universidad de león

FACULTAD DE DERECHO

UNIVERSIDAD DE LEÓN

CURSO 2018/2019

EL EFECTO ORWELL EN LA SOCIEDAD EN RED: CIBERSEGURIDAD, RÉGIMEN GLOBAL DE VIGILANCIA SOCIAL Y DERECHO A LA PRIVACIDAD EN EL SIGLO XXI

THE ORWELL EFFECT IN THE NETWORK SOCIETY: CYBERSECURITY, SOCIAL SURVEILLANCE GLOBAL REGIME AND RIGHT TO PRIVACY IN THE 21ST CENTURY

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR: D. JOÃO PEDRO SEEFELDT PESSOA

TUTOR: D. SALVADOR TARODO SORIA

You have zero privacy anyway. Get over it.

Scoot McNealy, ex CEO de Sun Microsystems.

SPRENGER, Polly. *Sun of privacy:* 'get over it'. [Wired, 26/01/1999] [en línea] [Fecha de consulta: 05/07/2019] Disponible en: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

ÍNDICE

RESUMEN

EL EFECTO ORWELL EN LA SOCIEDAD EN RED: CIBERSEGURIDAD, RÉGIMEN GLOBAL DE VIGILANCIA SOCIAL Y DERECHO A LA PRIVACIDAD EN EL SIGLO XXI

Autor: JOÃO PEDRO SEEFELDT PESSOA
Tutor: SALVADOR TARODO SORIA

En la sociedad en red, el desarrollo de las tecnologías de la información y comunicación han creado nuevos retos relacionados con la libre circulación de datos, lo que hace necesario repensar el derecho a la privacidad. La investigación estudia la vigilancia y el derecho a la privacidad en la sociedad en red, problematizando en qué medida el régimen global de vigilancia social de datos personales puede afectar el derecho a la privacidad en el siglo XXI. El trabajo se divide en dos bloques: el primer sobre la vigilancia practicada por las redes de poder; y el segundo, sobre la alteración del paradigma del derecho a la privacidad hacia un régimen colectivo. Se concluye que el derecho a la privacidad ha sufrido por transformaciones desde una concepción clásica, hacia nuevas dimensiones, como el derecho a la autodeterminación informativa y a la protección de datos personales. En relación a la sociedad de vigilancia, el derecho a la privacidad puede ser utilizado como contravigilancia, exigiendo una actuación transparente, controlada y vigilada de los responsables y encargados del tratamiento de datos personales.

Palabras-clave: Sociedad en red. Ciberseguridad. Vigilancia social. Derecho a la privacidad. Derecho a la protección de datos personales.

ABSTRACT

THE ORWELL EFFECT IN THE NETWORK SOCIETY: CYBERSECURITY, SOCIAL SURVEILLANCE GLOBAL REGIME AND RIGHT TO PRIVACY IN THE 21ST CENTURY

Author: JOÃO PEDRO SEEFELDT PESSOA
Advisor: SALVADOR TARODO SORIA

In the network society, information and communication technologies have created new challenges related to the free movement of data, which makes it necessary to rethink the right to privacy. This research studies the surveillance and the right to privacy in the network society, problematizing the extent to which the global regime of social surveillance of personal data can affect the right to privacy in time of cybersecurity in the 21st century. The work is divided into two blocks, the first chapter about the surveillance carried out by networks of power and the second on about the paradigm shift from the right to privacy to a collective regime of protection. As for the methodology of approach, the deductive method is used: regarding the procedure, the monographic method is used. It is concluded that the right to privacy underwent transformations from a classical conception, having new dimensions in the network society, such as the right to informational self-determination and the protection of personal data. In relation to the surveillance society, it is perceived that the right to privacy can be used as a counter-vigilance, requiring a transparent, controlled and monitored action of those responsible and in charge of the processing of personal data.

Keywords: Networked society. Cybersecurity. Social surveillance. Right to privacy. Right to protection of personal data.

RESUMO

O EFEITO ORWELL NA SOCIEDADE EM REDE: CIBERSEGURANÇA, REGIME GLOBAL DE VIGILÂNCIA SOCIAL E DIREITO À PRIVACIDADE NO SÉCULO XXI

Autor: JOÃO PEDRO SEEFELDT PESSOA
Orientador: SALVADOR TARODO SORIA

Na sociedade em rede, as tecnologias de informação e comunicação criaram novos desafios relacionados à livre circulação de dados, o que torna necessário repensar o direito à privacidade. A pesquisa estuda a vigilância e o direito à privacidade na sociedade em rede, problematizando em que medida o regime global de vigilância social de dados pessoais pode afetar o direito à privacidade em tempo de cibersegurança no século XXI. O trabalho é dividido em dois blocos, sendo o primeiro capítulo sobre a vigilância perpetrada pelas redes de poder e o segundo sobre a alteração de paradigma do direito à privacidade para um regime coletivo de proteção. Quanto à metodologia de abordagem, utiliza-se o método dedutivo: quanto ao procedimento, emprega-se o método monográfico. Conclui-se que o direito à privacidade passou por transformações desde uma concepção clássica, possuindo novas dimensões na sociedade em rede, como o direito à autodeterminação informativa e à proteção de dados pessoas. Em relação à sociedade de vigilância, percebe-se que o direito à privacidade pode ser usado como contravigilância, exigindo uma atuação transparente, controlada e vigiada dos responsáveis e encarregados do tratamento de dados pessoais.

Palavras-chave: Sociedade em rede. Cibersegurança. Vigilância social. Direito à privacidade. Direito à proteção de dados pessoais.

INTRODUCCIÓN

En la sociedad en red, nuevos actores sociales y nuevas relaciones sociales se entremezclan, de modo transversal y multidireccional, proporcionando un mayor flujo de comunicación y una distribución nodal de interacciones, incluso en lo que se refiere a las relaciones de poder. Las redes, formadas por nodos, aristas y *clusters*, compiten o cooperan entre sí, marcadas por el uso de nuevas tecnologías de la información y de la comunicación, en una horizontalización de la comunicación a gran escala, a medida que las nuevas plataformas permiten una interacción expansiva, sin la necesaria intervención de canales de comunicación o liderazgos.

La evolución tecnológica y la globalización han creado nuevos desafíos relacionados con la privacidad y la protección de los datos personales, ya que, en el horizonte del *Internet de las Cosas* y del *Internet de Todo*, la recogida, el tratamiento y el intercambio de datos registraron un aumento significativo, permitiendo que las corporaciones privadas y las instituciones públicas utilicen los datos personales en una escala sin precedentes durante el ejercicio de las actividades de las actividades cotidianas. Por otro lado, las personas suministran cada vez más su información, de manera pública y global, teniendo en cuenta que la disponibilidad de los datos personales es condición para el acceso de productos y servicios en la sociedad en red.

En el siglo XX, con la profusión de las tecnologías de información y comunicación, los mecanismos de control y vigilancia, especialmente estatales, se perfeccionaron y se convirtieron en herramientas útiles para una vigilancia general y diseminada, de forma institucional. En la sociedad en red, la vigilancia es líquida, omnipresente y, a veces, pasa desapercibida por los vigilados, ejerciendo sobre éstos un control sobre las formas de vivir. Y, en sentido inverso, los sujetos acaban renunciando a derechos y garantías fundamentales, en particular, a la privacidad, al suministrar información personal que les es exigida para acceder a productos y servicios, contribuyendo a una economía de vigilancia y circulación de datos, muchas veces sin verdadera conciencia de las implicaciones y de los impactos de esa subjetivación tecnológica.

OBJETO DEL TRABAJO

La presente investigación tiene por objeto el estudio acerca de la vigilancia social y la privacidad en la sociedad en red. Se pretende analizar la resignificación del derecho a la privacidad afectado por el régimen global de vigilancia social de datos personales en el contexto de la ciberseguridad del siglo XXI, en razón de la alteración de paradigma producida por el avance de las nuevas tecnologías de la información y comunicación.

El objetivo general de este trabajo es analizar los impactos de las tecnologías de información y la comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI. En lo que se refiere a los objetivos específicos, se pretende: a) investigar las implicaciones del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; b) identificar la contribución de las personas en dicho régimen global de vigilancia social a partir del suministro de datos para el acceso a productos y servicios; c) establecer la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y, finalmente, d) discutir la resignificación del derecho a la privacidad, basada en nuevos conceptos, nuevos espacios, nuevos límites y nuevas posibilidades en el contexto de la ciberseguridad.

La actualidad del tema está presente, porque el trabajo aborda discusiones de la posmodernidad y de la sociedad en red, panorama sociopolítico actual, marcado por el flujo continuo de informaciones entre sujetos y multitudes digitalmente conectadas, especialmente considerando los impactos de las nuevas tecnologías de información y la comunicación sobre los derechos y garantías fundamentales, que se mejoran y perfeccionan cada día. Sin embargo, se percibe que el derecho a la privacidad, uno de los pilares de los derechos fundamentales, está pasando por cambios, incluso de paradigma, en razón de la producción y suministro de datos personales en la red.

Además, el trabajo trata detalladamente del derecho a la privacidad y otras dimensiones derivadas, cuyo bien jurídico protegido ha sido recientemente tutelado por el Reglamento General de Protección de Datos de la Unión Europea, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por la que se deroga la Directiva 95/46 / CE, con aplicación obligatoria a partir de mayo de 2018, en atención a nuevos avances de las

tecnologías de la información y comunicación. En cuanto a España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se encargó de adaptar la normativa comunitaria en el territorio nacional.

La investigación pone de relieve las implicaciones sociales y doctrinales, teniendo en cuenta que el propio Reglamento pone relevancia en el hecho de que los principios y las reglas en materia de protección de las personas físicas en relación con el tratamiento de sus datos personales, independientemente de la nacionalidad o el lugar de residencia de dichas personas, deben respetar los derechos y libertades fundamentales. Así, cada vez más se hace necesario abordar la problemática del derecho a la privacidad frente a los avances de las tecnologías de información y comunicación, formando profesionales capaces de reflexionar críticamente sobre la materia.

Por último, la presente investigación se desarrolla en el ámbito del Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital de la Universidad de León, dado que una competencia a ser desarrollada por los estudiantes de ese curso es justamente conocer el sistema de fuentes, derechos y libertades fundamentales y los principios básicos del Derecho de la Ciberseguridad y del Entorno Digital, sabiendo integrar conceptos multidisciplinares para poder analizar, interpretar y resolver problemas y conflictos jurídicos, políticos y sociales que surgen en ese campo. En esa misma perspectiva, el proyecto se encuadra en el marco de cooperación entre la Fundación Carolina e INCIBE, ya que uno de los objetivos de esa institución, para enfrentar los desafíos planteados por los avances de las tecnologías de información y comunicación, es justamente intentar satisfacer adecuadamente la demanda social de profesionales altamente calificados en las normativas sobre ciberseguridad y entorno digital.

METODOLOGÍA

El recorrido metodológico del presente trabajo debe pasar, en vista de los objetivos a ser atendidos y del problema de investigación, por cuatro momentos: a) investigación preliminar sobre la temática del régimen global de vigilancia social por parte de las agencias institucionales; b) investigación preliminar sobre la temática de la vigilancia, pero desde el punto de vista de las personas físicas y colectivos: c) revisión de conceptos y normativas relativas al derecho a la privacidad y sus dimensiones, especialmente tratados internacionales, reglamentos comunitarios y leyes específicas; y, d) un debate más profundo sobre el derecho a la privacidad en la sociedad de vigilancia.

En cuanto a la metodología de abordaje, se utiliza el método deductivo, porque se realiza una conexión descendente entre los temas tratados, partiéndose de un plan general y premisa general para proceder al análisis de panoramas específicos, a fin de obtener una conclusión a partir de ese silogismo lógico. En otras palabras, se investiga, primero, el ascenso de una sociedad basada en una economía de datos, que permite la vigilancia de actores sociales por parte de agencias institucionales y por parte de grandes corporaciones, para posteriormente verificar cómo ese nuevo paradigma afecta al derecho a la privacidad.

En cuanto a la metodología de procedimiento, se utiliza el método de revisión y bibliográfica, con el objetivo de estudiar la vigilancia social, desde el punto de vista de la razón gubernamental dominante y también del tratamiento de datos personales por las grandes corporaciones, para analizar detalladamente el derecho a la privacidad en el siglo XXI. Para ello, a través del estudio científico de actores sociales, procesos comunicativos y factores organizativos de esta nueva sociedad en red involucrando la vigilancia de datos, se pretende obtener conclusiones sobre el tema e investigar críticamente los efectos en el derecho a la privacidad.

Para ello, se pretende aplicar las técnicas de investigación de documentación indirecta y documentación directa. Así, se utiliza la investigación documental y bibliográfica, considerando que gran parte de la revisión bibliográfica realizada en el presente estudio se centra en la literatura especializada en el tema, especialmente sobre derecho a la privacidad y los efectos de los nuevos paradigmas sociales sobre derechos y garantías fundamentales; otra parte vendrá de normativas internacionales, comunitarias y nacionales, así como de noticias y trabajos científicos realizados sobre la temática, entre otras.

El marco teórico de base adoptado se sirve de las construcciones de, principalmente, Michel Foucault (vigilancia como panóptico de poder), Gilles Deleuze (datos y vigilancia en la sociedad de control), Gleen Greenwald (régimen de vigilancia global), Zigmunt Bauman (vigilancia en la post-modernidad y post-panóptico), Manuel Castells (sociedad en red), Stefano Rodotà (privacidad en la sociedad de vigilancia), entre otros; ya que se intenta analizar el impacto del avance de las tecnologías de información y la comunicación en la comunidad global, evidenciando las relaciones de vigilancia características de la sociedad en red basadas en el tratamiento de datos personales, así como analizando el impacto de ese nuevo paradigma en el derecho a la privacidad

En términos estructurales, la investigación está desarrollada en dos grandes capítulos, demostrando la relación existente entre la premisa general y específica. En el primer capítulo, el primer apartado trata sobre el panóptico del siglo XXI y la vigilancia realizada por las agencias de seguridad nacionales; el segundo aborda la contribución de los usuarios para la provisión de datos para acceso a productos y servicios. Por otro lado, el segundo capítulo también está subdividido en dos grandes bloques: el primero analiza la evolución del derecho a la privacidad hasta el derecho a la protección de datos personales; el segundo reflexiona sobre el cambio del paradigma del derecho a la privacidad hacia un régimen colectivo de protección.

1. “EL GRAN HERMANO TE VIGILA”: LA VIGILANCIA SOCIAL Y LOS DATOS EN LA SOCIEDAD EN RED DEL SIGLO XXI

El título del presente capítulo hace referencia a una de las frases más conocidas de la obra “1984”, de George Orwell: “El Gran Hermano te vigila”, significando la vigilancia marcada de Oceanía, escenario de fondo para las reflexiones del personaje principal, Winston Smith. En la ciudad en que pasa la historia, hay carteles enormes, en diferentes lugares, con una imagen del Gran Hermano, líder del Partido, para recordar en todo momento que los ciudadanos están siendo vigilados y deben comportarse según lo determinado por las fuentes de poder.

La frase - y la propia historia referenciada - es oportuna para el presente capítulo, ya que el avance de las tecnologías de la información y comunicación, especialmente de la microelectrónica y de la nanoelectrónica, han posibilitado la creación de mecanismos de vigilancia de los ciudadanos, a partir de la interceptación de los datos personales que, a su vez, pueden ser entendidos como el oro de esta nueva arquitectura social surgida después del final de la Segunda Guerra Mundial, ya que el suministro de la información personal es condición para el acceso y la participación en la sociedad en red.

Considerando que el objetivo general de este trabajo es analizar los impactos de las tecnologías de información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI, este capítulo, como forma de introducir premisas generales sobre el tema, pretende: a) investigar las implicaciones del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; y b) identificar la contribución de las personas en dicho régimen global de vigilancia social a partir del suministro de datos para el acceso a productos y servicios.

1.1. LA BÚSQUEDA DEL ORO DEL SIGLO XXI: EL RÉGIMEN GLOBAL DE VIGILANCIA SOCIAL

El poder puede ser entendido como una práctica social construida a lo largo del tiempo, de forma heterogénea y dinámica, como resultado de una relación de fuerzas en una determinada sociedad, en un determinado momento, estando disuelto por todo el tejido social, siendo ejercido por medio de los dispositivos, es decir, caminos, formas y medios de

ejercicio del poder, como el castigo, la disciplina, la sexualidad, la locura, el examen[1]. A partir del siglo XVIII, la vigilancia se transformó en uno de los principales dispositivos para el ejercicio del poder, siendo, a lo largo del tiempo, amplificada y perfeccionada, con el objetivo de imprimir procesos de coerción sobre los sujetos vigilados[2].

1.1.1. Del panoptismo a la vigilancia como dispositivo de poder

En la sociedad disciplinar - el "tiempo de las disciplinas" -[3], los dispositivos de poder, entre ellos, utilizados en las instituciones totales - familia, escuela, cuartel, fábrica, hospital y prisión -, lograban vigilar y castigar a los individuos, en el intento de domesticar y someter los sujetos a moldes predefinidos y utilitaristas, en una especie de disciplina y control sobre el cuerpo[4]. El panoptismo, inspirado en el modelo de Jeremy Bentham, fue, entonces, el arquetipo arquitectónico ideal del "tiempo de las disciplinas", ya que, a través de técnicas ópticas y solares, especialmente en composiciones circulares, como prisiones, fábricas y manicomios, era posible crear una vigilancia literalmente institucional[5]. En ese modelo, el individuo sujeto a la disciplina entendía y propiamente visualizaba que estaba siendo permanentemente vigilado, aunque no siempre lo estaba de verdad, pero saber que podría estar siendo vigilado por alguien ya era suficiente para mantener la disciplina y el control, en un "funcionamiento automático del poder"[6].

En la segunda mitad del siglo XVIII, tras la profusión de las medidas disciplinarias, el ejercicio del poder, que antes estaba limitado al cuerpo-individuo en un espacio-tiempo definido, pasó a ser dirigido a una multiplicidad de cuerpos, por medio de procedimientos colectivos, en una biopolítica dirigida al cuerpo-población como masa modular[7]. Es decir, la idea no era sólo moldear al individuo en sí, sino modular una colectividad, para un mayor

---

[1] FOUCAULT, Michel. *Microfísica do poder*. 23 ed. São Paulo: Graal, 2004 [versión española: FOUCAULT, Michel. *Microfísica del poder:* genealogía del poder. Madrid: La Piqueta, 1978].
[2] FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013, p. 196 [versión española: FOUCAULT, Michel. *Vigilar y castigar:* nacimiento de la prisión. Ciudad del México: Siglo XXI, 2012].
[3] Ibid., p. 196.
[4] Ibid., pp. 197-198.
[5] BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: TADEU, Tomaz (Org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008, 17-30.
[6] FOUCAULT, 2013, op. cit., pp. 224-225.
[7] FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005, pp. 285-289. [versión española: FOUCAULT, Michel. *Hay que defender la sociedad:* curso del Collège de France (1976). Madrid: Akal, 2003].

control, de modo que, para ese fin, los dispositivos de poder deberían adaptarse, la vigilancia debería acompañar los nuevos desafíos, incluso como una táctica de guerra[8].

1.1.2. La revolución de las TICs y el régimen global de vigilancia social

Con el final de la Segunda Guerra Mundial, un sin número de transformaciones ayudaron al cambio de paradigma social, ya que cayeron los muros y las fronteras, permitiendo un flujo de interacciones entre actores sociales en un campo abierto[9]. La vigilancia sufrió intensos cambios y se perfeccionó proporcionalmente a la evolución de las tecnologías de información y comunicación, tornándose horizontalizada (no más verticalizada) y difundiéndose por innumerables campos de captación y actuación (no sólo instituciones cerradas), para afectar al mayor número de cuerpos de interés[10].

Durante el conflicto internacional mencionado, agencias estatales y organizaciones de diferentes países, especialmente Reino Unido y Estados Unidos, interceptaron, leyeron y analizaron diversas informaciones intercambiadas por las tropas alemanas y japonesas, creando desde el final de la guerra una red planetaria de inteligencia para escucha y captación de señales, desarrollada a través del Tratado de Seguridad UK-USA (también grafado UKUSA, remitiéndose a las iniciales de los países involucrados). Este acuerdo y la conjetura desarrollada contó con la ayuda de los "Cinco Ojos": Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos; siendo sólo revelado al final del siglo XX y confirmado a principios del siglo XXI[11].

Por lo tanto, el marco de cooperación de inteligencia secreta UKUSA, liderado sustancialmente por la Agencia de Seguridad Nacional de los Estados Unidos (*National Security Agency*, en inglés), entidad también mantenida en secreto por décadas, hizo crear

---

[8] FOUCAULT, 2005, op. cit., pp. 293-294,

[9] DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992, p. 220 [versión española: DELEUZE, Gilles. *Conversaciones.* Valencia: Pre-textos, 1995].

[10] PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. Director: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Universidade Federal de Santa Maria, Departamento do Direito, Santa Maria, 2018, p. 41.

[11] GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014 [GREENWALD, Gleen. *Sin un lugar donde esconderse*: Edward Snowden, la NSA y el Estado de Vigilancia en los Estados Unidos. Barcelona: Ediciones B, 2014]. NORTON-TAYLOR, Richard. *Not so secret: deal at the heart of UK-US intelligence*. [The Guardian, 25/06/2010]. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

un sistema de vigilancia global, denominado *Echelon,* con capacidad para captar y analizar virtualmente informaciones provenientes de llamadas telefónicas y mensajes de fax, télex, correo electrónico y otros dispositivos, enviados desde cualquier lugar del mundo[12]. Se trató, pues, de una red de espionaje, que, por interceptación, capta el tráfico de datos ocurrido por satélite, fibra óptica, frecuencia de radio, microondas, cables submarinos, internet y otras formas de procesamiento de información y comunicación, aunque hay un avance en las técnicas de encriptación.

Conforme a una investigación realizada por el Parlamento Europeo, divulgada en el Informe de 11 de julio de 2011, en el marco del sistema Echelon, datos brutos de comunicación captados por las agencias de inteligencia, tanto de voz, télex, fax e internet, pudieron ser interceptados, registrados, analizados, intercambiados, vendidos y clasificados por medio de filtros, permitiendo la elaboración fácil de perfiles y otros informes por las partes interesadas[13].

Los informes elaborados dan cuenta de que los programas de vigilancia global en masa se perfeccionaron durante el siglo XX, imprimiendo importantes avances tecnológicos para el sistema de inteligencia de señales[14]. En síntesis, se puede decir que, en la década de los 40, cuando el acuerdo de cooperación fue establecido, el objetivo principal de la vigilancia fue el espionaje militar y diplomático; en la década de los 60, el objetivo fue el espionaje comercial e industrial, pasando por sectores económicos y científicos; en la década de los 90, fue el combate contra el crimen organizado, el lavado de dinero, el tráfico de drogas, armas y personas y, más recientemente, y en los próximos años, el combate contra el terrorismo[15].

En 2006, Julian Assange, periodista y ciberactivista, constituyó la WikiLeaks, una organización transnacional en favor de la transparencia, a fin de publicar informaciones y datos confidenciales, especialmente sensibles, filtrados o hackeados de gobiernos u otras instituciones para que fueran objeto de conocimiento, acceso y crítica públicos[16]. Assange

---

[12] UNIÓN EUROPEA. *Parlamento Europeo. Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).* [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES.

[13] Ibid.

[14] Ibid.

[15] GREENWALD, op. cit.

[16] WIKILEAKS. *What is WikiLeaks*. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://wikileaks.org/What-is-Wikileaks.html.

defiende la figura de los *cypherpunks*, los que "defienden la utilización de la criptografía y de métodos similares como medio para provocar cambios sociales y políticos", de forma que "creado a principios de los años 1990, el movimiento alcanzó su auge durante las 'criptoguerras' y después de la censura de internet en 2011, en la Primavera Árabe" [traducción libre][17].

En 2010, Chelsea Manning, en la época, Bradley Manning, suministró a WikiLeaks más de 700.000 archivos secretos, vídeos de enfrentamientos y comunicaciones diplomáticas del Departamento de Estado de los Estados Unidos, siendo detenida en 2013 en una penitenciaría militar y sometida a técnicas de privación de sueño, desnudez forzada y tortura psicológica, detención considerada inhumana e ilegal por Amnistía Internacional[18]. La activista fue llevada a juicio y condenada a 35 años de prisión, pero el ex presidente de Estados Unidos, Barack Obama, conmutó su sentencia antes de dejar el cargo en 2017[19].

En 2013, Edward Snowden, analista de sistemas hasta entonces funcionario del gobierno estadounidense, hizo público una gran cantidad de informaciones confidenciales sobre la existencia y actuación de la Agencia Nacional de Seguridad de Estados Unidos, así como sobre los programas que componen un sistema de vigilancia global americano, entre ellos el PRISM[20]. En detalle, Snowden viajó a Hong Kong en mayo de 2013, donde entregó documentos probatorios a los periodistas Glenn Greenwald y Laura Poitras, los cuales fueron revelados por los portales *The Guardian*, *The Washington Post* y *The Intercept*, generando una crisis institucional y una incomodidad global, tanto que el activista vive actualmente bajo asilo político[21].

A partir de 2013, con la filtración de documentos ultrasecretos, se descubrió la existencia de otros programas de vigilancia global, tanto en el marco del sistema Echelon, es decir, vinculados a él o sometidos a él, o no. Por ejemplo, *PRISM*, de Estados Unidos, Australia, Reino Unido y Países Bajos; *XKeyscore*, de Estados Unidos, Alemania, Australia y Nueva Zelanda; *Project 6*, de Alemania y Estados Unidos; *Stateroom*, de Cinco Ojos; *Lustre*, de Estados Unidos y Francia; *Optic Nerve*, de Estados Unidos y Reino Unido;

[17] ASSANGE, Julian. *Cypherpunks*: liberdade e futuro da internet. São Paulo: Boitempo, 2013, p. 5. [versión española: ASSANGE, Julian. Cypherpunks: la libertad y el futuro de internet. Barcelona: Deusto S.A., 2013].
[18] AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] [en línea] [Fecha de consulta: 10/04/2019] Disponible en: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html.
[19] Ibid.
[20] GREENWALD, op. cit.
[21] GREENWALD, op. cit.

Turbine, de Estados Unidos, Reino Unido y Japón; *Operation Socialist*, de Reino Unido; *Tempora, Muscular, Follow The Money, Marina, Dishfire, Mystic*, estos todos de Estados Unidos, pudendo haber o no coordinación con otras agencias asociadas[22].

Los Estados Unidos, en el seno de la *National Security Agency*, admitieron tener dos programas: *PRISM* y *UPSTREAM.* PRISM es un programa de inteligencia que permite la obtención de material de inteligencia solicitado junto a los proveedores de servicios (desde que previa intervención judicial que debe autorizar la intervención), de manera detallada y direccionada, aunque sin gran capacidad de *data mining*, estando regulado por el *Foreign Intelligence Service Act* (FISA)[23]. Por su parte, UPSTREAM es un programa de inteligencia que recoge datos oriundos de comunicación por cables de fibra óptica e infraestructura de los proveedores de servicio, el cual permite acceso a los datos globales, incluso de ciudadanos no americanos[24].

El Reino Unido, a través de la agencia *Government Communications Headquarters*, con la sigla GCHQ, confirmó operar con el programa denominado *Tempora*, que hace posible el acceso y almacenamiento informaciones de datos de portadores.[25] El programa permite comparar el tráfico de datos con un rol de selecciones y búsquedas predeterminadas de un objeto específico para realizar una clasificación de la comunicación realizada[26]. La agencia argumenta que el sistema es refrendado por el *Regulation of Investigatory Powers Act 2000 (RIPA),* legislación interna que permite que el Secretario de Estado expida órdenes de interceptación de comunicaciones[27].

Importante tratar sobre otros tres de estos programas para comprender la magnitud del monitoreo de datos. Así, *XKeyscore*, uno de los primeros sistemas informáticos operados por la *NSA* y compartido con Alemania, Australia y Nueva Zelanda, en la forma de un motor de búsqueda, permite, según Snowden que ya tuvo autorización para acceder a él, la

---

[22] PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. *Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales*, Universidad de Barcelona, n.º 183, abr. 2014. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16.

[23] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15).* Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

recuperación de datos de todos los registros recolectados diariamente en todo el mundo, disponiendo de herramientas capaces de captar todo lo que los usuarios hacen en la red[28].

Por otra parte, el programa *Lustre*, dirigido especialmente por la *Direction Générale de la Sécurité Extérieure - DGSE*, agencia de seguridad de Francia, con cooperación de los Cinco-Ojos, especialmente de la *NSA*, se basa en la posición geoestratégica en el tráfico de datos electrónicos, puesto que la mayoría de los cables submarinos de comunicaciones que conecta África adentra al continente europeo por el territorio francés, de modo que el *DGSE* puede interceptar los datos transmitidos y compartirlos con sus socios[29]. Por último, el programa *Stateroom*, creado por las agencias de seguridad de Estados Unidos, Canadá, Australia y el Reino Unido, es un proyecto de interceptación global masiva basada en operaciones en más de ochenta embajadas y consulados estadounidenses repartidos por el globo, que, a través de un *exploit*, generado a partir de la infección de más de 50.000 (cincuenta mil) redes de comunicaciones en todo el mundo por un *malware* de vigilancia masiva, puede interceptar mensajes en cualquier momento, independientemente del conocimiento del usuario[30].

Además de agencias de seguridad e inteligencia de los países referidos, se verificó que importantes universidades también estuvieron involucradas en el proyecto para proveer bases científicas para tales programas de vigilancia, como, por ejemplo, *University of California, Stanford University, Massachusetts Institute of Technology (MIT), University of California Berkeley, California Institute of Technology (Caltech)* y *Johns Hopkins University*. Más aún, documentos secretos mostraron la cooperación y suministro de informaciones por parte de empresas y organizaciones de sectores económicos, como *Google, Facebook, Microsoft, Apple, Verizon, Vodafone, EDS, AT&T, Qwest, Motorola, Intel, IBM, Qualcomm, Cisco, H-P, Oracle*, entre otras[31].

[28] GREENWALD, op. cit.
[29] FOLLOUROU, Jacques. *Surveillance*: la DGSE a transmis des données à la NSA américaine. [Le Monde, 30/10/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.
[30] DERIX, Steven. MODDERKOLK, Huib. *50.000 pakketjes kwaardaardige software*. [NRC, 23/11/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.nrc.nl/nieuws/2013/11/23/50000-pakketjes-kwaardaardige-software-1316266-a1157982.
[31] GREENWALD, op. cit., p. 83.

1.1.3. El régimen global de vigilancia social en los discursos de legitimación

A través de las sistemáticas revelaciones, se observan extensas y complejas redes de cooperación y de competencia entre agencias de seguridad e inteligencia estatales, especialmente localizadas en países desarrollados, con el objetivo de interceptar, analizar, almacenar y monitorear informaciones y comunicaciones entre individuos, grupos, instituciones, corporaciones, empresas y gobiernos alrededor del globo. La principal justificación para la creación de zonas de excepción para permitir el monitoreo de informaciones y comunicaciones de la población de forma inconmensurable es la lucha contra el terrorismo, ya que, con la vigilancia electrónica realizada, es posible identificar redes de cooperación, anticipar actos terroristas y prevenir los crímenes resultantes.

Al respecto, la "guerra contra el terror", hace que las naciones de todo el mundo actúen buscando enemigos, especialmente a partir de 2001, luego de los atentados terroristas del 11 de septiembre en Estados Unidos. Oportunamente, el gobierno norteamericano dispuso y, con el tiempo, recrudeció, una política estratégica de antiterrorismo, con la formación de alianzas o con el mando de iniciativas de otros países en el marco del Consejo de Seguridad de las Naciones Unidas, de la Organización del Tratado del Atlántico Norte y de la Organización de los Estados Americanos, en contra de aquel enemigo común, el terror, aunque este enemigo, tácticamente, cambie para redes terroristas, para países financiadores del terrorismo o para gobiernos paralelos terroristas[32].

Documentos expuestos por los movimientos contravigilantes revelaron que el discurso del terrorismo parece ser mucho más una justificación para acciones tomadas con fines oscuros y una táctica gubernamental para infligir miedo social. Es decir, “un porcentaje importante de los programas no tenía nada que ver con la seguridad nacional”, ya que “los documentos no dejaban dudas de que la NSA practicaba también espionaje económico y diplomático, además de la vigilancia de poblaciones enteras sin base para sospechas” [traducción libre][33]. En virtud de ese miedo al terrorismo, la población, preocupada por la seguridad interna, acepta el ideal vigilante y, que pese a que tales programas de vigilancia hayan sido pensados en escala global, las innovaciones tecnológicas y el flujo de personas, permitieron monitoreo doméstico de ciudadanos, ya que la amenaza también puede ser interna.

[32] GREENWALD, op. cit., p. 74.
[33] GREENWALD, op. cit., p. 75

De este modo, una guerra justa se encuentra justificada por sí misma, aunque banaliza, por un lado, quién es el enemigo, puesto que cualquiera puede ser objeto de vigilancia, pero también, por otro lado, absolutiza al enemigo, ya que la amenaza al orden es permanente y debe ser constantemente combatida y aniquilada[34]. La guerra al terror se convierte, así, en un completo estado de excepción en tonos de guerra global permanente como fondo, exigiendo a las naciones que estén preparadas y combativas, anticipando, vigilando, actuando ante cualquier movimiento sospechoso en el juego del poder[35].

Además, los periodistas revelaron que las agencias de seguridad no sólo trabajan para romper los códigos de las conversaciones privadas de los individuos, sino también para boicotear la propia seguridad de la información para facilitar la vigilancia de la información, como, por ejemplo, el caso de la NSA que intenta obligar a que grandes compañías crearan *backdoors* en los códigos de criptografía de las redes sociales para permitir el acceso y manipulación de las informaciones dejadas por los usuarios, hecho este que la agencia alega tratarse de medida de seguridad contra ataques terroristas[36]. Se visualiza, entonces, una dicotomía de personajes públicos, a medida que, por un lado, "Assanges", "Mannings" y "Snowdens", que revelan la existencia de programas de vigilancia, son considerados villanos, mientras que "Gates", "Jobs" y "Zuckerbergs", que contribuyen, con sus plataformas, a esos sistemas, son considerados héroes de la tecnología.

1.1.4. La relevancia del *big data* y la toma de decisiones basadas en datos

En este contexto, se opera la obtención a gran escala de una cantidad exorbitante de datos, la cual tiene especial importancia, ya que, a partir de la recolección, del almacenamiento, de la manipulación y de la transferencia de dichos datos, es posible crear patrones y vigilar a individuos y masas. En este sentido, *big data* es una grandeza informacional, producida y suministrada por los usuarios de las redes sociotécnicas, cuya manipulación permite, por parte de corporaciones y gobiernos, "analizar, procesar y gestionar un conjunto de datos extremadamente grandes que pueden ser analizados

[34] HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012, p. 31 [versión española: HARDT, Michael; NEGRI, Antonio. *Imperio.* Barcelona: Paidos Iberica, 2005].
[35] HARDT, NEGRI, op. cit., p. 34.
[36] McCARTHY, Tom. *NSA director defends plan to maintain 'backdoors' into technology companies.* [The Guardian, 23/02/2015] [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies.

informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación a la conducta humana y a las interacciones de los usuarios"[37].

Aunque el concepto de *big data* sea relativamente nuevo y no tan difundido socialmente, ya es posible identificar al menos cinco aspectos que involucran esa grandeza, conocidos como "cinco Vs": *volumen, velocidad, variedad, veracidad* y *valor*. El *volumen* hace referencia a la cantidad de datos producidos, estimándose en la casa de *exabytes* y *zettabytes* diariamente; la *velocidad* se refiere a que la manipulación de tales datos se da en tiempo muy hábil y simultáneo; la *variedad* quiere decir sobre la diversidad de datos que se recogen; la *veracidad* asimila que el procesamiento de estos datos debe garantizar la confiabilidad e integridad de ellos; y, por último, el *valor* se refiere a los beneficios significativos provenientes del procesamiento de los datos recopilados[38].

De acuerdo con el estudio *The Economic Value of Data: discussion paper*, del Ministerio de Finanzas del Reino Unido, la explotación de datos, según lo previsto por la Unión Europea y la Organización para la Cooperación y el Desarrollo Económico, va, cada vez más, a generar valor público y privado[39]. La toma de decisiones basada en el procesamiento de datos (*data-driven decisión)* es capaz de mejorar el rendimiento, la productividad y la rentabilidad de las empresas, así como capaz de incrementar la eficiencia de los productos y servicios públicos, los datos poseen el potencial de agilizar y personalizar métodos y técnicas de negocios[40].

En ese ínterin, diversos mecanismos contribuyen a la recogida y almacenamiento de datos informativos de usuarios en la red, destacándose, entre otros, las *cookies*, *web beacons*, *spywares*, *tagging y tracking*. Por medio de tecnologías de todo tipo, incluso de técnicas de *doxxing* y *hacking*, es posible crear perfiles de usuarios, identificar cuáles y cuántos usuarios están involucrados en red y mapear cómo ocurre el comportamiento de esas personas.

---

[37] REAL ACADEMIA ESPAÑOLA. Diccionario del español jurídico. *Big data.* [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://dej.rae.es/lema/big-data.

[38] FERNÁNDEZ, Déborah. *Las cinco V's del Big Data.* [DataHack, 27/08/2018] [Fecha de consulta: 20/04/2019] Disponible en: https://www.datahack.es/cinco-v-big-data/.; TAURION, Cezar. *Volume, variedade, velocidade, veracidade e valor:* os cinco Vs do Big Data. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data.

[39] REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. p. 04-07. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

[40] Ibid.

Actualmente, estos mecanismos están dispersos en diversos ambientes y espacios, a través de los dispositivos móviles personales inteligentes, utilizados alrededor del globo por miles de millones de personas, como, por ejemplo, teléfonos móviles, *tablets*, ordenadores portátiles, relojes, televisores, entre otros.

Ante todo esto, es posible deducir que la sociedad actual vive bajo un superpanóptico, que tiene en el panoptismo analizado por Jeremy Bentham y Michel Foucault un modelo de inspiración, un punto de partida - ya que esas ideas de domesticación y disciplina del cuerpo todavía subsisten - pero esta técnica de biopoder sobrepasa progresivamente todos los límites ya pensados, a la medida del perfeccionamiento de las tecnologías de información y comunicación, ya que "lo que cuenta es que estamos al principio de algo" [traducción libre][41].

1.1.5. El Estado de vigilancia: la vigilancia social pública frente a los derechos humanos y garantías

En la doctrina del derecho administrativo, se impone la supremacía del interés público sobre los intereses privados y particulares, como propia razón de existir de la Administración Pública, que debe actuar orientada al bien de la colectividad. Bajo el temor generado por la guerra al terror, los gobiernos justifican esa vigilancia en masa en expresiones tales como: "seguridad nacional", "defensa nacional", "situaciones de emergencia", "mantenimiento de la paz", "garantía de la ley y del orden", "prevención de la práctica de infracciones", "garantía de la integridad territorial", "defensa de la soberanía" y otros sinónimos; de manera que, aunque inicialmente entendidos como limitación a la potestad del Estado para garantizar derechos y libertades humanas y fundamentales; hoy, en día, son resignificados.

En el ámbito comunitario europeo, el derecho a la privacidad, previsto como un derecho humano desde el final de la Segunda Guerra Mundial, tiene limitaciones ya definidas en el propio ordenamiento, lo que, por sí solo, constituye el fundamento de los programas de vigilancia social, bajo las expresiones antes mencionadas[42]. Sobre el derecho al respeto a la vida privada y familiar, la Convención menciona que puede haber injerencia de autoridad

[41] DELEUZE, op. cit., p. 225
[42] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950*, p. 11. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

pública en los casos de "seguridad nacional, para la seguridad pública, para el bienestar económico del país, la defensa del orden y la prevención infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y libertades de terceros"[43].

Sin embargo, en septiembre de 2018, en importante posicionamiento judicial aún pasible de revisión vía recurso, la Corte Europea de Derechos Humanos juzgó el caso intitulado *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15),* propuesto por diversas entidades, entre ellas *Big Brother Watch,* en contra del Reino Unido, sede de la GCHQ[44]. En ese caso, el Tribunal ponderó que, aunque los programas de vigilancia están dentro del margen de aplicación de los Estados y se justifican en las excepciones existentes, la forma en que fueron y vienen siendo desarrollados por las agencias de seguridad puede violar los derechos fundamentales de los administrados, debido a la falta de supervisión pública del proceso de interceptación, a la falta de garantías adicionales a sectores específicos que pueden ser objeto de investigación y a la falta de publicidad relacionada con los programas. Pudiera estar justificado que los programas no fueran completamente públicos, pero no que vulneran los derechos humanos sino se cumplen los requisitos para limitarlos, y no olvidemos que la propia existencia de estos programas únicamente fue revelada bajo polémicas internacionales[45].

Este *Estado de vigilancia,* característico de las sociedades contemporáneas, tiende a incorporar la vigilancia en los más diversos dispositivos, ambientes y sectores, haciéndose omnipresente en la vida de las personas de forma invisible, no jerárquica, descentralizada, individualizada, personalizada[46]. Esta vigilancia permanente y desmedida es, sino la principal, una de las características de esta nueva arquitectura social iniciada a partir de la Segunda Guerra Mundial y que se perfecciona a lo largo de los años, cuyo poder intenta, por excelencia, modular los individuos y las masas para, al fin y al cabo, controlar todas las formas de vida en esa sociedad en red.

---

[43] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950,* p. 11. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

[44] UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Case of Big Brother Watch and Others v. The United Kingdom (Applications nº. 58170/13, 62322/14 and 24960/15).* Recurrente: Big Brother Watch y Otros. Recorrido: Reino Unido. Presidente: Juez Linos-Alexandre Sicilianos. Estrasburgo, Francia, 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.

[45] Ibid.

[46] PESSOA, op. cit., pp. 47-60.

1.2. EL HOMBRE-CARACOL: LOS DATOS COMO *LOGIN* EN LA SOCIEDAD EN RED

Como antes mencionado, las relaciones de poder dependen de las características de la arquitectura social en que los actores sociales interactúan entre sí en un determinado contexto histórico El siglo XX está marcado por diferentes transformaciones sociales, culturales y económicas, a partir de los cambios originados por el incremento de la velocidad de las relaciones sociales y de las complejidades del ser, especialmente con la proliferación y desarrollo de la microelectrónica durante la Segunda Guerra Mundial y posteriormente de la nanoelectrónica.

1.2.1. La sociedad en red: nuevos caminos en la mundialización

Con el desarrollo de las tecnologías de información y comunicación, el concepto de red ha adquirido un nuevo significado, teniendo una importante relevancia en las relaciones intersubjetivas, lo que inauguró, inicialmente en los Estados Unidos, pero poco después extendiéndose en todo el globo, la denominada *Era de la Información.*[47] Sin embargo, la visualización de los procesos por medio de redes no es única y exclusiva de las sociedades del siglo XXI, porque "la red es una estructura común a cualquier vida; donde quiera que veamos vida, vemos redes" [traducción libre][48].

En realidad, la idea de red viene siendo utilizada en diversas áreas del conocimiento, adquiriendo resignificación propia, con intento de explicar, visualizar y contestar estructuras y procesos, sean biológicos, físicos, espaciales, temporales y sociales. Esto, pues, no hay como perder de vista que "el nuevo paradigma puede ser llamado una visión de mundo holística que concibe el mundo como un todo integrado y no como una colección de partes disociadas" [traducción libre][49]. La evolución de las tecnologías de información y comunicación posibilitó la introducción y remoción de nuevos actores sociales y nuevos

[47] CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura, vol. 3. 3. ed. São Paulo: Paz e Terra. 2002 [versión española: CASTELLS, Manuel. *La Era de la Información:* economía, sociedad y cultura. La sociedad en red, vol. 1. Madrid: Alianza Editorial, 2005].
[48] CAPRA, Fritjof. *As conexões ocultas*. São Paulo: Cultrix, 2002 [versión española: CAPRA, Fritjof. *Las conexiones ocultas*: implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo. Barcelona: Anagrama, 2006].
[49] CAPRA, Fritjof. *A Teia da Vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996 [versión española: CAPRA, Fritjof. *La trama de la vida:* una nueva perspectiva de los sistemas vivos. 3. ed. Barcelona: Anagrama, 2009].

procesos en las redes, otorgando autonomía y multidireccionalidad necesarias para proporcionar un mayor flujo de comunicación y autoconciencia.

Esta nueva arquitectura social, se ha caracterizado por una refundación de las fronteras entre el mundo real-vivo y el mundo virtual-artificial, permitiendo la visualización de las relaciones sociales a partir de nodos y aristas, debido a la horizontalización del proceso comunicativo. Para Castells, la sociedad en red "es aquella cuya estructura social está compuesta de redes activadas por tecnologías digitales de comunicación e información basadas en microelectrónica", de modo que "las redes digitales son globales por su capacidad para autoconfigurarse de acuerdo con las instrucciones de los programadores, trascendiendo los límites territoriales e institucionales a través de redes de ordenadores conectados entre sí" [traducción libre][50].

En ese contexto, las innovaciones traídas por los avances de las tecnologías de información y comunicación, han provocado la aparición de nuevos actores sociales, espacios sociales y procesos en red, que han otorgado autonomía y multidireccionalidad a las relaciones. En la sociedad en red, las actividades básicas que configuran y controlan la vida humana en cada rincón del planeta se organizan en redes globales, afectando a todo el mundo, aunque no necesariamente todas las personas participen en las redes, ya que el proceso de inclusión y exclusión de redes también forma parte de esa nueva arquitectura social, lo que, a su vez, influye en la propia formación de la identidad humana[51].

1.2.2. La construcción de una identidad por *big data*

Si en las configuraciones sociales anteriores, el sujeto era identificado, principalmente, por medio de una firma y un número de matrícula o registro general; en las nuevas sociedades, importa la cifra, que es una contraseña, un lenguaje numérico de información y control, que logra transformar a los individuos en dividendos divisibles y las masas en muestras, mercados, porcentajes[52]. Así, por medio de la cifra, está permitido o prohibido el acceso a determinada información y está permitida o prohibida determinada comunicación entre actores sociales, ya que, por ejemplo, pagos con tarjetas de crédito, envío

[50] CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013, p. 59 [versión española: CASTELLS, Manuel. *Comunicación y Poder*. Madrid: Alianza Editorial, 2009].
[51] Ibid.
[52] DELEUZE, op. cit., p. 222.

de mensajes, acceso a perfiles en redes sociales, entre otras acciones, dependen necesariamente de una contraseña, de un código, de una identificación peculiar[53].

Es importante señalar que, para que el individuo acceda a la información deseada sobre la base de una cifra específica utilizada, una máquina de procesamiento de datos, basada en algoritmos, necesita determinar, permitiendo o rechazando, el proceso de comunicación[54]. Entonces, además de la barrera de acceso a la información creada por la necesidad de utilizar de una cifra específica para acceso a determinados procesos comunicacionales, se percibe que, en ese sentido, las tecnologías de la información y comunicación identifican a cada individuo, en una modulación universal y matemáticamente conocida, de forma autónoma y automática, haciendo que sea la cifra relevante y no la persona que la utiliza[55].

1.2.3. ¿Quién soy yo?: la creación de perfiles a través de algoritmos

Se hace posible, por medio de las cifras elegidas y con base en criterios cartográficos, catalogar datos, manipular informaciones, rastrear patrones de comportamiento, prever acciones, reduciéndose las masas en menores grupos para análisis y control[56]. De esta forma, se pueden visualizar, por ejemplo, grupos de personas con determinada condición financiera, específico nicho mercadológico, índice de propensión a alguna enfermedad, gusto por actividad deportiva, orientación sexual, diagnóstico de crédito de algún grupo poblacional, monitoreo de transferencias de los valores, acompañamiento de llamadas y conexiones entre personas y grupos y otros varios ejemplos de lo cotidiano, características de esta nueva sociedad, caracterizada por la grandeza del *big data*.

Se puede decir que la sociedad en red crea sus propios dispositivos de poder, como, por ejemplo, la sustitución de la firma, que, por muchos siglos fue el principal signo de identidad personal por el código informativo, con el objetivo de una mayor seguridad y singularidad[57]. De esta forma, el individuo pasa a ser identificado por los códigos que los sistemas producen, como en los casos del número de la tarjeta de identidad en el registro

[53] DELEUZE, op. cit.
[54] BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008, p. 11 [versión española: BAUMAN, Zygmunt. *Vida de consumo.* Madrid: S.L. Fondo de Cultura Económica de España, 2007].
[55] DELEUZE, op. cit., p. 223.
[56] Ibid., p. 222.
[57] Ibid.

general, del número de seguridad social, del número del pasaporte, del número de la tarjeta de cliente bancario o de la combinación de números, letras y signos en un *username* en determinada red social, entre otros ejemplos; pero también pasa a ser monitoreado y catalogado por los datos que, consciente o inconscientemente, produce.

Por otro lado, las técnicas publicitarias, como dispositivos de control, fueron ampliadas y perfeccionadas en virtud de la profusión de las tecnologías de información y comunicación, ya que han podido avanzar en el campo digital y ser dirigidas a una pluralidad de individuos, que en todo momento buscan consumir en diferentes nichos mercadológicos. La publicidad acaba por involucrar a los sujetos en una nueva lógica consumista, basada en un mercado de informaciones y comportamientos, ya que los datos personales recogidos y monitoreados por las empresas con fines comerciales posibilita una mercadotécnica especial, direccional y colaborativa[58].

Además, a través de ese rastreo de informaciones y cruzamiento de datos, es factible modular grupos de control y forjar identidades, determinándose lo que necesita, cuánto necesita y cómo necesita ser consumido, en un verdadero proceso de subjetivación continua[59]. Este consumismo, marcado por la insatisfacción perpetua del consumidor, ya que siempre hay algo mejor y más nuevo para consumir, y por la lógica de la exclusión social, ya que si no hay el consumo de determinados bienes y servicios no participada en la vida social; acaba afectando la dignidad del individuo y lo esclaviza, porque "apuesta por la irracionalidad de los consumidores, y no sus estimaciones sobrias y bien informadas; estimula emociones consumistas y no cultiva la razón" [traducción libre][60].

1.2.4. El panóptico está vivo: el post-panóptico, el banóptico y el sinóptico

Se da así un control sobre la población, como un todo objeto, no sólo caracterizado por personas físicas, sino por datos informativos multiplicados y multiplicables, de tal modo que es posible sujetar ese cuerpo social a un proceso de subjetivación y modulación continua de la identidad en la sociedad en red. Se ve que el poder es diseminado por todas las formas de vida en un *sin tiempo* y en un *sin espacio*, en razón de la ausencia de las barreras y límites físicos, posibilitando la actuación de dispositivos específicos, entre ellos la vigilancia de los

[58] BAUMAN, op. cit., p. 20.
[59] Ibid.
[60] Ibid., p. 65.

datos personales, que hace necesario repensar la propia noción del panóptico en la nueva arquitectura social.

Se vive, pues, en un post-panóptico, con el prefijo sugerido por Bauman, que nace del mejoramiento y recrudecimiento de las tecnologías de vigilancia, de forma que el panoptismo está vivo y bien de salud, en realidad, armado de músculos (electrónicamente reforzados, ciborguizados) tan poderosos que Bentham, o incluso Foucault, no serían capaces ni siquiera de imaginarlo[61]. El post-panóptico, con nuevas formas de vigilancia y de panoptismo posibilitadas por las innovaciones tecnológicas, se remite a una vigilancia liquida, fundamentada en la fluidez de las relaciones entre sujetos e instituciones, permitiendo la volatilidad de la mirada vigilante, microcapilarizada en diferentes dispositivos informáticos[62]

Aliado a ello, el banóptico, sugerido por Didier Bigo, sobre la base de la idea de seguridad nacional, señala que las tecnologías de la información y la comunicación ayudan en la elaboración de perfiles de individuos, definiendo quién debe ser puesto bajo vigilancia por los agentes de seguridad y estableciendo quién está del lado de dentro y quien está del lado de afuera[63]. Estos dispositivos se asignan en las entradas de los espacios comunitarios, no sólo en términos internacionales, como fronteras viales o aeropuertos, sino también domésticos, en centros comerciales, supermercados y otros departamentos constantemente vigilados, confinando a quienes están del lado de dentro y excluyendo quienes están del lado fuera[64].

1.2.5. El hombre-caracol: la vigilancia personal

Por último, el sinóptico invierte el vector de vigilancia, haciendo que muchos observen a pocos, a partir del hecho que se espera que los propios sujetos y objetos de vigilancia se autodisciplinen y paguen por los costos materiales y psíquicos de esa disciplina, para ejercerla sobre sí mismo y sobre los demás un control continuo[65]. Sucede, así, una distribución de minipanópticos, representados por el tipo *do it yourself*, donde, por medio de

[61] BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013, pp. 22 [versión española: BAUMAN, Zygmunt. *Vigilancia líquida*. Barcelona: Planeta, 2015].
[62] Ibid., pp. 22-23.
[63] BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.
[64] Ibid..
[65] BAUMAN, op. cit., p. 26.

dispositivos móviles y portátiles, suministrados comercialmente, los usuarios, por medio de innumerables acciones, vigilan a todos en todo momento, en una servidumbre contemporánea de ese régimen de vigilancia[66].

En este contexto, Bauman trae la idea del hombre caracol, que lleva en su concha un panoptismo personal, posibilitando una autovigilancia y la vigilancia del otro, en una metodología más económica y popular que el panoptismo clásico[67]. Cada sujeto, emprendedor de sí mismo, transporta, consigo, dispositivos de control, sujetándose al mismo tiempo en que sujeta a los demás, en una retroalimentación de datos, de tal manera que la vigilancia no es impuesta verticalmente por poderes hegemónicos, sino surge del proprio individuo, que no necesariamente consciente, se ve obligado a consumir una autovigilancia y una vigilancia de los demás para poder pertenecer a la sociedad en red y produce, de nuevo no necesariamente consciente, un infinito número de datos personales.

1.2.6. Los datos: del *Internet de las Cosas* al *Internet de Todo*

En el siglo XXI, esta cuestión reviste especial importancia si se considera el avance de las tecnologías de información y comunicación, como el uso de la identificación por radiofrecuencia (RFID), el *Quick Responde Code* (QRCode) y la red de sensores inalámbricos (RSSF) revolucionando la comunicación máquina a máquina (*machine to machine*, en inglés, o por el acrónimo M2M). En la etapa actual, en *Internet de las Cosas* (*Internet of Things*, en inglés, o por el acrónimo IoT), es posible la interconexión digital de los objetos a través de Internet, formando una red inteligente de cosas a disposición de los usuarios, de donde derivan conceptos como *smart things, smart phones, smart TV, smart watchs, smart home, smart cities,* entre otros.

En este escenario, muchas cosas que rodean al usuario se configuran y se conectan a Internet, capturando, monitoreando y procesando datos para un buen funcionamiento. De esta forma, el individuo puede, a través de la red mundial de computadoras y dispositivos inteligentes, controlar remotamente tales objetos o permitir que los proveedores de servicios utilicen tales objetos para una determinada función, lo que genera un abanico de

[66] BAUMAN, op. cit., p. 26.
[67] Ibid., pp. 22-23.

oportunidades y desafíos en el campo tecno-social[68]. Se observa que la IoT, aunque puede ser mejor extendida con el advenimiento de mejores protocolos de Internet, ya es una realidad social, inscrita, inclusive, como técnica de publicidad para consumo de dispositivos[69].

Al avanzar en ese panorama, según algunos expertos en el área, se llegará a *Internet de Todo* (*Internet of Everything*, en inglés, o por el acrónimo IoE), donde habrá un flujo continuo e inimaginablemente inmenso de conexiones entre personas, procesos, datos y cosas, abarcando todo el ecosistema de conectividad alrededor de un universo común[70]. Ocurre que, en este caso, la información que circula por Internet no será colocada en la red por personas, sino por sensores y objetos que intercambian datos entre sí, posiblemente todo el tiempo, generando incontables valores diarios o combinaciones, para experiencias *indoors* u *outdoors*[71].

Básicamente, los datos personales recogidos sirven como mecanismo de estadísticas, acceso a contenido, personalización de experiencia o para uso de un producto o servicio por el usuario, siendo fundamentales en términos de navegación electrónica y comercio electrónico. En primer lugar, al navegar por la red, algunas informaciones que se transmiten automáticamente entre dispositivos se recogen como requisitos tecnológicos vinculados a la navegación, con fines estadísticos, como el nombre de dominio de Internet, la dirección IP, tipo de navegador y del sistema operativo, fecha, ubicación y hora, entre otras, para que el servidor transmita la información compatible con el equipo del usuario.

Además, algunas informaciones personales se obtienen en el registro en determinadas páginas, a través de un formulario de registro, como nombre, dirección de correo electrónico y otra información personal, cuya exactitud puede mejorar cada vez más la personalización de la experiencia del usuario. Esta información recopilada, junto con la información estadística, se utiliza para personalizar un contenido y/o servicios disponibles, desde la personalización del acceso a la propia página hasta el ofrecimiento de contenidos,

---

[68] BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything: A $4.6 trillion public-sector opportunity*. San Jose: Cisco. 2013. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.
[69] Ibid.
[70] BRADLEY, DIXIT, GUPTA, op. cit.
[71] BAJARIN, Tim. *The next big thinh of tech:* the Internet of Everything. [Time, 13/01/2014] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

productos y servicios que tienen relación con el perfil que se crea con los perfiles datos del usuario.

No raras veces (y, aquí, adentra toda una cuestión de consentimiento y legalidad), la información personal individual se comercializa o se suministra a terceros, como socios, patrocinadores, anunciantes u otras empresas externas, con el fin de crear nichos de mercado y perfiles de consumidores para futuras ofertas, propagandas u otros tipos de comunicaciones. En este mismo sentido, a menudo se concede el permiso para que ciertas páginas recopilen periódicamente información personal del usuario a partir de instituciones afiliadas, socios de negocios y otras fuentes de terceros independientes, añadiendo al perfil creado del individuo, datos provenientes de las redes sociales.

1.2.7. El suministro de datos como condición de acceso a la sociedad en red

Las redes sociales o plataformas de interacción social son una de las principales razones por las que miles de millones de usuarios navegan por la red diariamente, como *Facebook, YouTube, WhatsApp, Messenger, Instagram, Twitter, LinkedIn, Snapchat, Viber, Pinterest, Telegram, Tumblr, Reddit,* de entre muchas otras, ya que, a partir de ellas, es posible crear infinitas conexiones entre personas, empresas e instituciones alrededor del mundo, siendo, por lo tanto, una de las mayores fuentes de recogida y almacenamiento de datos personales. Sin embargo, aunque el registro, acceso y funcionamiento de la red social es, en la mayoría de las veces, gratuito, desde el punto de vista del individuo, depende del suministro de datos personales a la plataforma, lo que sirve como mecanismo de ganancia en la creación de espacios publicitarios en esas aplicaciones.

Otro mecanismo importante de la navegación en red es el uso de *cookies*, pequeño paquete de datos que, cuando un usuario visita por primera vez un sitio, recibe del navegador para el almacenamiento de información, de forma que, siempre que el usuario revise dicha página, el navegador devuelve la *cookie* al servidor para recordar actividades anteriores del usuario. El uso de *cookies* proporciona, a primera vista, contenidos, productos y servicios diferenciados y personalizados, desde el momento en que es posible recordar al usuario a cada acceso, reconocer hábitos de navegación, calcular la dimensión de la audiencia y la visualización de páginas, el relleno de formularios, entre otras acciones, que parecen facilitar el consumo por parte del usuario.

Estas cuestiones, usualmente, se aclaran en las políticas de privacidad, en las políticas de *cookies*, en los términos y condiciones de uso de producto y servicio y en otros documentos vinculantes, los cuales el usuario debe leer, y autorizar las condiciones previstas para permitir el acceso al contenido deseado. En la mayoría de los casos, estos documentos son verdaderos contratos de adhesión, que, según la mejor doctrina, se caracterizan por la imposibilidad de discusión o modificación de cláusulas por el adherente, debiendo sujetarse a las cláusulas impuestas por el proponente.

Además, es muy común que estos términos y condiciones de uso de determinadas aplicaciones y plataformas sean amplios y complicados, compuestos por innumerables documentos diferentes y diversas páginas de palabras difíciles y complejas, ya sea en el campo informativo o jurídico. Y, como sabido, la concordancia con esos documentos, exteriorizada por medio de un simple *clic* en una caja de selección o un botón específico, es condicionante de la navegación del usuario en determinada aplicación o plataforma, haciendo que el individuo se vincule a derechos y obligaciones, sin que necesariamente posea total conocimiento de las implicaciones que de ello derivan.

Esto ocurre, especialmente, con los permisos que el usuario concede a determinadas aplicaciones, sin saber realmente lo que está permitiendo, como posibilitando que la plataforma, cuando quiera, sin necesariamente explicitar que lo está haciendo, acceda al calendario, a la cámara, a la lista de contactos, a los sensores, al micrófono, a los SMS, al almacenamiento, a la ubicación, al *bluetooth*, al estado de la red; instale paquetes, utilizar sincronización de datos, gestionar procesos de fondo, habilitar y deshabilitar *keyguard* (información de la pantalla de bloqueo, como contraseñas, patrones, sensores biométricos y faciales); modifique la configuración del dispositivo, transferir infrarrojos, utilizar NFC, entre otras posibles acciones[72]. Estas acciones pueden implicar innumerables nuevos riesgos para el usuario y para la protección de sus derechos, entre los que se encuentra el derecho a la autonomía informacional y a los datos personales. Como ejemplo de esto, basta citar el *software Alphonso*, utilizado por diferentes aplicaciones, que, una vez permitido por el usuario, capta datos del micrófono del teléfono celular sobre hábitos de consumo televisivo

[72] DAUER, Stella. *Entenda tudo sobre as permissões de aplicativos e proteja seu Android.* [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.androidpit.com.br/permissoes-aplicativos.

u otros audios de fondo para suministro a anunciantes para que éstos ofrecen productos y servicios personalizados al individuo[73]

1.2.8. Los ataques maliciosos y riesgos a la autonomía informacional

Sin embargo, no necesariamente, el acceso al micrófono y a la cámara, por ejemplo, ocurre bajo el prisma de un permiso del usuario, pues puede ocurrir a causa de ataques maliciosos dirigidos a los usuarios, incluso por parte de agencias gubernamentales, como ha sido revelado por el portal *Wikileaks,* que mostró que la CIA y el FBI, agencias de investigación estadounidenses, accedían remotamente a estas salidas de audio y video de *persons of interest*[74] (de ahí, el porqué de una fotografía publicada por el CEO de Facebook Inc., compañía dueña de la red social Instagram, se tornó viral en la red no por el hecho de que esta red social hubiera alcanzado medio billón de usuarios, sino por el uso de las cintas adhesivas para cubrir la cámara y el micrófono de su equipo portátil)[75].

Así, se percibe, sea en el estado actual de las cosas, sea en previsiones futurísticas, sea en el campo interpersonal, social, económico, industrial o político, que los datos personales son el principal dispositivo de esta nueva arquitectura social, bajo el argumento de una necesidad de personalización única y aprovechamiento máximo de las experiencias de vida. El individuo deja de ser solo una representación corpórea, exteriorizada por su apariencia, palabras, ideas y actos, para pasar a ser identificado, monitoreado, calificado y controlado debido al conjunto de magnitudes informacionales producidas en todo momento y a todo lugar, no necesariamente de forma consciente, siendo los datos personales el *login* de esa sociedad en red.

A pesar de la protección necesaria que estos datos presuponen por las propias razones de existieren, hubo en los últimos años grandes pérdidas de datos que causaron incomodidad internacional, ya sea por ataques deliberados contra sistemas de información, sean bancos

---

[73] BLASCO, Lucía. *Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto*. [BBC News, 05/07/2018] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.bbc.com/mundo/noticias-44724389.

[74] PHAM, Sherisse. *WikiLeaks dice que la CIA espía a través celulares y televisores, ¿qué tan preocupado debes estar?* [CNN, 08/03/2017] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://cnnespanol.cnn.com/2017/03/08/wikileaks-dice-que-la-cia-espia-a-traves-de-smartphones-televisores-y-mas-que-tan-preocupado-debes-estar/.

[75] RODRÍGUEZ-PINA, Gloria. *El método nada tecnológico que usa Mark Zuckerberg para protegerse de los hackers.* [El País, 22/06/2016] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://verne.elpais.com/verne/2016/06/22/articulo/1466617774_991020.html.

de datos olvidados por empresas de seguridad, sean transferencias y/o compra-y-venta de información entre corporaciones y agencias estatales. De acuerdo con un informe de *Avast*, las diez peores fugas de datos de 2018, involucraron, como poco, treinta y siete millones de usuarios, y el más grave, mil millones de personas[76].

En abril de 2018, el *The New York Times* reveló que en 2013 los datos de al menos treinta millones de usuarios de *Facebook* - hay noticia de que, en verdad, el número de afectados pudo haber superado los ochenta y siete millones – fueron indebidamente compartidos con la consultora *Cambridge Analytica*, que prestó servicios durante la campaña electoral de Estados Unidos al Presidente Donald Trump, en lo cual pudo haber comprometido la limpieza de las elecciones, ya que, en la época candidato, tuvo acceso a diversos datos personales, como nombres, género, edad, lugar de residencia y los resultados de personalidad proyectados por un *quizz* realizado por los usuarios, así como a los intereses y datos más elementales de la cuenta, como e-mail o fecha de nacimiento[77].

El reportaje hizo estallar un escándalo sobre el tratamiento y la gestión de datos personales en la red, especialmente después de que el CEO de Facebook Inc., Mark Zuckerberg, admitiera que la mayoría de los casi dos billones de usuarios pudieron haber tenido los datos personales abiertos de forma indiscriminada. Zuckerberg manifestó que la aplicación iba a implantar un sistema de seguridad con más precauciones, aunque aclaró que el modelo de negocio de la herramienta se basa en el intercambio de información con otras empresas para la publicidad. El creador de la red social fue llamado a declarar y explicarse ante el Congreso de Estados Unidos, asumiendo responsabilidades y un compromiso de implementación de nuevas políticas de protección[78].

A pesar de todo, las investigaciones revelaron que la red social en cuestión dio permiso especial a más de 150 empresas, entre ellas *Apple, Amazon, Microsoft, Netflix* y *Spotify*, plataformas conocidas del público, para acceder a datos de amigos de los usuarios y

---

[76] HRON, Martin. *Os últimos 10 maiores vazamentos de dados.* [Avast, 14/02/2019] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados.

[77] CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. *How Trump Consultants Exploited the Facebook Data of Millions***.** **[**The New York Times, 17/03/2018]. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

[78] MARS, Amanda. *Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia*. [El País, 11/04/2018]. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html.

para ver mensajes privados de las personas, aunque negado vehemente[79]. Se tratan de acuerdos firmados en otra época, cuando la red social intentaba expandirse rápidamente con la ayuda de una personalización instantánea para integrar a los usuarios, que, en muchos casos, siguen valiendo, pese ya estar vigente la supuesta necesidad de adquirir el consentimiento del usuario para la cesión de datos, lo que nuevamente trae a la superficie la cuestión del consumismo en la red[80].

1.2.9. Perspectivas de futuro: la economía de vigilancia

Frente a todas las noticias de existencia de programas de vigilancia masiva por parte de agencias de seguridad estatales y de fuga de datos personales de los usuarios, se percibe un escenario de monitoreo real de los procesos comunicativos a escala mundial, con una insuficiencia, con propósito o no, de medidas de seguridad para proteger al usuario de esos nuevos riesgos, que, a su vez, se encuentra en absoluta debilidad frente a las tecnologías disruptivas. El individuo acaba, incluso, contribuyendo aún más con los engranajes de ese sistema, porque se ve obligado a consumir esas tecnologías de información y comunicación para participar efectivamente de la sociedad en red.

Nos encontramos, entonces, con un determinismo tecno-social en una relectura de la formación del propio Estado, pero ahora, como un Estado vigilante. En otras palabras, parece que el individuo, por miedo al terror y otros enemigos, renuncia a las propias libertades a favor de un ente, que garantice una seguridad deseada, aceptando programas de vigilancia masiva de combate al terrorismo. En esta misma línea de pensamiento, el individuo, queriendo formar parte de la sociedad, se somete a la cultura del consumo, conscientemente o no, dejando de preocuparse por la autorización del monitoreo y manipulación de los datos personales recogidos, ya que el coste-beneficio de ser excluido de la red, si no entrega los datos, no compensa en este nuevo entorno digital.

Por un lado, las agencias estatales promueven programas de vigilancia masiva de nacionales y extranjeros, a través de la supervisión y evaluación del tráfico de datos alrededor del globo; por otro lado, los individuos consumen, en todo momento, productos y

[79] COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html.
[80] Ibid.

servicios que generan datos de todo orden, sobre sí y sobre otras personas; en el medio de eso, grandes corporaciones cooperan con la actuación de las agencias de seguridad, transmitiendo datos o permitiendo el acceso a ellos, inventan nuevos productos y servicios tecnológicos, ofreciendo para consumo de todos, incluso con obsolescencia programada, así como colaboran con otras grandes corporaciones en un el mercado mundial para la compra-venta y la transferencia de datos de los usuarios.

Así, impera una economía de la vigilancia, en la que los datos de los usuarios adquieren valor de mercado y basan la creación y el desarrollo de productos y servicios, públicos y privados, en un sin número de interacciones, competiciones y cooperaciones, entre diferentes actores sociales. En una sociedad en red, por su propia arquitectura informacional, el procesamiento de datos producidos en los procesos comunicativos se convierte en el nuevo oro del siglo XXI, de forma que, en un Estado general de vigilancia, se hace necesario analizar esta nueva arquitectura social, bajo el prisma de los derechos y garantías humanas y fundamentales de los individuos, especialmente del derecho a la privacidad.

2. "1984 ALL OVER AGAIN": EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL

El título del presente capítulo hace referencia a que el mundo descrito en la obra "1984", de George Orwell, está sucediendo nuevamente o salió a la luz de nuevo, aunque es un escenario ficticio de sociedad distópica imaginada en 1949. Por un lado, se observa un régimen global de vigilancia social, marcado por la interceptación de datos personales y por el monitoreo de los procesos comunicativos entre ciudadanos, empresas, organismos públicos y otros países, con la diferencia de que no hay un Partido definido, porque la vigilancia y el control social están dispersos y perfeccionados con el avance tecnológico de la sociedad en red.

Por otro lado, al igual que las telepantallas, televisores bidireccionales que funcionaban al mismo tiempo como emisores de mensajes oficiales y como cámara de monitoreo y estaban en todas las residencias del país, las tecnologías de información y comunicación, especialmente aquellas equipadas con internet, están diseminados por todos los rincones del mundo, permitiendo a los ciudadanos interactuar uno con los demás, pero también proporcionar datos personales para acceder a productos y servicios variados. Así, la privacidad, como era antes conocida, parece ser cada vez más una memoria de un pasado distante, tales como los recuerdos de los tiempos antes del gobierno del Gran Hermano.

Considerando que el objetivo general de este trabajo es analizar los impactos de las tecnologías de información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI, este capítulo, tras el análisis realizado anteriormente sobre el régimen global de la vigilancia social, pretende: a) establecer la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y, finalmente, b) discutir la resignificación del derecho a la privacidad, basada en nuevos conceptos, nuevos espacios, nuevos límites y nuevas posibilidades en el contexto de la ciberseguridad.

2.1. LA PRIVACIDAD COMO LA CONOCEMOS: LA (R)EVOLUCIÓN DE UN CONCEPTO EN EL CUADRO NORMATIVO

Los marcos normativos de derechos humanos y los ordenamientos jurídicos nacionales reconocen el derecho a la privacidad, en sus diferentes matices, como derecho a

la intimidad o como derecho a la vida privada, elevándolo a la categoría de derecho humano. Aunque la motivación legal guarde estricta relación con el desarrollo de los *mass media*, los avances tecnológicos producidos desde la mitad del siglo XX y finales del siglo XX han exigidos adaptaciones a las recientes necesidades y nuevas interpretaciones jurídicas, especialmente en el campo de la tutela de la personalidad.

2.1.1. Breves consideraciones sobre el concepto de la privacidad en la historia

Para conceptuar la privacidad y, específicamente, el derecho a la privacidad, es necesario volver a la distinción entre privado y público en la antigüedad clásica griega -traspasada a la cultura romana posteriormente -, donde se distinguía el *oikos*, espacio particular de los individuos, y la *pólis*, espacio común a los ciudadanos libres[81]. En ese sentido, el ciudadano necesitaba una esfera privada y tenía un "lugar que le pertenecía", para poder recibir una segunda vida, *bio politikos*, y participar de la esfera pública, donde, en este lugar, no trataba de lo que le era propio, *idion*, sino de lo que le era común, *konion*, de modo que la diferencia, en un primer momento, de privado y público era el ámbito familiar y el ámbito político[82].

En la Edad Media, siglos después, urgió, cada vez más, la necesidad de aislamiento en un espacio privado en detrimento de lo que era común y giraba en torno al espacio público, convirtiéndose la casa en el lugar ideal de separación entre esas esferas y el nuevo centro de poder político, tanto que las dinastías empiezan a vincularse a casas, apellidos[83]. Con el declive de la economía feudal y el surgimiento de la burguesía, el deseo por la individualidad fue aumentado exponencialmente, habiendo el burgués ocupado espacios, acumulado riquezas, levantado barreras, de modo que la búsqueda por la protección de un lugar solamente suyo fortaleció la noción de aquello que es privado, en una estrecha relación con el derecho a la propiedad[84].

Esta cuestión asumió especial relevancia en el marco filosófico del liberalismo, en particular en las obras de John Lock, considerado el padre del liberalismo, cuando éste

[81] ARENDT, Hannah. *A condição humana*. 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 33 [versión española: ARENDT, Hannah. La condición humana. Barcelona: Paidos Iberica, 2016].
[82] Ibid., pp. 38-39.
[83] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 125.
[84] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 26.

defendía "la existencia de una esfera de libertad natural a todo sujeto, espacio que debe ser impermeable a la coactividad despliega la ley civil", de modo que "la 'privacy' es considerada la propiedad más sagrada de la persona humana, pues todo hombre tiene una propiedad en su propia persona" [traducción libre][85]. En sentido parecido, John Stuart Mill sostuvo que las conductas humanas pasibles de análisis eran aquellas que producían deberes y obligaciones sociales, cuando afectar a terceros, de manera que los aspectos que sólo se refieren al individuo, es decir, las características privadas, la esfera pública, siendo el sujeto soberano sobre sí[86].

2.1.2. El derecho a la privacidad desde una perspectiva jurídica

Como categoría analítica y autónoma de ponderación, el derecho a la privacidad es una construcción reciente estadounidense. Samuel Warren, motivado por hechos íntimos del matrimonio de su hija divulgados por periódicos, y Louis Brandeis publicaron en 1890 un artículo sobre el *right to privacy* (derecho a la privacidad), inspirado en la expresión acuñada por Thomas McIntyre Cooley, *right to be alone* (derecho de ser dejado en paz), con base en las necesidades de la burguesía norteamericana de finales del siglo XIX[87]. La doctrina de Warren y Brandeis aleja el derecho a la privacidad de la necesidad de protección de la propiedad y aproxima la necesidad de protección de la vida privada con factores relacionados con la personalidad humana[88].

Los autores refieren que recientes innovaciones dan lugar a un nuevo nivel de protección de la personalidad humana y de la seguridad del ciudadano norteamericano, ya que las nuevas tecnologías de comunicación, las máquinas, las fotografías, las empresas de chismes, entre otras, acabaron por invadir el espacio privado del hogar, pero el individuo tiene el derecho de estar solo, o mejor, el derecho de ser dejado en paz[89]. Se trata de una protección que va más allá de la tutela del material que contenga una determinada revelación

---

[85] TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 136.
[86] MILL, John Stuart. *A liberdade*. São Paulo: Martins Fontes, 2000 [versión española: MILL, John Stuart. *Sobre la libertad*. Madrid: Verbum, 2016].
[87] BRANDEIS, Louis. WARREN, Samuel. The right to privacy. *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.
[88] Ibid.
[89] Ibid.

íntima, pues alcanza sustancialmente a la propia información, confiriendo a la persona el derecho de ser dejada en paz y no hacer en público aquello que considera privado[90]

Esta construcción doctrinal va ganando fuerza en los ordenamientos jurídicos nacionales con el paso de los años, de forma que, a partir del desarrollo de las tecnologías de la información y comunicación y la globalización de las relaciones sociales a lo largo del siglo XX, el derecho a la privacidad, antes considerado como inherente a los derechos de la personalidad, pasa a ser tratado como un derecho de naturaleza humana y fundamental. Se presenta el derecho de cada uno de garantizar una paz, una tranquilidad, una reserva de parte de su vida que no esté afectada por una actividad pública; o de evitar que los hechos de su vida que son entendidos privados sean expuestos y el Estado debe abstenerse de interferir indebidamente en tal ámbito de cada individuo e incluso prohibir la injerencia también de terceros.

En la esfera social, las personas pasan la mayor parte del tiempo interactuando unas con otras, debido a la necesidad de ganarse la vida, seguir una vocación, aliarse a otros con los mismos intereses o negocios; mientras que en la esfera de la vida íntima, con base en el principio de la exclusividad formulado por Hannah Arendt, a su vez, inspirado en Kant, las personas escogen aquellos con los cuales quieren vivir, compartir momentos, hechos, informaciones, estando intrínsecamente conectada a la persona en su singularidad[91]. El derecho a la intimidad está, en esa concepción, caracterizado por tres atributos, que son: la *soledad*, el derecho de estar solo; el *secreto*, el derecho de exigir secreto; y la *autonomía*, el derecho de decidir sobre sí mismo[92].

2.1.3. El derecho a la privacidad y figuras afines

La idea de categorización del derecho a la privacidad es compleja y susceptibles de críticas, ya que el término puede derivar en innumerables figuras afines, como “vida privada”, “intimidad”, “sigilo de las correspondencias”, “sigilo de las comunicaciones”, “inviolabilidad del domicilio”, “sigilo de la fuente”, “derecho a la imagen”, “derecho al honor”, “protección de datos personales”, entre otros. Esta significación dependerá del sujeto, del ordenamiento jurídico y del contexto abordado, ya que, según la fluidez de los

[90] BRANDEIS; WARREN, op. cit.
[91] ARENDT, Hannah. Reflections on Little-Rock. En: *Dissent Magazine*, v. 6, n. 1, invierno, 1959, pp. 52-53.
[92] Ibid.

contenidos, existe la posibilidad de migración de conceptos, pudiendo considerarse el derecho a la privacidad como un género con diversos contenidos.

Sin embargo, una importante distinción recae sobre el derecho a la vida privada y el derecho a la intimidad, ya que tales expresiones se utilizan en algunos ordenamientos jurídicos. En el derecho a la privacidad, el derecho a la vida privada puede ser considerado como la tutela de la vida personal y familiar del sujeto, así como del círculo cercano de la persona, entre la intimidad y la vida social del individuo, lugar en que éste practica los actos jurídicos privados y donde se desarrollan las interacciones relevantes a los seres humanos[93]. Es decir, la vida privada de la persona son las relaciones de proximidad emocional, que pueden ser de conocimiento de aquellos que están cerca y fueron elegidos para saber y participar de esa singularidad.

Por otro lado, el derecho a la intimidad puede ser definido como aquel que intenta proteger a las personas frente a la indiscreción ajena, en la medida en que pretende excluir del conocimiento ajeno algo sobre sí, sobre su núcleo esencial como persona, sobre su espacio más reservado de la existencia, o prohibir que otros se inmiscuyan en esa esfera más particular[94]. La intimidad puede, pues, guardar relación con las informaciones del ámbito exclusivo de una persona, que ella reserva para sí mismo, alejándose de cualquier repercusión social y, pudiendo determinar ella misma el alcance de su vida privada, tomando decisiones sobre los límites de ese espacio[95].

En un primer momento, la doctrina alemana de la teoría de las esferas sirvió como base para representar los niveles de privacidad. A partir de las ideas de círculos concéntricos, el primero, más amplio, es la esfera de la vida privada (*Privatsphäre*), donde están las informaciones que el sujeto no quiere que sean de dominio público; el segundo, en el interior, menor, es la esfera de la intimidad (*Vertrauensphäre*), donde están las informaciones que el sujeto confía solamente a ciertas personas, en carácter reservado; y el tercero, más aún en el interior, es la esfera del secreto (*Geheimnsphäre*), donde están las informaciones que el sujeto no comparte con nadie o sólo con algunas personas[96].

[93] RODOTÀ, op. cit.
[94] DONEDA, op. cit.
[95] RODOTÀ, op. cit.
[96] HUBMANN, Heinrich. *Das persönlichkeitsrecht.* Münster: Böhlau-Verlag, 1953 apud COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995, pp. 30-36.

Esta teoría acabó perdiendo credibilidad por considerar al individuo como una persona como una "cebolla pasiva", siendo superada, en razón de la insuficiencia técnica, de la necesidad de subjetivismo en cuanto al grado de las esferas y de las recientes innovaciones tecnológicas[97]. En su lugar, adviene la teoría del mosaico, sosteniendo que las informaciones, *a priori*, pueden ser irrelevantes bajo determinado prisma o si se las considera aisladas; pero si se analizan en relación con otras informaciones, a veces también irrelevantes por sí solas, pueden servir para formar una coyuntura plena de significado, de modo que la protección de la privacidad debe tener en cuenta el mosaico resultante y la posible revelación que la percepción global hace de la vida privada[98].

2.1.4. El derecho a la privacidad en los textos normativos

Aunque el derecho a la privacidad ha sido una construcción inicialmente doctrinal y luego utilizada en algunos precedentes jurisprudenciales, luego esta tutela pasó a ser insertada en las cartas positivas de derechos humanos y en los ordenamientos jurídicos comunitarios y nacionales. Sin embargo, como es notable y como se discutió anteriormente, el derecho a la privacidad, en estos marcos normativos, aparece bajo diversas formas, a veces como privacidad en sentido estricto, a veces como vida privada, otras veces como intimidad, pero en todos los casos se percibe intención de tutelar ese aspecto privado del ser humano.

2.1.4.1. Marco normativo universal, internacional y regional

La Declaración de los Derechos del Hombre y del Ciudadano de 1789 ya contenía ideas embrionarias de esa protección, al establecer en su art. 10, que "nadie debe ser incomodado por sus opiniones, inclusive religiosas, siempre y cuando su manifestación no perturbe el orden público establecido por la Ley" y, en su art. 11, que "[...] cualquier

[97] BURKERT, 2000, p. 46 apud DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Âmbito Jurídico*, Rio Grande, XI, n. 51, mar. 2008. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460.

[98] CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984, p. 45.

Ciudadano puede hablar, escribir e imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la Ley" [traducción libre][99].

Expresamente, el derecho a la vida privada aparece por la primera vez reconocido en la Declaración Universal de los Derechos Humanos de 1948, en el marco de la Asamblea General de las Naciones Unidas, que lo reconoce como un derecho humano, en su art. 12, al disponer que "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" y "que toda persona tiene derecho a la protección de la ley contra tales injerencias"[100].

En la esfera americana, la Declaración Americana de los Derechos y Deberes del Hombre de 1948 fue uno de los primeros instrumentos normativos en recoger ese derecho, cuando, en su art. V, dispone 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 familiar"[101]. Más tarde, la Convención Americana de Derechos Humanos de 1969 dicta, en su art. 11, sobre la protección del honor y la dignidad, que "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"[102].

En el ámbito europeo, el Convenio Europeo de Derechos Humanos de 1950, refiere, en su art. 8.1, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"[103]. En este mismo sentido, la Carta de los Derechos Fundamentales de la Unión Europea de 2000 menciona, en su art. 7, que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"[104].

---

[99] FRANCIA. *Déclaration des Droits de l'Homme et du Citoyen de 1789*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789.

[100] ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Declaración Universal de Derechos Humanos de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.un.org/es/universal-declaration-human-rights/.

[101] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Declaración Americana de los Derechos y Deberes del Hombre de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp.

[102] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de 1969*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.

[103] CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950.* [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

[104] UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

En el ámbito africano, la Organización para la Unidad Africana, cuando aprobó la Carta Africana sobre los Derechos Humanos y de los Pueblos, aunque no se refería directamente sobre la privacidad, establece, en su art. 4, que "todo ser humano tendrá derecho al respeto de su vida y de la integridad de su persona" [traducción libre][105]. En concreto, la Declaración de los Derechos Humanos en el Islam de 1990, documento oriundo de la Organización de la Conferencia Islámica, promulga, en su art. 18, que "todos deben tener el derecho a la privacidad en la conducción de asuntos privados, en su casa, en su familia, con respecto a sus bienes y relaciones" y que "no será permitido espiar, someterlo a vigilancia o dañar su reputación" [traducción libre][106]. La Carta Árabe sobre Derechos Humanos de 2004, documento proveniente de la Liga Árabe, cita, en su art. 21, que "nadie será sometido a injerencias arbitrarias o ilegales con respecto a su privacidad, familia, domicilio o correspondencia, ni a ataques ilegales a su honor o su reputación" [traducción libre][107].

Finalmente, la Carta Asiática de Derechos Humanos de 1998, documento creado por la Comisión Asiática de Derechos Humanos, organización fundada por un grupo de juristas y activistas de derechos humanos, ya que, todavía, no hay declaración intergubernamental en ese sentido, trae especialmente el "derecho a vivir en paz". Así, prevé, en su art. 4.1, que "todas las personas tienen el derecho a vivir en paz para que puedan desarrollar todas sus capacidades físicas, intelectuales, morales y espirituales, sin ser objeto de ningún tipo de violencia" [traducción libre][108].

2.1.4.2. Marco normativo comparado: Brasil y España

En términos específicos, en el caso brasileño, país de origen del autor, el tema está previsto en la Constitución Federal de 1988, la cual, en su art. 5º, inc. X, sobre los derechos

---

[105] ORGANIZACIÓN PARA LA UNIDAD AFRICANA. *Carta Africana sobre los Derechos Humanos y de los Pueblos de 1981*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2002/1297.pdf.

[106] ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA. *Declaración de los Derechos Humanos en el Islam de 1990*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oic-iphrc.org/en/data/docs/legal_instruments/OIC_HRRIT/571230.pdf.

[107] LIGA ÁRABE. *Carta árabe sobre los derechos humanos 2004*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A.pdf.

[108] COMISIÓN ASIÁTICA DE DERECHOS HUMANOS. *Carta Asiática de los Derechos Humanos de 1998*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.humanrights.asia/wp-content/uploads/2018/07/Asian-Human-Rights-Charter-2nd-Edition-English.pdf.

y deberes individuales y colectivos, garantiza que "son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a indemnización por el daño material o moral resultante de su violación" [traducción libre][109]. En la legislación ordinaria, el Código Civil de 2002, en el capítulo sobre los derechos de personalidad, señala, en su art. 21, que "la vida privada de la persona natural es inviolable, y el juez, a petición del interesado, adoptará las providencias necesarias para impedir o hacer cesar acto contrario a esta norma" [traducción libre][110].

Por último, en el caso español, el derecho también aparece reconocido en la Constitución Española de 1978, la cual, en su art. 18.1, en la sección sobre los derechos fundamentales y las libertades públicas, deduce que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"[111]. En el mismo artículo, pero en el apartado 4, la Constitución Española innova en la cuestión de las tecnologías de información y comunicación e incluye la denominada libertad informática, al establecer que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[112]. Por último, en el ámbito ordinario, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, dispone, en su art. 1 que "el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas"[113].

2.1.5. El derecho a la privacidad y los avances de las tecnologías de la información y comunicación

Es posible percibir que la expansión indiscriminada del uso de informaciones personales, provocado por el avanzo de las novedades cibernéticas, ha posibilitado

[109] BRASIL. Constituição da República Federativa do Brasil de 1988. *Diário Oficial da União,* n. 191-A, 05 de octubre de 1988, pp. 1-32
[110] BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*, 11 de enero de 2002, pp. 1-76..
[111] ESPAÑA. Constitución Española de 1978. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424.
[112] Ibid.
[113] ESPAÑA. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. *Boletín Oficial del Estado*, 14 de mayo de 1982, núm. 115, pp. 12546 a 12548.

innovadoras formas de violación de la privacidad, ya que, en la red, toda operación o conjunto de operaciones, realizada propiamente por el usuario o con la ayuda de medios automatizados, permite la recolección, almacenamiento, selección, evaluación, monitoreo, comparación, modificación, transferencia, utilización y tratamiento de información personal, en este caso, de datos personales.

En ese contexto, la preocupación con el derecho a la privacidad "decae en pro de definiciones cuyo centro de gravedad está representado por la posibilidad de cada uno de controlar el uso de las informaciones que le conciernen" [traducción libre], siendo más propio hablar de un derecho a la autodeterminación informativa[114]. La expresión "derecho a la autodeterminación informativa" fue utilizada en primer lugar por el Tribunal Federal Constitucional Alemán, en una resolución de un proceso relacionado con las informaciones personales recogidas de un censo en el año 1983[115]. De acuerdo con el Tribunal, el derecho general de protección de la persona, reconocido en el texto constitucional, abarca, considerando el procesamiento tecnológico y moderno de datos, la tutela del sujeto contra la recolección, almacenamiento, utilización y divulgación ilimitada de sus datos personales, debiendo se considerar un derecho fundamental la facultad del ciudadano de disponer libremente de sus datos[116].

Se ve que el derecho a la protección de datos personales supera el contenido esencial del tradicional derecho a la intimidad, ya que no se basa solamente en la tutela del contenido de naturaleza íntima de los datos recogidos; sino que abarca la facultad, primero de conocer, pero también de decidir sobre la recogida, sobre el tratamiento y sobre la posible transferencia de tales registros, ya que, en la sociedad en red informacional, las posibilidades de generación de datos, en ocasiones, no depende de tiempo, espacio y dispositivo determinado. Así, el derecho a la autodeterminación informativa es un derecho autónomo al derecho a la intimidad, constituyéndose como instrumento jurídico para garantizar la dignidad humana y el desarrollo de la personalidad, reposando sobre la facultad del sujeto

[114] RODOTÀ, op. cit., p. 24.
[115] MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016, p. 55-63. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877.
[116] Ibid.

de disponer de las propias informaciones personales, frente al uso indiscriminado de las tecnologías informáticas.

En el caso español, como se ha dicho, el propio texto constitucional separa el derecho a la intimidad (artículo 18.1) del derecho a la limitación de los usos informáticos para garantizar ese derecho (artículo 18.4). El Tribunal Constitucional, en la decisión STC nº 292/2000, delimita y define la protección de datos personales y señala que el objeto de este derecho "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual"[117].

Sobre el tema, en el derecho comunitario europeo, precisamente por la libre circulación de personas, bienes y datos, ese derecho está previsto autónomamente en la Carta de Derechos Fundamentales de la Unión Europea, que, en su art. 8, señala que "todas las personas tienen derecho a la protección de los datos de carácter personal que les conciernen", de modo que "esos datos deben ser objeto de un trato leal, con fines específicos y con el consentimiento de la persona interesada o con otro fundamento legítimo previsto por la ley", y que "todas las personas tienen derecho a acceder a los datos recopilados que les conciernen y obtener su rectificación"[118]. Por último, establece que "el cumplimiento de estas normas está sujeto a la supervisión por parte de una autoridad independiente"[119].

Además, algunas directivas ya apuntaban el camino para la tutela de este nuevo derecho, como fue el caso de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que se refiere tratamiento de datos personales y la libre circulación de estos datos[120]; de la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, refiere al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[121]; y de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo,

[117] ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, n. 4, 4 de enero de 2001, pp. 104-118.
[118] UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.
[119] Ibid.
[120] UNIÓN EUROPEA. Parlamento Europeo. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea*, L 281, 23 de noviembre de 1995, pp. 31-50.
[121] Ibid.

de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[122].

2.1.6. Los nuevos derechos de la protección de datos y la ciberseguridad bajo el Reglamento General de Protección de Datos

Considerando que las directivas no son de aplicación directa, sino que necesitan ser transpuestas a los ordenamientos jurídicos nacionales, se redacta, entonces, el Reglamento General de Protección de Datos (RGPD), con entrada en vigor el 25 de mayo de 2018, substituyendo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, siendo ese marco normativo de obligatorio cumplimiento y directamente aplicable, sin necesidad de transposición, aunque las nuevas leyes nacionales están siendo creadas para adaptar la normativa interna anterior al nuevo reglamento[123]. El RGPD presupone un cambio en relación a la normativa anterior, ya que, además de una protección represiva, establece una aproximación proactiva, exigiendo un enfoque basado en el riesgo (no sobre el tipo de dato o sobre el tipo de tratamiento), así como una responsabilidad activa, consciente y diligente por los órganos responsables del tratamiento (ya que no existe un paquete cerrado de medidas de seguridad, dependiendo de la propia política de gestión de riesgos)[124].

Ocurre que la injerencia del RGPD acaba por avanzar en las fronteras físicas mundiales, ya que la protección no solo es aplicable al tratamiento de datos por una empresa establecida en la Unión Europea, independientemente del lugar de tratamiento de esos datos o de la nacionalidad del titular de los mismos; sino también, tratamiento de datos por una empresa no establecida en la Unión Europea que ofrezca bienes y servicios o monitoreo a

[122] UNIÓN EUROPEA. Parlamento Europeo. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de la Unión Europea* L 201, 31 de julio de 2002, pp. 37-47.
[123] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88
[124] Ibid.

los usuarios que allí se encuentren. Además de servir como fuente de inspiración para normativas sobre protección de datos personas en países de otros continentes[125].

El RGPD se basa en los principios de la licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva[126]. Se han producido cambios significativos en la forma de obtener el consentimiento. Pues cuando el tratamiento se basa en el consentimiento del usuario (existen otras hipótesis en las que el consentimiento es independiente), éste debe ser explícito, claro, simple, activo (no se permite solamente el silencio como permiso para la recolección), debiendo contar con la aprobación del internauta para cada propósito de monitoreo de datos, aunque sea de forma electrónica y por opción de caja de selección[127]. Además, el Reglamento obliga a informar sobre la base legal del tratamiento de datos, el plazo de conservación y transferencia de los mismos, garantizando el ejercicio de los derechos de los titulares de los datos, como la portabilidad, la eliminación de los datos y la notificación de terceros sobre la rectificación o supresión o limitación de tratamiento solicitados por los titulares[128].

2.1.7. ¿Hay que pensar en un nuevo derecho a la privacidad?

De ahí que, en virtud de este cambio de reglas, un sin número de políticas de privacidad, políticas de cookies, políticas de uso de aplicaciones y dispositivos, entre otros tipos de documentos y términos de adhesión firmados por los usuarios, deben ser actualizados, divulgados y aceptados, además de la adaptación en cuanto a las cuestiones técnicas, científicas, sociales, publicitarias, laborales y sectoriales involucrando tales productos y servicios. De esta manera, la autonomía informativa, el derecho a la protección de datos personales - y en última instancia, el derecho a la privacidad - se somete a un régimen de ciberseguridad, es decir, a un conjunto de actividades dirigidas a proteger el

[125] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88
[126] Ibid.
[127] Ibid.
[128] Ibid.

ciberespacio contra el uso indebido del mismo, defendiendo la infraestructura tecnológica, los servicios que presta y la información que maneja[129].

A pesar de los compromisos políticos y normativos internacionales firmados por parte de las naciones y de las corporaciones en favor del derecho a la protección de datos personales, y del desarrollo del derecho a la privacidad; la vigilancia social a la que los ciudadanos son sometidos y la propia subjetividad formada por el miedo al terror acaban poniendo en jaque estos derechos fundamentales, ya que el límite entre conocimiento público, vida privada, intimidad y secreto es fluido. En la sociedad en red de vigilancia social, la privacidad, como conquista popular y derecho de primera generación de libertad individual, puede necesitar una reformulación.

2.2. HACIA UN NUEVO DERECHO A LA PRIVACIDAD: DESAFÍOS Y CAMINOS EN TIEMPOS DE CIBERSEGURIDAD

El siglo XX representó la era de oro para la normatividad de los derechos y garantías fundamentales y, a medida en que los avances sociales y la propia configuración del Estado fue cambiando debido al perfeccionamiento de las tecnologías de la información y comunicación, nuevas generaciones/dimensiones de derechos fundamentales fueron surgiendo. Entre ellos, el derecho a la privacidad, en la concepción moderna, también pasó por transformaciones, habiendo invadido, conquistado y colonizado la esfera pública social, aunque en los últimos años ha sido marcada por las caídas vertiginosas del apogeo de su gloria.

2.2.1. El cambio de paradigma y el nuevo concepto de privacidad

Se trata, pues, de una alteración de paradigma y una necesaria resignificación de conceptos, marcada por el flujo informacional masivo, abarcando nuevos matices sobre el derecho al secreto, el derecho a la intimidad, el derecho a la vida privada y familiar, el derecho a la autodeterminación informativa y el derecho a la protección de datos personales. Aunque al final sobre el pasado siglo se ha hablado del final de la privacidad, parece más

[129] ESPAÑA. Ministerio de Defensa. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. *Boletín Oficial de Ministerio de Defensa*, 26 de febrero de 2013, n. 40, pp. 4154-4156.

oportuno intentar conceptualizar el derecho a la privacidad como una superación de la concepción sólida y estática de los textos normativos cerrados de auto confinamiento para alcanzar una perspectiva abierta, dinámica y fluida en una sociedad tecnológica[130].

El derecho a la privacidad, en los ordenamientos jurídicos modernos, está fundado en la concepción clásica de la privacidad relacionada con la idea aislacionista del ser, en una lógica excluyente de "persona-información-sigilo", posibilitando al individuo protegerse de intromisiones indeseadas en lo que le era más reservado, aunque que "a partir de la crítica del denominado pensamiento postmetafísico se hace muy complicado sostener que el sujeto pudiera ser algún género de yo como sustancia autoconsciente de los inicios cartesianos de la filosofía de la conciencia"[131]. Con el desarrollo de las tecnologías de la información y comunicación, se ha producido una relativización de lo que es considerado secreto, de manera que el sujeto, en el panorama de las relaciones sociales conectadas globalmente, se adhiere al virtual – aquí no como digital, sino como potencia de ser – y posee la prerrogativa y la necesidad de compartir información para formar una identidad en red[132], provocando que en ese contexto que el concepto de privacidad deba ser reformulado.

De esta forma, la definición de la privacidad sólo como el derecho de ser dejado sólo (*right to be let alone)* y de restringir el conocimiento público de informaciones consideradas privadas perdió hace algunos años el valor de ser el único fundamento de esta tutela, aunque esta cuestión es un aspecto esencial a ser aplicado a situaciones determinadas cuando se exige esa protección. Se trata, entonces, del fin de un largo proceso evolutivo experimentado por el concepto de privacidad: de una definición original como el derecho de ser dejado en paz, hasta el derecho de control que permite al sujeto ser dueño de su propia información y determinar cómo quiere construir su propia esfera privada[133].

Esto no quiere decir que ese aspecto de control del sujeto sobre la propia esfera de privacidad estuviera ausente de las definiciones tradicionales, ya que el control era utilizado justamente como una herramienta para realizar la finalidad de ser dejado sólo y definir lo que debería quedar fuera del conocimiento ajeno, pero bajo ángulo exclusivamente

[130] PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica.* Madrid: Editorial Universitas, S.A., 2012, p. 93.
[131] MUGUERZA, J. De la conciencia al discurso ¿un viaje de ida y vuelta? In: *La filosofía moral y política de Jürgen Habermas*. Madrid: Biblioteca Nueva, 1997, pp. 63-110, p. 98.
[132] CASTELLS, Manuel. *O poder da identidade*. 2. ed. São Paulo: Paz e Terra, 2000 [versión española: CASTELLS, Manuel. *La Era de la Información:* economia, sociedade y cultura. El poder de la identidad, vol. 2. Madrid: Alianza Editorial, 2003].
[133] RODOTÀ, op. cit., p. 17.

individualista y privado, que el desarrollo actual de las tecnologías ya no permite. Por otro lado, actualmente, la cuestión de la privacidad como control llama la atención sobre la posibilidad de que los sujetos ejerzan los poderes conquistados por el suministro de datos personales, entre ellos los de conocer, controlar, enderezar, oponer, interrumpir y prohibir el flujo de informaciones que se relacionan con él.

Así, se introduce una nueva concepción de privacidad, pudiendo ser definida más precisamente, en una primera aproximación, como el derecho de mantener el control sobre las propias informaciones, identificada con la tutela de las elecciones de vida contra toda forma de control público y de estigmatización social, en un cuadro caracterizado precisamente por la libertad de las elecciones existenciales[134]. Se verifica, entonces, que la privacidad como la conocemos, relacionando privado con ámbito personal y secreto, dio espacio a nuevos caminos, pudiendo ser entendida en una lógica de "persona-información-circulación-control", no más restringida a la burguesía del siglo XX sino destinada a la multitud en la sociedad en red[135].

2.2.2. Las paradojas de la privacidad en el siglo XXI

Considerando la difusión de las tecnologías de información y comunicación y la producción en masa de *big data*, se percibe que el objeto de tutela de la privacidad también ha sufrido cambios, comprendiendo un número creciente y exponencialmente mayor de informaciones y situaciones jurídicas relevantes que necesitan de un control del individuo. En este sentido, la privacidad no necesariamente guarda relación con algo privado y, a su vez, lo privado ya no hace referencia a algo secreto, derivándose de allí, al menos, cuatro paradojas y el surgimiento de una nueva dimensión de la privacidad, la extimidad.

2.2.2.1. La primera paradoja: de las murallas digitales

La primera paradoja de la privacidad guarda relación con la propia idea que originó el régimen jurídico moderno de ese derecho, o sea, la necesidad de reservar aquello que es privado. Las tecnologías de la información y comunicación, por más que faciliten el contacto interpersonal mundial y creen nuevas formas de relacionarse, también contribuyen a la

[134] RODOTÀ, op. cit., p. 92.
[135] Ibid., p. 93.

construcción de la esfera privada en la creación de un torre de marfil personal, a medida que evitan aquellos contactos sociales consolidados y cotidianos, aumentando la sensación de autosuficiencia, como, por ejemplo, en los casos de la ampliación del teletrabajo, de la realización de videoconferencias, de la preferencia por el comercio electrónico y por las transacciones bancarias en línea, de predilección por el entretenimiento de los dispositivos inteligentes y conectados, entre otros[136].

En la aldea global, esas tecnologías de la información y comunicación han provocado el enclaustramiento de los individuos en fortalezas electrónicas digitales y han distanciado a los sujetos de las formas de control social posibilitadas por el actuar en público y por la modulación de grupos de interés a partir de la vigilancia sólida. Sin embargo, es verdad que, como se ve en el primer capítulo, las formas de control social son cada vez más invasivas y la vigilancia cada vez más líquida, es decir, dispersa como un fluido por todos los dispositivos sociales, justamente haciendo uso de la recogida, del tratamiento y la transferencia de datos provenientes de esas tecnologías informacionales, como si fueran *backdoors* en esas murallas digitales erigidas.

2.2.2.2. La segunda paradoja: el núcleo duro de la privacidad

En otro sentido, la segunda paradoja de la privacidad se refiere a la propia resignificación de la protección de las informaciones íntimas y secretas, es decir, aquellas que el sujeto quiere que sean excluidas en determinada medida de la circulación en público. Esto, porque los textos normativos, internacionales, comunitarios o nacionales, siguen, en cierta forma, construyendo un "núcleo duro" de la privacidad relativo a la información sensible, que tradicionalmente exigían una mayor capa de protección y secreto, cuyo tratamiento discrecional podría originar una cierta discriminación, como, por ejemplo, los datos relacionados con la salud, el origen étnico, la opinión política, la orientación sexual, la filiación sindical, la creencia religiosa, entre otros[137].

Ocurre que muchas de esas informaciones calificadas como sensibles no están reservadas solamente a la esfera privada del individuo, sino que, por el contrario, en contextos democráticos, están relacionadas con la esfera pública, en la medida en que forman

[136] RODOTÀ, op. cit., pp. 94-95.
[137] Ibid., 95-96.

parte de la identidad del sujeto, pudiendo éste utilizarlas para manifestarse como persona, para encontrar semejantes y diferentes o para ocupar el espacio público, para reconocerse como actor político. De ese modo, se atribuye un estatuto de más privado y se limita fuertemente la circulación y el tratamiento de los datos sensibles no porque sean secretos, sino justamente para que el individuo pueda hacerlos públicos.

2.2.2.3. La tercera paradoja: el derecho y el poder de la privacidad

La tercera paradoja de la privacidad trata de la propia evolución de ese derecho, conforme analizado en el capítulo anterior, ya que la existencia de riesgos derivados de la recogida y tratamiento de datos personales hizo surgir el derecho a la autodeterminación informativa, abarcando la potestad del individuo de preguntar, recibir información, limitar la circulación, oponerse, prohibir y eliminar la información que de ahí se deriva. En verdad, el derecho fundamental a la privacidad, además de un derecho o un conjunto de derechos, también es la atribución de una serie de poderes a los interesados, como si fuera el reconocimiento de derechos implícitos a los derechos de personalidad.

Así, el derecho a la privacidad, en ese nuevo matiz que permite al sujeto acompañar la manipulación de sus datos personales por otras personas o empresas, pone de relevancia el derecho al acceso a dicha información. Es decir, por un lado está el criterio formal de posesión de las informaciones, basada en la legitimidad de la recogida o en el consentimiento del individuo por parte de los responsables y encargados del tratamiento, pero, por otro lado, está la prevalencia del derecho del individuo sobre los propios datos, de forma que el derecho a la privacidad, que, precisamente regula aquello que es privado, íntimo o secreto, acaba por convertirse en instrumento capaz de hacer más transparente y pública la esfera de actuación de los responsables o encargados del tratamiento[138].

2.2.2.4. La cuarta paradoja: el Estado en red

Por último, la cuarta paradoja de la privacidad, pensada a partir del presente trabajo, está desarrollada en el sentido de que el derecho a la privacidad, en comparación con otros derechos fundamentales, trata de la propia subjetividad del ciudadano y exige una actuación

[138] RODOTÀ, op. cit., pp. 96-97.

del Estado para garantizar la protección de esas informaciones personales, ya sea a través de una regulación, o de mecanismos de control, u otros instrumentos normativos. El problema deriva del hecho de que el Estado, siendo un actor social y un nudo de la sociedad en red, para sobrevivir a esa nueva dinámica de poder en red, acaba por violar sistemáticamente la privacidad de los individuos, nacionales y extranjeros, bajo la justificación del interés público, tal como se ha puesto de relieve en el capítulo anterior.

2.2.3. La extimidad como nueva dimensión de la privacidad

Como se mencionó anteriormente, el perfeccionamiento de las tecnologías de información y comunicación y la democratización del acceso a dispositivos informáticos, con la consiguiente popularización de las redes sociales, han hecho aparecer una nueva modalidad híbrida de privacidad, con del surgimiento de un individuo que quiere mantener algunos aspectos de su vida en la esfera privada, de forma ajena al conocimiento general, pero que, al mismo tiempo, también quiere transformar esa esfera privada, en cierta medida, en una esfera pública, en una especie de publicidad de lo privado. Se trata de un desplazamiento del núcleo de la privacidad, a partir de la espectacularización de sí mismo, de la ficcionalización del yo y de la socialización de la intimidad[139].

En otras palabras, en la sociedad digitalmente conectada e influenciada globalmente, no puede hablarse ya más de "la dualidad entre el hombre prisionero de sus secretos y el hombre que nada tiene que esconder; entre la 'casa-fortaleza', que glorifica la privacidad y favorece el egocentrismo, y la 'casa-vitrina', que privilegia los intercambios sociales" [traducción libre][140]. Se configura, entonces, una nueva dimensión de la privacidad, caracterizada por la exteriorización de la interioridad del individuo, resignificando el criterio de público-privado, en razón de los procesos comunicativos de la sociedad en red, en un ejercicio de extimidad[141].

La extimidad, desde el punto de vista psicoanalítico, está fundamentada en la exteriorización de la intimidad, es decir, en la necesidad de dar visibilidad al propio "yo", sea por medio de la revelación de secretos, de la exposición del singular, de la

[139] LIMBERGER, Têmis. *Cibertransparência informação pública em rede:* a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016, p. 60.
[140] RODOTÀ, op. cit., p. 25.
[141] BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

espectacularización de la intimidad o de la ficcionalización de sí mismo, abriendo esa esfera privada al mirar de los demás para que sea validada la propia existencia, para que sea confirmado el propio ser y existir[142]. Considerando que el coste social de la no exposición puede ser grande, los individuos acaban por exponer la intimidad y el secreto, deseando fama, seguidores, interacciones, *likes*, *scores* y visualizaciones, en una autoafirmación constante, terminando por revelar datos personales, patrones sociales e informaciones de preferencias.

Así, en una supuesta autoviolación de la privacidad, los individuos, con el objetivo de formar parte de esa sociedad en red, caracterizada por el consumismo de la información, proporcionan datos relevantes para el acceso y el mantenimiento de productos y servicios, especialmente redes sociales. No se puede, por lo tanto, "trazar un límite, como si el mundo de la defensa de la privacidad y el de la acción pública fueran hostiles o no comunicantes; no existe una separación, sino un *continuum*" [traducción libre], convirtiéndose la privacidad, pues, en un fluido[143].

2.2.4. ¿Se trata de un consentimiento informado libre la aceptación de términos y condiciones?

Cabe señalar, sin embargo, que el suministro de datos personales a cambio de los beneficios sociales que las personas supuestamente aprovechan de los productos y servicios ofrecidos no es la única contrapartida de esa relación, ya que el tratamiento de datos por las organizaciones públicas y privadas puede hacer surgir nuevas concentraciones de poder o el fortalecimiento de poderes ya existentes, como si fuera *plus-poder*. En otras palabras, el ofrecimiento de productos y servicios, a menudo gratuitos, exige del usuario el suministro de datos personales, que no necesariamente sirven para la propia existencia del producto o servicio que llega al individuo, sino para agregar valor a la propia organización como nudo social en la malla del poder en red.

De esta forma, considerando que se vuelve cada vez más difícil determinar sobre qué tipos de información los sujetos están dispuestos a renunciar a una mayor protección, el

[142] LACAN, Jacques. *O seminário:* livro 16: de um Outro ao outro. Rio de Janeiro: Jorge Zahar, 2008, p. 241 [versión española: LACAN, Jacques. *El seminario:* libro 16: de un Outro al otro. Barcelona: Paidos Iberica, 2008].
[143] RODOTÀ, op. cit., p. 47.

control del tratamiento de datos personales depende de la legitimidad y legalidad de esa decisión. En este sentido, se percibe una alteración de paradigma, incluso por el advenimiento del Reglamento General de Protección de Datos Personales de la Unión Europea, superando el *implied consent*, es decir, el consentimiento implícito que suponía que la mera utilización del producto o servicio implicaba en concordancia con la manipulación de los datos; por el *informed consent*, que determina la provisión del mayor número de explicaciones al usuario para que éste concuerde conscientemente con las circunstancias y finalidades del tratamiento de los datos, inicialmente pensado en el ámbito de la salud[144].

En este contexto, se puede cuestionar en qué medida el consentimiento informado tiene potencial de ser un control social y un ejercicio de autodeterminación informativa en lo que se refiere al permiso de circulación de datos. En primer lugar, es importante recordar que el suministro del consentimiento es *conditio sine qua non* para el acceso de productos y servicios en la sociedad en red, sin el cual el usuario no puede disfrutar de las interacciones sociales allí permitidas, convirtiéndose la autorización en una mera etapa en este proceso. En segundo lugar, la obtención del consentimiento informado se limita a un simple *clic* del usuario en un botón predeterminado o en una caja de selección (*blank selection*), eximiendo del real entendimiento de los términos y condiciones presentados, ya que basta la aceptación formal del individuo para que supuestamente se legitime el tratamiento de los datos.

Por otro lado, no siempre el usuario sabe lo que está aceptando, dada la extensión de los textos y la utilización de expresiones jurídico-técnicas, queriendo, además, acceder al producto o servicio, independientemente de lo que esté aceptando en las entrelíneas de las políticas de privacidad. En el marco de la teoría de los mosaicos que refiere que no es el dato, por sí solo, relevante, sino el contexto de informaciones de ahí derivadas[145], no siempre quedan claras las reales finalidades de la recogida de informaciones, ya que es posible generar un sin número de variables para ser manipuladas, confiriéndose valor a depender del tratamiento de datos utilizado y del reconocimiento de patrones informacionales deseados.

Es importante citar, como se ha observado en el capítulo anterior, que esa cuestión de consentimiento pierde relevancia cuando se enfrenta a las justificaciones del régimen de vigilancia electrónica global de personas e informaciones, una vez que el interés privado se

[144] TARODO, op. cit., pp. 143-144.
[145] CONESA, op. cit., p. 45.

pliega al interés público de protección y prevención de amenazas contra la seguridad pública. El propio Reglamento General de Protección de Datos de la Unión Europea contempla esta excepción al régimen jurídico de aplicación general[146]. Sin embargo, la propia existencia de los programas de vigilancia masiva para salvaguardar la seguridad nacional fue descubiertos bajo polémicas internacionales, demostrando ser desconocidas o insuficientes las condiciones de supervisión pública o garantías seguras y reales del cumplimiento de los derechos y garantías de los ciudadanos por parte de esas agencias institucionales.

En lo que se refiere al consentimiento, cabe la crítica de que éste no es necesariamente consciente o libre, en el propio sentido de las palabras, porque sometido a esa lógica informacional y a ese proceso de subjetivación creado por el consumo de las tecnologías de la información y comunicación, "raramente el ciudadano es capaz de percibir el sentido que la recogida de determinada información puede asumir en organizaciones complejas y dotadas de medios sofisticados para el tratamiento de datos" [traducción libre], siendo posible que no conozca o hay reflexionado sobre la peligrosidad del uso de tales informaciones por parte de diferentes responsables, lo que convierte en inerme al individuo frente a esas organizaciones[147].

2.2.5. De las nuevas características de la privacidad del siglo XXI: el interés colectivo por la protección a la privacidad

Es necesario tener en cuenta que, en realidad, las normativas en cuanto a la regulación de datos no sirven para prohibir el tratamiento de la información, ya que la libre circulación de datos personales es una realidad de la sociedad en red. No se puede olvidar que se camina hacia un contexto espacio-temporal marcado por los datos personales como bien económico, especialmente si se considera la perspectiva de *Internet of Things* e *Internet of Everything*, donde la inteligencia artificial y el proceso de *data learning* y *machine learning* imperan en una economía de la información con el flujo continuo de datos personales.

---

[146] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

[147] RODOTÀ, op. cit., p. 37.

Así, por un lado, parece haber un justificación social pública que permite la recogida y el tratamiento de datos en los casos de interés general y de defensa nacional, no habiendo poder de disposición de tales informaciones por los usuarios (hasta porque ni siquiera saben que son blancos de monitoreo en estos casos); por otro lado, parece haber un determinismo social que obliga a los individuos a producir y entregar informaciones relevantes a los proveedores de productos y servicios para que aquellos participen en la sociedad en red. En otras palabras, por un lado, los datos son recolectados compulsivamente por parte de las agencias institucionales de seguridad, pero por otro lado los datos también se recolectan obligatoriamente como moneda de cambio para acceso a productos y servicios informacionales.

En cualquier caso, el interesado parece estar obligando a disponer de sus datos, siendo que, a partir de esos nuevos reglamentos de protección de datos, esta disposición está legítimamente fundada, ya que, por ejemplo, en el ámbito del RGPD, la licitud del tratamiento de datos se observa cuando los datos se obtienen a partir del consentimiento del usuario, o para la ejecución de un contrato, o para el cumplimiento de una obligación a la que el responsable esté sujeto, o para la defensa de los intereses vitales del interesado, o para el ejercicio de funciones de interés público o al ejercicio de la autoridad pública de la que está investido el responsable del tratamiento o, aún, a efectos de los intereses legítimos perseguidos por el responsable del tratamiento o por terceros[148].

Así pues, no se trata de limitar la circulación de información en la sociedad en red, sino de defender los derechos y las libertades fundamentales de las personas físicas, en particular, su derecho a la protección de los datos personales. En esta línea de pensamiento, se evidencia el cambio de paradigma de la privacidad, de "persona-información-sigilo" a "persona-información-circulación-control", llegando a un problema ulterior, que, en realidad, desafía el derecho a la privacidad en tiempo de ciberseguridad: el control, que, a su vez, debe dejar de ser individual y pasar a ser colectivo.

En este escenario de "persona-información-circulación-control", hay que tener en cuenta que, en el panorama anterior, la información personal estaba bajo dominio del

[148] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

interesado, de forma que era el quien tenía el control sobre lo que divulgar o no, pero, actualmente, estas informaciones son compartidas y quedan esparcidas en la red. Y si, antes, la violación de la privacidad era esencialmente el chisme y la revelación de secretos, ahora, la violación se da por métodos desconocidos, abstractos, por la manipulación de datos informáticos, el empleo de algoritmos y otras herramientas oscuras, produciéndose un aumento del valor agregado de las informaciones personales, de modo que el valor de la persona deja de estar en ella misma y pasa a sus datos, sometiéndose a la lógica del mercado.

El control del flujo de información es tanto interno, es decir, de las informaciones que salen del individuo y van hacia el exterior, como externo, o sea, de las informaciones que llegan al individuo (derecho de no saber, no querer publicidad, no participar). Las tecnologías de la información y la comunicación, por el propio papel de aproximar a las personas y acortar distancias, ha hecho extremadamente sutil la frontera entre la esfera pública y la privada, siendo que la autodeterminación personal y la construcción libre de la esfera privada pasaron a ser condición para el desarrollo y la efectividad de la esfera pública.

Por estas razones, la función sociopolítica del derecho a la privacidad sobrepasa los límites de los intereses individuales y se convierte en un elemento importante en la construcción de la ciudadanía. En una sociedad digitalmente conectada, la definición de la privacidad sólo como el "derecho a ser dejado sólo" es insuficiente, debiendo ser extendida a una tutela global y colectiva, en un cuadro caracterizado por la libertad de las elecciones personales y existenciales. El derecho a la privacidad deja de ser sólo un derecho de una persona a limitar las intromisiones de otros individuos o del Estado en lo que es privado o un derecho de exigir del Estado que impida tales intromisiones, pasando a ser un derecho colectivo, de una multitud. Un derecho que el Estado necesita asegurar por defecto, considerando las nuevas paradojas y paradigmas de la sociedad en red[149].

2.2.6. Para un nuevo derecho a la privacidad: estrategias de tutela

El derecho a la privacidad, en esta lógica de "persona-información-circulación-control", presupone nuevas estrategias de tutela, de modo que el derecho a la autodeterminación informativa y el derecho a la protección de los datos personales, que se configuran como condiciones de ciudadanía, que no pueden dejarse a merced de la

[149] RODOTÀ, op. cit., pp. 128-129.

autorregulación o de las relaciones contractuales, exigiendo del Estado una tutela positiva y proactiva; tales como garantías institucionales, que remite a "la existencia de determinadas instituciones, a las que se considera como componentes esenciales y cuya preservación se juzga indispensable para asegurar los principios constitucionales"[150].

Para ello, es necesario apuntar cinco estrategias para la protección de este nuevo derecho a la privacidad. La primera estrategia es reforzar y ampliar el derecho a la oposición contra determinadas formas de recogida, tratamiento y circulación de datos personales, posibilitando tanto iniciativas individuales, como proposiciones colectivas, en la medida que fortalece el equilibrio de poderes para permitir que los interesados se opongan al tratamiento de datos y ejerzan sus derechos[151]. El RGPD, en su art. 21, establece que "el titular de los datos tiene el derecho de oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de los datos personales que le conciernen", incluso en lo que se refiere a la recogida de datos a efectos de comercialización directa y la creación de perfiles basada en esa relación[152].

Junto al derecho de oposición, la segunda estrategia debe tener en cuenta y perfeccionar el derecho a no saber, es decir, el derecho de resistir al tratamiento y de recibir la información procedente, que pueda causar algún trauma o incomodidad a la paz y al bien del presunto interesado[153]. Se trata, pues, de la posibilidad de rechazar marketing directo o indirecto, de no recibir publicidad no deseada o no solicitada o basada en tratamiento de datos sensibles, cancelar inscripciones en listas para recibir correos de diferentes tipos, como publicidad, noticias, *newsletters*, *spam*, incluso los anuncios políticos.

La tercera estrategia debe poner de relevancia el derecho al olvido, es decir, el derecho de supresión de los datos personales, sin demora injustificada, especialmente en los casos en que las informaciones dejen de ser necesarias para la finalidad que había motivado el tratamiento, o cuando el titular retira el consentimiento en que se basa la manipulación de las informaciones, siendo ese derecho extensible, incluso, a los buscadores e indexadores de

[150] ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 32/1981, de 28 de julio. *Boletín Oficial del Estado*, n. 193, 13 de agosto de 1981, p. 31.
[151] RODOTÀ, op. cit., p. 133.
[152] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.
[153] RODOTÀ, op. cit., pp. 133-134.

páginas electrónicas[154]. Sin embargo, hay que considerar que el derecho al olvido es una de las categorías más polémicas del derecho a la protección de los datos personales, ya que, por otro lado, existe la argumentación sobre la prevalencia de motivos de interés público, libertad de expresión, libertad de información, persona o hecho público, cumplimiento de determinada obligación legal, entre otros casos.

La cuarta estrategia se refiere a la necesidad de hacer más claro, más urgente, más visible y más comprensible el principio de la finalidad, es decir, la condición que ratifica la recogida y el tratamiento de los datos personales por parte de los responsables y encargados, determinado, explícito y legítimo, según, por ejemplo, establece el art. 5.1, "b", del RGPD[155]. Esto quiere decir que no debería bastar el mera enunciado de la indicación de la finalidad, sino la importación de recursos y herramientas para que el usuario tenga el completa conocimiento de las causas, consecuencias e impactos del consentimiento que está proporcionando, teniendo en cuenta, inclusive, la crítica anteriormente mencionada sobre el consentimiento en la era del consumo de productos y servicios en red.

Por último, la quinta estrategia es, en realidad, un giro en el pensamiento. Si es verdad que el suministro de datos personales es el *login*, condición de entrada a la sociedad en red, y el consentimiento del titular está virtualmente viciado en razón de la necesidad de consumir irracionalmente las redes sociotécnicas, en detrimento del correcto entendimiento de las implicaciones derivadas de la entrega y el tratamiento de la información personal; entonces la privacidad puede y debe servir como herramienta para el equilibrio de poderes en esta nueva arquitectura social a partir de la limitación de los intereses de las agencias institucionales de seguridad y de las corporaciones económicas, de modo que, nacida como una particularidad, la privacidad puede ser entendida, cada vez más, como un instrumento colectivo de trascendencia social, siendo que los defectos y los fracasos de las leyes y reglas "[...] son resultado de asociar la privacidad con los intereses de las personas, los que al final suelen verse opacados por necesidades sociales antagónicas"[156].

[154] RODOTÀ, op. cit., p. 134.
[155] UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.
[156] NISSENBAUM, Helen. *Privacidad amenazada*: tecnología, política y la integridad de la vida social. Tradujo: Enrique Mercado. México: Editorial Océano, 2011, p. 95

2.2.7. El Efecto Orwell: el derecho a la privacidad en la sociedad de vigilancia

Con la popularización de las tecnologías de información y comunicación, parece emerger una democratización del "público", a medida que cada vez se habla más de motivos, intereses e identidades públicas; y menos, de lo que es privado, reservado, íntimo, aunque el tema de la privacidad esté en el imaginario colectivo. A finales del siglo XX, se hablaba del "fin de la privacidad", pero la discusión se adentra en el nuevo siglo con la creación de escudos de privacidad, leyes de acceso a la información, leyes de regulación de Internet, de telecomunicaciones y de servicios de la sociedad de información, así como regulaciones y leyes de protección de datos personales por todo el mundo, además de decisiones y sentencias defendiendo la garantía de las diversas dimensiones del derecho a la privacidad.

Hay, sin embargo, quien defiende que la privacidad es un paréntesis de la modernidad, quedando entre las pequeñas comunidades del mundo pre-moderno que ya no existen y la comunidad global de la postmodernidad aún por venir, ambas, marcadas por el control social y vigilancia de los ciudadanos[157]. En este contexto, la tutela de la privacidad queda condicionada a los intereses y avances económicos o a una autorregulación por el mercado, lo que puede comprometer aún más la verdadera protección de ese derecho, ya que las redes de poder financiero tienden a eliminar los espacios propios de la privacidad haciendo prevalecer el beneficio lucrativo y la publicidad[158].

Por otro lado, la privacidad, entendida como algo más que el "derecho de ser dejado sólo", puede ser transformada en herramienta social en el juego de poderes de la sociedad en red, cuando logra limitar y controlar directamente a los sujetos públicos y privados que recogen y tratan los datos personales. Si la información personal es el oro más importante del nuevo siglo, la exigencia de un derecho a la privacidad positivo, regulado, explícito y sancionador puede contribuir a equilibrar los intereses, de modo que, siendo un contrapeso en esa balanza, puede representar un ejercicio de democracia.

Se debe, por lo tanto, rechazar la justificación de que el ciudadano honesto no tiene nada que esconder, tampoco qué temer, a partir de la difusión de las informaciones y del tratamiento derivada de esa recogida, una vez que la metáfora del hombre de cristal es una expresión totalitaria, que subraya la pretensión del Estado de saber todo, incluso los aspectos más íntimos de los individuos. El Efecto Orwell debe ser al revés, posibilitando a los sujetos

[157] RODOTÀ, op. cit., p. 144.
[158] Ibid.

vigilar al Gran Hermano, bajo todos los lados y esferas, en un Estado de cristal, ya que el ente estatal, caracterizado por la defensa del interés público, debe estar sometido al control de la multitud.

El derecho a la privacidad y, especialmente la regulación de ese derecho, puede ser utilizado como moneda de cambio para exigir cada vez más transparencia a la Administración Pública, no necesariamente una transparencia recibida, pues es necesario una transparencia exigida/impuesta[159]. Es el caso de la contravigilancia, ejercida sustancialmente por movimientos y actores de hackativismo, activismo mediático, *cypherpunks* y *whistleblowers*, que intentan "invertir el vector dominante de vigilancia social, para, con ello, producir nuevas narrativas sociales por medio de prácticas adyacentes de control y vigilancia del propio Estado y/o de las grandes corporaciones empresariales, especialmente por movimientos sociales" [traducción libre][160].

La contravigilancia trata de los conjuntos de actores, procesos, actuaciones y dispositivos, normalmente conectados en redes, para proteger "contra la vigilancia perpetrada por los órganos institucionales y por las corporaciones empresariales y, más aún, vigilar a quién también vigila al cuerpo social, en el intento de hacer cesar la violación de derechos y garantías fundamentales y humanas" [traducción libre][161]. La contravigilancia en sentido estricto trata de la específica tentativa de neutralizar la vigilancia realizada por el Estado y por las grandes corporaciones, a partir de técnicas de bloqueo de una vigilancia dominante o desestabilización del vigilante, revelando y divulgando su actuación, haciendo públicos documentos e informaciones de interés público, informando sobre violaciones de derechos y garantías, entre otras prácticas[162].

Es decir, si no hay otra alternativa para los individuos en el siglo XXI que no sea el control de la circulación de las informaciones, una vez que la economía de vigilancia y el suministro de datos personales es la realidad determinista que se aproxima, es posible utilizar las propias tecnologías de información y comunicación para vigilar al Estado y a las grandes corporaciones, promoviendo un control público para que cada vez sean más públicas,

[159] CASTELLS, Manuel. *A galáxia internet:* reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007, p. 220 [versión española: CASTELLS, Manuel. *La galaxia internet:* reflexiones sobre internet, empresa y sociedad. Madrid: Debolsillo, 2003].
[160] PESSOA, op. cit., p. 102.
[161] PESSOA, op. cit., p. 102.
[162] Ibid., p. 103.

transparentes y cristalinas[163]. Se trata de vigilar a quien vigila, para que estén incómodos lo suficiente, para seguir las reglas; se trata de aumentar la transparencia pública de quien viola la privacidad para que estén preparados para respetar las nuevas dimensiones del derecho a la privacidad en la sociedad en red.

[163] ROSANVALLON, Pierre. *La contrademocracia*: la política en la era de la desconfianza. Buenos Aires: Manantial, 2007.

CONCLUSIONES

Con el presente trabajo, se ha podido reflexionar sobre los impactos de las tecnologías de la información y comunicación y del régimen global de vigilancia social en el derecho a la privacidad, en el contexto de la ciberseguridad del siglo XXI. Objetivamente, se han analizado a) las implicaciones del régimen de monitoreo social global y los impactos en la sociedad del siglo XXI; b) la contribución de las personas en dicho régimen a partir del suministro de datos para el acceso a productos y servicios; c) la estructura normativa global y regional del derecho a la privacidad, el cambio y los enfoques del concepto a lo largo del tiempo; y d) la resignificación del derecho a la privacidad en el contexto de la ciberseguridad.

I. En la sociedad en red del siglo XXI, se ha constatado la existencia de un recrudecimiento de un régimen global de vigilancia social, basado en la cooperación entre agencias estatales para monitoreo del flujo de datos en la sociedad y control de personas y grupos de interés, por medio de la manipulación de las informaciones personales. La vigilancia social, desde hace siglos, funciona como un dispositivo para el ejercicio de poder, de forma que tal dominación se ha visto acrecentada con el desarrollo de las tecnologías de información y comunicación y con el advenimiento de la grandeza informática del *big data.*

Ese régimen global de vigilancia social está fundamentado en discursos oficiales legitimadores, transpuestos a normativas nacionales e internacionales, justificando el monitoreo de ciudadanos nacionales y extranjeros en favor del combate a enemigos abstractos, como el terror, para garantizar la seguridad y defensa nacional, entre otros argumentos, sin el debido conocimiento público y publicidad necesaria, tanto que los programas de monitoreo fueron descubiertos entre polémicas y vergüenza internacionales. Entonces, se hace perceptible el advenimiento de un Estado de vigilancia, haciéndose presente en la vida de las personas de forma invisible, no jerárquica, descentralizada y personalizada en una nueva arquitectura social de sociedad en red.

II. En el marco de esta nueva arquitectura social, los usuarios contribuyen con el funcionamiento de este sistema, marcado por la manipulación de algoritmos y la creación

de patrones de comportamiento, a partir del suministro de datos personales. En esta sociedad en red de flujos comunicacionales mundiales, hay una lógica consumista de tecnologías de información y comunicación y un proceso de subjetivación continua y modulada, ya que la construcción de una identidad pública depende de la entrega de las informaciones personales.

Si antes la vigilancia dependía de dispositivos institucionales, ahora está distribuida en los dispositivos personales, en una reinvención del panóptico de poder por el hombre caracol, es decir, el que lleva en sí mismo una vigilancia, que, por otro lado, también permite la vigilancia del otro, en una retroalimentación de datos. En el panorama del *Internet de las Cosas* y del *Internet de Todo*, se trata de una economía de vigilancia, a partir del suministro de datos personales para acceso a productos y servicios, como si fuese un nuevo oro del siglo XXI, que, al fin y al cabo, se ha convertido en condición para participar en este nuevo paradigma social tecnológico.

III. El derecho a la privacidad, incluso a partir de figuras afines, como "vida privada y familiar" e "intimidad", se establece en las principales normativas internacionales, comunitarias, regionales y nacionales. El reto es que la privacidad como la conocemos, a partir de una perspectiva histórica, filosófica y jurídica, como substancialmente el "derecho de ser dejado solo" y de no sufrir interferencias ajenas y estatales en lo que es privado, ha sufrido una revolución en ese nuevo paradigma social derivado de los avances de las tecnologías de la información y comunicación.

De ahí, han surgido nuevos riesgos y amenazas, que hacen posibles otras formas de violación de la privacidad teniendo en cuenta los diferentes procesos de manipulación y tratamiento de datos personales, de característica automatizada y continua. De ese modo, el concepto tradicional se ha vuelto insuficiente para tratar este nuevo marco tecnológico, en especial, con referencia a nuevos matices que han surgido, como el derecho a la autodeterminación informativa y el derecho a la protección de datos personales, de manera que la privacidad se extiende también al control sobre la circulación de la propia información personal.

Existe una preocupación estatal-normativa por tutelar el derecho a la privacidad (aunque muy basada en la lógica de "persona-información-sigilo"), tanto que esa protección aparece, aunque como otras figuras, en diferentes normativas internacionales,

comunitarias, regionales y nacionales. Sin embargo, debe haber un esfuerzo por ampliar ese derecho frente a las nuevas tecnologías de información y comunicación, como ocurrió con el establecimiento del derecho a la autodeterminación informativa y el derecho a la protección de datos personales como derechos fundamentales, lo que se puede percibir con el advenimiento de nuevas normativas, como es el caso del Reglamento General de Protección de Datos Personales de la Unión Europea y de otras leyes de tutela de informaciones personales.

IV. Ante el recrudecimiento del régimen global de vigilancia social, con dispositivos de vigilancia distribuidos por el globo, personales y personalizadas, así como ante la necesidad de proporcionar datos personales para acceso y consumo de productos y servicios de la sociedad en red, en una lógica de subjetivación, el concepto de privacidad como el "derecho a ser dejado en paz" o el "derecho a ser dejado solo" es insuficiente para tutelar esa nueva realidad social, aunque esa propia característica de reservado no ha dejado de existir en sí, sino que hay nuevas dimensiones que necesitan una mayor reflexión.

En efecto, la privacidad, en la concepción tradicional, ha sufrido diferentes tipos de violaciones de protección. Ahora bien, el panorama anterior de "persona-información-sigilo", en el que el sujeto podía protegerse de intromisiones no deseadas en lo que le es reservado, acaba por ser insuficiente, convirtiéndose ese régimen global de vigilancia social y ese suministro de datos como en condición de ingreso del sujeto a la sociedad en red.

Esto, porque, por un lado, aunque el individuo quiera mantener el secreto sobre ciertas informaciones y definir lo que es su privacidad, las agencias de seguridad nacional y las agencias estatales, en asociación con empresas de tecnologías, interceptan, monitorean, clasifican e intercambian datos personales recogidos. Por otro lado, el determinismo social que exige el suministro de datos personales para acceso de productos y servicios tecnológicos también rompe con la lógica de la reserva, aún más cuando el sujeto no tiene plena conciencia y consentimiento sobre la entrega de la información personal.

En una realidad en que todo y todos están interconectados, aunque no necesariamente digitalmente, en una sociedad en red, hay que reconocer que el paradigma

de la arquitectura social está cambiando, exigiéndose una adaptación frente a las complejidades de ser. Es decir, si el derecho y la normatividad necesitan acompañar a la evolución social, buscando ajustarse a los cambios y novedades, es imprescindible desapegarse de dogmas jurídicos y actualizar las condiciones de regulación. Es el fin del derecho a la privacidad, pero no en el tono aterrorizado de finales del siglo XX, sino tal y como se le conoce y como fue transpuesto en normativas alrededor del globo.

V. En conclusión, es necesario repensar el derecho a la privacidad, considerando el régimen global de vigilancia social y la alteración del paradigma permitido con las tecnologías de la información y comunicación. Es decir, es preciso aceptar que ha llegado al fin un largo proceso evolutivo de conceptualización del derecho a la privacidad como un derecho de ser dejado en paz, pasando a tratarse de un derecho de control sobre las informaciones personales. Dicho nuevo derecho debe llevar en consideración las diferentes paradojas que la privacidad abraza en el siglo XXI; especialmente, en lo que se refiere a la fluidez de los espacios público-privado, al advenimiento de una nueva dimensión de extimidad y a la supuesta falacia del consentimiento informado.

El derecho a la privacidad ha cambiado a una lógica "persona-información-circulación-control", apuntándose, para tutela de ese nuevo derecho, cinco estrategias: la ampliación del derecho a la oposición contra el tratamiento de datos personales; la ampliación del derecho de no saber y de resistir al recibimiento y al tratamiento de la información; el establecimiento del derecho al olvido, especialmente digital; la mejora del principio de la finalidad; y, finalmente, el giro de pensamiento sobre lo que puede significar la privacidad en tiempos de ciberseguridad. Así, se puede concluir que la privacidad del siglo XXI puede ser entendida como un derecho colectivo para exigir cada vez más transparencia de aquellos que tratan los datos; para que se sienten incómodos hasta el punto de respetar las reglas y proteger la privacidad de los ciudadanos en una revisión de la obra orwelliana.

VI. El siglo XX ha revolucionado los procesos comunicativos y el flujo de ideas en la sociedad hiperconectada, pero el siglo XXI comienza proyectando un mayor intercambio de informaciones, en una economía de datos personales, siendo cada vez más inminente la libre circulación de personas, productos, servicios y datos en comunidades digitales del

mundo, incluso en un *Internet de Todo*. Se trata de una fuerza imparable, en la que el derecho a la privacidad, sólo entendido en la concepción individual de "persona-información-sigilo" no puede ser un objeto inamovible, bajo peligro de una catástrofe normativa y una falacia reguladora.

En el régimen global de vigilancia social, aquí entendido como el panorama de monitoreo de información personal y de suministro de datos personales para acceso de productos y servicios en la sociedad en red, el derecho a la privacidad puede suponer un régimen global de contravigilancia social. Por lo tanto, se puede invertir el vector determinante de vigilancia, para vigilar a quien vigila, tornándose los que, hasta entonces, eran objetos de vigilancia en sujetos de vigilancia, de modo que ese régimen, inevitable por sí solo ante los avances de las tecnologías de la información y comunicación, siga las reglas del juego democrático.

En una visión holística del mundo, bajo la lógica "persona-información-circulación-control", se debe comprender el derecho a la privacidad, además de todas las dimensiones antes discutidas y antes previstas, también como un derecho de interés social colectivo, perteneciente a una colectividad, a una transindividualidad. Esto es, además de ser un derecho individual, en que el sujeto puede requerir la tutela para sí, el derecho a la privacidad también puede ser visto como una garantía institucional, un derecho de todos a exigir una protección especial y difusa, dirigida al cuerpo social, al cuerpo multitud.

REFERENCIAS BIBLIOGRÁFICAS

ARENDT, Hannah. *A condição humana.* 10. ed. Rio de Janeiro: Forense Universitária, 2005. [versión española: ARENDT, Hannah. *La condición humana*. Barcelona: Paidos Iberica, 2016]

ARENDT, Hannah. Reflections on Little-Rock. En: *Dissent Magazine*, v. 6, n. 1, inv, 1959.

ASSANGE, Julian. *Cypherpunks*: liberdade e futuro da internet. São Paulo: Boitempo, 2013. [versión española: ASSANGE, Julian. *Cypherpunks*: la libertad y el futuro de internet. Barcelona: Deusto S.A., 2013]

AYUSO, Silvia; PEREDA, Cristina. *Obama conmuta la pena de la soldado Chelsea Manning.* [El País, 18 jan. 2017] [en línea] [Fecha de consulta: 10/04/2019] Disponible en: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245.html.

BAJARIN, Tim. *The next big thinh of tech:* the Internet of Everything. [Time, 13/01/2014] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

BAUMAN, Zygmunt. *Vida para consumo***.** A transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar, 2008. [versión española: BAUMAN, Zygmunt. *Vida de consumo.* Madrid: S.L. Fondo de Cultura Económica de España, 2007]

BAUMAN, Zygmunt. *Vigilância líquida***:** diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013. [versión española: BAUMAN, Zygmunt. *Vigilancia líquida*. Barcelona: Planeta, 2015]

BENTHAM, Jeremy. O panóptico ou a casa de inspeção. In: TADEU, Tomaz (Org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008. p. 13-88.

BIGO, Didier; TSOUKALA, Anastassia. *Terror, insecurity and liberty:* illiberal practices of liberal regimes after 9/11. New York: Routledge, 2008.

BLASCO, Lucía. *Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto*. [BBC News, 05/07/2018] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.bbc.com/mundo/noticias-44724389.

BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

BRADLEY, Joseph. DIXIT, Amitabh. GUPTA, Vishal *et al. Internet of Everything:* A $4.6 trillion public-sector opportunity. San Jose: Cisco. 2013. [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-public-sector-vas-white-paper.pdf.

BRANDEIS, Louis. WARREN, Samuel. The right to privacy. En: *Harvard Law Review*, v. IV, n. 5, dez. 1890. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://faculty.uml.edu/sgallagher/brandeisprivacy.htm.

CADWALLADR, Carole; CONFESSORE, Nicholas; ROSENBERG, Matthew. *How Trump Consultants Exploited the Facebook Data of Millions*. [The New York Times, 17/03/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

CAPRA, Fritjof. *A Teia da Vida:* uma nova compreensão científica dos sistemas vivos. São Paulo: Cultrix, 1996. [versión española: CAPRA, Fritjof. *La trama de la vida:* una nueva perspectiva de los sistemas vivos. 3. ed. Barcelona: Anagrama, 2009]

CAPRA, Fritjof. *As conexões ocultas*. São Paulo: Cultrix, 2002. [versión española: CAPRA, Fritjof. *Las conexiones ocultas*: implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo. Barcelona: Anagrama, 2006]

CASTELLS, Manuel. *A Era da Informação*: economia, sociedade e cultura. A sociedade em rede, vol. 1. 3. ed. São Paulo: Paz e Terra. 2002. [versión española: CASTELLS, Manuel.

La Era de la Información: economía, sociedad y cultura. La sociedad en red, vol. 1. Madrid: Alianza Editorial, 2005]

CASTELLS, Manuel. *A galáxia internet:* reflexões sobre internet, negócios e sociedade. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007. [versión española: CASTELLS, Manuel. *La galaxia internet:* reflexiones sobre internet, empresa y sociedad. Madrid: Debolsillo, 2003]

CASTELLS, Manuel. *O poder da comunicação*. São Paulo: Paz e Terra, 2013. [versión española: CASTELLS, Manuel. *Comunicación y Poder*. Madrid: Alianza Editorial, 2009]

CASTELLS, Manuel. *O poder da identidade*. 2. ed. São Paulo: Paz e Terra, 2000. [versión española: CASTELLS, Manuel. *La Era de la Información:* economia, sociedade y cultura. El poder de la identidad, vol. 2. Madrid: Alianza Editorial, 2003]

COLOMÉ, Jordi Pérez. *Facebook compartió datos sensibles de sus usuarios con más de 150 grandes empresas.* [El País, 20/12/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html.

CONESA, Fulgencio Madrid. *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia, 1984.

COSTA JR. Paulo José da. *O direito de estar só:* tutela penal da intimidade. 2. ed. São Paulo: RT, 1995.

DAUER, Stella. *Entenda tudo sobre as permissões de aplicativos e proteja seu Android.* [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://www.androidpit.com.br/permissoes-aplicativos.

DELEUZE, Gilles. *Conversações:* 1972-1990. São Paulo: 34, 1992. [versión española: DELEUZE, Gilles. *Conversaciones.* Valencia: Pre-textos, 1995]

DERIX, Steven. MODDERKOLK, Huib. *50.000 pakketjes kwaardaardige software*. [NRC, 23/11/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.nrc.nl/nieuws/2013/11/23/50000-pakketjes-kwaardaardige-software-1316266-a1157982.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Âmbito Jurídico*, Rio Grande, XI, n. 51, mar. 2008. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460.

FERNÁNDEZ, Déborah. *Las cinco V's del Big Data.* [DataHack, 27/08/2018] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.datahack.es/cinco-v-big-data/.

FOLLOUROU, Jacques. *Surveillance*: la DGSE a transmis des données à la NSA américaine. [Le Monde, 30/10/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html.

FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). 4. ed. São Paulo: Martins Fontes, 2005. [versión española: FOUCAULT, Michel. *Hay que defender la sociedad:* curso del Collège de France (1976). Madrid: Akal, 2003]

FOUCAULT, Michel. *Microfísica do poder*. 23 ed. São Paulo: Graal, 2004 2004 [versión española: FOUCAULT, Michel. *Microfísica del poder:* genealogía del poder. Madrid: La Piqueta, 1978].

FOUCAULT, Michel. *Vigiar e punir:* História da violência nas prisões. 41. ed. Petrópolis: Vozes, 2013. [versión española: FOUCAULT, Michel. *Vigilar y castigar:* nacimiento de la prisión. Ciudad del México: Siglo XXI, 2012]

GREENWALD, Gleen. *Sem lugar para se esconder:* Edward Snowden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014. [GREENWALD, Gleen. *Sin un lugar donde esconderse*: Edward Snowden, la NSA y el Estado de Vigilancia en los Estados Unidos. Barcelona: Ediciones B, 2014]

GREENWALD, Glenn. *XKeyscore*: NSA tool collects 'nearly everything a user does on the internet'. [The Guardian, 31/07/2013] [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

HARDT, Michael; NEGRI, Antonio. *Império*. São Paulo: Record, 2012. [versión española: HARDT, Michael; NEGRI, Antonio. *Imperio.* Barcelona: Paidos Iberica, 2005]

HRON, Martin. *Os últimos 10 maiores vazamentos de dados.* [Avast, 14/02/2019] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://blog.avast.com/pt-br/os-ultimos-10-maiores-vazamentos-de-dados.

HUBMANN, Heinrich. *Das persönlichkeitsrecht.* Münster: Böhlau-Verlag, 1953.

LACAN, Jacques. *O seminário:* livro 16: de um Outro ao outro. Rio de Janeiro: Jorge Zahar, 2008, p. 241. [versión española: LACAN, Jacques. *El seminario:* libro 16: de un Outro al otro. Barcelona: Paidos Iberica, 2008]

LIMBERGER, Têmis. *Cibertransparência informação pública em rede:* a virtualidade e suas repercussões na realidade. Porto Alegre: Livraria do Advogado, 2016, p. 60.

MARS, Amanda. *Zuckerberg pide perdón en el Senado y advierte de la amenaza de Rusia*. [El País, 11/04/2018] [en línea] [Fecha de consulta: 21/04/2019] Disponible en: https://elpais.com/internacional/2018/04/10/actualidad/1523380980_341139.html.

MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão:* decisões anotadas sobre direitos fundamentais. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo:

Konrad-Adenauer Stiftung – KAS, 2016. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877.

McCARTHY, Tom. *NSA director defends plan to maintain 'backdoors' into technology companies.* [The Guardian, 23/02/2015] [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies.

MILL, John Stuart. *A liberdade*. São Paulo: Martins Fontes, 2000. [versión española: MILL, John Stuart. *Sobre la libertad.* Madrid: Verbum, 2016]

MUGUERZA, J. De la conciencia al discurso ¿un viaje de ida y vuelta? In: *La filosofía moral y política de Jürgen Habermas*. Madrid: Biblioteca Nueva, 1997, pp. 63-110,

NISSENBAUM, Helen. *Privacidad amenazada*: tecnología, política y la integridad de la vida social. México: Editorial Océano, 2011.

NORTON-TAYLOR, Richard. *Not so secret: deal at the heart of UK-US intelligence*. [The Guardian, 25/06/2010]. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica*. Madrid: Editorial Universitas, S.A., 2012, p. 93.

PESSOA, João Pedro Seefeldt. *"Verás que um filho teu não foge à luta":* a contravigilância na sociedade em rede e a nova ação conectiva dos movimentos sociais do século XXI. Director: Rafael Santos de Oliveira. [Trabajo Final de Máster]. Universidade Federal de Santa Maria, Departamento do Direito, Santa Maria, 2018.

PHAM, Sherisse. *WikiLeaks dice que la CIA espía a través celulares y televisores, ¿qué tan preocupado debes estar?* [CNN, 08/03/2017] [en línea] [Fecha de consulta: 22/04/2019]

Disponible en: https://cnnespanol.cnn.com/2017/03/08/wikileaks-dice-que-la-cia-espia-a-traves-de-smartphones-televisores-y-mas-que-tan-preocupado-debes-estar/.

PIRES, Hindenburgo Francisco. Geografia das indústrias globais de vigilância em massa: limites à liberdade de expressão e organização na internet. *Ar@cne Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales*, Universidad de Barcelona, n.º 183, abr. 2014. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: http://www.ub.edu/geocrit/aracne/aracne-183.htm#_edn16.

REAL ACADEMIA ESPAÑOLA. Diccionario del español jurídico. *Big data.* [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://dej.rae.es/lema/big-data.

REINO UNIDO. *The economic value of data:* discussion paper. Londres: HM Treasury, 2018. [en línea] [Fecha de consulta: 20/04/2019] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODRÍGUEZ-PINA, Gloria. *El método nada tecnológico que usa Mark Zuckerberg para protegerse de los hackers.* [El País, 22/06/2016] [en línea] [Fecha de consulta: 22/04/2019] Disponible en: https://verne.elpais.com/verne/2016/06/22/articulo/1466617774_991020.html.

ROSANVALLON, Pierre. *La contrademocracia:* la política en la era de la desconfianza. Buenos Aires: Manantial, 2007.

SPRENGER, Polly. *Sun of privacy:* 'get over it'. [Wired, 26/01/1999] [en línea] [Fecha de consulta: 05/07/2019] Disponible en: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

TARODO, Salvador Soria. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: *Derecho y Salud*, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006.

TAURION, Cezar. *Volume, variedade, velocidade, veracidade e valor:* os cinco Vs do Big Data. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://computerworld.com.br/volume-variedade-velocidade-veracidade-e-valor-os-cinco-vs-do-big-data.

WIKILEAKS. *What is WikiLeaks*. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: https://wikileaks.org/What-is-Wikileaks.html.

REFERENCIAS NORMATIVAS

BRASIL. Constituição da República Federativa do Brasil de 1988. *Diário Oficial da União,* n. 191-A, 05 de octubre de 1988, pp. 1-32

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União,* 11 de enero de 2002, pp. 1-76.

COMISIÓN ASIÁTICA DE DERECHOS HUMANOS. *Carta Asiática de los Derechos Humanos de 1998*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.humanrights.asia/wp-content/uploads/2018/07/Asian-Human-Rights-Charter-2nd-Edition-English.pdf.

CONSEJO DE EUROPA. *Convenio Europeo de Derechos Humanos de 1950*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf.

ESPAÑA. Constitución Española de 1978. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311, pp. 29313 a 29424.

ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 32/1981, de 28 de julio. *Boletín Oficial del Estado*, n. 193, 13 de agosto de 1981, p. 31.

ESPAÑA. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. *Boletín Oficial del Estado,* 14 de mayo de 1982, núm. 115, pp. 12546 a 12548.

ESPAÑA. Tribunal Constitucional de España (Pleno). Sentencia nº 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, n. 4, 4 de enero de 2001, pp. 104-118.

ESPAÑA. Ministerio de Defensa. Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. *Boletín Oficial de Ministerio de Defensa*, 26 de febrero de 2013, n. 40, pp. 4154-4156.

FRANCIA. *Déclaration des Droits de l'Homme et du Citoyen de 1789*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789.

LIGA ÁRABE. *Carta árabe sobre los derechos humanos 2004*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.lasportal.org/ar/sectors/dep/HumanRightsDep/Documents/%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A.pdf.

ORGANIZACIÓN DE LA CONFERENCIA ISLÁMICA. *Declaración de los Derechos Humanos en el Islam de 1990*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oic-iphrc.org/en/data/docs/legal_instruments/OIC_HRRIT/571230.pdf.

ORGANIZACIÓN DE LAS NACIONES UNIDAS. *Declaración Universal de Derechos Humanos de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.un.org/es/universal-declaration-human-rights/.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Declaración Americana de los Derechos y Deberes del Hombre de 1948*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. *Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de 1969*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.

ORGANIZACIÓN PARA LA UNIDAD AFRICANA. *Carta Africana sobre los Derechos Humanos y de los Pueblos de 1981*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2002/1297.pdf.

UNIÓN EUROPEA. Parlamento Europeo. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea,* L 281, 23 de noviembre de 1995, pp. 31-50.

UNIÓN EUROPEA. Parlamento Europeo. Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. *Diario Oficial de la Unión Europea*, L 24, 30 de enero de 1998, pp. 1-8.

UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea de 2000*. [en línea] [Fecha de consulta: 17/04/2019] Disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

UNIÓN EUROPEA. Parlamento Europeo. *Informe de 11 de julio de 2001 sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON).* [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//ES.

UNIÓN EUROPEA. Parlamento Europeo. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de la Unión Europea* L 201, 31 de julio de 2002, pp. 37-47.

UNIÓN EUROPEA. Parlamento Europeo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General sobre la protección de datos). *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, pp. 1-88.

UNIÓN EUROPEA. Tribunal Europeo de Derechos Humanos. *Caso de Big Brother Watch and Others contra Reino Unido (Applications nº. 58170/13, 62322/14 and 24960/15).*

Sentencia de 13 de septiembre de 2018. [en línea] [Fecha de consulta: 16/04/2019] Disponible en: http://hudoc.echr.coe.int/eng?i=001-186048.