pasa a ser protagonista en el mundo educacional. Ya sea en cuanto a la comunicación con otros compañeros de estudio o con los profesores, al uso de plataformas de estudio o (y esto tal vez lo más importante) a la cantidad indiscriminada de información que se encuentra disponible en línea donde los estudiantes deben aprender a utilizar y "depurar" la información para descubrir información valiosa, darle una mirada crítica, y un fin utilitario. En otras palabras, el estudiante debe aprender a utilizar la información y el conocimiento para innovar o solucionar determinados problemas o necesidades con el objetivo de modificar el mundo que lo rodea, como la calidad de vida, de sus allegados y la de la comunidad o incluso el país o región.

El otro problema es el acceso a la tecnología, la conectividad y el contenido académico disponible para el estudiante. En los países del primer mundo, las mayorías de las comunas y las universidades ofrecen acceso a los ciudadanos, a través de bibliotecas locales, a contenido académico online o digital que fácilmente pueden analizar en sus computadoras en sus casas. En tiempos pasados, no era difícil encontrar estudiantes de universidades provenientes de países subdesarrollados, presentar dificultad para acceder a libros, publicaciones o apuntes académicos. En otras palabras, la sociedad del conocimiento requiere la inclusión de todos sus miembros para ser exitosa. La UNESCO (2005, citada por Forero en el 2009) señala que uno de los grandes obstáculos que existen para cumplir con los Objetivos de Desarrollo para el Milenio es la considerable inversión en educación y formación que se requiere para la construcción de una sociedad del conocimiento. Sumado a esto, se necesita el conocimiento para dominar la tecnología y por supuesto el acceso al material educativo.

Como resultado, se genera una situación donde, según Tedesco (2003), es la que se pretende incluir solo a los individuos que desarrollen las capacidades básicas vinculadas con la educabilidad y empleabilidad excluyendo al resto de la población que, tal vez solo por no tener acceso, sea considerada "no útil" y por lo cual termina siendo marginado por no tener las características que este nuevo sistema requiere haciendo prácticamente imposible salir de los bajos niveles de pobreza, ignorancia y violencia (Acevedo, 2019).

3.3. Inteligencia Artificial

Actualmente nos encontramos lejos de generar un consenso con respecto al implementar parámetros legales en cuanto a "Cosas inteligentes", aunque podríamos ver algunos consensos en cuanto a ciertas pautas éticas. Los diferentes tipos de tecnología de inteligencia artificial que comenzaron a convivir con las personas en su vida diaria podrían influir relaciones entre personas, modificando comportamientos y visiones de la vida, especialmente en cuanto a las técnicas de "aprendizaje profundo". Desde esta perspectiva, pareciera que la tecnología influye y da forma al comportamiento humano y no a la inversa.

Para que la ley actúe apropiadamente como una "meta-tecnología", tendría que estar respaldada por pautas éticas que sean consistentes con la era de la "hiperconectividad". Por esta razón es importante entender la capacidad de influencia de estos agentes "in-humanos" en aras de lograr una mejor regulación, especialmente en cuanto a tecnologías autónomas, con los ojos puestos en preservar los derechos fundamentales de los individuos.

Por último, con tecnologías que se desplazan desde ser herramientas simples para convertirse en factores influyentes y con capacidad de toma de decisiones, la ley debe construirse a si misma y transformarse desde un mundo tecno-céntrico a un mundo centrado en los seres humanos donde los modelos de diseños que se establezcan de acuerdo con valores constitucionales. Los principios éticos para seguir deberían ser: justicia, confianza, seguridad, privacidad, protección de datos, "inclusividad", transparencia y responsabilidad.

En conclusión, es importante considerar a las maquinas inteligentes no solo como herramientas sino como maquinas morales que interactúan con ciudadanos en la esfera pública entrelazada con sistemas socio técnicos.

De hecho, el concepto de Inteligencia Artificial deja de ser tal para convertirse en algo tangible al encontrarse presente en el Internet de las cosas, automóviles autónomos, sistemas de diagnóstico médico, bolsa de valores, drones, mapas, redes sociales, y en el día a día de las personas (como *Alexa* o *Google Voice* en Estados Unidos), y obviamente los teléfonos celulares con sistemas de reconocimiento de voz como *Siri* en los *IPhones*, entre otros. Lo que se consideraba excentricidad o ciencia ficción hace unos años, hoy existe en cada detalle de la vida diaria como algo común. Esa nueva modalidad de la vida diaria genera nuevos desafíos legales.

3.4. Internet de las Cosas

Esta denominación se refiere a los billones de aparatos físicos que se encuentran conectados a Internet y compartiendo datos. Gracias a la llegada de chips a un precio muy accesible y a la posibilidad de acceso a la tecnología *Wireless*, es posible convertir casi todo, desde una pequeña pastilla hasta un avión. Solamente agregando un sensor a los objetos se podría generar en ellos un

nivel de inteligencia digital a objetos que de otra manera se los podría considerar "tontos", y otorgándoles la capacidad de enviar datos en tiempo real y sin la necesidad de la presencia humana.

Parisier (2011) define que hemos llegado a una era donde el "usuario es el contenido" pues gracias al IoT (*Internet of Things* o Internet de las Cosas) se puede almacenar datos como los de preferencias, locaciones, desplazamientos, compras, elecciones, opiniones, amistades, frecuencia de la comunicación, entre otros. Un artículo periodístico del 2016 acerca de IOT por un estudioso de la cuarta enmienda concluyó: "Si millones de sensores llenos con datos personales quedaran afuera de las protecciones de la cuarta enmienda, una red de vigilancia a larga escala existiría sin límites constitucionales" (Guthrie Ferguson 2015).

3.5. Capitalismo de Vigilancia

Shoshana Zuboff (2019), en el libro "La era del capitalismo de vigilancia" denomina *"Surveillance Capitalism"* o "Capitalismo de Vigilancia" al sistema donde la experiencia humana se convierte en materia prima gratuita que se puede traducir en datos de comportamiento. Aunque parte de estos datos se son aplicados en mejorar productos o servicios, el resto es declarado como *"behavioural surplus"* o "excedente de comportamiento" de las empresas capitalistas de la vigilancia y utilizado para predecir productos que anticipan lo que las personas hacen ahora, harán pronto y más adelante. La dinámica competitiva de estos nuevos mercados impulsa a los capitalistas de la vigilancia a adquirir fuentes de excedente de comportamiento cada vez más predictivas: desde nuestras voces hasta nuestras personalidades e incluso nuestras emociones.

Los capitalistas de la vigilancia descubrieron que los datos de comportamiento más predictivos se obtienen interviniendo en la marcha misma de las cosas para empujar a, persuadir de, afinar y estimular ciertos comportamientos a fin de dirigirlos hacia unos resultados rentables como veremos en el caso de *Cambridge Analytica*. Zuboff sostiene que, a partir de esa reorientación desde el conocimiento hacia el poder, ya no basta con automatizar los flujos de información referida a nosotros, el objetivo ahora es automatizarnos. De ese modo, el capitalismo de la vigilancia da a luz a una nueva especie de poder que Zuboff llama "instrumentarismo".

El poder instrumentario conoce el comportamiento humano y le da forma, orientándolo hacia los fines de otros. En vez de desplegar armamentos y ejércitos, obra su voluntad a través del medio ambiente automatizado conformado por una arquitectura informática cada vez más ubicua de dispositivos "inteligentes", cosas y espacios conectados en red.

Un ejemplo de este capitalismo de vigilancia y que resulta aplicado a nuestros casos es el de la hasta la implacable expropiación de excedente tomado de los perfiles de *Facebook* con el propósito de influir en la conducta individual, ya sea haciendo que alguien compre crema anti acné a las 17.45 horas de un viernes, o que cliquee «sí» en la oferta de unas nuevas zapatillas para correr cuando tiene el cerebro lleno de endorfinas tras haber participado en una larga carrera un domingo, o haciendo que vote la semana siguiente por el candidato "adecuado". Del mismo modo que el capitalismo de la era industrial tendía a la continua intensificación de los medios de producción, los capitalistas de la vigilancia y sus actores de mercado están ahora atrapados en una dinámica de intensificación continua de los medios de modificación de la conducta y de creciente fortalecimiento del poder instrumentario. El capitalismo de vigilancia desmiente que estar "conectados" sea algo inherentemente pro-social o inclusivo por naturaleza, o que ayude a la democratización del conocimiento.

La conexión digital es un medio para satisfacer los fines comerciales de otros y en este sentido el capitalismo de vigilancia es parasítico y autorreferencial. Resucita aquella vieja metáfora de Karl Marx, que retrató el capitalismo como un "vampiro" que se alimenta del trabajador, pero en lugar de ser los trabajadores, la fuente de alimento del capitalismo de vigilancia es cualquier aspecto de la experiencia de cualquier ser humano. *Google* fue uno de los pioneros en este nuevo modelo de capitalismo y de alguna manera abrió camino en su práctica. Se lanzó en un territorio que no tenía límites legales o competidores

Luego se extendió con rapidez a *Facebook*, a *Microsoft* y *Amazon*. En los inicios, las grandes compañías de internet estaban concentradas en la publicidad en la red. Hoy, los mecanismos y los imperativos económicos se han convertido en el modelo por defecto de la mayoría de los negocios basados en Internet expandiéndose hacia el mundo offline o el que no está conectado en línea: la vida cotidiana de las personas. Estos mecanismos expropian los "*clicks*" y los "me gusta" de las personas y generan predicciones que luego se comercian en mercados de futuros comportamientos

para luego extenderse más allá de los anuncios dirigidos en la red y abarcar ahora otros muchos sectores, como los seguros, el comercio minorista, las finanzas y un elenco creciente de compañías de bienes y servicios decididas a participar de estos nuevos (y rentables) mercados. Ya sea un dispositivo doméstico "inteligente", o aquello que las aseguradoras llaman "seguro conductual", o miles de transacciones posibles, ahora los usuarios pagan por ser "dominados".

Así, los usuarios son atraídos como rebaños y sus experiencias personales son empaquetadas para convertirlas en medios para los fines de otros y pasan a ser los objetos de una operación tecnológicamente avanzada de extracción de materia prima a la que resulta cada vez más difícil escapar. Las empresas pasan a ser los clientes del capitalismo de vigilancia al comerciar en los mercados que este tiene organizados acerca de nuestros comportamientos futuros. A su vez, Internet se ha convertido en esencial para la participación social, la cual se encuentra saturada de comercio, el cual se encuentra supeditado al capitalismo de la vigilancia. La dependencia de los usuarios es un elemento básico del proyecto de la vigilancia comercial, en el que las necesidades que sienten de aumentar la eficacia en sus vidas compiten con su inclinación a resistirse. Este conflicto produce un entumecimiento psíquico que los habitúa a la realidad de ser monitorizados, analizados, explotados como minas de datos y finalmente modificados.

El capitalismo de vigilancia también actúa por medio de unas asimetrías de conocimiento y de poder sin precedentes: los capitalistas de vigilancia lo saben todo sobre los usuarios, pero sus actividades se encuentran diseñadas de manera tal que no puedan ser conocidas por ellos. En otras palabras, los conocimientos provienen de la vida de los usuarios, pero se predice su futuro para el beneficio de otros, pero no para el de ellos. La propiedad de los nuevos medios de "modificación de comportamiento" pasa a tener más importancia y generar mayor riqueza y poder capitalista en el siglo XXI, que la propiedad de los medios de producción de los modelos económicos anteriores.

El capitalismo de la vigilancia es una fuerza sin escrúpulos impulsada por unos novedosos imperativos económicos que ignoran las normas sociales y anulan los derechos elementales asociados a la autonomía individual y que tan imprescindibles resultan para que las sociedades democráticas sean posibles. De la misma manera que los nativos de las islas caribeñas no sabían el futuro que se les venía cuando vieron a los soldados españoles caminando trabajosamente por la arena y con sus armaduras, la nueva realidad sin precedente consigue confundir las capacidades de

comprensión. Es difícil para los usuarios captar los cambios de un modo adecuado desde el punto de vista de los conceptos existentes. Desde este punto de vista, es importante destacar que el punto crítico debe estar puesto en las características del "titiritero" y no del 'títere". Asimismo, no se debe confundir el capitalismo de vigilancia con las tecnologías. El capitalismo de vigilancia es la lógica que impregna la tecnología y que la pone en acción. Es una forma de mercado que resulta inimaginable fuera del medio ambiente digital, pero al mismo tiempo no es "lo digital".

En el 2009, la opinión pública tomó conocimiento que *Google* conserva historiales de los usuarios indefinidamente y esos datos están al servicio de los servicios de inteligencia policiales de los gobiernos. Cuando le preguntaron al director de *Google*, este afirmo: "Los buscadores y *Google* entre ellos, sí conservan la información durante un tiempo". A esto se podría responder: los buscadores no son los que lo conservan sino el capitalismo de vigilancia. Y este tipo de declaraciones son un ejemplo de cómo confundir a la opinión pública al mezclar imperativos comerciales con la inevitabilidad tecnológica. En este caso pareciera que las prácticas del capitalismo de vigilancia son inevitables, pero en realidad todo está meticulosamente calculado y luego financiado con el objeto de alcanzar fines comerciales.

Max Weber (1978) sostuvo que los fines económicos determinan ciertos objetivos y la tecnología proporciona los medios adecuados para lograrlos. En términos del propio Weber, "la cabal orientación económica del llamado proceso tecnológico por las probabilidades de ganancia es uno de los hechos fundamentales de la historia de la técnica". Una sociedad capitalista moderna, la tecnología era, es y siempre será una manifestación de los objetivos económicos que dirigen su acción. Al borrar la palabra "tecnología" del vocabulario es fácil descubrir los objetivos del capitalismo.

El capitalismo de la vigilancia emplea muchas tecnologías, pero no se equipara con ninguna en particular. Puede que utilice ciertas plataformas, pero estas actividades no son lo mismo que las plataformas de las que se vale para ellas. Emplea inteligencia de máquinas, pero no es reducible a esas máquinas. Produce algoritmos y depende de ellos, pero el capitalismo de la vigilancia y algoritmos no son lo mismo. El capital de la vigilancia es el que manda en el mundo o medio digital y así orienta la trayectoria hacia un futuro.

El capitalismo de vigilancia comienza con *Google*. Pese a la habilidad técnica y el talento informático de *Google*, el verdadero mérito de su éxito corresponde a la imposición que comenzó por despreciar todas las fronteras de la experiencia humana privada. A través de *Google*, el capitalismo de la vigilancia afirmó su derecho a invadir y a usurpar los derechos de decisión individuales, en beneficio de la vigilancia y de la extracción "autoautorizada" de la experiencia humana para lucro de los capitalistas de la vigilancia.

Estas prácticas invasivas, fueron alimentadas por la ausencia de una legislación que impidiera su materialización, por tal vez estar adelantado a las leyes (como se encuentra usualmente la tecnología), y por el apoyo de la comunidad de intereses entre los capitalistas de la vigilancia y las agencias de inteligencia de los Estados, y por supuesto por la firmeza con la que defendió sus nuevos territorios. Al final, *Google* logró institucionalizar sus actividades capitalistas de la vigilancia hasta convertirlas en la forma dominante de capitalismo informacional, atrayendo así a nuevos competidores ansiosos de participar en la carrera por obtener ingresos de la vigilancia. Así, *Google* y su universo en expansión de competidores han disfrutado y siguen disfrutando de descomunales asimetrías de conocimiento y poder, sin precedente en la historia humana.

CAPÍTULO IV.

MARCO JURÍDICO: LA EVOLUCIÓN DE LOS ACUERDOS

"La ley de la UE prohíbe el envío de datos personales a naciones ´incivilizadas´, como Estados Unidos"

Robert Brownstone[16]

[16] Presidente del grupo EIM en Fenwick & West, sobre privacidad de datos en Estados Unidos.

4.1. Safe Harbor

Los principios de Safe Harbor fueron postulados que se desarrollaron entre el año 1998 y el año 2000 con el objetivo de prevenir que organizaciones privadas dentro de los Estados Unidos (EUA) o la Unión Europea (UE) y que guardan información privada, accidentalmente compartan o pierdan estos datos.

En el 2015, un defensor de la privacidad de nacionalidad austriaca llamado Max Schrems (ver casos en Fuentes Consultadas), comenzó un proceso legal al comisionado irlandés de protección de datos en contra de *Facebook*. En la documentación, Schrems presentó quejas en contra de la transferencia de sus datos desde Europa hacia los Estados Unidos a través de *Facebook*. Como consecuencia de este caso, la Corte de Justicia de la Unión Europea invalidó el acuerdo de Safe Harbor el 6 de octubre del 2015.

El caso Schrems pone en evidencia una de las tensiones más importantes entre la ley de privacidad en EUA y la UE y los tratados internacionales y contratos que han sido utilizados para cubrir la brecha en cuanto a protección de datos. El punto clave en ambas legislaciones es si EUA protege adecuadamente los datos personales, como es requerido en la UE para permitir la transferencia de datos internacionalmente.

Los datos que Schrems, como usuario de *Facebook,* proporcionó a *Facebook* fueron transferidos desde la subsidiaria irlandesa de *Facebook* (*Facebook* Irlanda) a los servidores de Facebook ubicados en los Estados Unidos (*Facebook*, Inc.). Schrems presentó una queja ante la autoridad irlandesa de protección de datos, considerando que, a la luz de las revelaciones hechas en 2013 por Edward Snowden sobre las actividades de los servicios de inteligencia de los Estados Unidos (en particular la Agencia de Seguridad Nacional), la ley y las prácticas de EUA, no ofrecen una protección real contra la vigilancia por parte de EUA de los datos transferidos a ese país. La autoridad irlandesa rechazó la denuncia basándose, en particular, en que, en una decisión de 26 de julio de 2000, la Comisión consideró que, con arreglo al régimen de "puerto seguro", los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos (Epic, ver Fuentes Consultadas)

Los principios internacionales Safe Harbor en materia de privacidad hacen referencia a un proceso de cooperación por el que las organizaciones de EUA cumplen con la Directiva 95/46/CE de la UE, relativa a la protección de datos personales.

Pensados para organizaciones que operen entre EUA y la UE y que alojen datos personales de sus clientes y/o usuarios, los principios internacionales Safe Harbor están pensados para prevenir pérdidas o filtraciones no autorizadas de información. Para optar a incorporarse al programa Safe Harbor deberán cumplir con los siete principios de la Directiva 95/46/CE.

Los principios fueron desarrollados por el Departamento de Comercio de EUA en colaboración con la UE.

El 6 de octubre de 2015, los acuerdos de "Safe Harbor" entre la UE y EUA fueron declarados inválidos, como consecuencia de las revelaciones de Edward Snowden.

Para entender la creación de los principios *Safe Harbor* hemos de situarnos en el contexto proteccionista que la UE establece para la privacidad de sus ciudadanos. Esta protección es mucho más fuerte en Europa que en otras regiones del mundo.

Las organizaciones que operan en la UE no están autorizadas a realizar transferencias internacionales de datos a países ubicados fuera del Espacio Económico Europeo a no ser que los mismos ostenten niveles adecuados de protección.

Dicha protección puede producirse a nivel nacional (si las leyes del país se comprometen a ofrecer la misma protección) o a nivel de organización (si una multinacional elabora y cumple sus controles internos de protección de datos).

Los principios internacionales *safe harbor* permiten a las organizaciones de EUA registrar su certificado si cumplen con los requisitos de la UE.

Son siete los principios clave que recoge la Directiva 95/46/CE y que deben cumplir aquellas organizaciones que quieran ostentar el calificativo de *Safe Harbor*:

- **Información:** los interesados deberán ser informados de que sus datos personales están siendo recogidos y que serán tratados únicamente con la finalidad para la que fueron recogidos.

- **Elección:** los interesados tendrán el derecho de cancelación y oposición a que sus datos sean recogidos una vez sean recabados y a oponerse a la cesión o transferencia a terceros.

- **Transferencia progresiva:** la cesión de datos a terceros se llevará a cabo con organizaciones que también garanticen un adecuado nivel de cumplimiento de protección de datos.

- **Seguridad:** se deben establecer y cumplir determinadas medidas de seguridad para prevenir pérdidas de información y accesos no autorizados.

- **Integridad de los datos:** los datos deberán ser relevantes y exactos para el propósito para el que fueron recogidos.

- **Acceso:** los interesados podrán acceder en todo momento a la información que haya sido recabada acerca de ellos y podrán corregirla o eliminarla si es inexacta o inadecuada.

- **Ejecución:** se deben destinar medios y recursos para garantizar el debido cumplimiento de estos principios.

A diferencia de los Estados Unidos, la regla en la UE es que la transferencia de datos no está autorizada. Solamente está permitida bajo el cumplimiento de ciertos criterios. Las directivas con respecto a la trasmisión de datos a un tercer país pueden realizarse solamente si ese país asegura un nivel adecuado de protección de datos.

En Julio del 2000, la Comisión Europea adoptó la decisión de declarar que los EUA provea protección adecuada para la protección de datos. La decisión de la comisión fue basada en Safe Harbor Framework (O marco de referencia de Safe Harbor). Luego de la apelación de Schrems a la alta corte de Irlanda, esta dio lugar a sus pedidos. La decisión fue de finalizar Safe Harbor pues el tratado no proveía los requisitos legales de protección bajo las leyes de la UE. En uno de los documentos presentados por Schrems a la Corte de Justicia de la Unión Europea, se afirmaba que al declarar Safe Harbor nulo, se avanzaría en limitar las opciones legales para las autoridades de EUA para conducir vigilancia masiva en los datos adquiridos por empresas europeas.[17]

En abril del 2010, *Facebook* introdujo el botón de "Like" o "Me gusta" en su plataforma. En noviembre del mismo año, un estudiante de doctorado e investigador de privacidad, llamado Arnold Roosendaal (2010), quien demostró que el botón era una herramienta poderosa para capturar y transmitir los comportamientos y gustos de los consumidores, instalando *cookies* en las computadoras de los usuarios, aun así hicieran o no *"click"* en ciertas páginas, y no necesariamente *Facebook*, el investigador descubrió que *Facebook* estaba potencialmente recolectando información de todos los usuarios de la red. El 25 de septiembre un *hacker* australiano llamado Nick Cubrilovic publicó que había descubierto que *Facebook* seguían "tracking" o siguiendo a los usuarios, aun cuando no se encuentran navegando en la plataforma. En varias oportunidades la empresa se defendía alegando que son "*bugs*" o "*glitchs"* (virus o errores) del sistema, pero no tomando responsabilidad por sus acciones. Solo tres días antes de la publicación de Cubrilovic, algunos periodistas descubrieron que *Facebook* había recibido una patente en técnicas especializadas para seguir a los usuarios a través de diferentes sitios fuera de la plataforma Zuboff, 2017). El nuevo método de colección de datos permitía a *Facebook* seguir a los usuarios, crear perfiles personales de individuos y sus redes sociales, recibir reportes de otras empresas en cada acción de los usuarios e ingresar esas acciones en los sistemas de *Facebook* para generar una relación con publicidades relevantes para cada individuo. La compañía negó la relevancia de esta patente.

En el 2011, *Facebook* llegó a un acuerdo con el FTC (*Federal Trade Commission*) luego de haber sido acusado de engañar sistemáticamente a los usuarios prometiéndoles que su información

[17] https://epic.org/2015/09/decision-by-eu-legal-advisor-s.html

se iba a mantener privada, para luego permitir repetidamente que se comparta públicamente. La organización EPIC y una unión de defensores de la privacidad llevaron este caso al FTC, el cual comenzó una investigación que generó múltiples evidencias de las promesas faltas de la corporación. Una de las evidencias encontradas fue lo que más tarde generaría el escándalo de *Cambridge Analítica*: la posibilidad de recibir datos por aplicaciones de otras compañías que se conectaban con *Facebook*, inclusive permitiendo el acceso a datos personales aún después de haber eliminado la aplicación. Todas estas prácticas fueron consideradas violaciones del acuerdo de Safe Harbor entre los EUA y la UE. La orden de la FTC prohibió a la compañía continuar realizando violaciones a la privacidad, requería que los usuarios deban aceptar las nuevas políticas de privacidad. El presidente de la FTC Jon Leibowitz insistió que "Las innovaciones de *Facebook* no tienen por qué existir a expensas de la privacidad de los consumidores".[18] (Ver FTC en Fuentes Consultadas).

4.2. Privacy Shield

Dos años después del escándalo de Edward Snowden -2013- (que explicaremos en el Capítulo V de esta tesis) y poco tiempo luego de la declaración de la invalidez de Safe Harbor, la UE y los EUA comenzaron a negociar un acuerdo para reemplazar este tratado. En febrero del 2016, la Comisión Europea y la Administración del Presidente de Estados Unidos, Barack Obama, lanzaron la propuesta de Privacy Shield para la UE y los EUA. Así, el nuevo Acuerdo comenzó a regir, reemplazando el anterior de Safe Harbor.

Privacy Shield es un acuerdo que se logró entre los Estados Unidos y la Unión Europea para implementar ciertas reglas en cuanto a la transferencia de datos personales de la Unión Europea a los Estados Unidos. El acuerdo reguló desde el 2016 al 2020, cuando fue considerado nulo por no garantizar la protección de datos del Reglamento General de Datos (GDPR). De acuerdo con varios

[18] https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

grupos de defensa de la privacidad y del consumidor, el acuerdo no provee protección adecuada contra el mal uso comercial de la información personal y la vigilancia masiva.

Vera Jourová, Notaria de la Comisión Europea por la Justicia, afirmó: *"La protección de los datos personales es mi prioridad tanto dentro de la UE como a nivel internacional. Privacy Shield UE-EUA, es un marco nuevo y sólido, basado en una aplicación y un seguimiento sólidos, una reparación más sencilla para las personas y, por primera vez, una garantía por escrito de nuestros socios estadounidenses sobre las limitaciones y salvaguardias con respecto al acceso a los datos por parte de las autoridades por motivos de seguridad nacional. Además, ahora que el presidente Obama ha firmado la Ley de reparación judicial que otorga a los ciudadanos de la UE el derecho a hacer valer los derechos de protección de datos en los tribunales de EUA, podremos proponer próximamente la firma del acuerdo "umbrela" (paraguas) que abarca UE-EUA y que garantiza protección para la transferencia de datos con fines policiales. Estas sólidas medidas permiten a Europa y América restaurar la confianza en los flujos de datos transatlánticos".*

Las autoridades de EUA se comprometieron fuertemente a respetar y aplicar Privacy Shield para asegurar que no habrá descuidos o vigilancia masiva por parte de las autoridades de seguridad nacional. Esto garantizaría:

- **Obligaciones sólidas para las empresas y aplicación rigurosa:** el nuevo acuerdo será transparente y contendrá mecanismos de supervisión eficaces para garantizar que las empresas respeten sus obligaciones, incluidas las sanciones o la exclusión si no cumplen. Las nuevas reglas también incluyen condiciones más estrictas para las transferencias posteriores a otros socios por parte de las empresas que participan en el esquema.

- **Garantías claras y obligaciones de transparencia sobre el acceso del gobierno de los EUA a la información europea**: por primera vez, el gobierno de los EUA ha dado a la UE una garantía por escrito de la Oficina del Director de Inteligencia Nacional de que cualquier acceso de las autoridades públicas con fines de seguridad nacional estará sujeto a limitaciones claras, mecanismos de salvaguarda y fiscalización, que impidan el acceso generalizado a los datos personales. El entonces Secretario de Estado de los Estados Unidos,

John Kerry, se comprometió a establecer una posibilidad de reparación en el área de inteligencia nacional para los europeos a través de un mecanismo de Defensor del Pueblo dentro del Departamento de Estado, que será independiente de los servicios de seguridad nacional. El Defensor del Pueblo hará un seguimiento de las quejas y consultas de las personas y les informará si se han cumplido las leyes pertinentes. Estos compromisos escritos se publicarán en el registro federal de EUA.

- **Protección efectiva de los derechos de los ciudadanos de la UE con varias posibilidades de reparación:** las quejas deben ser resueltas por las empresas en un plazo de 45 días. Habrá disponible una solución alternativa de resolución de disputas gratuita. Los ciudadanos de la UE también pueden acudir a sus autoridades nacionales de protección de datos, que trabajarán con la Comisión Federal de Comercio para garantizar que las quejas no resueltas de los ciudadanos de la UE se investiguen y resuelvan. Si un caso no se resuelve por ninguno de los otros medios, como último recurso habrá un mecanismo de arbitraje que garantice un recurso exigible. Además, las empresas pueden comprometerse a cumplir con los consejos de las APD (Autoridad de Protección de Datos) europeas. Esto es obligatorio para las empresas que manejan datos de recursos humanos.

- **Mecanismo de revisión conjunta anual:** el mecanismo supervisará el funcionamiento de Privacy Shield, incluidos los compromisos y la garantía en lo que respecta al acceso a los datos con fines policiales y de seguridad nacional. La Comisión Europea y el Departamento de Comercio de EUA. Realizarán la revisión y asociarán a expertos en inteligencia nacional de las autoridades de protección de datos de EUA y Europa. La Comisión se basará en todas las demás fuentes de información disponibles, incluidos los informes de transparencia de las empresas sobre el alcance de las solicitudes de acceso del gobierno. La Comisión también celebrará una cumbre anual de privacidad con ONG´s y partes interesadas para discutir desarrollos más amplios en el área de la ley de privacidad de EUA Y su impacto en los

europeos. Sobre la base de la revisión anual, la Comisión emitirá un informe público al Parlamento Europeo y al Consejo.[19]

El 16 de julio del 2020, la Corte de Justicia de la Unión Europea declaró inválida la decisión de la Comisión Europea en cuanto a la adecuación de la protección generada por Privacy Shield, por lo cual el acuerdo dejó de ser un mecanismo válido para los requerimientos de protección de datos solicitados por la Unión Europea.[20]

A continuación, enumeramos algunas de las diferencias entre Safe Harbor y Privacy Shield:

- En Safe Harbor el Departamento de Comercio de EUA tenía un rol más bien "ministerial", solamente registrando los hechos y los cambios. A partir de la llegada de Privacy Shield, el DOC (*Department of Commerce* de EUA) jugó un rol mucho más activo, aprobando certificaciones y asegurándose que la lista de las compañías certificadas se mantuviera al día.

- La FTC (*Federal Trade Commission* de EUA) aseguro que bajo Privacy Shield daría lugar a los reclamos generados por residentes de la UE si su información personal no hubiera sido tratada de manera apropiada.

- Bajo Privacy Shield, el gobierno estadounidense crearía una nueva posición: la de *Ombudsperson* o Defensor del Pueblo, separado de las comunidades de inteligencia con el propósito de investigar y responder reclamos de usuarios provenientes de la UE si sus datos hubieran sido mal apropiados o procesados por los servicios de inteligencia de EUA.

[19] Sitio oficial de la Comisión Europea. Traducción realizada por la autora. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_433
[20] https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update

- Otro punto importante se refiere a que la Corte Europea considera que la información de residentes europeos acumulada por la Agencia de Seguridad Nacional (la NSA, para la cual trabajaba Edward Snowden), violaba la ley de la UE. Por lo cual la UE insistió en que cualquier acuerdo posterior debía tener algún mecanismo para proteger contra la vigilancia masiva impropia por parte del gobierno de EUA.[21]

4.3. General Data Protection Regulation (GDPR) de la Unión Europea

El Reglamento General de Protección de Datos (*General Data Protection Regulation* o el Reglamento General de Protección de Datos, Reglamento 2016/679) es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE). También se ocupa de la exportación de datos personales fuera de la UE. El objetivo principal del GDPR es dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la UE.

El GDPR amplía el ámbito de aplicación de la legislación para la protección de datos de la UE a todas las empresas extranjeras que procesan datos de residentes de la UE, haciendo más fácil que estas empresas no europeas cumplan con las nuevas normas.

Las razones porque se conformó el GDPR son las siguientes:

[21] https://www.lexisnexis.com/lexis-practical-guidance/the-journal/b/pa/posts/the-demise-of-safe-harbor-and-rise-of-privacy-shield-how-can-personal-information-now-be-exported-from-the-eu-to-the-united-states

- **Primera razón:** la UE quiere dar a las personas más control sobre cómo se utilizan sus datos personales, teniendo en cuenta que muchas empresas como *Facebook* y *Google* intercambian el acceso a los datos de las personas para el uso de sus servicios. La legislación actual fue promulgada antes de que Internet y la tecnología de la nube crearan nuevas formas de explotar los datos, y el GDPR busca abordar eso. Al reforzar la legislación sobre protección de datos e introducir medidas de aplicación más estrictas, la UE espera mejorar la confianza en la economía digital emergente.

- **Segunda razón:** la UE tenía el objetivo de dar a las empresas un entorno jurídico más simple y claro para operar, haciendo que la ley de protección de datos sea idéntica en todo el mercado único (la UE estima que esto ahorrará a las empresas un colectivo de 2.300 millones de euros al año).

Cuando el GDPR tuvo sus primeros impactos sustituyó a la Directiva de Protección de Datos (oficialmente Directiva 95/46 / CE) de 1995. El Reglamento fue adoptado el 27 de abril de 2016. Y se convirtió en Documento Ejecutivo a partir del 25 de mayo de 2018 tras una transición de dos años y, a diferencia de una directiva, no obliga a los gobiernos nacionales a aprobar ninguna legislación habilitante, por lo que es directamente vinculante y aplicable[22]. En el artículo 2.1, la GDPR refiere a una persona identificable ya sea por su nombre, número de identificación, localización y otros metadatos. Esto implica que los datos son relacionados con una persona en particular y dejan así de ser datos anónimos (Masseno, 2019)

En cuanto a la aplicación de la normativa, los "controladores" y los "procesadores" de datos deben atenerse al GDPR, es importante señalar que un controlador de datos indica cómo y por qué se procesan los datos personales, mientras que un procesador es la parte que realiza el procesamiento real de los datos. El controlador podría ser cualquier organización, desde una

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

empresa privada hasta una organización benéfica o un gobierno. Un procesador podría ser una empresa de tecnología que realice el procesamiento de datos. Si los controladores y procesadores están fuera de la UE, el GDPR seguirá aplicándose a ellos mientras se trate de datos pertenecientes a residentes de la UE. Es responsabilidad del controlador o empresa asegurar que su procesador cumpla con la ley de protección de datos y los procesadores deben respetar las reglas para mantener registros de sus actividades de procesamiento. Si los procesadores están involucrados en una violación de datos, son mucho más responsables bajo GDPR que estaban bajo la Ley de Protección de Datos.

La UE ha ampliado sustancialmente la definición de datos personales en el marco del GDPR. Para reflejar los tipos de organizaciones de datos que ahora recopilan sobre personas, los identificadores online, como las direcciones IP, ahora son considerados datos personales. La información económica, cultural o de salud mental, de los individuos también se considera información de identificación personal. Los datos personales pseudónimos también pueden estar sujetos a las reglas de GDPR, dependiendo de lo fácil o difícil que sea identificarlos. Cualquier dato que antes era considerado como personal bajo la Ley de Protección de Datos también califica como datos personales bajo el GDPR.

Muchas esperanzas se encuentran puestas en la regulación de GDPR a partir del 2018. El acercamiento de Estados Unidos difiere ampliamente del de la Unión Europea en referencia con la justificación que las compañías deben responder al GDPR de sus actividades en cuanto al manejo de datos. La regulación europea introduce varios puntos nuevos incluido el de requerir que la compañía notifique a los usuarios cuando hubo un *Data Breech* (acceso a la información por acción de un *hacker* o similar, logrando acceder a los datos personales), la prohibición de hacer publica cualquier información privada, requerimientos de utilizar sistemas que garanticen la privacidad, el derecho de borrar información por parte del usuario y la protección expandida contra de decisiones automáticas llevadas a cabo por sistemas que impongan efectos secundarios en la vida de las personas.

CAPÍTULO V.

EL CASO EDWARD SNOWDEN
Y
EL CASO CHRISTOPHER WYLIE

"Juguemos en el bosque mientras el Lobo no está"

Shoshana Zuboff[23]

[23] Profesora de la Universidad de Harvard y autora del libro "La era del capitalismo de vigilancia".

5.1. El caso Edward Snowden

"Argumentar que no te importa el derecho a la privacidad porque no tienes nada que ocultar no es diferente a decir que no te importa la libertad de expresión porque no tienes nada que decir"

Edward Snowden

Edward Snowden es un ciudadano de los Estados Unidos, especialista en computadoras quien comenzó a trabajar en el 2005 para diferentes agencias de seguridad estadounidenses como la CIA y la agencia de seguridad estadounidense o National Security Agency (NSA) a través de la empresa *Booz Allen Hamilton*, quien actuaba como contratista empleando candidatos para trabajar en proyectos de la NSA.

Snowden era un administrador de sistemas responsable de mantener y reparar redes. Esta responsabilidad le otorgaba accesos a programas y archivos clasificados. Así descubrió de la existencia de varios programas de inteligencia que almacenaba información privada, como llamadas *e-emails*, de una cantidad abismal de ciudadanos estadounidenses y extranjeros que no pertenecían a grupos terroristas ni estaban conectados con ningún acto ilegal. Snowden consideró que el público debería conocer lo que el gobierno estaba haciendo con su información privada.

En junio del 2013 Barack Obama luchaba por ganar la presidencia estadounidense y para ello presentó un discurso donde prometía el fin del espionaje hacia los ciudadanos comunes, quienes

no poseen ningún tipo de historial criminal. Sin embargo, años más tarde y luego de asumir la presidencia continuaría las políticas de sus predecesores, eliminando las investigaciones de violaciones a la ley y expandiendo programas abusivos. Snowden había tenido esperanzas en las promesas de Obama pero cuando éstas no se cumplieron, comenzó a recolectar documentos secretos que probaban que la NSA estaba espiando a los norteamericanos a gran escala.

Así Snowden comenzó a intercambiar *emails* con seguridad encriptada con Glenn Greenwald, un columnista de *The Guardian*, con Barton Gellman del periódico *The Washington Post* y con Laura Poitras, ciudadana estadounidense, realizadora cinematográfica y quien habría generado la conexión inicial entre Snowden y Greenwald. Al principio se mostró extremadamente misterioso, como un fantasma que no dejaba rasgos, pero que poseía archivos secretos de calidad remarcable. Los archivos demostraban que la agencia de inteligencia no solo espiaba a los actores "malos", como los terroristas, los rusos o los miembros de *Al-Qaeda*, sino también a las comunicaciones de millones de ciudadanos privados estadounidenses. En otras palabras, a la población en general.

Snowden le propuso a Greenwald que se encontraran en Hong Kong en el hotel *Kowlong's Mira*. Greenwald viajaría con Poitras, y quien también habría sostenido comunicación con él por varios meses. Snowden les proporcionaría una serie de instrucciones que denotaban lo que luego los periodistas describirían como "extremo cuidado" para no ser descubiertos (*The Snowden files*, 2014).

En la primavera del 2013, a días de cumplir sus 30 años, y luego de guardar la información en un pequeño disco, Snowden, tomó un avión desde los Estados Unidos hacia Hong Kong, donde se hospedó por algunas semanas. En esos días, entregó los documentos clasificados en persona a este grupo selecto de periodistas, generando atención internacional hacia la manera de operar de la NSA. Luego pudo volar a Rusia, donde el gobierno le otorgó asilo temporal y en donde todavía se encuentra residiendo.

En la película "Snowden"[24] se muestran varias escenas como el protagonista cubría las cámaras de las computadoras para no ser visto o los micrófonos para no ser escuchado. Ted Rall[25], un caricaturista, periodista y novelista grafico, diseñó un libro llamado "Snowden", donde cuenta a través de caricaturas cómo apenas terminada la Segunda Guerra Mundial, un autor llamado George Orwell comenzó a escribir una novela donde imaginaba el peor gobierno posible. La novela se llamaría 1984 y describía un nivel de opresión mucho más aterrador que el totalitarismo de la Alemania nazi y la Unión Soviética de Stalin.

Orwell advertía un Estado paranoico, constantemente en guerra y obsesionado con el terrorismo, que explotaría tecnología de última generación para observar cada movimiento de sus ciudadanos. No existiría privacidad, lugar donde correr, u ocultarse o hasta correr si fuera necesario: "Ningún lugar donde ser tú mismo". Cada comunicación: cada carta o llamada telefónica seria interceptada, analizada y guardada en los archivos. Esta información podría ser utilizada en contra de cualquier sujeto que el gobierno considerara como "blanco". Cámaras de seguridad, helicópteros y satélites monitoreando todos los movimientos de las personas mientras estas se mueven por las calles. Espías del gobierno observarían a los sujetos 24 horas por día 7 días por semana. Cada hogar tendría una pantalla desde donde podrían ser observados en cualquier momento. Esta ciudad imaginaria se llamaba *Oceanía.* Ted Rall (2015) considera que en el presente vivimos en Oceanía.

Snowden comenzó explicando a Greenwald y Poitras las capacidades extraordinarias que poseía la NSA para vigilar en masa al público "normal". En teoría, la Agencia sólo estaba supuesta a recolectar señales de inteligencia en objetivos extranjeros, mejor conocida como SIGINT y cuya misión es recolectar información acerca de terroristas internacionales, poderes extranjeros, organizaciones o personas[26].

Pronto se generó una división mundial entre los que lo consideraron héroe por proteger los intereses de la vida privada de las personas y los que lo consideraron un criminal, por haber

[24] Snowden es una película basada en el libro "Los archivos Snowden" y "Los tiempos del pulpo" de Anatoly Kucherena donde se cuenta la historia de Snowden desde los comienzos de su carrera hasta las últimas charlas que había presentado en público luego de haber entregado los documentos secretos a los medios.
[25] Snowden, Ted Rall. Ediciones Seven Stories Press. 2015. Para más información sobre este caricaturista ver: www.tedrall.com
[26] SIGINT https://www.nsa.gov/what-we-do/signals-intelligence/

divulgado información clasificada y por lo tanto traicionado a su país. Entre estos últimos se destacaban aquellos oficiales gubernamentales que ordenaron su captura.

Fue uno de los filtros más grandes y escandalosos de la historia. Algunos senadores norteamericanos se mostraron furiosos al descubrir que la NSA había mentido cuando había respondido negativamente en el Congreso a la pregunta si la NSA estaba espiando a la población en general. James Clapper, el entonces Director de Inteligencia Nacional había mentido en el Congreso bajo juramento en su testimonio del 12 de marzo del 2013, tres meses antes de que las noticias publicaran la explicación de los documentos entregados por Snowden. Clapper había negado que la NSA colectaba datos de millones de estadounidenses[27]. Líderes extranjeros también se mostraron ofuscados al descubrir que estaban siendo espiados. Luego de que Snowden entregara esta información a algunos periodistas selectos, lo cual generó que los programas de la NSA se hicieran públicos, hubo una polarización entre diferentes posiciones ya sea a favor o en contra de Snowden. La mayoría de las figuras políticas ya sea del Partido Demócrata o Partido Republicano, tomaron una posición negativa al opinar que Snowden y los periodistas que publicaron la información, fueron unos traidores al gobierno de los Estados Unidos al exponer al país a un alto riesgo frente a terroristas u otras potencias. Estas polémicas consideraban que Snowden debía ser encarcelado y procesado por haber realizado actividades criminales al divulgar información clasificada.

Un artículo periodístico publicado en el periódico *The Guardian* del primero de agosto del 2013, afirmó que los archivos presentados por Snowden demostraban que no solo Estados Unidos estaba involucrado en estos proyectos de vigilancia masiva sino también Inglaterra. La agencia paralela a la NSA del lado inglés, la CGHQ[28], habría mantenido relaciones con la NSA incluso *The Guardian* recibiendo fondos de ésta para construir la infraestructura necesaria para recolectar y decodificar información[29] del público en general.

[27] https://www.forbes.com/sites/andygreenberg/2013/06/06/watch-top-u-s-intelligence-officials-repeatedly-deny-nsa-spying-on-americans-over-the-last-year-videos/?sh=a770c3918d2f

[28] Government Communications Headquarters o GCHQ es una agencia de inteligencia y seguridad creada por el gobierno de Inglaterra para prevenir y eliminar actos terroristas, ataques cibernéticos, amenazas de estados hostiles, crimen organizado.

[29] https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden

Al momento de entregar los documentos donde se explicaban los pormenores de algunos programas que estaba desarrollando la NSA y la CGHQ llamados *Prism* y *Xcor* a los diarios *The Guardian* y *The Washington Post*, el puesto de Snowden dentro de la NSA era el de analista de infraestructura. Estos programas garantizaban acceso directo a los emails y chats en vivo dentro de *Google, Facebook, Microsoft* y *Apple*, entre otros gigantes de Internet[30]. Además, entregó información clasificada a explicando como la NSA recolectaba información de llamadas provenientes de clientes de *Verizon*, una de las compañías celulares más grandes de Estados Unidos. A su vez, Snowden demostró con la documentación presentada, que la CGHQ habría desarrollado un programa llamado *Tempora,* donde podría acceder a los cables de fibra óptica que permiten las llamadas telefónicas mundiales, así como el tráfico Web. Gracias al desarrollo de este programa, habrían encontrado una forma una forma ingeniosa de guardar esta información por al menos 30 días[31].

En una de las entrevistas realizadas por Glenn Greenwald, Snowden enfatizaba que la NSA tenía como objetivo recolectar las comunicaciones de todas las personas que viven en los Estados Unidos, como también en otros países. La Agencia de Seguridad recolectaba la información de manera automática, la filtraba, la analizaba, generaba mediciones y la almacenaba en el sistema por una determinada cantidad de tiempo. Gracias a la utilización de *software* de reconocimiento de voz, los analistas podían buscar determinadas palabras que se considerarían sospechosas tales como "bomba", "terrorismo", o "revolución", así como la locación de donde proviene la voz. Luego se examinaba la información para determinar si era una amenaza y si necesitaba mayor investigación o no. Además, recolectaban *metadatos* como horario y números de teléfono. Otros programas de la NSA llamados *"Blarney", "Fairview",* "*Oakstar*", entre otros, pueden interceptar y colectar el 75 % de todo el tráfico de internet en los Estados Unidos como *emails*, mensajes de textos, búsquedas en la Web, actividad con aplicaciones, llamadas realizadas por Internet, actividades bancarias en línea y videos (Rall, 2015). Cuando Greenwald le preguntó a Snowden por qué había quebrantado

[30] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[31] https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden

la Ley, Snowden contestó: *"El público necesita decidir si lo que implica estos programas está bien o mal"*.

Según Rall, estos programas marcaron la despedida del balance entre seguridad y privacidad. Antes de los episodios terroristas del 11 de septiembre de 2001, las Agencias de Inteligencia y los Departamentos de Policía que quisieran espiar a un ciudadano estadounidense debían convencer a un juez demostrando pruebas suficientes de actos ilegales para recibir esta autorización. Los documentos que tomó Snowden mostraban que la NSA interceptaba y guardaba el 99% de los *metadatos* de las llamadas telefónicas de los estadounidenses[32]. Un programa llamado *"Mystic"* graba el 100% del contenido de audio de las llamadas telefónicas en ciertos países y el 80% en Estados Unidos. Otros programas como *"Blarney"* interceptan y almacenan el 75% del tráfico de internet en Estados Unidos: emails, mensajes de texto, actividades en los buscadores.

[32] Rall describe algunos de los metadatos telefónicos: numero desde donde se llamó, numero al que se llamó, duración de la llamada, lugar físico donde se encuentra la persona que llamo y la persona que recibió la llamada.

Nota: "El denunciante. "No puedo permitir que el gobierno de Estados Unidos destruya la privacidad y las libertades básicas". Edward Snowden, de 29 años, resurge luego de refugiarse en Hong Kong. El contratista de tecnología afirma que sus inquietudes fueron ignoradas y que por ello tuvo que revelar los hechos al público. Diario *The Guardian*, 10 de Octubre del 2013 (*Aclaración: la traducción corresponde a la autora de la tesina)*.

Los medios de comunicación social y la opinión pública consideraron a Edward Snowden un *whistleblower* o denunciante, que alude a una persona que denuncia a una organización o figura pública sobre la presencia de actos ilícitos. Este término tiene una denotación "positiva" pues el denunciante estaría defendiendo el derecho de las personas como entidades públicas. En el caso de Snowden, no contaba con la protección de la figura de denunciante por las leyes de Estados Unidos al ser un contratista de la NSA y no un empleado.

También se consideró a Snowden un recurso de información, evitando connotaciones positivas o negativas sino neutrales.

En subsecuentes entrevistas y declaraciones escritas, Snowden ha dejado en claro que el objetivo principal de haber revelado esta información clasificada fue *provocar un debate público en los Estados Unidos y en otros países, acerca del poder que ejercen los gobiernos al llevar a cabo operaciones de vigilancia masiva sobre las comunicaciones telefónicas y digitales de las personas privadas sin consultar a estas sobre su consentimiento o denegación del uso de esta información por parte de las diferentes agencias de inteligencia en el mundo*. El caso Snowden también generó un quiebre en el liderazgo de los Estados Unidos en seguridad y tecnología cibernética.

Foto: Berlín, Alemania 14 de Diciembre del 2014. El ex ministro de interior alemán Gerhard Baum presentando mientras el ex contratista de la Agencia de Seguridad Nacional (NSA) y denunciante Edward Snowden es visto en una pantalla de videoconferencia durante la ceremonia de los Premios al periodismo Carl von Ossietzki el 14 de diciembre del 2014 en Berlín, Alemania. La cinematógrafa Laura Poitras y el periodista Glenn Greenwald (ambos ausentes) fueron premiados por la Liga Internacional de Derechos Humanos por haber puesto su propia libertad en riesgo al exponer abuso de poder por parte de Alemania y los Estados Unidos en sus revelaciones acerca del grado de vigilancia gubernamental en ciudadanos comunes en nombre de la "seguridad nacional" en el marco de los ataques terroristas. El nombre del premio fue generado en conmemoración al periodista y ganador del premio Nobel de la Paz Ossietzky, quien murió a causa de complicaciones por haber sido apresado como disidente en un campo de concentración Nazi. Sigue en pie una propuesta para permitir a Snowden, quien posee asilo temporal en Moscú, a testificar en Berlín frente a un parlamento de la NSA. Foto por Adam Berry/Getty Images.

Si hablamos de legalidad, el caso Snowden se encuentra bajo la Sección 215 de la Ley Federal USA Patriótica, que se formó con las siguientes siglas: "Ley para unir y fortalecer América, es decir los Estados Unidos, proveyendo las herramientas apropiadas para impedir y obstaculizar el terrorismo". Esta Ley fue aprobada en el 2001 bajo la presidencia de George Bush, con el objetivo

de “mejorar” las agencias de seguridad de los Estados Unidos, otorgándoles mayores poderes de vigilancia con el objetivo de controlar y eliminar delitos terroristas. Esta Ley fue criticada por varios organismos de derechos humanos por generar una reducción de las libertades y garantías constitucionales para ciudadanos de todo el mundo.

La Agencia Independiente de Supervisión de Privacidad y Libertades Civiles (PCLOB) establecida por el congreso estadounidense en el 2004 para aconsejar al presidente acerca de temas de privacidad, presentó su primer informe en el 2014, luego de analizar los programas de la NSA denunciados por Snowden. El informe determinó que los programas de vigilancia masiva de la NSA carecen de base legal viable. Además, sostuvo que existe escasa evidencia de que la colección masiva de registros telefónicos de la NSA haya arrojado resultados materiales contra el terrorismo. Además, sostuvo que solo el FBI tiene autorización para recopilar datos a granel para investigaciones y no la NSA. Finalmente, el informe sustentó que el proceso llevado a cabo por la NSA no sólo violaba la Ley de Privacidad de las Comunicaciones Electrónicas, sino que la complejidad tecnológica y el amplio alcance de los programas de vigilancia junto con el potencial de abuso de poder por parte del gobierno representaban un riesgo inherente para los estadounidenses.

La misma agencia finalmente recomendó un principio general para el futuro: “el gobierno no debería tener permitido colectar y guardar información bruta y privada a nivel masivo de personas dentro del territorio estadounidense con el propósito de habilitar posibles búsquedas o exploración de datos futuro” (*The Snowden Reader*, Ver Fuentes Consultadas).

Por otro lado, oficiales del gobierno se encontraron en situaciones comprometedoras luego de que la evidencia abismal entregada por Snowden fuera divulgada por los medios. Meses antes, James Clapper, director de inteligencia nacional, declaro ante el Congreso y bajo juramento que la NSA no colectaba información de personas dentro del territorio estadounidense, cuando la evidencia muestra la colección de billones de llamadas. Luego de la evidencia entregada por Snowden, Clapper tuvo un mal momento tratando de justificar sus falsos testimonios. Utilizaba juegos semánticos para justificar los actos expuestos de la NSA, como testificar bajo juramento frente al senado que guardar información privada de las personas no es lo mismo que “colectarla” hasta que alguien en la NSA la analizara. El general Keith Alexander, había testificado ante el

Congreso sobre un artículo publicado en la revista *Wired,* reclamando que la NSA estaba vigilando masivamente a los estadounidenses. Alexander también había negado cualquier tipo de recolección de datos por parte del gobierno.

En todas estas situaciones vemos un patrón de ocultamiento hacia el congreso estadounidense por parte de los oficiales del gobierno que lideran las agencias de inteligencia de las prácticas de recolección de datos masiva como las llamadas telefónicas.

La extensión de las prácticas para recolección de datos por parte de la NSA es difícil de explicar desde un punto de vista no técnico, pero dentro de la información divulgada por Snowden se encuentran pruebas de innumerables ataques cibernéticos a nivel masivo a computadoras privadas por parte de la agencia donde esta protege su identidad a través de sitios Web reales. Como si fuera una película de ciencia ficción, Snowden describe que hasta ciertas máquinas que no están conectadas a Internet pueden ser comprometidas gracias a la tecnología en miniatura que la agencia ha instalado en computadoras que transmitirían información a distancia a radios locales.

Los documentos de Snowden describen un gobierno que intercepta y guarda nuestras comunicaciones y "hackea" nuestras computadoras y nuestros archivos sin diferenciar entre ciudadanos y enemigos potenciales del Estado. A diferencia de sistemas totalitarios como en Cuba donde las llamadas se escuchaban en tiempo real, la forma de operar de la NSA es automática, producto del modelo de "big data" (grandes datos) del de compañías como *Facebook.* El objetivo de la NSA es recolectar todas comunicaciones, todos los hechos, de todas las personas en la tierra.

Aunque los Estados Unidos justifican que lo único que están investigando es por propósitos de inteligencia militar, los documentos revelados por Snowden muestran operaciones de los Estados Unidos en contra de la red de la compañía china *Huawei*, así como *Petrobras* en Brasil, prueba de que estas agencias de inteligencia no se limitan solo a estrategias militares sino también comerciales y políticas[33]. Estas revelaciones eliminan distinciones o delimitaciones entre espionaje militar y espionaje industrial.

[33] https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated

De acuerdo con la documentación presentada por Snowden, la NSA no se ha limitado a recolectar información nacional sino aquella proveniente de individuos utilizando redes de telefonía como la *Huawei* en China, accediendo de esta manera a información privada de individuos en este país y en otros países fuera de los Estados Unidos. Máquinas que no se encuentran conectadas con internet pueden también ser comprometidas a través de tecnología en miniatura que utilizan señales de radio-frecuencia conectadas con estaciones cercanas. No sólo computadoras son comprometidas sino también teléfonos móviles, y servidores de conectividad extensos.

La hipocresía del gobierno de los Estados Unidos en su constante crítica hacia el gobierno de China por su espionaje a compañías privadas con el objetivo de beneficios económicos, deja de tener fundamento con la documentación revelada por Snowden donde se demuestra que Estados Unidos se encuentra haciendo lo mismo.

5.2. El caso Christopher Wylie

"Facebook sabe más sobre ti que cualquier otra persona en tu vida, incluso sabe más que tu esposa".

Christopher Wylie

En junio de 2018 Christopher Wylie se presentó ante el Congreso de los Estados Unidos para testificar en el caso contra *Cambridge Analytica* (CA), una compañía contratista del ejército estadounidense para la cual trabajaba y a la que caracterizó por instrumentar una "guerra psicológica"[34] en la compleja red que involucró a *Facebook*, Rusia, *WikiLeaks*, la campaña de Donald Trump y el referéndum de *Brexit (Wylie, 2018).* En el documental "The Great Hack" se explica el concepto de "Operaciones Psicológicas" o PSYOP (*Psychological Operations*), un termino militar utilizado para describir acciones llevadas a cabo en un estado de guerra de manera no necesariamente combativa donde una cantidad selecta de información e indicadores son

[34] Guerra psicológica o Propaganda es con un concepto definido por varios autores como un conjunto de tácticas y métodos psicológicos generadas por un gobierno, organización, grupos e individuos con el objeto de influir una reacción, un sistema de creencias en un público en general o particular. Autores como Chekinov, S.C.; Bogdanov, S.A. consideran que el desarrollo tecnológico abismal de nuestros tiempos ha cambiado significativamente la naturaleza, métodos y técnicas utilizadas por el Estado, los gobiernos y las agencias políticas y económicas afectando las relaciones sociales y la naturaleza, los métodos y técnicas de las operaciones militares, creando nuevos los desafíos y las amenazas informaciones. https://web.archive.org/web/20150220060800/http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf

expuestos a ciertas audiencias con el objetivo de influenciar sus emociones, sus motivos, y su razonamiento objetivo (su mente en general)[35]. En el documental se define este concepto como "persuasión versus bombardeo" o "guerra comunicacional".

[35] https://www.merriam-webster.com/dictionary/psyops

Nota: Revelación: 50 millones perfiles de *Facebook* fueron utilizados por *Cambridge Analytica* en una gran filtración de datos. Denunciante describe cómo la firma conectada con el ex asesor de Trump, Steve Bannon, compiló datos de usuarios para apuntar a los votantes americanos. “He creado la herramienta para la guerra psicológica de Steve Bannon”.

Conoce al denunciante de la guerra de datos. Mark Zuckerberg rompe el silencio en relación con *Cambridge Analytica*. Diario *The Guardian*, 17 de Marzo del 2018 *(Aclaración: la traducción corresponde a la autora de la tesina)*.

En su libro *MindF*ck*, Wylie narra su experiencia como Director de Investigación en la compañía desde donde pudo acceder y recolectar evidencia de la utilización por parte de CA de ciertos datos obtenidos de *Facebook* como arma informacional con el objetivo de crear sistemas de propaganda que dejaron vulnerable a millones de ciudadanos estadounidenses.

Meses antes de su decisión de denunciar los hechos ocurridos, Wylie había visitado a un profesor de la Universidad de Cambridge, Alexandr Kogan, quien había desarrollado una aplicación llamada *"This is your digital life"* ("Esta es tu vida digital"). La aplicación presentaba una prueba de personalidad a los usuarios que la desearan bajar. CA habría abonado a ciertos usuarios para que respondieran estas preguntas. La aplicación también podía colectar información personal de las cuentas de *Facebook* no solo de estos usuarios, sino también de su red de amigos, sus actividades, sus "likes" ("Me gusta") y sus preferencias personales. A través de esta aplicación, Kogan accedió y colectó datos de perfiles de más de 87 millones de usuarios de *Facebook* y se los otorgaría a CA. Esta red adicional de amigos de aquellos usuarios no tenía ningún conocimiento de que sus datos estaban siendo utilizados o extraídos. Todos los "likes", los cambios en sus estados, y los mensajes privados fueron accedidos. Según lo que explica Wylie, la intención de CA era sistematizar la información de cada usuario basado en su actividad en *Facebook* no como un votante sino como un perfil de personalidad (*Targeting*[37]). Con esta metodología, solamente tendrían que acceder a unos 200 mil usuarios para crear un perfil psicológico de cada votante en los Estados Unidos para la campaña de Trump 2016. En su libro Wylie considera este experimento como completamente falto de ética.

[37] Targeting: En Marketing, Targeting se denomina a la estrategia que separa un Mercado grande en pequeños segmentos para concentrar un grupo de clientes específicos dentro de esta audiencia. Define a los posibles clientes de acuerdo a ciertas características y solo se enfoca en servir a ese pequeño universo.

Originalmente, la aplicación había sido creada por David Stillwell en el 2007 en el Centro de Psicométricas de la Universidad de Cambridge. Los creadores trabajaron hasta el 2012 para motivar a usuarios de *Facebook* a tomar diferentes pruebas de personalidad. Durante este tiempo, los datos de alrededor de 6 millones de voluntarios fueron recolectados y analizados por colaboradores resultando en 45 publicaciones académicas que serían revisadas por otros eruditos (Kanter & Kanter, 2018).

En el 2008 Michael Kosinski se incorporó a trabajar con Stillwell y decidieron recolectar la información de los voluntarios de Facebook a partir de 5 rasgos de personalidad:

1. Disposición: ¿Cuán abierto se encuentra a nuevas experiencias?

2. Minuciosidad: ¿Cuán perfeccionista es?

3. Extroversión ¿Cuán sociable es?

4. Amabilidad ¿Cuán considerado y cooperativo eres?

5. Neuroticismo ¿Cuán fácilmente te enojas?.

De acuerdo con estas cinco dimensiones, los analistas determinaban el tipo de personalidad de cada individuo. Luego de responder a las preguntas, los usuarios podían elegir compartir su perfil de *Facebook* con los investigadores (Rehman, 2019). Las respuestas del cuestionario se comparaban con la actividad de *Facebook* como los *"likes"* ("me gusta"), cualquier información de interés o que fuera compartida con otros, su edad, lugar de residencia, y sexo. Las correlaciones que fueron creadas a partir de estos diferentes puntos de datos y acciones en línea generaron deducciones sorprendentes. Cuando cientos y miles de puntos específicos de datos se combinaban, las predicciones que aparecían como resultado eran sorprendentemente acertadas.

En el 2012, Konsinksi y su equipo probaron que era posible predecir el color de piel de un individuo, su orientación sexual, y su asociación con el partido demócrata o republicano solamente

basado en el promedio de 68 *"likes"* por usuario. También podían determinar su coeficiente intelectual, si fumaban cigarrillos o usaban drogas o alcohol y hasta su afiliación religiosa[38].

Tres meses antes de presentarse a testificar frente al Congreso de Estados Unidos, el 18 de marzo del 2018, los diarios *The Guardian* y el *The New York Times*, así como el canal 4 de Inglaterra publicaron simultáneamente la investigación conjunta de más de un año estimulada por la decisión de Wylie de revelar los hechos que sucedieron dentro de *Cambridge Analytica* y *Facebook*[39]. La investigación fue complejizada por la existencia del Reporte de Mueller[40] unas semanas antes de lanzarse la historia, así como la posible conexión con el caso *Brexit*[41], inteligencia Rusa, y *hackers* internacionales.

[38] https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win
[39] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump
[40] https://www.bbc.com/mundo/noticias-internacional-47983354
[41] El 31 de enero del 2020 se produjo la salida de Inglaterra de la Unión Europea (UE), gracias a un referéndum en el que el Reino Unido voto a favor de abandonarla. https://www.bbc.com/mundo/noticias-internacional-46521624


The New York Times

How Trump Consultants Exploited the Facebook Data of Millions

Christopher Wylie, who helped found the data firm Cambridge Analytica and worked there until 2014, has described the company as an "arsenal of weapons" in a culture war. Andrew Testa for The New York Times

By Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr

March 17, 2018

2076

Nota: Cómo los consultores de Trump explotaron los datos de millones en Facebook. Christopher Wylie, quien ayudó a fundar la firma *Cambridge Analytica* y trabajo allí desde el 2014, ha descripto la empresa como un "arsenal de armas" en una guerra cultural. Andrew Testa para el Diario *The New York Times*, 17 de marzo del 2018 *(Aclaración: la traducción corresponde a la autora de la tesina)*

El 20 de marzo del 2018, el diario *The Guardian* publicó otro artículo donde explicaba que David Carroll, un Profesor de *Parsons School of Design* en New York, presentó un caso al Parlamento de Inglaterra para reclamar sus datos personales, los cuales habrían sido retenidos por *Cambridge Analytica* y *SCL*, la compañía que la abarcaba. A su vez, este acontecimiento generó que el Senador de Oregón (USA), Ron Wyden, enviara una carta a Mark Zuckerberg, el CEO de *Facebook* (FB), preguntándole la razón por la cual CA habría adquirido datos de más de 50 millones de personas y porqué FB no habría solicitado explicaciones a CA acerca del abuso de estos datos para manipular a millones de votantes americanos sin su consentimiento ni conocimiento[42].

Carroll demandó a la Corte Británica a que le informaran absolutamente todo sobre los posibles usos de sus datos, dónde y cómo los habían colectado, cómo lo procesaban, con quién lo habrían compartido, y si existía la posibilidad de *"opting-out"*.[43]

CA habría generado 5,000 puntos de datos para predecir la personalidad de cada adulto votante de los Estados Unidos. De acuerdo con estos datos, eligieron aleatoriamente una cantidad de usuarios que pertenecían a diferentes estados en Estados Unidos donde había empate entre los demócratas y los republicanos (tales como Michigan, Wisconsin, Pennsylvania y Florida). El grupo selecto se denominaría los "persuasibles" y serían bombardeados con contenido específico con el objetivo de generar apoyos por el partido republicano y eventualmente la votación por Donald Trump[44]. El contenido no era solamente enfocado en la publicidad sino también videos, *banners*, artículos *blog* y contenido similar que provendrían de recursos anónimos y sin marca.

En el documental The Great Hack[45], se presenta la investigación que realizó Carole Cadwalladr, una periodista que escribe para *The Guardian* y otros periódicos británicos. A través de una serie de entrevistas, Cadwalladr logro recopilar información del proceso llevado a cabo por

[42] https://www.theguardian.com/uk-news/2018/mar/20/david-carroll-cambridge-analytica-uk-courts-us-professor
[43] La ley de "Opt-Out" se refiere a una clausula contenida dentro de varios acuerdos arbitrarios donde se permite a los consumidores rechazar información, publicidad, llamados, emails, o comunicaciones de marketing, sobre productos que no han sido solicitados. https://definitions.uslegal.com/o/opt-out-clause/
[44] ''The Great Hack'' es un documental televisivo acerca del escándalo de datos *Facebook-Cambridge Analytica*. El documental se enfoca en el profesor Davir Carroll, la denunciante Brittany Kaiser (quien trabajaba con Christopher Wylie), y las investigaciones de la periodista Carole Cadwalladr en relación con la campaña *Brexit, Facebook, Cambridge Analytica* y la campaña de Donald Trump del 2016.
[45] https://www.wired.com/story/the-great-hack-documentary/

CA para la selección de datos y sus posteriores operaciones con el objetivo final de influir al electorado estadounidense a favor de Donald Trump en las elecciones del 2016, así como al electorado de Inglaterra con respecto a *Brexit*[46].

En el mismo documental, Brittany Kaiser, quien era Directora de Desarrollo de Negocios en CA explica como en los últimos años, los datos pasaron a ser el activo más valorado del mercado mundial, sobrepasando su valor al mercado petrolífero. Según Kaiser, esta es la razón, por la cual compañías como *Facebook, Google* y *Amazon* poseen un alto valor monetario, al poseer una extraordinaria cantidad de datos personales.

En el documental, Kaiser narra cómo CA generó una muestra de datos personales que la denominarían los "persuasibles" para referirse a aquellos votantes que serían fácilmente manipulados. Luego un equipo creativo se encargó de diseñar contenido personalizado con el objetivo de lograr un cambio de preferencia política en aquellos votantes. El contenido sería luego bombardeado hacia su perfil en todas las plataformas de las redes sociales posibles, en formatos como videos, *blogs,* páginas Web sin marca, artículos, publicidad. Kaiser menciona que el objetivo era "generar en el votante una visión del mundo que deseábamos que tuviera para que votaran por nuestro candidato. (…). El santo grial de la comunicación es cuando se comienza a cambiar el comportamiento de los usuarios. Tácticas de comunicación tan poderosas como armas de guerra fueron utilizados para la campaña *Uk Leave* y las elecciones de Trump"[47] .

Estos usuarios persuasibles se encontraban en Estados como Michigan, Wisconsin, Pennsylvania y Florida. Estos Estados son denominados los *"swing states"* ya que se encuentran en una situación de empate en cuanto a las preferencias "democráticas" o "republicanas". Por esta razón, estos Estados son importantes para enfocarse al objetivo de persuadir al electorado en las elecciones presidenciales.

[46] *Brexit* se denomina al movimiento que generó Inglaterra para separarse de la Unión Europea con el objetivo de lograr su autonomía en decisiones que antes eran tomadas por la región. El proceso finalizó el 31 de enero del 2020 y parte de su éxito fue gracias a la campaña *Vote Leave* (vote por irse de la Unión Europea) a la que Wylie denunció por haber utilizado practicas con falta de ética para influenciar a los votantes.
[47] ' *'The Great Hack''*, 2019 (Documental).

En un artículo periodístico de la revista *Wired* sobre las diferencias en estrategias comunicacionales utilizadas por Trump versus su oponente Clinton en el 2016, se explica cómo Clinton utilizó la mayor parte del dinero de la campaña política en publicidad en televisión, mientras que Trump utilizó solo la mitad de ese dinero en televisión y se focalizó más en las redes sociales. Estas redes permitían al usuario "interactuar" con el contenido, a través de comentarios, "me gusta".

Gary Coby, Director de Publicidad en el Comité Republicano Nacional, quien también trabajó en la campaña de Trump, dijo lo siguiente: "(*Facebook)* es una plataforma construida para informarte lo que a la gente le gusta o no le gusta". El equipo de Coby tomó ventaja de la plataforma generando diferentes pruebas para eliminar aquellos avisos que no eran exitosos y solamente publicitar aquellos que generaban resultados. La campaña publicaba entre 40 mil y 50 mil avisos diarios con todas las variaciones posibles: con o sin subtítulos, estática versus video, entre otras pequeñas diferencias. El día del tercer debate presidencial, 175 mil avisos fueron publicados. Las redes sociales fueron el foco principal donde Trump concentró su campaña electoral. No fue una plataforma para publicar avisos previamente generados, como son los avisos en TV, sino para interactuar y generar conversaciones con los usuarios[48].

[48] https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/

CAPÍTULO VI.

TENSIONES Y DESAFÍOS EN LA PROTECCIÓN DE DATOS PERSONALES Y EL DERECHO A LA PRIVACIDAD

"Estamos pagando para ser dominados".

Shoshana Zuboff [49]

[49] Profesora de la Universidad de Harvard y autora del libro "La era del capitalismo de vigilancia".

6.1. Tensiones y desafíos en el caso Edward Snowden

A continuación, desarrollaremos las tensiones y desafíos que presentó el caso Snowden:

Seguridad debilitada

Uno de los problemas con las vastas operaciones de ciber-espionaje de la NSA es que, a pesar de sus esfuerzos por mejorar la seguridad nacional, la Agencia está generando el efecto contrario y debilitándola. Según el periódico *The New York Times* y de acuerdo con los documentos revelados por Snowden, las operaciones de generación de vulnerabilidades dentro de sistemas comerciales llevadas a cabo por la NSA, ha contribuido a debilitar la seguridad y la privacidad de los individuos invirtiendo millones de dólares en operaciones que generan inseguridad a través de ingresos por las "puertas traseras" de diferentes productos en detrimento de las encripciones utilizadas por el público[50].

Sector privado

Antes de la explosión del caso Snowden, algunas provincias de Canadá y varios países de la Unión Europea (UE) generaron políticas para evitar la exportación de datos hacia los Estados Unidos luego de haber descubierto el amplio acceso del gobierno estadounidense a datos del sector privado.

Luego de las revelaciones de Snowden, varias compañías financieras, de telecomunicaciones, tecnología de la información reportaron la pérdida de clientes preocupados por los datos almacenados en "la nube" estadunidense.

[50] Documentos secretos revelan la campana de la NSA en contra la Encripcion. "Secrets documents reveal N.S.A. Campaign against Encryption"
https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

Perspectiva del gobierno

En el 2004 un comité asignado por el gobierno (*Technology and Privacy Advisory Committee)* reporto que las leyes que regulan la protección de la privacidad de las personas no son adecuadas con nuestros tiempos modernos y los vastos avances de la tecnología en cuanto a uso de tecnologías digitales como Internet[51].

A pesar de la desprotección de los usuarios, los intentos de generar nuevas leyes que protejan a los usuarios han organizado un escenario de disputas políticas sin resolución. Los oficiales del gobierno estadounidense usualmente responden a los reclamos sobre generar leyes que protejan la privacidad de los usuarios reclamando que cualquier límite aplicado a sus programas va a reducir la efectividad de la seguridad nacional e inteligencia extranjera.

En el caso de los ataques del 11 de septiembre de 2001 a las Torres Gemelas, las agencias de inteligencia no pudieron evitarlo aun habiendo tenido los datos disponibles. En otras palabras, la extrema cantidad de información recolectada no significa que sea la información necesaria para generar mayor seguridad nacional.

Por otro lado, aun siendo más difícil resguardar la seguridad nacional a través de la protección de los derechos de los usuarios, los derechos constitucionales son importantes y como tales tienen un costo.

Lee Hamilton (2015) sostiene que lo sorprendente de las revelaciones de Snowden es la falta de información por parte de los oficiales del gobierno acerca de los programas de la NSA, así como las continuas negaciones de la NSA (declaraciones en la Corte y bajo juramento) de la existencia de éstos. Edward Snowden permitió que esta realidad saliera a la luz, pues anteriormente todos estos programas se mantenían dentro del más absoluto secreto. Según Hamilton, la pasividad del Congreso muestra que sus miembros han sido y siguen siendo permanentemente seducidos por los representantes de la comunidad de inteligencia que se suponen que deberían estar supervisando.

[51] Comité de Consejo en Tecnología y Privacidad, Departamento de Defensa. “Protegiendo la privacidad en la lucha contra el terrorismo”. Marzo 2004, 5-6

La desprotección de los usuarios

El caso Snowden también ha puesto en perspectiva y análisis las leyes sobre privacidad que se encuentran vigentes en los Estados Unidos, habiendo sido estas descriptas como inadecuadas, fragmentadas y difíciles de implementar pues niega los derechos a la privacidad de ciudadanos extranjeros, el cual es inconsistente con la posición del gobierno con respecto a los derechos humanos en el ciberespacio.

El problema principal es que es difícil determinar la nacionalidad del sujeto que es centro de investigación, especialmente si esta información es generada en forma masiva. De hecho, con la ley vigente de los Estados Unidos, terroristas y aliados reciben el mismo nivel de protección de datos

El caso "*Smith vs. Maryland*" en 1979 generó una jurisprudencia importante dentro de la ley pues el juez consideró que los datos recibidos de una empresa de telecomunicaciones, que había entregado los datos de ciertas llamadas telefónicas de un individuo y que se usaron luego en su contra, no se encontraban bajo la protección de la Cuarta Enmienda de la Constitución de los Estados Unidos de América porque "los usuarios telefónicos típicamente tienen conocimiento de que la compañía telefónica debe guardar datos numéricos de las llamadas y que es legítimo que las compañías puedan guardar estos datos por razones de mejoras de la calidad y el negocio en general"[52].

Fred Cate considera que excluir este tipo de datos almacenados por terceros de la protección de la Cuarta Enmienda es un gran problema por el gran incremento en la cantidad de datos sensibles que son generados por usuarios y usualmente archivado por diferentes empresas como *Google, Google, Verizon* y muchas más. En el mundo tecnológico que vivimos, prácticamente toda la información que generamos es almacenada por terceros: *email*, redes sociales, palabras en buscadores, archivos, fotos, mensajes de voz, etc. En otras palabras, toda la información virtual es fácilmente accesible para inspeccionar por agencias de gobierno. La Suprema Corte de Justicia de

[52] Smith vs Maryland, 442 US 735, 743 (1979).

los Estados Unidos de América también ha considerado en varias ocasiones la falta de protección constitucional que poseen los individuos en cuanto al uso de esos datos por parte del gobierno, aun habiendo adquirido esa información en forma ilegal[53].

La Cuarta Enmienda establece el derecho de los ciudadanos a la libertad contra "búsquedas y expropiaciones irracionales". En este contexto es importante destacar que los programas de la NSA ignoran la Cuarta Enmienda constitucional.

Cate sugiere también que aun siendo más dificultoso resguardar la seguridad nacional a través de la protección de los derechos de los usuarios, los derechos constitucionales son importantes y como tales traen aparejado un costo que hay que tener en cuenta a la hora de desarrollar programas de seguridad. Las actividades de inteligencia no deberían estar por encima de la ley. Antes de Snowden, los oficiales del gobierno habían negado en varias oportunidades la colección ilegal de datos. Y las revelaciones de Snowden han puesto en descubierto que la NSA ha violado la ley.

Una encuesta de opinión sobre el caso Snowden

Algunas semanas después de que Edward Snowden y los diarios *The Guardian* y *The Washington Post*, denunciaran los programas de las agencias de inteligencia en Estados Unidos y en Inglaterra, la revista *Time* generó una encuesta a la opinión general para saber si la población estadounidense apoyaba las acciones de Snowden o las repudiaban. El 54% de los encuestados respondieron que Snowden hizo bien al denunciar estos programas de inteligencia donde se recolectaba los números de teléfono, *email* y las búsquedas realizadas en Internet en aras de prevenir ataques terroristas. Solamente el 30 por ciento estuvo en desacuerdo. Sin embargo, casi el mismo porcentaje que estuvo de acuerdo con la denuncia de Snowden, también afirmaban que debía enfrentar cargos legales y ser condenado, comparado con el 28% que sostuvo que era inocente.

[53] "United States vs Leon" 468 U.S.897 (1984); "United States vs Calandra" 414 U.S. 338, 354 (1974); "Walder vs United States", 347 U.S. 62 (1954).

En cuanto a las edades de los encuestados: los estadounidenses entre 18 y 34 años muestran más apoyo a las acciones de Snowden, lo que podría relacionarse con el grupo que más se encuentra utilizando tecnología de última generación en su vida cotidiana. Con respecto al uso de programas de vigilancia masiva por parte del gobierno, los estadounidenses se encuentran divididos bruscamente: mientras que el 48% aprueba los programas, el 44% los desaprueba, considerado estadísticamente empatados por ser solo un 4% de diferencia. El conocer de la existencia de estos programas provocó en su momento un alboroto masivo en Washington y entre los defensores de la privacidad y la tecnología digital. El presidente Barack Obama, quien se opuso a muchos de los mismos programas durante la administración Bush antes de extenderlos como presidente, dijo que estos programas son supervisados por las tres ramas del gobierno federal y afirmó: “Si la gente no confía en el Poder Ejecutivo, y tampoco en el Congreso o en los jueces federales para asegurarse de que estamos cumpliendo con la Constitución, el debido proceso y el estado de derecho, entonces, vamos a tener algunos problemas".

La mayoría de los encuestados dijeron que los programas de vigilancia masiva han ayudado a proteger la seguridad nacional, con el 63% afirmando que han tenido ya sea algún o un gran impacto en proteger al país. Sólo el 31% sostuvo que los programas no han hecho mucho o directamente nada. Entre el 43% y el 48 % sostuvo que el gobierno federal está logrando el equilibrio correcto entre proteger la privacidad de los estadounidenses y proteger su bienestar físico o que el gobierno debería hacer más para prevenir el terrorismo. El 60% sostuvo que las revelaciones no forzarán al gobierno a reducir estos programas de vigilancia, pero el 76% de los estadounidenses creen que pronto habría más revelaciones de que los programas espías son más extensos y grandes de lo que se conoce actualmente.[54].

[54] https://swampland.time.com/2013/06/13/new-time-poll-support-for-the-leaker-and-his-prosecution/

6.2. Tensiones y desafíos en el caso Christopher Wylie

A continuación, desarrollaremos las tensiones y desafíos que presentó el caso Wylie:

Las consecuencias

Días después de la primera publicación de la investigación desarrollada[55], el Parlamento de Inglaterra considero que *Facebook* había fallado en prevenir que su plataforma se convirtiera en una red de propaganda hostil dentro de las elecciones generando implicancias en diferentes democracias.

Una colección de documentos entregados por Wylie a la policía revelaron que *Vote Leave*, la campaña para la salida de Inglaterra de la Unión Europea o *Brexit*, habría utilizado subsidiarias secretas de *Cambridge Analytica* para gastar "dinero oscuro" (dinero donado con el objetivo de influenciar las elecciones por entidades sin fines de lucro que no tienen obligación de revelar su identidad) para propagar desinformación en las redes de publicidad de *Facebook* y *Google.* La comisión electoral de Gran Bretaña determinó que todo fue ilegal. Una semana después, las acciones de *Facebook* bajaron un 18% lo cual significaron pérdidas de 80 billones de dólares en valuación. En su libro *MindF*ck*, Wylie enfatiza: *"La historia de Cambridge Analytica muestra cómo nuestras identidades y comportamiento se han convertido en productos básicos en el comercio de datos de alto riesgo".*

El cierre de Cambridge Analytica y la responsabilidad de Facebook

Luego de las revelaciones de Christopher Wylie, en mayo del 2018, *Cambridge Analytica* cerró sus operaciones y archivó oficialmente su cierre por falta de solvencia económica. La firma

[55] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

había sido denunciada por generar información de votantes a partir de 87 millones de perfiles de *Facebook* que habrían sido utilizados con el objetivo de influenciar a esos usuarios a favor del candidato Donald Trump. En abril de este año, Mark Zuckerberg, el fundador de *Facebook,* testificó frente al Congreso de Estados Unidos para explicar el escándalo denominado por los medios como "El Escándalo de Filtración de Datos de *Facebook-Cambridge Analytica*". La mayoría de su testimonio frente al Congreso repitió lo que ya había publicado en su plataforma unos días antes: el 21 de marzo del 2018, Mark Zuckerberg generó un post en *Facebook* explicando la situación con *Cambridge Analytica*. A continuación, hemos traducido sus palabras:

> *"Mark Zuckerberg*
> *21 de marzo de 2018 · Menlo Park, CA ·*
>
> *Quiero compartir una actualización sobre la situación de Cambridge Analytica, incluidos los pasos que ya hemos tomado y nuestros próximos pasos para abordar este importante problema.*
>
> *Tenemos la responsabilidad de proteger los datos de nuestros usuarios, y si no podemos, no merecemos servirlos. He estado trabajando para entender exactamente qué sucedió y cómo asegurarme de que esto no vuelva a suceder. La buena noticia es que las acciones más importantes para evitar que esto vuelva a ocurrir hoy ya las habíamos tomado hace algunos años. Pero también cometimos errores, pues queda mucho más por hacer y tenemos que dar un paso adelante para poder hacerlo.*
>
> *La siguiente es una cronología de los eventos:*
>
> *En el 2007, lanzamos la plataforma de Facebook con la visión de lograr que más aplicaciones tuvieran un perfil social. Los calendarios deberían mostrar los cumpleaños de sus amigos, los mapas deberían mostrar dónde viven sus amigos y las libretas de direcciones deberían mostrar sus fotos. Para hacer esto, permitimos que las personas*

inicien sesión en las aplicaciones y compartieran quiénes eran sus amigos y alguna información sobre ellos.

En el 2013, un investigador de la Universidad de Cambridge llamado Aleksandr Kogan creó una aplicación de prueba de personalidad. Fue instalada por alrededor de 300,000 personas que compartieron sus datos, así como algunos de los datos de sus amigos. Dada la forma en que nuestra plataforma funcionaba en ese momento, esto significaba que Kogan podía acceder a decenas de millones de datos de sus amigos.

En el 2014, para evitar aplicaciones abusivas, anunciamos que estábamos cambiando toda la plataforma para limitar drásticamente el acceso de las aplicaciones de datos. Lo que es más importante, las aplicaciones como la de Kogan ya no pueden solicitar datos sobre los amigos de una persona a menos que sus amigos también hayan autorizado la aplicación. También exigimos a los desarrolladores que obtuvieran nuestra aprobación antes de que pudieran solicitar datos confidenciales a las personas. Estas acciones evitarían que cualquier aplicación como la de Kogan pueda hoy acceder a tantos datos.

En el 2015, gracias a los periodistas de (el periódico) The Guardian supimos que Kogan había compartido datos de su aplicación con Cambridge Analytica. Es contrario a nuestras políticas que los desarrolladores compartan datos sin el consentimiento de las personas, por lo que inmediatamente prohibimos la aplicación de Kogan en nuestra plataforma y exigimos que Kogan y Cambridge Analytica certificaran formalmente que habían eliminado todos los datos adquiridos de forma incorrecta. Ellos nos proporcionaron estas certificaciones.

La semana pasada (alrededor del 18 de marzo del 2018), supimos por los medios The Guardian, The New York Times y Channel 4 que Cambridge Analytica no habría eliminado los datos como lo habían certificado. Inmediatamente les prohibimos usar cualquiera de nuestros servicios. Cambridge Analytica afirmó que ya habían eliminado los datos y

aceptaron una auditoría forense por parte de una empresa que contratamos para confirmar esto. También estamos trabajando con los reguladores mientras investigan lo que sucedió.

Esta fue una transgresión de la confianza entre Kogan, Cambridge Analytica y Facebook. Pero también fue una transgresión de la confianza entre Facebook y las personas que comparten sus datos con nosotros y esperan que los protejamos. Necesitamos arreglar esto.

En este caso, ya tomamos los pasos más importantes en el 2014 para evitar que los malos actores accedan a la información de las personas de esta manera. Pero hay más que debemos hacer y resumiré esos pasos aquí:

Primero, investigaremos todas las aplicaciones que tenían acceso a grandes cantidades de información antes del 2014, cuando habíamos cambiado nuestra plataforma para reducir drásticamente el acceso a datos, y realizaremos una auditoría completa de cualquier aplicación con actividad sospechosa. Prohibiremos a cualquier desarrollador al acceso y uso de nuestra plataforma si no acepta una auditoría exhaustiva. Y si encontramos desarrolladores que hicieron un mal uso de la información personal, les prohibiremos el acceso a Facebook y les informaremos de los hechos a todos los usuarios afectados por esas aplicaciones. Eso incluye a las personas cuyos datos Kogan también usó de mala manera.

En segundo lugar, restringiremos aún más el acceso a la cantidad de datos que los desarrolladores tengan acceso para evitar otros tipos de abuso. Por ejemplo, eliminaremos el acceso de los desarrolladores a los datos de aquellas personas que no hayan utilizado la aplicación en 3 meses. Reduciremos los datos que se proporcionen a una aplicación cuando inicie sesión, a solamente su nombre, foto de perfil y dirección de correo electrónico. Exigiremos a los desarrolladores que no solo obtengan aprobación, sino que también firmen un contrato para solicitar a cualquier persona el acceso a sus publicaciones u otros datos privados. Y tendremos más cambios para compartir en los próximos días.

En tercer lugar, queremos asegurarnos de que comprendan qué aplicaciones han permitido acceder a sus datos. En el próximo mes, mostraremos una herramienta en la parte superior de tu "Home" con las aplicaciones que han utilizado y la manera más fácil de revocar los permisos de esas aplicaciones a sus datos. Ya tenemos una herramienta para hacer esto en su configuración de privacidad, y ahora colocaremos esta herramienta en la parte superior de su "Home" para asegurarnos de que todos la vean.

Más allá de los pasos que ya habíamos tomado en 2014, creo que estos son los próximos pasos que debemos seguir para continuar creando seguridad dentro de nuestra plataforma.

Fundé Facebook, y al final del día soy responsable de lo que sucede en nuestra plataforma.

Me tomo en serio la tarea de hacer lo que se necesite para proteger a nuestra comunidad. Si bien este problema específico relacionado con Cambridge Analytica ya no debería ocurrir con las nuevas aplicaciones, eso no cambia lo que sucedió en el pasado. Aprenderemos de esta experiencia para generar mayor seguridad dentro de nuestra plataforma y hacer que nuestra comunidad se encuentre a salvo y para todos de ahora en delante.

Quiero agradecerles a todos ustedes que continúan creyendo en nuestra misión y trabajan para construir esta comunidad juntos. Sé que lleva más tiempo solucionar todos estos problemas de lo que quisiéramos, pero les prometo que trabajaremos en esto y crearemos un mejor servicio a largo plazo".

Donald Trump ganó la presidencia en los Estados Unidos

Basado en los testimonios de Brad Parscale, *Facebook* fue un gran influyente en los resultados de las elecciones del 2016, generando una victoria para el actual Presidente Donald

Trump. *Facebook* también ayudó a recaudar más de 250 millones de dólares en fondos que ayudarían a la campaña. Solamente en publicidad en línea Trump gastó 90 millones de dólares, la mayoría alocada a *Facebook.* De esta manera el equipo de Trump fue capaz de romper con los modelos de campañas políticas tradicionalmente utilizados.[56]

Sumado a la publicidad con la marca de Trump, el contenido sin marca creado para generar cambios en la mentalidad y comportamiento de los votantes, asistido por el trabajo de *Cambridge Analytica*, fue también de gran ayuda para el triunfo de Trump. CA también genero una reputación de "exagerar" su rol dentro de la victoria de Trump o de *Brexit,* tomando como propio crédito, el apoyo y las estrategias utilizadas por el partido republicano o por Brad Parscale. Sin embargo, Trump negó haber utilizado la información filtrada de FB por CA, sosteniendo que él no había tenido acceso a ella cuando CA se sumó a la campaña en el 2016.

Algunas fuentes mencionan que el *Proyecto Alamo* no habría utilizado datos que hubiera proporcionado *Cambridge Analytica*, lo cual dejaría a Trump en una posición libre de culpabilidad de ninguna acción legal. Algunas de las fuentes mencionadas lo conectan con Cambridge Analytica y la información que habría sido filtrada ilegalmente de *Facebook*. Un artículo de la cadena de noticias CNBC sostiene que Wylie afirmó que los datos filtrados de *Facebook* fueron vendidos a *Cambridge Analytica* para luego ser utilizados por esta para generar perfiles psicográficos de los usuarios y enviar información a favor de Donald Trump a los mismos[57]. La psicografía[58] es una práctica en marketing comúnmente utilizada, donde se divide a un mercado determinado en diferentes grupos de acuerdo con ciertas características de personalidad que diferencian los consumidores. El problema es que estos datos habrían sido ilegalmente adquiridos, sin el consentimiento de los usuarios. A su vez, las redes sociales generan un sentimiento de "comodidad" gracias a la conexión con amigos, por lo cual hay una disposición natural a compartir información intima como experiencias, gustos y rasgos personales que no lo comunicarían fácilmente en otro contexto.

[56] https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/

[57] https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html
[58] https://www.merca20.com/como-funciona-la-segmentacion-psicografica/

Políticas de protección de datos personales

El escándalo generado por el caso *Facebook-Cambridge Analytica* ha introducido una revuelta general sobre la protección de los datos personales con el advenimiento, el 25 de mayo del 2018, del Reglamento General de la Protección de Datos o GDPR (General Data Protection Regulation). Basado en la Unión Europea y en el Área Económica Europea, el reglamento puede infringir multas de hasta 20 millones de euros. El principal objetivo es el de proporcionar a los ciudadanos europeos una mayor protección y control de sus datos personales, así como simplificar y unificar el escenario de normas internacionales, con un reglamento vigente dentro de toda la Unión Europea[59]. Los requerimientos principales en cuanto a privacidad y protección de datos incluyen:

- Requerir el consentimiento de los usuarios para procesar sus datos.
- Generar anonimato de los datos colectados para proteger la privacidad.
- Proveer información sobre acceso ilegal o ilegitimo de sus datos (*Data Breach*).
- Transferir datos en forma segura a través de diferentes países y fronteras.
- Requerir a ciertas empresas contratar a un representante para que se encargue de que las reglas dentro de GDPR sean respetadas[60] .

[59] Fire and fury for Facebook. International Financial Law Review; London (Apr 27, 2018).
[60] https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

No obstante, esta ley no aplica en los Estados Unidos. Por el momento no existe ninguna ley federal en el país que rija en todo el territorio. Algunos estados han comenzado a establecer algunas regulaciones y leyes. Este es el caso de California, con la Ley de Privacidad del Consumidor de California que fue aprobada el 28 de Junio del 2018 y empezó a regir en junio de 2020. Hasta el momento, esta ley es la más contundente en Estados Unidos en cuanto a protección de derechos personales y por otorgar mayor poder al consumidor en cuanto a sus datos. Algunas empresas a las que aplica la ley por encontrarse en territorio californiano son *Facebook* y *Google*, ambas habiendo sufrido filtraciones de datos (*Data Breach*).

Los principales términos definidos por la ley se refieren principalmente a dos grupos: todos los residentes de California por un lado, y ciertas empresas por el otro. Estas últimas se definen como:

- Entidades con fines de lucro que realizan negocios en California y colectan información de los consumidores.

- Deben generar ganancias anuales de más de 25 millones de dólares.

- Más del 50% de sus ganancias anuales deben provenir de comercializar información personal del consumidor.

Otro termino importante definido en la ley es el de información personal con referencia a una lista amplia de características y comportamientos, personales y comerciales, así como ciertas deducciones derivadas de esta información. Docenas de datos específicos son mencionados en la ley como datos biométricos, compras dentro de los hogares, geo locación, información financiera y hábitos del sueño, entre otros.

La ley provee la siguiente protección para los consumidores:

- *Transparencia:* si una empresa colecta cualquier tipo de información personal, esto tiene que ser informado con sus términos legales en su página Web. Vale aclarar que los consumidores muy pocas veces se toman el tiempo de leer tres páginas de términos legales que por lo general requiere un "click" para aceptar y seguir adelante con las actividades que se encontraba realizando.

- *Peticiones específicas:* Si un consumidor desea saber cuál información está siendo colectada, la compañía debe responder, específicamente acerca del individuo. Algunas de las indagaciones que un consumidor podría solicitar incluye:

  - Categorías de información colectadas.
  - Métodos utilizados para colectar los datos.
  - El propósito de la compañía para colectar esa información.
  - La información de las compañías tercerizadas a las cuales esa información puede ser transferida.
  - Eliminación de datos: si el consumidor así lo requiere, estos datos deben ser descartados por la compañía.

  Por otra parte, las compañías deben ofrecer:

- *Colección de datos organizada:* la ley permite a los consumidores solicitar la información específica colectada acerca de ellos. La compañía debe generar las condiciones necesarias para poder buscar rápidamente, compilar y enviar estos reportes al consumidor sin costo alguno.

- *Políticas claras y transparentes:* los consumidores pueden pedir un reporte de los tipos de datos colectados, las fuentes de donde se colectaron esos datos, los métodos utilizados para colectar esta información y los usos de estos datos[61].

El Proyecto Alamo

Brad Parscale es el dueño de una compañía de especializada en marketing y publicidad en Internet y páginas Web. En el 2004, uno de sus clientes conoció en un avión a un miembro de la Organización Trump (OT) y le preguntó si estaría interesado en presentar una oferta para armar una página Web para la campaña de Trump. Parscale ofreció realizar la página por U$10,000 (dólares diez mil) la cual seria 100% reembolsable si la organización no estaba satisfecha. En los años siguientes la OT dedico cientos de miles de dólares a la compañía Parscale en trabajos relacionados con su página Web. Pronto Parscale se convertiría en el dueño de una de las agencias más remuneradas de Texas y la mano derecha de Trump en cuanto a sus campañas políticas.

En febrero del 2015, Trump solicitó a Parscale que diseñara una página web para un comité de exploración presidencial. En junio del mismo año, Trump abono U$10,000 a Parscale para que diseñara la página Web de su campana, la cual sería lanzada días después. Cinco meses más tarde, Parscale recibió una llamada del cuñado de Trump, Jared Kushner, consultando a Parscale su perspectiva en cuanto a estrategia digital. Parcale recomendó utilizar *Facebook* pues esta plataforma había dejado de tener actividad por parte de la población joven de ciudad, para pasar a ser mayormente utilizada por la población rural de edad más avanzada, exactamente la población que Trump quería influir. Eventualmente, el trabajo de Parscale en cuanto a generación de contenido y publicidad fue creciendo hasta llegar ser una operación de 100 personas llamada "*Project Alamo*".[62]

[61] https://digitalguardian.com/blog/what-california-data-privacy-protection-act

[62] https://www.washingtonpost.com/politics/how-brad-parscale-once-a-nobody-in-san-antonio-shaped-trumps-combative-politics-and-rose-to-his-inner-circle/2018/11/09/b4257d58-dbb7-11e8-b3f0-62607289efee_story.html

El Proyecto Alamo es la conexión entre el escándalo de *Cambridge Analytica* y la campaña de Donald Trump del 2016. *Cambridge Analytica* relocalizo a tres empleados a Texas, de los cuales dos eran científicos de datos, con el objetivo de generar información de votantes y una base de datos para la recaudación de fondos. Los datos se generaron en conjunto entre el Comité Nacional Republicano, la campaña de Trump, la firma de Parscale y *Cambridge Analytica*. Esta base sería utilizada por Parscale para desplegar información, ya sea a través de publicidad en línea o de contenido o videos sin marca con el objetivo de generar un cambio en la mentalidad y comportamiento en esta audiencia[63].

En octubre del 2016, Parscale se había mudado a la oficina de Trump en Nueva York y manejaba un presupuesto de U$200.000.000 (doscientos millones de dólares) en publicidad. La mitad de ese presupuesto sería utilizado en publicidad en televisión. La otra mitad en plataformas digitales, especialmente *Facebook.*

[63] https://slate.com/news-and-politics/2018/03/what-were-the-trump-campaigns-ties-to-cambridge-analytica.html

CONCLUSIONES

Hemos utilizado una estructura de tesina para poder describir, analizar y dar cuenta de los actores y de las temáticas involucradas en nuestro objeto de estudio. Al respecto, establecimos una hipótesis, un objetivo general y un conjunto de objetivos específicos.

La información recolectada por esta investigación, en relación con el marco metodológico fueron fuentes primarias destacando informes, publicaciones, libros, tratados, normas jurídicas, que nos permitieron reconocer en profundidad a los actores, a las temáticas y a los intereses en cuestión. Al encontrarnos viviendo en los Estados Unidos, hemos podido acceder a libros digitales o físicos a través de *Amazon* o a investigaciones académicas provenientes de sitios como *ProQuest* a través de la Biblioteca Municipal de la Ciudad de Seattle[64]. La Biblioteca también ha sido de gran ayuda en la búsqueda de libros digitales y físicos, aunque durante los primeros 6 meses de pandemia no hemos podido retirar los libros de papel por las posibilidades de contagio del COVID-19.

Por otro lado, el marco teórico, fue constituido a partir de las siguientes palabras claves/conceptos: Estado, derecho a la comunicación, derecho a la privacidad, derecho a la protección de datos personales y datos sensibles, de los cuales dimos cuenta de las definiciones alcances, responsabilidades, límites y tensiones entre el Estado, las empresas y los ciudadanos.

En el capítulo vinculado al marco histórico desarrollamos una descripción de la realidad donde a partir de una revolución tecnológica vivimos un nuevo modelo de sociedad y de vinculaciones y relaciones económicas, educativas, políticas e institucionales. **El siglo XXI nos presenta tres dimensiones de esta revolución tecnológica: la inteligencia artificial, el Internet de las cosas y el capitalismo de vigilancia.**

Recordemos que la hipótesis presentada fue la siguiente: *"La ausencia del Estado y la carencia de un marco jurídico real y simple para proteger los datos personales y el derecho a la*

[64] La autora de esta tesina se encuentra residiendo hace 15 años en los Estados Unidos, actualmente en la ciudad de Seattle, Washington y anteriormente en la ciudad de Nueva York.

intimidad en la revolución tecnológica fortalecería a las empresas de Internet y debilitaría el ejercicio del derecho de los ciudadanos".

En relación a la ausencia del Estado en el caso Snowden, basado en la teoría de Guillermo O'Donnell (1984), la relación de dominación entre el Estado y el ciudadano es desigual y el dominado la asume como justa. Es justamente lo que encontramos en la encuesta presentada al final de nuestra descripción del caso Snowden donde los ciudadanos consideran que lo que hizo Snowden "estuvo bien", al denunciar a las agencias, pero al mismo tiempo aceptan las acciones del Estado en cuanto a la invasión de la privacidad en aras de defender al país de posibles ataques terroristas. En este sentido, el Estado no protege a los ciudadanos en pos de su privacidad, pero sí los protege en pos de defenderlos contra actos terroristas. La pregunta sería si esta "defensa" por parte del Estado es realmente ubicándose en el lugar de los ciudadanos y defendiéndolos o, por el contrario, manteniendo su lugar de dominancia, a nivel local e internacional, a través de políticas secretas en aras de proteger esta supremacía. Consideramos que la segunda opción es la más acertada.

Por otro lado, y siguiendo la teoría de O'Donnell, el lugar de las agencias de inteligencia es el de institución estatal, el cual genera una idea de "agente externo" al gobierno, pero en realidad esto no es más que otra forma más de encubrir su dominación. Explicamos el ciclo de disposición por parte de las empresas privadas, cuando ciertos casos generan escándalo público y como las empresas manejan las crisis o en otras palabras "apagan el fuego". No tenemos duda alguna que mientras Estados Unidos protegía su integridad defendiendo sus acciones de invasión de la privacidad, en aras de la defensa del terrorismo y a espaldas de sus ciudadanos, al mismo tiempo continuaba recolectando información privada, ya sea a través de los programas denunciados o a través de nuevos desarrollos tecnológicos.

Siguiendo a O'Donnell, el Estado se encuentra ausente en su obligación de defender los derechos civiles del conjunto de la población y se establecen redes de responsabilidad en donde los agentes públicos estén sujetos a controles apropiados y legalmente establecidos sobre la legalidad de sus actos. Estados Unidos hace "oídos sordos" a esta responsabilidad y obligación, dejando a los ciudadanos una vez más desprotegidos de sus derechos básicos y como si estuvieran viviendo el sueño aterrador de encontrarse caminando desnudos en público. A su vez, los mismos ciudadanos que se encuentran "desnudos en público" pero esta vez no en sueños sino en la realidad, aceptan el

hecho de que el Estado "le sacó sus ropas" y justifican sus acciones por que los están defendiendo de posibles atacantes externos. Es una paradoja difícil de escapar, reconocida como "contradicciones de la sociedad civil" (Oszlak, 1980).

Por otra parte, en relación a la ausencia del Estado en el caso Christopher Wylie se demuestra principalmente por estar casi siempre algunos o varios pasos "atrás" en cuanto a desarrollo tecnológico con las gigantes como *Facebook* y *Google*. Esto no significa que el Estado no posee capital humano de alto conocimiento, como es el caso de Snowden, sino que la naturaleza de las gigantes inventa nueva tecnología en un proceso permanente de intercambio con los usuarios, al cual el Estado no posee acceso. En primer lugar, un ciudadano no va a tener disposición para compartir su información privada con plataformas del Estado, por lo cual las gigantes se encuentran "jugando en el bosque mientras el lobo no está", o como afirma Zuboff "estamos pagando para ser dominados". En segundo lugar, al encontrarse de alguna manera "atrasado" con respecto a los avances tecnológicos generados por los capitalistas de vigilancia, en este caso por *Cambridge Analytica* y *Facebook*, el Estado falla al no poder generar legislación adecuada para "agiornarse" con esta tecnología de avanzada. En tercer lugar, el capital informacional pasó a ser el activo más valorado mundialmente, superando al petróleo, lo cual ofrece a las empresas como *Google* y *Facebook*, una ventaja económica y por lo tanto de poder que resulta mayor que el Estado, aun el de los Estados Unidos, considerado uno de los países más poderosos del mundo.

En todo caso, el escándalo de *Cambridge Analytica* tendría que haber "descalificado" a Donald Trump por haber utilizado técnicas sin ética, con el objetivo de influenciar a los votantes. Lo mismo sucedió con el caso de Gran Bretaña, donde la campaña *Vote Leave* utilizó prácticas similares para influenciar a los votantes.

Mark Zuckerber tuvo que dar cuenta de los hechos al congreso estadounidense pero la pregunta es si hubo consecuencias o represalias reales e importantes por parte del Estado. La respuesta es más que evidente: no. Las gigantes (empresas trasnacionales) continúan desarrollando este tipo de prácticas "alrededor de la ley". En el caso de Trump, a pesar de haber utilizado estas prácticas sin ética, pudieron encubrir sus acciones explicando que la agencia de publicidad y de creación de contenido "no habría utilizado la información que había sido generada por *Cambridge*

Analytica, dejando a Trump libre de cualquier consecuencia legal y situando en evidencia una vez más al rol ausente que posee el Estado al no proteger a sus ciudadanos y a sus datos personales.

En relación a la protección de datos personales en el caso Snowden como lo explicamos oportunamente en el capítulo específico que trata el caso en cuestión, la legislación en Estados Unidos han sido descriptas como inadecuadas, fragmentadas (por la existencia de diferentes leyes por cada estado) y que presenta problemas a la hora de implementarla pues no respeta el derecho de ciudadanos extranjeros al no poder determinar si los sujetos investigados son extranjeros o estadounidenses y como se resolverían los servicios de espionaje en este sentido. Esto simplemente tomando presente la encuesta desarrollada en el caso Snowden, donde la mayoría de los ciudadanos consideran aceptables los esfuerzos del Estado en aras de proteger la seguridad de los ciudadanos y en detrimento de sus dados privados.

Es importante recordar el significado de la Cuarta Enmienda de la Constitución de los Estados Unidos de América porque ésta protege a los individuos contra "búsquedas no razonables" por parte del gobierno. Entonces, desde este documento legal, el mismo Estado, a través de las agencias de seguridad, se encuentran ignorando la Cuarta Enmienda Constitucional, al generar búsquedas no razonables de los ciudadanos y sin su consentimiento. En el caso de Snowden, tal vez diferente del caso de Wylie, los datos no fueron recolectados con aceptación por parte de los ciudadanos, aunque son relativamente fáciles de acceder por los *softwares* desarrollados por las agencias de inteligencia; siendo datos obtenidos ilegalmente. Claramente hay una falta de protección institucional de los datos de los ciudadanos por parte del gobierno. Las agencias de inteligencia no pueden estar por encima de la ley y la denuncia de Snowden ha puesto en descubierto el terreno ilegal en donde generan sus prácticas.

Por otra parte, en relación con la protección de datos personales en el caso Wylie podemos destacar que el escándalo de *Cambridge Analytica* provocó la llegada del GDPR en Europa (ver Políticas de protección de datos personales en el caso Wylie) con multas de hasta 20 millones de euros. No obstante, existen tres problemas nodales con esta legislación.

El primer problema se refiere a que de la misma manera que Safe Harbor fue reemplazado por Privacy Shield y luego por el GDPR, vendrán otros escándalos y adelantos tecnológicos para los que la ley quedara obsoleta nuevamente. Como hemos descripto a lo largo de esta investigación,

el Estado y las legislaciones se encuentran usualmente "reaccionando" a los avances de las gigantes, pues se encuentran usualmente caminando atrás de ellas, "quemando fuegos, y en varias ocasiones dando algunos tirones de orejas". Estas medidas paliativas, usualmente no son suficientes para proteger a los ciudadanos de la invasión masiva de su privacidad. Los ciudadanos aceptan y se exponen o lo que se hace con sus datos sensibles y privados sin tener idea de lo que realmente sucede a sus espaldas y con un entendimiento mucho más ingenuo que el Estado, y continuamente ofreciendo su información privada en "bandeja de plata".

El segundo problema está vinculado con el GDPR porque no afecta a los Estados Unidos, donde casualmente se encuentran *Facebook* y *Google*. Hay una ausencia de leyes federales que protejan al territorio estadounidense en cuanto a la protección de datos personales. La única ley fuerte del país solo afecta a los residentes del Estado de California, donde se encuentran las casas centrales de *Google* y *Facebook*, entre otras, pero es el único Estado con la ley más "fuerte" en cuanto a la protección de datos. Resulta paradójico que el país donde se encuentran las gigantes no posea legislación fuerte para proteger a los ciudadanos del uso indebido de sus datos. Claramente Estados Unidos carece de una legislación que sea apropiada para la protección de los datos privados que están siendo explotados por compañías privadas en asociación con las gigantes tecnológicas.

Y el tercer problema se relaciona con la paradoja legal que, siguiendo a Banisar, los datos deben ser adquiridos de manera legal y bajo el consentimiento de los sujetos propietarios de los datos. Los datos "donados" de manera voluntaria por parte de los usuarios a las redes sociales como *Facebook* o *Instagram*, o de manera más solapada aquellas búsquedas que los usuarios generan en *Google*, fueron aceptados por ellos mismos mediante el uso de estas redes sociales, aunque obviamente no para los objetivos que están siendo utilizados. Banisar agrega que los datos personales no deben ser entregados por motivos ajenos a los especificados en el objeto de la recolección a menos que el titular de los datos otorgue consentimiento o mediante la autorización expresa de unos funcionarios, lo cual claramente está siendo violado en el caso relacionado con *Cambridge Analytica.*

En relación con el derecho a la intimidad en el caso Snowden, retomando a Nino, el derecho a la intimidad es una esfera que está exenta del conocimiento generalizado por parte de los demás. Y "los demás" incluyen a las agencias de gobierno que Snowden denunció, los cuales

incluyen grabaciones, rasgos del cuerpo, hechos de la vida familiar, entre otros. Claramente encontramos una violación a esta intimidad por parte de las agencias de seguridad. En la película de Snowden, la escena donde él se encuentra susurrando con su novia luego de tapar la cámara de su computadora muestra claramente que él conoce como son los procedimientos de la NSA y que fácilmente podrían "entrar a su casa". Mientras nos encontrábamos realizando esta investigación, recibíamos por momentos la visita de "paranoia", pues las palabras claves buscadas para la realización de este trabajo, podrían fácilmente activar una búsqueda exhaustiva por parte de la NSA en nuestra computadora. Se podría considerar paranoia al sentimiento que experimentaba Snowden o se podría entender como una clara violación de los derechos de intimidad y privacidad, lo cual genera un cambio en su actitud y en la manera de hacer sus cosas en su esfera privada. Aun permaneciendo sentado en su casa y con las persianas cerradas, Snowden sabía que podían acceder a sus actividades diarias.

Por otra parte, en relación con el derecho a la intimidad en el caso Wylie, podríamos introducir en el caso de Wylie el concepto de *Habeas Data*, donde es una especie de derecho a la intimidad, pero relacionado con lo informático. Este derecho permite a los usuarios la posibilidad de reclamar la supresión, rectificación, confidencialidad o actualización de esta información, ya sea que esta fuera falsa o utilizada con fines (posibles o actuales) discriminatorios. Cualquiera de los usuarios a cuya información accedió *Cambridge Analytica* con una total falta de ética, podrían reclamar este resarcimiento.

Sumado a esto, el problema en el caso Snowden es lo que Zuboff denomina *Capitalismo de Vigilancia* y de alguna manera es una forma de invadir su intimidad. La razón es simple: a un usuario le pueden gustar ciertas cosas, tener ciertos amigos, tener su pelo de cierto color y por estos y otros muchos datos más, los capitalistas de vigilancia pueden generar contenidos adecuado para generar un cambio de comportamiento en ese usuario, sin este saber nada de estas prácticas. Desde ese lugar, su intimidad pasa a ser violada, pues las campañas publicitarias o el contenido "ad hoc" se realizó en base a su información íntima. En el final de esta tesina podemos recordar el chiste citado en el capítulo vinculado con el derecho a la privacidad: "Mi esposa me preguntó porque yo estaba hablando tan suavemente en la casa. Le dije que tenía miedo que Mark Zuckerberg (creador

y dueño de *Facebook* e *Instagram* entre otras) estuviera escuchando. Ella se rio. Yo me reí. *Alexa* se rio. *Siri* se rió".

En relación a las empresas en Internet en el caso Snowden, señalamos que la única forma que el Estado pudiera acceder a información privada es: a) negociar, presionar u obligar a la compañía (*Google* o *Facebook* por ejemplo) a que les comparta esos datos (usualmente en casos legales de investigación, esto se reduce a información de usuarios específicos, no de una muestra), b) generar y crear software de inteligencia y acceder a las computadoras de estos usuarios para rastrear su vida privada a través de su comportamiento en la red, como fue el caso de los programas de seguridad denunciados por Snowden o c) generar una relación de complicidad con las grandes empresas tecnológicas.

El caso Snowden pone al descubierto la complicidad encubierta entre las agencias de seguridad y las grandes empresas tecnológicas. A su vez demuestra que en pos del "interés general", en este caso la defensa contra el terrorismo, el derecho de los ciudadanos a resguardar su privacidad o su misma personalidad, sus sentimientos y sus mas privados secretos como los diálogos dentro de su propia casa, pasan a ser secundarios y a "no importar". Es casi como robar los dientes de marfil al elefante sin que su vida importe en lo absoluto, en aras de generar ganancias millonarias. Así, el ser humano pasa a ser materia prima sin importar nada mas.

Por su parte, el Estado, aun si pudiera acceder a la información "cruda" de los usuarios a través de una relación generada con estos gigantes tecnológicos, no posee los medios para generar un cambio de comportamiento "en masa" como si la poseen las empresas tecnológicas. En otras palabras, "necesita" a *Facebook*, a *Google* o a otras empresas, si es que desean modificar una conducta o predecir un comportamiento pues esta información es generada permanentemente y se alimenta del pasado y del futuro. En otras palabras, deben trabajar, al menos en parte, a través de lo que explicamos antes: los "capitalistas de vigilancia". Las amenazas terroristas orientan a los oficiales públicos hacia la intensificación de un poder que no le fue conferido por los ciudadanos.

Por otra parte, en relación con las empresas en Internet en el caso Wylie, como lo hemos explicado con respecto a *Cambridge Analytica* (CA) y la denuncia de Christopher Wylie se suma a prácticas que vienen realizando en *Facebook* desde sus ciernes, como "SOP" (por sus siglas en ingles "Procedimientos de Operación Estándar"). Un documento adquirido por *The Intercept*

demuestra cómo trabaja *Facebook* para generar productos de predicción, confirma la orientación primaria de la compañía a los mercados futuros de comportamiento y revela el grado con el que CA refleja estas operaciones como "normales" en el mundo de *Facebook.* Describe la habilidad de *Facebook* para guardar y utilizar, sin rivales, datos altamente íntimos con el objetivo de "predecir comportamientos futuros", apuntando a individuos basado en cómo se van a comportar, que van a comprar, a quien van a votar y cómo van a pensar. En otras palabras, se relacionan la predicción (análisis de datos), con la intervención (campaña publicitaria o de medios) y la modificación (que ese individuo cambie de opinión y/o acción acerca de algo, por ejemplo, de un candidato/partido político, de un producto o de un servicio, entre otros. *Facebook* también posee un servicio llamado "*Loyalty Prediction"* (predicción de lealtad) (Zuboff, 2019: 279) para las empresas que presentan anuncios o campañas hacia una muestra especifica de individuos que están en riesgo de cambiar su preferencia de cierta marca o candidato político hacia otras u otros a través de mensajes agresivos con el objetivo de cambiarles la lealtad y de esta manera generar resultados garantizados, alterando el curso del futuro.

Es la base de los servicios y contenidos *"ad hoc"* o generados específicamente para el usuario basado en Inteligencia Artificial y que resulta la clave de experiencias ultra personalizadas, entregando contenido específicamente diseñado para ese usuario en particular. En otras palabras, los datos personales, íntimos y sensibles de los usuarios en manos de los gigantes tecnológicos como *Apple, Google y Facebook*, pasan a ser la materia prima que las compañías utilizan para la predicción, intervención y modificación del comportamiento de los usuarios, con el objetivo de generar a través de ellos, ganancias económicas, políticas y sociales sin precedentes en la historia de la humanidad.

Y los datos no se reducen al lugar donde se encuentra el usuario, su conexión *Wi-Fi* o la información de su computadora sino a la proveniente de sus videos, análisis de afinidades, detalles de amistades y similitudes con amigos, entre otros, parar generar un perfil de personalidad creado por inteligencia artificial y "*machine learning"* o aprendizaje de máquinas.

En relación con los Ciudadanos en Internet en el caso Snowden, se puede confirmar que la explosión tecnológica generó al mismo tiempo que la mayoría de los ciudadanos que se encontraban participando políticamente en las redes, se enteraran de las noticias de la denuncia de

Snowden casi al instante de haberse publicado, lo cual lo hizo imposible de ocultarlas por parte de las agencias de inteligencia. Las nuevas prácticas sociales de las personas conectadas a internet día y noche, utilizando sus teléfonos inteligentes para emails, locación, redes sociales, textos, videos y más, facilitó las prácticas con falta de ética llevadas a cabo por la NSA con el supuesto objetivo de salvaguardar la seguridad de los ciudadanos.

La llegada de la técnica a la vida de las personas, a través del uso de computadoras con cámaras y micrófonos, aparatos inteligentes con los que los ciudadanos conviven en sus casas "escuchando" toda lo que sucede como si fuera un integrante más de una película, o uno de los robots de *Stars Wars* que tienen casi forma humana son todos ejemplos de las condiciones adecuadas para espiar la vida de todos y cada uno de los ciudadanos. Sumado a estas prácticas, la dependencia absoluta de los ciudadanos al uso constante de la tecnología y el uso de las redes sociales como nuevo habito de vida para relacionarse permanentemente con otros usuarios, generan incluso más facilidades para "espiar" a los individuos y reconocer como parte de los datos "robados", los nodos o redes de personas con las que los usuarios se relacionan.

Finalmente, la participación ciudadana, vista por algunos autores amantes de la tecnología como algo bueno, al generar que más personas conectadas a la red puedan involucrarse en actividades políticas o comunitarias, y generar cambios, presenta algunos peligros como el de ser investigado por pertenecer a ciertas afiliaciones políticas.

Por otra parte, en relación con los Ciudadanos en Internet en el caso Wylie, la explosión de Internet obviamente ha facilitado las prácticas de empresas sin ética alguna como CA y de las empresas o los candidatos políticos que la han contratado. Cuando Wylie denunció los hechos, los "ciudadanos en red" se encontraban divirtiéndose de lo lindo en *Facebook*, espiando a sus exparejas, mostrando fotos de bebes recién nacidos y publicando la ubicación en donde se encontraban cenando. Toda la información compartida por estos usuarios y la relación que estos tenían con otros usuarios en *Facebook* fue explotada de una manera sin igual por CA, hasta generar el acceso a poder de Donald Trump, quien no tenía gran popularidad ni era un candidato que prometía muchas posibilidades.

Por otra parte, en referencia a los hackers, queremos señalar que, como consecuencia de todos estos cambios tecnológicos revolucionarios, que influyen todas y cada una de las esferas

de nuestras vidas, en nuestros días, los ataques de hackers resultan tal vez aún más peligrosos que las bombas plantadas por terroristas.

La segunda semana de mayo del 2021, una de las compañías más grandes de gas de Estados Unidos, *Colonial Pipeline Co*, que distribuye gasolina a todo el país fue *hackeada* por un grupo proveniente de Europa del Este. El sistema interno de *software* de la compañía dejo de funcionar por lo cual no pudieron seguir entregando gas a las gasolineras[65]. El grupo pidió 5 millones de dólares, que fueron abonados por la empresa a cambio de restablecer el servicio y generar acceso a gasolina a millones de ciudadanos estadounidenses. El pago se habría realizado a través de Criptomoneda, lo cual lo hizo difícil de rastrear. Una vez recibido el pago, el grupo *hacker* envió a la compañía una herramienta para "descriptar" el *hackeo* y para restaurar su red informática deshabilitada[66]. El hecho nos hace reflexionar acerca de la importancia de los sistemas informáticos en la economía actual. ¿Quién hubiera pensado que los ciudadanos de un país entero se podrían quedar sin gasolina para manejar sus autos, como resultado de un ataque *hacker*?

Al mismo tiempo, tenemos que sentenciar una posición en relación a las *cookies* porque las *cookies* son piezas de información que se guardan cuando un usuario está en línea y lo rastrean mientras navega. Supongamos que un usuario visita un sitio Web sobre el tiempo e ingresa su código postal para ver qué está sucediendo en su área; la próxima vez que visite el mismo sitio, recordará su código postal debido a las cookies. Hay *cookies* de origen que se colocan en el sitio que visita, y luego hay *cookies* de terceros, como las que colocan los anunciantes para ver lo que les interesa a los usuarios y, por supuesto, mostrarle anuncios "ad hoc", incluso cuando abandona el sitio original que había visitado.

La proliferación de alertas sobre *cookies* en cada uno de los sitios que un usuario se encuentra navegando, es el resultado de una confluencia de eventos, principalmente fuera de la UE. Pero en el panorama general, estas alertas subrayan el debate sobre la privacidad digital, que incluye la pregunta de si es mejor pedir a los usuarios que opten por participar o no en la recopilación de datos, y la cuestión de quién debe poseer los datos y ser responsable de protegerlos.

[65] https://wlos.com/news/local/explained-how-pipeline-hack-triggered-gas-issues-how-you-can-protect-yourself
[66] https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

En mayo de 2018, cuando el GDPR entró en vigor en Europa; miles de millones de bandejas de entrada se inundaron con correos electrónicos de política de privacidad. La ley de privacidad está diseñada para garantizar que los usuarios conozcan los datos que las empresas recopilan sobre ellos y para darles la oportunidad de dar su consentimiento para compartirlos. Requiere que las empresas sean transparentes sobre la información que están recopilando y por qué las recogen. A su vez, las personas tienen derecho a acceder a todos sus datos personales, controlar el acceso y el uso de ellos, e incluso eliminarlos.

Luego del surgimiento del GDPR, la mayoría de los sitios Web comenzaron a agregar notificaciones de *cookies*, aunque el GDPR en realidad solo menciona las cookies una vez, mencionando que, en la medida en que se utilizan para identificar a los usuarios, califican como datos personales y están sujetos al GDPR, lo cual permite a las empresas procesar datos siempre que obtengan el consentimiento o tengan lo que los reguladores consideran un "interés legítimo". Otra regulación también gobierna el empleo de *cookies*, la cual tiene más de una década en vigencia: la *ePrivacy Directive*. Lamentablemente la mayoría de los usuarios simplemente *cliquean* "aceptar" sin entender las consecuencias de la existencia de estas cookies en sus buscadores. [67]

Como resultado de este trabajo, en el escenario de las metaconclusiones, reconocemos como investigadores que nos encontramos en un lugar de mucho mayor control y pocos cambios en aras de proteger a los ciudadanos en el sector público o a los usuarios en el privado. No existe un marco jurídico previo o un proceso judicial que corresponda a la realidad actual de los ciudadanos. No existe tampoco un país modelo en el mundo que promueva y proteja los datos personales y el derecho a la intimidad. Existirán denuncias de otros usuarios similares a Snowden o Wylie cada dos o tres años, donde el mundo verá la aparición de un nuevo caso donde se lesionan los datos personales y el derecho a la intimidad.

El rol de las agencias de inteligencia es simplemente continuar con la hegemonía del Estado a nivel nacional e internacional y poco tiene que ver con la fachada que demuestra su "lucha contra el terrorismo para la seguridad nacional".

[67] https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy

El Estado no protege a sus ciudadanos, aun luego de presentar procesos legales, en donde *Facebook* o *Google* tienen que sentarse enfrente a un juez y dar cuenta de sus acciones. El rol del Estado es continuar manteniendo su poder hegemónico y negociar con las empresas de tecnología cuando es conveniente ya sea acceder a datos personales o demostrar a la opinión pública que se les implementaron límites. El Estado tampoco respeta la Cuarta Enmienda de la Constitución de los Estados Unidos de América, ni los derechos constitucionales de los ciudadanos.

En cuanto a las grandes tecnológicas y su relación con el Estado, el interés privado económico prevalece y lo puede hacer a través de tecnología de última generación a la que el Estado se encuentra siempre unos pasitos atrás, como si fuera su sombra. En este proceso, los datos personales y la intimidad de los usuarios son dañados pues a nadie le interesa proteger los intereses de los ciudadanos.

Los acuerdos son basados en jurisprudencia o acuerdos anteriores de los que se basan para generar el siguiente acuerdo, como un tren de acuerdos donde los vagones de atrás van cayendo al precipicio o son soltados en las líneas del tren y los de adelante permiten seguir en camino. Al llegar a una nueva estación se agregan vagones, pero esto no significa que, en los conflictos generados entre el Estado y las empresas privadas, las soluciones hayan sido ejemplares o que hayan modificado sustancialmente las responsabilidades de las empresas en cuanto a la protección de los datos personales y el derecho a la intimidad.

En la actualidad, las empresas poseen más información de los ciudadanos que el propio Estado y como hemos descripto antes, esta información pertenece al universo de los datos sensibles. El Estado sigue teniendo la potestad de conocer los datos públicos de las personas mientras que las empresas poseen la información de los datos sensibles y los datos privados y nadie puede garantizar o proteger la circulación y reproducción de la información privada de las personas en otros destinos del planeta.

A modo de reflexión personal sobre las bases de datos personales y sensibles que poseen las empresas de los ciudadanos y como último punto de nuestra tesina, resulta importante plantearse cuánto resulta de importante compartir nuestras vidas en las redes sociales, cuan necesario es mostrar nuestros intereses, nuestros gustos, nuestros planes, de quienes nos rodeamos, y miles de datos más. Parte de la escritura de esta tesina se realizó durante la pandemia

mundial del COVID-19 del año 2020-2021. Un año difícil para todos por la falta de socialización. Sin embargo, *Facebook* nos ayudó a comunicarnos con otros tesistas, a encontrar grupos políticos afines en las elecciones estadounidenses del 2020, a relacionarnos con otros, aunque sea a través de una llamada de *Zoom*, a chatear, a compartir fotos y videos. Y eso nos ayudó a sentirnos parte de algo, a socializar, aunque sea de una manera diferente, porque los seres humanos necesitan relacionarse, aun en el medio de las peores crisis. Lamentablemente esta es la paradoja que los usuarios enfrentan a la hora de compartir sus datos personales en las redes sociales.

Finalmente, nos gustaría explicar los ciclos de disposición por los que pasan no sólo las gigantes tecnológicas sino también el Estado cuando su credibilidad queda dañada por denuncias públicas como las de Snowden y Wylie.

Luego de las denuncias de Snowden, Mark Zuckerberg, "se arrepintió" ante los medios y el Congreso de los Estados Unidos, asegurando que "no tenían idea de que estas funcionalidades podrían ser usadas de esta manera". Zuckerberg inició lo que Zuboff llama el *"Ciclo de Disposición"* en donde la compañía genera una convergencia de operaciones políticas, sociales, administrativas y técnicas a su favor. En primer lugar, se accede a la información "ultra privada" de los usuarios, desde una caminata en un parque hasta lo que éste habla con *Alexa* en su propia casa. Luego, llegan algunos juicios, algunas quejas o denuncias y deben dar cuenta de sus acciones a las instituciones, siguiendo el tedioso ritmo de las esferas públicas. Mientras tanto continúan sus operaciones al ritmo de la luz, avanzando y ganando camino sin pedir permiso alguno. Ocasionalmente deben alterar algunas de sus prácticas y adaptar sus operaciones, para mantener al público "contento" y generando de esta manera prácticas más dinámicas para continuar la marcha. En este ciclo, la compañía aprendió a lidiar y transformar la resistencia publica, lo cual era y es una condición sine qua non para su continua expansión.

Luego de haber realizado todo este recorrido a lo largo de la tesina y en estas conclusiones podemos finalmente destacar que hemos presentado dos casos que tuvieron impacto en el escenario internacional, reconocidos a través de las figuras de Edward Snowden y Christopher Wylie. Estos casos marcaron un punto de ruptura en la evolución del tratamiento de la problemática relacionada con el derecho a la privacidad y a la protección

de datos personales. El impacto más notorio se determinó en la modificación del marco jurídico internacional a través de la evolución progresiva de Safe Harbor, reemplazado por Privacy Shield y posteriormente actualizado por el GDPR (Reglamento General de Datos Personales de la Unión Europea).

El caso Edward Snowden significó un cierto "abrir de ojos" para la conciencia pública, aunque tan solo fuese por unos días, un reconocimiento de la falta de protección de los datos privados por parte del Estado y recordarnos que el Estado seguirá manteniendo su poder hegemónico a cualquier precio.

El caso Christopher Wylie significó un "abrir de ojos" de los usuarios de las redes sociales y un darse cuenta de lo poderosas que son estas compañías y que *Facebook* tampoco protege los datos personales de los usuarios, aun así, cuando en público demuestra lo contrario.

En referencia a todo lo manifestado podemos sostener que nuestra hipótesis se cumpliría, teniendo presente que la ausencia del Estado y la carencia de un marco jurídico para proteger los datos personales y el derecho a la intimidad permite que las empresas generadoras de contenidos y proveedoras de servicios de internet "jueguen en el bosque mientras el lobo no está".

FUENTES CONSULTADAS

Bibliografía

- Aguiar, Henoch.: 2007. *El futuro no espera. Políticas para desarrollar la sociedad del conocimiento.* 1ra Edición. Buenos Aires, Editorial La Crujía.
- Banisar, David.: 2006. *Freedom of Information Around the World 2006: A Global Survey of Access to Government Information Laws.* Privacy International.
- Basterra, Marcela.: 2012. *Derecho a la Información vs. Derecho a la Intimidad.* Rubinzal Culzoni Editores, 1° edición, Santa Fe, Argentina.
- Becerra, M.: 2005. *Educación y Sociedad de la Información.* Secretaría de Posgrado, Universidad Nacional de Quilmes.

- Benjamin, Walter. 1973. *"La obra de arte en la época de su reproductibilidad técnica".* Discursos interrumpidos I. Taurus. Madrid.
- Bergman, Michael K. 2001. *The Deep Web: Surfacing Hidden Value.* Journal of Electronic Publishing.
- Blok, Mariano Rubén.: 2018. *El derecho de acceso a la información publica en México.* Tesina de graduación. UBA, Facultad de Ciencias Sociales. Lic. Ciencias de la Comunicación. Buenos Aires.
- Boyd, D., & Ellison, N.: 2008. *Social Network Sites: Definition, History, and Scholarship.* Journal of Computer-Mediated Communication.

- Bourdieu, Pierre y Wacquant, Loïc: 2005. Una invitación a una sociología reflexiva. Siglo XXI. Buenos Aires.

_____Bourdieu, Pierre; Chamboredon, Jean-Claude; Passeron, Jean-Claude: 2002 y 2004 (1972). *El oficio de sociólogo. Presupuestos epistemológicos.* Siglo XXI Editores Argentina. Buenos Aires.

_____(2004 (1972)).Bourdieu, Pierre; Chamboredon, Jean-Claude; Passeron, Jean-Claude: *El oficio de sociólogo. Presupuestos epistemológicos.* Siglo XXI Editores Argentina. Buenos Aires.

- Burch, Sally; León, Osvaldo, Tamayo, Eduardo. 2003. *"Se cayó el sistema". Enredos de la Sociedad de la Información.* Agencia Latinoamericana de Información. Quito.
- Cafassi, Emilio, 1998. *"En los umbrales".* En Internet: políticas y comunicación, CAFASSI, Emilio (editor). Editorial Biblos. Buenos Aires.
- Caldevilla-Domínguez, David.: 2010. *Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual.* Complutense University of Madrid. Madrid.
- Castells, Manuel.: 2006. *La Era de la Información: Economía, sociedad y cultura. Volumen I: La Sociedad Red.:* Siglo XXI. México.

_____2001. *The Internet Galaxy, Reflections on the Internet, Business and Society.* Oxford University Press. Oxford.

_____2002. *The Information Society and the Welfare State: The Finnish Model.* (co-author, Pekka Himanen). Oxford UP, Oxford

_____1996. *The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I.:* Blackwell. Cambridge, Massachusetts; Oxford, UK.

- Cobo Romaní, Cristóbal.: 2005. *Organización de la información y su impacto en la usabilidad de las tecnologías interactivas.* Tesis de Doctorado. Ciudad de México.

- Collins, A.: 1997. *National science education standards: looking backward and forward.* The Elementary School Journal.
- Dahl, Robert A.: 1989. *Democracy and Its Critics,* Yale University Press.
- Dalhgren, Peter.: 1995. Television and Public Sphere. Democracy and the media. Sage. London.
- De Carlucci, Aída Kemelmajer.: 2015. *El derecho a la intimidad de niños, niñas y adolescentes.* Tomo III, p. 501/528. Editorial Thomson Reuters. La Ley.
- De Kerckhove, Derrick.: 1999. *Inteligencias en conexión*. Gedisa. Barcelona.

_____. 1997. *The skin of culture: investigating the new electronic reality.* Kogan Page Limited. London.

- Depetris, B., Feierherd, G., De Giusti, A., Sanz, C., González, A. y Pousa, A. 2008. *TICs en Educación. X Seminario de Investigadores en Ciencias de la Computación.* Red de Universidades con Carreras en Informática.
- Dery, Mark. 1998. *Velocidad de escape. La cibercultura en el final del siglo*. Siruela. Madrid.

- Duhalde, Eduardo Luis y Alén, Luis Hipólito.: 1980. *Teoría Jurídico-Política de la Comunicación. Segunda Edición.* Capitulo III: La UNESCO y la sistematización científica del derecho a comunicar. Londres.
- Echeburúa, Enrique; De Corral, Paz. 2010. *"Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: un nuevo reto"*.
- Foucault, Michel:. 2005. Foucault, Michel. *Vigilar y Castigar.* Siglo XXI.

_____(1979). *El ojo del poder.* En Bentham, J., El Panóptico. La Piqueta. Madrid,

_____ 2000. *Defender la sociedad.* Fondo de Cultura Económica. Buenos Aires.

- Fraguas de Pablo, María: 1985. *"Teoría de la desinformación".* España.

- García Canclini, Néstor. 1999. *"Narrativas sobre fronteras móviles entre Estados Unidos y América Latina".* en BAYARDO, Rubens y Mónica LACARRIEU (comp.). La dinámica global/local. Cultura y comunicación: nuevos desafíos. Ediciones Ciccus-La Crujía. Buenos Aires.
- Gramci, Antonio.: 1967. *Cultura y literatura*.: Península. Madrid.

- Habermas, Jürgen.: 1997. *Historia y crítica de la opinión pública. La transformación estructural de la vida pública*. Ediciones Gustavo Gili. México.
- Hamilton, Lee.: 2015. *From passivity to Eternal Vigilance: NSA Surveillance and Effective Oversight of Government Power. (De la pasividad a la eternal vigilancia eterna: la Vigilancia de la NSA y la efectiva ligereza por el poder del gobierno).* "The Snowden Reader". Indiana University Press. Indiana.

- Heidegger, Martin.: *"La pregunta por la técnica*". Filosofía, ciencia y técnica. Santiago: Editorial Universitaria. 2007.
- Innis, Harold Adams.: 1964. *The bias of communications and Monopolies of power.* Intro. Marshall McLuhan. 1951. Toronto: University of Toronto Press.
- Joyanes, Luis.: 1997. *Cibersociedad, los retos sociales ante un nuevo mundo digital.*: McGraw-Hill. Madrid
- Laje, Alejandro.: 2008. *El derecho a la privacidad en la jurisprudencia de la corte suprema de la justicia de la nación.* Trabajo en derecho civil I de la carrera de doctorado de la Universidad de Ciencias empresariales y sociales.
- Lévy, P. 1999. *Qué es lo virtual.* Paidós Editorial. Barcelona.

- Loreti, Damián.: 1995. *El Derecho a la Información. Relación entre medios, público y periodistas.* Editorial Paidós. Buenos Aires.
- Luhmann, N.: 1997/1990. *Sociedad y sistema: la ambición de la teoría.* Paidós. Barcelona.
- Mangabeira Unger, Robert.: "The dictatorship of No alternatives", in What should the left propose? Verso. London. 2006.

- Marcuse, Herbert.. 1993. *El hombre unidimensional.* Planeta de Agostini. Barcelona.
- Marques, P. 2001. Las TICs y sus aportes a la sociedad. Barcelona: UAB.
- McLuhan, Marshall.: 1995. *La aldea global,:* Gedisa. Barcelona.

—— 1994. *Understanding media*. MIT Press. Massachusetts.

——1962. *The Gutenberg galaxy.* University of Toronto Press. Toronto.

- Mill, John Stuart.: 2007. *Sobre la libertad.* Traducción de Pablo de Azcárate, Alianza, Madrid, 2005, en Mill, Vida, pensamiento y obra, Planeta DeAgostini, Madrid.
- Morris, R. D.: 2011. *Web 3.0: Implications for Online Learning.* TechTrends. New York.
- Moragas, M.: 2001. *Las ciencias de la comunicación en la sociedad de la información. Retos de la sociedad de la Información.* Universidad pontificia de Salamanca. Salamanca.
- Muñoz de Alba Medrano, M., & Cano Valle, A.: 2002. Derechos de las personas con Síndrome de Inmunodeficiencia Adquirida. Cámara de Diputados - UNAM. México.
- Negroponte, N.: 1995. *El mundo digital.* Ediciones B. Barcelona.
- Nino, Carlos Santiago.: 1992. *Fundamento del Derecho Constitucional*. Editorial Astrea. Buenos Aires.
- Nonaka, I.: A 1994. *Dynamic Theory of Organizational Knowledge Creation.* Institute for operations research ant the management sciences.
- Nora, Simon; Minc, Alain; Bell, Daniel (Introduction).: 1978. 1981. *The Computerization of Society* y First English language edition. The MIT Press. Boston.
- Novoa Monreal, Eduardo.: 1989. *Derecho a la vida privada y libertad de información. Un conflicto de derechos.* Siglo XXI Editores, México.
- Orwell, George. *1984*. Barcelona. Destino. 2003
- Oszlak, Oscar.: 1978."Formación histórica del estado en América Latina: elementos teórico-metodológicos para su estudio". Estudios CEDES, vol.1, No 3.

- Oszlak, Oscar.: 1981. Orden y progreso: Ensayos sobre la formación histórica del estado argentino. Instituto de desarrollo económico y social. Buenos Aires.

- Patten, Steve.: 2013. *"Assessing the Potential of New Social Media".* Canadian Parliamentary Review.

- Pérez, D.: 2005. *Contribución de las tecnologías de la información a la generación de valor en las organizaciones: un modelo de análisis y valoración desde la gestión del conocimiento, la productividad y la excelencia de la gestión*. Tesis Doctoral, Universidad de Cantabria. España.
- Parisier, Eli.: 2011. *The filter bubble. What the internet is hiding from you*. The Penguin Press. New York.
- Piscitelli, Alejandro: 2002. *Ciberculturas 2.0 en la era de las máquinas inteligentes*. Editorial: Paidós.
- Pinch, Trevor.; Bijker, Wiebe.: 1984. *"The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other".* Social Studies of Science.

- Rall, Ted: *Snowden.* Ediciones Seven Stories Press. 2015.
- Rehman, Ikhlaq:. 2019. *Facebook-Cambridge Analytica data harvesting: What you need to know.* Library Philosophy and Practice. Lincoln.
- Rheingold, Howard.: 2000. *Tools for Thought: The History and Future of Mind-Expanding Technology*. The MIT Press; Revised, Subsequent edition.
- Rivera, Julio César. 1989. *"El derecho. La vida privada. Su regulación y contenido en la legislación y jurisprudencia comparadas"*. Revista de derecho privado. Madrid.
- Robert Mangabeira Unger.: 2006. *"The dictatorship of No alternatives",* in What should the left propose? Verso. London.
- Sampedro, Víctor; Resina, Jorge. 2010. *"Opinión pública y democracia deliberativa en la Sociedad Red".* Ayer.

- Scalvini, Elda, y Leyva, Claudio.: 2002. *"Las medidas precautorias y la tutela efectiva del derecho a la intimidad"*, en Derecho a la información, habeas data e Internet, Armagnague, Juan F.(dir), Ediciones la Roca, Buenos Aires.

- Schmucler, Héctor; 1989. Lechner, Norbert; y Sutz, Judith.: *Nuevas tecnologías de información: el ocultamiento de la historia.* Puntosur-ILET. Buenos Aires.
- Scolari, Carlos.: 2008. *Hipermediaciones. Elementos para una Teoría de la Comunicación digital interactiva.* Gedisa. Barcelona.
- Silva, Alberto J. Cerda.: 2011. *Legislación sobre Protección de las Personas frente al Tratamiento de Datos Personales.* Universidad de Chile. Chile.
- Shapiro, F.: 2002. *Paradigms, processing, and personality development.* American Psychological Association Press. Washington, DC.

- Smolla, Rodney.: 1992. Free Speech in an open society. Knof. New York.
- The Snowden Files.: 2014. *The Inside Story of the World's Most Wanted Man Paperback.* Compilado de autores. Editorial Vintage.

- Thorstein, Veblen.: 1923. *Absentee Ownership and Business Enterprise in Recent Times*. *Case of America.* Viking Press. New York.
- Tofts, Darren John; Mckeich, Murray. 1998. *Memory Trade: A Prehistory of Cyberculture.* Newark: Gordon & Breach Publishing Group.
- Underwood, J. The impact of digital technology: A review of the evidence of the impact of digital technologies. Becta. 2009
- Villanueva, Ernesto. 2002. *Derecho Comparado de la Información.* 2a ed, Edit. Miguel Ángel Porrúa. México.
- Virilio, Paul.: 2002ª. *El Crash Visual.* En Ramonet, I (Ed), La Postelevision. Icaria Antrazyt. Barcelona.

_____2002b. *Videovigilancia y delación generalizada.* En Ramonet, I (Ed), La Postelevision. Icaria Antrazyt. Barcelona.

_____1999. *La inercia polar*. Trama Editorial/Prometeo Libros. Madrid.

_____1997a. *¿Fin de la historia o fin de la geografía? Un mundo sobreexpuesto.* Le monde Diplomatique. Ed. Española.

_____1997b. *El cibermundo, la política de lo peor.* Catedra. Madrid.

_____1995. *The Art of the Motor.* University of Minnesota Press. Minneapolis.

_____1989. *The imposture of Immediay. War and cinema: the logistic of perception.* Verso. Londres.

- Weber Max.: 1978. *Economy and society: An outline of Interpretative Sociology*. University of California Press. Berkeley, CA.

- Williams, Raymond. 2000. *"The Technology and the Society".* En Thornton Cadwell, J. Electronic Media and Technoculture. Rutgers University. New Jersey.
- Wolff, Michael.: 2018. *Fire and fury for Facebook. International Financial Law Review;* London.

- Wylie, Christopher: 2018. *MindF*ck.* Random House Publishing Group. Kindle Edition.
- Zuboff, Shoshana, *The age of Surveillance Capitalism. The fight for a human future at the new frontier of power.* PublicAffairs, New York, 2019.

Publicaciones, libros en línea e investigaciones académicas

- Acevedo Mena, M.Sc. Karen María, Romero Espinoza, M.Sc. Skarlet. 25 de octubre del 2019. *La educación en la sociedad del conocimiento.* Revista Torreón Universitario. https://www.researchgate.net/publication/338092243_La_educacion_en_la_sociedad_del_conocimiento
- Amezcua, Manuel; Gálvez, Alberto.: 2002. *Los modos de análisis en investigación cualitativa en salud: perspectiva critica y reflexiones en voz alta*. Madrid. https://www.redalyc.org/pdf/170/17076505.pdf
- Area Moreira, Manuel. 10 de agosto 2013. *"Las redes sociales en Internet como espacios para la formación del profesorado".* Razón y Palabra 63. http://www.razonypalabra.org.mx/n63/marea.html
- Banisar, David: 2011. *The Right to Information and Privacy: Balancing Rights and Managing Conflicts*. Project: Tracking Growth of Data Protection Globally. https://www.researchgate.net/publication/228125289_The_Right_to_Information_and_Privacy_Balancing_Rights_and_Managing_Conflicts.
- Baudrillard, J. Dust Breeding. En Kroker A., Kroker, M (Eds), 2001. https://journals.uvic.ca/index.php/ctheory/article/view/14593/5444 .
- Blejman, Mariano.: 2014. ¡Ciudadanos a la red!. Los vínculos sociales en el ciberespacio. Susana Finkelevich, coordinadora. https://bibliodarq.files.wordpress.com/2014/03/finquelievich-s-c2a1ciudadanos-a-la-red.pdf
- Bonilla, E.; Rodríguez, P.: 2018. *Más allá del dilema de los métodos.* Uniandes –Norma Bogotá. https://laboratoriociudadut.files.wordpress.com/2018/05/mas-alla-del-dilema-de-los-metodos.pdf.

- Campal García, Felicidad.: *Las redes ciudadanas: de la información a la participación democrática.* Salamanca. http://eprints.rclis.org/10110/1/ARTÍCULO_PARA_EDUCACIÓN_Y_BIBLIOTEC1+.pdf
- Castells, Manuel.: 2011. *"A Network Theory of Power"*. International Journal of Communication. México. https://ijoc.org/index.php/ijoc/article/view/1136/553.
- Cerón-Martínez, Armando Ulises: 2020. *La construcción del objeto de estudio. Lecciones epistemológicas a partir de la obra de Pierre Bourdeau*. Universidad Autónoma del Estado de Hidalgo. México https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0717-554X2020000100075
- Congreso Vircomm'99. Abril de 1999 San Francisco http://www.vir-comm.com/index.html
- De Kerckhove, Derrick. 1995. "Network Art and Virtual Communities". http://www.va.com.au/parallel/x2/journal/derrick_dk/ddk.html ._____.2005. *"Los sesgos de la electricidad.* http://www.uoc.edu/inaugural05/esp/kerckhove.pdf
- Deusdad Ayala, Ma Blanca: Diciembre, 2001. *El carisma político en la teoría sociológica.*. Tesis doctoral de la Universidad de Barcelona. Barcelona. https://www.tdx.cat/bitstream/handle/10803/2962/TESIS_BDEUSDAD.pdf?sequence=1
- Domínguez Sanchez-Pinilla, Mario.: (2003). *Las tecnologías de la informacion y la comunicación: sus opciones, sus limitaciones y sus efectos en la enseñanza.* Nómadas, Num 8. Universidad Complutense de Madrid. Madrid.
- Edelman, Gilad.: Jan 13th, 2021. *The Parler Bans Open a New Front in the 'Free Speech' Wars.* Wired. https://www.wired.com/story/parler-bans-new-chapter-free-speech-wars/
- ESCO. (Unesco). 2014. *Tendencias mundiales en libertad de expresión y desarrollo de los medios.* http://unesdoc.unesco.org/images/0022/002297/229704S.pdf. .
- Fisher, Desmond.: 1984. *El derecho a comunicar*. UNESCO. Paris. https://www.scribd.com/document/373946231/Desmond-Fisher
- Flórez Romero, Marcela,; Aguilar, Andrea J. Barreto; Hernández, Peña Yurley K.; Salazar, Juan Pablo Torres; Pinillos Villamizar, Jesús Alexander; Pérez Fuentes, Carlos A.: 21 de abril

del 2017. *Sociedad del conocimiento, las TIC y su influencia en la educación*. Revista Espacios. https://www.revistaespacios.com/a17v38n35/a17v38n35p39.pdf

- Forero, I. 2009. *La sociedad del conocimiento.* Revista Científica General José María Córdova. https://www.redalyc.org/pdf/4762/476248849007.pd
- Gonzalez Santana, Alazne:, Junio, 2007. *La mirada panóptica. El poder de la mirada dentro de la Ciber-ciudad.* https://issuu.com/alaznegonzalez/docs/2008_mirada.pan__ptica.v.2.0
- Hobbes, Thomas. Enero-Junio 2009. Explicado por Arbeláez Herrera, Ángela M en el seminario de investigación titulado: *"Thomas Hobbes y la fundación de la política moderna"* Programa de doctorado en Ciencias Políticas de la Pontificia Universidad Católica Argentina. Buenos Aires. https://www.redalyc.org/pdf/1514/151412842005.pdf
- Isuani, Ernesto Aldo: *Tres enfoques sobre el concepto de Estado.* Maestría en Administración Pública Universidad de Buenos Aires. Buenos Aires. https://administracionpublicauba.files.wordpress.com/2016/03/03-isuani-aldo-tres-enfoques-sobre-el-concepto-de-estado.pdf
- Izaquirre, Anthony.: March 7, 2021. *GOP pushes bills to allow social media 'censorship' lawsuits*. Associated Press. https://apnews.com/article/donald-trump-legislature-media-lawsuits-social-media-848c0189ff498377fbfde3f6f5678397

- Kobie, Nicole.: 17 Mar 2010. *Q&A: Conrad Wolfram on Communicating with Apps in Web 3.0.* IT Pro. http://www.itpro.co.uk/621535/qa-conrad-wolfram-on-communicating-with-apps-in-Web-30 . 2010
- Krüger, Karsten.: 2015. *El concepto de sociedad del conocimiento. Universidad de Barcelona.* Barcelona. https://www.researchgate.net/profile/Karsten-Krueger-5/publication/245535884_El_concepto_de_%27sociedad_del_conocimiento%27/links/556af53f08aeccd7773a16ca/El-concepto-de-sociedad-del-conocimiento.pdf
- Lévy, Pierre. 2007. *Cibercultura: La cultura de la sociedad digital. Rubí, Barcelona*. Anthropos Editorial: Universidad Autónoma Metropolitana. México. https://antroporecursos.files.wordpress.com/2009/03/levy-p-1997-cibercultura.pdf

- Locke, John.: 1690. *Segundo tratado sobre el gobierno.* https://www.webdianoia.com/moderna/locke/textos/locke_text_3.htm
- Macbride, Sean y otros. 1980. *Un solo mundo, múltiples voces. Comunicación e información de nuestro tiempo.* Fondo de cultura económica. Unesco, París. https://agmer.org.ar/index/wp-content/uploads/2014/05/Informe-MacBride-parte1.pdf
- Mann, Michael: 2007. *El poder autónomo del Estado: sus orígenes, mecanismos y resultados.* http://politicasyplanificacion.sociales.uba.ar/wp-content/uploads/sites/121/2014/07/Unidad1_Teorico_Mann.pdf.

  _____Mann, Michael: *El poder autónomo del Estado: sus orígenes, mecanismos y resultados,.* http://politicasyplanificacion.sociales.uba.ar/wp-content/uploads/sites/121/2014/07/Unidad1_Teorico_Mann.pdf

- Mattelard, Armard (Entrevista).: *Sociedad del conocimiento, sociedad de la información, sociedad de control.* Armand Mattelart y Antonia Garcia Castro. https://journals.openedition.org/conflits/2682
- Mills, Lane B.: Dec 2007. *The Next Wave Now: Web 2.0 Scholarly Journals.* The Education Digest. https://www.researchgate.net/publication/234609149_The_Next_Wave_Now_Web_20

- Mittelstadt, Brett & Russell, Chris; by Sandra Watcher. 2018. *Counterfactual Explanations without opening the black Box: Automatic Decisions and the GDPR.* Harvard Journal of Law & Technology. Volumen 31 Number 2 Spring. Boston. https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf .
- Navarro, L. & Serra, A. BCNet Barcelona Red Ciudadana. Barcelona. http://www.bcnet.upc.es/papers1.html

- Needleman, Sarah E. Updated May 17, 2021. C*onservative Social-Media App Parler Has Returned to Apple's App Store. Here's What That Means.* The Wall Street Journal. https://www.wsj.com/articles/what-is-parler-app-apple-android-11610478890
- O'Donnell, Guillermo.: 2001. *La irrenunciabilidad del Estado de Derecho.* Universidad de Notre Dame, Departamento de Gobierno. Instituto Kellogg de Estudios Internacionales. https://corteidh.or.cr/tablas/19745a.pdf 2001.
- O'Donnel, Guillermo: 1978. *Apuntes para una teoría del Estado.* Universidad Nacional Autónoma de México. México. http://www.top.org.ar/ecgp/FullText/000000/O%20DONNELL%20Guillermo%20-%20Apuntes%20para%20una%20teoria%20del%20estado.pdf
- Oszlak, Oscar: 1998. "*Políticas publicas y regímenes políticos: reflexiones a partir de algunas experiencias latinoamericanas",* https://repositorio.cedes.org/bitstream/123456789/3470/1/Est_c3%2c2.pdf .
- Oszlak, Oscar: Políticas publicas y regímenes políticos: reflexiones a partir de algunas experiencias latinoamericanas", https://repositorio.cedes.org/bitstream/123456789/3470/1/Est_c3%2c2.pdf 1980
- Paur, A., Rosanigo, Z. y Bramati, P. 2006. *La educación en la sociedad del conocimiento.* Facultad de Ingeniería, UNPSJB. http://sedici.unlp.edu.ar/bitstream/handle/10915/19258/Documento_completo.pdf?sequence=1&isAllowed=y .
- Reusser, Monsálvez, Carlos.: 2003. *¿Qué es la sociedad de la información?. Centro de estudios en derecho informático.* http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14670%2526ISID%253D292,00.html
- Rodríguez Salas, José Antonio.: 2002. *Teledemocracia: el empuje para la ciudadanía activa.* Asociación Andaluza de Redes Ciudadanas. Valladolid. .www.redciudadand.org

- Roosendaal, Arnold. 2010. *"Facebook tracks and Traces Everyone: Like This!.* (SSRN Scholarly Paper, Social Science Research Network). Rochester, NY. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563
- Rousseau, Jean-Jackes.: 1936. .El contrato social. Publicado en España. https://es.wikisource.org/wiki/El_contrato_social_(1836)
- Rudman, Riaan and Bruwer, Rikus.: 2016. *Defining Web 3.0: opportunities and challenges.* Scholarly Journals The Electronic Library. https://www.emerald.com/insight/content/doi/10.1108/EL-08-2014-0140/full/html
- Serra, A. 1998. *Las redes ciudadanas: ¿Qué son y cómo funcionan?*. http://www.canet.upc.es/articleeuz.html.
- Tedesco, J. (2003). Investigación educativa: de la ciencia social a la filosofía social. Revista Electrónica de Investigación Educativa, 5 (2). Recuperado de https://redie.uabc.mx/redie/article/view/86
- Thwaites Rey, Mabel:. 1999. *El Estado: Notas sobre su(s) significado(s)*. Publicación de la FAUD, Universidad Nacional de Mar del Plata. Mar del Plata. http://www.catedras.fsoc.uba.ar/thwaites/est_conc.pdf .
- Torres, Natalia: *Acceso a la información y datos personales: una vieja tensión, nuevos desafíos*. https://www.palermo.edu/cele/pdf/DatosPersonales_Final.pdf
- Warren and Brandeis: 1890-2012. *The right to Privacy.* En "La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario Legado de Warren y Brandeis. Revista de Derecho Político". Saldaña Díaz, Maria Nieves. https://www.academia.edu/11782378/THE_RIGHT_TO_PRIVACY_LA_GÉNESIS_DE_LA_PROTECCIÓN_DE_LA_PRIVACIDAD_EN_EL_SISTEMA_CONSTITUCIONAL_NORTEAMERICANO_EL_CENTENARIO_LEGADO_DE_WARREN_Y_BRANDEIS_THE_RIGHT_TO_PRIVACY_THE_GENESIS_OF_THE_PROTECTION_OF_PRIVACY_IN_THE_AMERICAN_CONSTITUTIONAL_SYSTEM_THE_CENTENARY_LEGACY_OF_WARREN_AND_BRANDEIS

Artículos y Notas Periodísticas

- NY Times (Archive article: Date unavailable). *"Secrets documents reveal N.S.A. Campaign against Encryption".* https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
- Cadwalladr, Carole; Graham-Harrison, Emma.: Sat 17 Mar 2018. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
- Cadwlladr, Carole.: Sun 18 Mar 2018. *'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower.* The Guardian. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump
- Gomez Gonzalez, Janet.: Marzo 19, 2915. ¿Cómo funciona la segmentación psicográfica?. Merca2.0. https://www.merca20.com/como-funciona-la-segmentacion-psicografica/
- Grassegger, Hannes & Krogerus, Mikael.: January 28, 2017. *The Data That Turned the World Upside Down. How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election.* Vice. *https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win*
- Greenberg, Andy.: Forbes. Junio 6, 2013. *"Watch Top U.S. Intelligence Officials Repeatedly Deny NSA Spying on Americans Over the Last Year (Videos)".* Forbes. https://www.forbes.com/sites/andygreenberg/2013/06/06/watch-top-u-s-intelligence-officials-repeatedly-deny-nsa-spying-on-americans-over-the-last-year-videos/?sh=a770c3918d2f .
- Greenwald, G., MacAskill E., The Guardian. June 6th, 2013. *NSA Prism program taps into user data of Apple, Google and others.* The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

- Goldsmith, Jack, 22 de Marzo, 2014. *"The NYT on NSA's Huawei Penetration",* Lawfare blog. https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated
- Hannon, Elliot.: March 21st, 2018. *What Were the Trump Campaign's Ties to Cambridge Analytica?*. Slate. https://slate.com/news-and-politics/2018/03/what-were-the-trump-campaigns-ties-to-cambridge-analytica.html
- Helmore, Edward.: Tue, 20 Mar 2018. *David Carroll, the US professor taking on Cambridge Analytica in the UK courts.* The Guardian. https://www.theguardian.com/uk-news/2018/mar/20/david-carroll-cambridge-analytica-uk-courts-us-professor
- Hopkins, Nick; Borger, Julian; & Harding, Luke.: Thu 1 Aug 2013. *GCHQ: inside the top secret world of Britain's biggest spy agency*. The Guardian. https://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden
- Jack Goldsmith.: *22 de Marzo, 2014*. "The NYT on NSA's Huawei Penetration", *Lawfare blog*. https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated
- Kanter, J., & Kanter, J. Business Insider. June18th, 2018. *"Facebook is investigating another app created by Cambridge University academics after it hoovered up the data of millions of users"*. Business Insider. https://www.businessinsider.in/facebook-is-investigating-another-app-created-by-cambridge-university-academics-after-it-hoovered-up-the-data-of-millions-of-users/articleshow/64173953.cms
- Kranish, Michael.; Nov 9, 2018. *"How Brad Parscale, once a 'nobody in San Antonio,' shaped Trump's combative politics and rose to his inner circle"*. The Washington Post (Online), Washington, D.C. https://www.washingtonpost.com/politics/how-brad-parscale-once-a-nobody-in-san-antonio-shaped-trumps-combative-politics-and-rose-to-his-inner-circle/2018/11/09/b4257d58-dbb7-11e8-b3f0-62607289efee_story.html
- Lapowski, Issie.: November, 15th, 2016. *Here is how Facebook Actually won Trump the presidency.* Wired Magazine. https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news/

- Meredith, Sam.: Tue, Apr 10, 2018. *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal.* CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html
- Patel, Anjali May 11th 2021. *Explained: How pipeline hack triggered gas issues, how you can protect yourself.* https://wlos.com/news/local/explained-how-pipeline-hack-triggered-gas-issues-how-you-can-protect-yourself
- Pramuk, Jacob.: Thu, Jan 4th 2018. *"Trump lawyer demands a halt to publication of tell-all book, 'Fire and Fury,' seeks full retraction and apology*". CNBC. https://www.cnbc.com/2018/01/04/trump-lawyer-demands-a-retraction-over-michael-wolff-fire-and-fury-book.html
- Redacción BBC. 12 diciembre 2018. *Qué es el Brexit y otras 5 preguntas básicas para entender la salida de Reino Unido de la Unión Europea*. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-46521624
- Stewart, Emily. :*Why every website wants you to accept its cookies. Cookies alerts are supposed to improve our privacy online. But are they? https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy*
- TIME POLL June 13th, 2013: *Support for Snowden—and His Prosecution. 54% of respondents said the leaker, Edward Snowden, did a "good thing" in releasing information about the government programs.* https://swampland.time.com/2013/06/13/new-time-poll-support-for-the-leaker-and-his-prosecution/

Turton, W.; Riley, M.; Jacobs, J.: May 13, 2021. *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*. Bloomberg. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

Publicaciones legales y casos

- Califano, Bernardette.: Febrero, 2021. *Análisis del proceso de debate de iniciativas legales sobre protección de datos personales y sus conflictos con el derecho a la libertad de expresión. Los casos de Argentina y Ecuador.* Articulo 6 en la Ley 25.326. Universidad de Palermo. https://www.palermo.edu/Archivos_content/2021/cele/datos-personales-argentina-ecuador/Datos-personales-Argentina-y-Ecuador.pdf
- Caso Schrems https://epic.org/privacy/intl/schrems/
- De Groot, Juliana.: Tue Dec 1st, 2020. *What is the California Consumer Privacy Act?*. Digital Guardian. https://digitalguardian.com/blog/what-california-data-privacy-protection-act
- De Groot, Juliana.: Wed Sept 30th, 2020. *What is the General Data Protection Regulation? Understanding & Complying with GDPR Requirements in 2019*. Digital Guardian. https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection
- Descripción de la cuarta enmienda: https://www.govinfo.gov/content/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf
- FTC (Federal Trade Comission).: November 29, 2011. *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*. https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
- GDPR.: Novemberm 8th, 2016. *The Demise of Safe Harbor and Rise of Privacy Shield: How Can Personal Information Now Be Exported from the EU to the United States?* https://www.lexisnexis.com/lexis-practical-guidance/the-journal/b/pa/posts/the-demise-of-safe-harbor-and-rise-of-privacy-shield-how-can-personal-information-now-be-exported-from-the-eu-to-the-united-states
- GDPR (2). Mayo, 2018. *Lo que debes saber sobre el reglamento general de protección de datos.* Power Data. https://www.powerdata.es/gdpr-proteccion-datos

- Goldsmith, Jack.: 22 de Marzo, 2014. *"The NYT on NSA's Huawei Penetration",* Lawfare blog. https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated
- Guthrie Ferguson, Andre.: 2015. *"The internet of Things and the Fourth Amendment of Effects"*. California Law Review. https://papers.ssrn.com/abstract=2577944 .
- Hinley, Henry y Cocca, Aldo Armando.: Diciembre 2, 2014. *Capitulo 3: el universo jurídico de la comunicación* - Derecho a la Información - Cátedra: Duhalde. http://resumenes-comunicacion-uba.blogspot.com/2014/12/capitulo-3-el-universo-juridico-de-la.html
- La ley de "Opt-Out" se refiere a una clausula contenida dentro de varios acuerdos arbitrarios donde se permite a los consumidores rechazar información, publicidad, llamados, emails, o comunicaciones de marketing, sobre productos que no han sido solicitados. https://definitions.uslegal.com/o/opt-out-clause/
- Ley modelo de Acceso a la información administrativa. Secretaría general de la Organización de los Estados Americanos (OEA). https://www.oas.org/juridico/english/ley_modelo_acceso.pdf
- Masseno, Manuel David:. November 14th, 2019. *On The Waterfront: Personal And Non-personal Data At Both Eu Regulations.* En "Ley, tecnología e innovación". (Traducción por la autora de esta tesis). https://www.academia.edu/40925092/On_the_Waterfront_Personal_and_Non_Personal_Data_at_Both_EU_Regulations
- NSA Security Service. *What is SIGINT?*. https://www.nsa.gov/what-we-do/signals-intelligence/
- Smith vs Maryland, 442 US 735, 743 (1979) United States vs Leon 468 U.S.897 (1984); United States vs Calandra 414 U.S. 338, 354 (1974); Walder vs United States, 347 U.S. 62 (1954)

Películas y documentales

- ‘’The Great Hack’’ es un documental televisivo acerca del escándalo de datos Facebook-Cambridge Analytica. El documental se enfoca en el profesor Davir Carroll, la denunciante Brittany Kaiser (quien trabajaba con Christopher Wylei), y las investigaciones de la periodista Carole Cadwalladr en relación con la campaña Brexit, Facebook, Cambridge Analytica y la campaña de Donald Trump del 2016.

- “Snowden” es una película basada en el libro “Los archivos Snowden” (ver nota al pie 7) y “Los tiempos del pulpo” de Anatoly Kucherena donde se cuenta la historia de Snowden desde los comienzos de su carrera hasta las ultimas charlas que había presentado en publico luego de haber entregado los documentos secretos a los medios.