Derecho PUCP
ISSN: 0251-3420
ISSN: 2305-2546
revistaderechopucp@pucp.edu.pe
Pontificia Universidad Católica del Perú
Perú

Santos Divino, Sthéfano Bruno
Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos
Derecho PUCP, núm. 83, 2019, pp. 179-206
Pontificia Universidad Católica del Perú
Perú

DOI: https://doi.org/10.18800/derechopucp.201902.006

https://doi.org/10.18800/derechopucp.201902.006

DERECHO PUCP
N° 83, 2019
diciembre-mayo
pp. 179-206
REVISTA DE LA FACULTAD DE DERECHO

Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos

Skeptical, Theoretical and Economic Reflections on the Necessary Consent for Data Processing

STHÉFANO BRUNO SANTOS DIVINO*
Universidade Federal de Lavras (Brasi)l

Resumen: ¿Existe correspondencia o afinidad entre las concepciones jurídico-principiológica y fáctico-económica respecto a la efectiva protección del consentimiento del titular de datos personales en la contratación en red? Bajo el manto del presente cuestionamiento, se pretende analizar el escenario contractual contemporáneo bajo la óptica de la política de privacidad y de la Ley General de Protección de Datos (LGPD) brasileña. En este contexto, se propone una reflexión escéptica acerca de las directrices principiológicas y económicas defendidas por la ley y la doctrina para verificar si el consentimiento es un instrumento de real eficacia para la tutela de los sujetos en red. El primer tópico se corresponde con el análisis conceptual y principiológico del consentimiento en la LGPD y en la doctrina especializada. El segundo tema aborda la racionalidad limitada de los usuarios de los servicios en red con relación a la comprensión de las disposiciones de las políticas de privacidad y en términos de servicios electrónicos. Al final, se concluye que —a pesar de la defensa jurídico-principiológica destinada a solidificar el consentimiento como herramienta indispensable para la recolección y tratamiento de datos— el actual modelo contractual electrónico no posibilita su efectiva concreción, proponiendo, en este caso, una alternativa. Se ancla el razonamiento en los métodos deductivos, de investigación bibliográfica e integrada, y en la técnica de estudio de casos.

Palabras clave: consentimiento, LGPD, tratamiento de datos, privacidad, protección de datos

Abstract: Is there a correspondence or affinity between the juridical-principiological and factual-economical conceptions for the effective protection of the consent of the holder of personal data when hiring in a network? Under the mantle of the present question, it aims to analyze the contemporary contractual scenario under the perspective of the privacy policy and the Brazilian General Data Protection Law (LGPD). In this context, it is proposed a skeptical reflection on the principles and economic guidelines defended by law and doctrine to verify if the consent is an instrument of real effectiveness to the tutelage of the subjects in network.

* Máster en Derecho Privado por la Pontificia Universidad Católica de Minas Gerais (2019). Licenciado en Derecho por el Centro Universitario de Lavras (2017). Profesor suplente de Derecho de Propiedad Privada en la Universidade Federal de Lavras. Abogado.
Código ORCID: https://orcid.org/0000-0002-9037-0405. Correo electrónico: sthefanodivino@ufla.br

The first topic concerns the conceptual and conceptual analysis of consent in the LGPD and in the specialized doctrine. The second topic deals with the limited rationality of the users of the network services in understanding the dispositions in the policies of privacy and in the terms of electronic services. At the end, it is concluded that despite the juridical and legal defense aimed at solidifying consent as an indispensable tool for collecting and processing data, the current electronic contractual model does not allow its effective concretization, proposing, in this case, an alternative. The rationale is anchored in the deductive, bibliographical and integrated research methods and in the case study technique.

***Key words*:** consent, RGPD, data processing, privacy, data protection

I. INTRODUCCIÓN

Las nuevas dimensiones de la recopilación y el procesamiento de datos establecidas por la Ley Brasileña de Protección de Datos (LGPD) permiten esbozar un proceso de protección dirigido principalmente al derecho a la privacidad. Al identificar las raíces del poder establecido en el primer dispositivo normativo de la norma antes mencionada, el legislador optó por adoptar algunas posiciones cuestionables durante la aplicación legal.

Inspirada por la literatura distópica —*1984,* de George Orwell (2004) y *Un mundo feliz,* de Aldous Huxley (1978)—, la recopilación de información para vigilar y castigar (Foucault, 2004) al individuo —manteniéndolo en la máquina panóptica (Bentham, 2000), con o sin violencia (Orwell y Huxley, respectivamente)— es una de las formas más efectivas de control y manipulación conductual individual en torno a los reflejos sociales. Lo mismo ocurre con la caracterización de nuestra organización social como una sociedad cada vez más compleja en lo referente a la acumulación y circulación de información. Ello implica el nacimiento de un nuevo recurso básico, que vincula el establecimiento de nuevas situaciones de poder: el poder basado en la información (Rodotà, 2008, p. 28).

«Poder» y «sociedad de la información» son dos términos utilizados que, sin una delimitación adecuada, se presentan como vacíos interpretativos que quedan a discreción del lector. Una definición más elaborada brinda una mayor posibilidad de control sobre nuestros objetivos. Por ello,

buscaremos dicha precisión, comenzando por lo más problemático. El poder no fue ni puede ser definido en pocas palabras. Para Hannah Arendt, «el poder corresponde a la capacidad humana no solo de actuar, sino de actuar en concierto» (2001, p. 36). Significa que el poder nunca es propiedad individual, sino que pertenece a un grupo. La existencia del poder continuará siempre que el grupo permanezca unido (Arendt, 2001, p. 36). Cuando el grupo del que se origina el poder desaparece, su poder también se desvanecerá. Según la autora, el poder se distingue principalmente de la violencia. Esta tiene carácter instrumental. Los usos de la violencia están diseñados para multiplicar el vigor[1] natural hasta que, en su última etapa de desarrollo, puedan reemplazarlo (Arendt, 2001, p. 37).

Para Castells,

> el poder[2] es la capacidad relacional que permite a un actor social influir asimétricamente en las decisiones de otros actores sociales de manera que favorezca la voluntad, los intereses y los valores del actor empoderado. El poder se ejerce a través de la coerción (o su posibilidad) y/o construyendo un significado basado en los discursos a través de los cuales los actores sociales guían su acción. Las relaciones de poder están enmarcadas por la dominación, que es el poder que se encarna en las instituciones de la sociedad. La capacidad relacional del poder está condicionada, pero no determinada, por la capacidad estructural de dominación. Las instituciones pueden entablar relaciones de poder que dependen de la dominación que ejercen sobre sus sujetos (2009, p. 10).

Dado que el ejercicio del poder se realiza mediante la coerción o la construcción de significado mediante el cual los actores sociales guían su acción, la descripción ontológica de Castells parece coincidir con la de Arendt. Si bien la naturaleza del poder se abstrae del grupo social, su ejercicio se instrumentaliza de otras maneras. El poder, al lado de la

1 «El vigor designa inequívocamente algo singular, una entidad individual; es la propiedad inherente de un objeto o persona y pertenece a su carácter y puede probarse a sí mismo en relación con otras cosas o personas, pero es esencialmente diferente de ellos» (Arendt, 2001, p. 37).

2 Para M. Foucault (1989, pp. 183-184), el poder no puede entenderse como propiedad de nadie, ya que está descentralizado. No existe un centro de poder desde el cual el poder fluya, se extienda, se reproduzca y se difunda hasta alcanzar finalmente los niveles moleculares. El análisis del poder debe realizarse por medio de lo que lo circula, como algo que funciona en cadena. No hay forma de verificar si se encuentra aquí o allá; nunca está en manos de algunos; nunca es propiedad de algunos, como riqueza o bien. Su significado relacional lo caracterizaría como una red de la que nadie puede escapar. No hay límites externos o fronteras que puedan detenerlo. Y, dialécticamente, por un lado, el individuo es utilizado por las relaciones de poder, mientras que por otro sirve como vehículo para dichas relaciones. Un punto destacado importante es lo que Foucault llama la descentralización del ejercicio del poder. En la época moderna y contemporánea, el poder asumió nuevas características: la descentralización y la difusión. Así, el poder puede ser ejercido por todos los individuos, manifestándose de diversas maneras en innumerables prácticas diarias. «El poder es un conjunto de relaciones; en lugar de derivar de la superioridad, el poder produce asimetría; en lugar de actuar de forma intermitente, actúa de forma permanente; en lugar de actuar de arriba hacia abajo, sometiéndose, irradia de abajo hacia arriba, manteniendo las instancias de autoridad; en lugar de aplastar y confiscar, alienta y produce productos» (Albuquerque, 1995, p. 109).

producción[3] y la experiencia[4], es una perspectiva teórica que subyace al enfoque de la organización social mediante relaciones históricamente determinadas (Castells, 2017, p. 72)[5].

El término «sociedad de la información» tiene una conceptualización compleja. Castells (2017, p. 81), responsable de la formulación de este término, advierte que no se debe compartir la visión tradicional de la sociedad formada por niveles superpuestos, con tecnología y economía subterránea, poder de entrepiso y cultura de techos. A pesar de la definición audaz, Castells recuerda que una sociedad no puede considerarse enteramente informativa. Hay núcleos en varios lugares que ni siquiera se ponen en contacto y conocen los dispositivos tecnológicos. El uso de esta terminología debe hacerse con precaución, porque un sector muy amplio o incluso mayoritario de la población del mundo utiliza medios tecnológicos para mantenerse informada. La principal característica especial de la sociedad de redes es la conexión de red entre lo local y lo global. Debería referirse específicamente a la aparición de una nueva estructura social, en la que la información se utiliza como recurso y entrada al propio poder.

Los rasgos fundamentales de la disciplina de protección de datos personales sirven como punto clave para ilustrar y redimensionar su problemática actual, vinculada a la transformación tecnológica, social y económica. Primero, la concepción contemporánea de la privacidad como un derecho no es la misma concepción que se defendió en siglos pasados. Su reinterpretación como un derecho luego de ser considerada como un bien perteneciente solo a los sujetos de la nobleza y el clero se produjo solo en 1890, con el ensayo «The Right to Privacy», de Warren y Brandeis (1890). Los autores reconocieron la noción legal de este derecho como *the right to be alone* (el derecho a estar solo). Este esquema, en un contexto actualmente computarizado y conectado, parece verse debilitado frente a la vigilancia y la observación de la red.

Lo que es notable hoy en día es, sobre todo, según Rodotà, «la posibilidad de que individuos y grupos controlen el ejercicio de poderes basado en la disponibilidad de información, contribuyendo así a establecer equilibrios sociopolíticos más apropiados» (2008, p. 24). La privacidad «está en el

3 «La producción es la acción de la humanidad sobre la materia (naturaleza) para apropiarse y transformarla en su beneficio, obteniendo un producto, consumiendo (irregularmente) parte de él y acumulando excedentes para la inversión de acuerdo con varios objetivos socialmente determinados» (Castells, 2017, p. 72).

4 «La experiencia es la acción de los sujetos humanos sobre sí mismos, determinada por la interacción entre las identidades biológicas y culturales de estos sujetos en relación con sus entornos sociales y naturales. Está construido por la eterna búsqueda de la satisfacción de necesidades y deseos» (Castells, 2017, p. 72).

5 «El poder se basa en el estado y su monopolio institucionalizado sobre la violencia, aunque lo que Foucault llama la microfísica del poder, encarnada en instituciones y organizaciones, se extiende por toda la sociedad, desde los lugares de trabajo hasta los hospitales, encerrando a los sujetos en una estructura estricta de deberes formales y agresiones informales» (Castells, 2017, p. 72).

campo legal, son actos humanos externos a la intimidad, reservados por la persona o por su naturaleza» (Maceira, 2015, p. 65)[6], trascendiendo la simple noción de intimidad, entendida como la esfera más reservada del individuo. Allí, «su información personal está protegida para que no llegue al conocimiento de otra persona, convirtiéndose en un campo inviolable, protegido infra y constitucionalmente, también se refiere a su propia imagen ante los medios de comunicación» (Nery, 2010).

El lugar de la autodeterminación informativa es el reconocimiento de que la privacidad tiene características positivas y negativas. Esto resulta más reconocible y detectable cunado se expresa en el comportamiento de terceros con el fin de evitar interferencias en la esfera particular del titular de dicho derecho. La concepción positiva, por otro lado, consiste en acciones o conductas en las que el titular de la privacidad actúa para protegerla, corroborando sus facultades y preceptos informativos —los cuales pueden o no entrar en su esfera legal—. En resumen, se trata del control informativo del titular de los derechos sobre lo que puede hacerse público o mantenerse en privado, ya sea yendo de lo primero a lo segundo o de lo segundo a lo primero.

Por lo tanto, «el derecho a la privacidad o el derecho a la protección se basa en la defensa de la personalidad humana contra los mandatos o las intrusiones de otros» (Paesani, 2014, p. 34), así como «abarca el derecho del individuo a controlar la recopilación y el uso de sus datos personales» (Martínez, 2014, p. 53).

Dado este escenario, a continuación, se resumen algunas tendencias. Por un lado, podemos notar la resignificación del concepto de privacidad: así, el nuevo enfoque — trascendiendo la aproximación tradicional desde el poder de exclusión— le atribuye una relevancia más amplia y clara al poder de control. Por el contrario, el objeto del derecho a la privacidad se expande: cuando se habla en privado, las áreas que reciben una protección específica relacionada con la intimidad no se identifican necesariamente (Rodotà, 2008, p. 93). Aquí es donde surge una de las paradojas de la privacidad, descrita por Rodotà como «la situación en la que la tensión relativa a la privacidad (aparentemente) se contradice o produce consecuencias (aparentemente) inesperadas» (2008, p. 95). En resumen: como vivimos en una sociedad de la información en la que estamos rodeados de instrumentos de vigilancia constante, la búsqueda de la privacidad (según su concepto tradicional) se convierte en una paradoja. Por esta razón, debe entenderse ahora como «el derecho

6 Para José Afonso da Silva (2008, p. 100), «el conjunto de información sobre el individuo que puede decidir mantener bajo su exclusivo control, o comunicar, decidir a quién, cuándo, dónde y en qué condiciones, sin poder estar legalmente sujeto sería el concepto ideal de privacidad».

a mantener el control sobre las propias informaciones» (Rodotà, 2008, p. 92)[7].

Frente a los desafíos contemporáneos descritos, el problema que se investiga en el presente artículo resulta estimulante: ¿existe una correspondencia o afinidad entre las concepciones jurídicas de principios y las fácticas-económicas con respecto a la protección efectiva del consentimiento del titular de los datos personales en la contratación de la red? Teniendo en cuenta el presente cuestionamiento, el objetivo es analizar el escenario contractual contemporáneo desde la perspectiva de la política de privacidad y la Ley General de Protección de Datos (LGPD) brasileña.

Este trabajo se justifica por la compatibilidad incongruente entre las proposiciones defendidas por la legislación y la doctrina y las pautas prácticas utilizadas para la recopilación y el procesamiento de datos. Por un lado, tenemos la protección internacional de la privacidad defendida en la Declaración Universal de Derechos Humanos (artículo XII). Por otro lado, las prácticas económicas utilizan modalidades contractuales contemporáneas (esencialmente la adhesión) para hacer cumplir la política de privacidad con pocas restricciones derivadas de la privacidad y de la voluntad del titular de los datos.

En este escenario, proponemos una reflexión escéptica sobre las directrices y principios de la economía defendidos por la ley y la doctrina, con el fin de verificar si el consentimiento es un instrumento eficaz para proteger a los sujetos en la red. El primer tema es el análisis conceptual, basado en los principios del consentimiento en la LGPD y la doctrina especializada. El segundo punto aborda la racionalidad limitada de los usuarios de servicios de red para comprender las disposiciones de las políticas de privacidad y los términos de los servicios electrónicos. Por último, se concluye que —a pesar de la defensa de principios legales dirigida a solidificar el consentimiento como una herramienta indispensable para la recopilación y procesamiento de datos— el modelo contractual electrónico actual no permite su implementación efectiva.

7 Puede surgir una pregunta sobre la diferencia entre los derechos de privacidad y la protección de datos. En principio, la divergencia entre ellos es aparentemente terminológica. Sin embargo, tratemos de delimitar el alcance de ambos. Si bien el derecho a la privacidad es un instituto autónomo de la personalidad del propietario que le permite controlar lo que entra y sale de su esfera privada a través de su autodeterminación informativa, la protección de datos puede considerarse como un tipo de privacidad. Se puede decir que son dos caras de la misma moneda. El ejercicio de la protección de datos se basa no solo en la autodeterminación informativa, sino también en la privacidad, ya que está incluido en ella. Aunque la protección de datos está restringida a un solo aspecto de la privacidad —si se la considera como un todo—, es posible afirmar que es un elemento complementario. Desde esta perspectiva, no parece lógico estipular una dicotomía y estratificar, por un lado, el derecho a la privacidad y, por otro, la protección de datos. Ontológicamente están unificados. Sin embargo, para delimitar y abordar aspectos didácticos, la protección de datos está consagrada como un tipo de privacidad con respecto a la atención y delimitación de los actos informativos que se toman del ámbito privado de su titular, mientras que el derecho a la privacidad aborda algo más amplio, no restringiéndose solo a la información recopilada y procesada en el ámbito virtual.

Existe una incompatibilidad entre la dogmática legal y el pragmatismo económico. Por un lado, se encuentra la idealización de una protección aparentemente utópica. Por otro lado, está la existencia de un nicho capitalista que utiliza oportunidades aparentemente indispensables y la provisión de servicios en la sociedad contemporánea para la recolección y procesamiento de datos. Para que las directrices legales sean efectivamente concretas, se propone reestructurar los contratos electrónicos, de modo tal que exista la posibilidad de que el propietario pueda manifestar expresamente su voluntad de ceder o no sus datos.

Para la elaboración del razonamiento actual, se utilizan diferentes metodologías. La metodología de investigación bibliográfica e integrada se utilizará para buscar obras doctrinales de académicos en el área que puedan contribuir a generar una teoría más amplia y concisa, a fin de definir y delimitar los significados teóricos para restringir el objeto de estudio a la protección de datos y de la privacidad. La metodología deductiva se utilizará junto con la técnica de estudio de caso. El punto de partida son las situaciones legales y económicas expresadas por los titulares de datos personales en el mercado de consumo. A partir de ello, analizaremos su inclusión y participación efectiva en la creciente rama del *e-commerce* y, deductivamente, su inclusión en y adhesión a los contratos electrónicos que regulan este tipo de relación comercial (especialmente la política de privacidad y los términos del servicio).

II. EL CONSENTIMIENTO REQUERIDO PARA LA RECOPILACIÓN Y PROCESAMIENTO DE DATOS EN LA LEY GENERAL DE PROTECCIÓN DE DATOS: REFLEXIÓN ACERCA DE LOS PRINCIPIOS

La lógica de principios de LGPD reitera los preceptos fundamentales de la libertad de expresión, información, comunicación y opinión. El primero de estos derechos puede entenderse como «el derecho a expresar libremente una opinión, un pensamiento o una idea —no necesariamente, estrictamente, con respecto a los hechos, eventos o datos que han tenido lugar; sino también, eventualmente, con relación a un mundo de ideas, sin que necesariamente estos puntos de vista sean verídicos e imparciales; debiéndose respetarse la privacidad de los demás» (Cavalieri Filho, 2014, p. 144). «La libertad de expresión es, más precisamente, la libertad de expresar opiniones, juicios de valor sobre hechos, ideas; por lo tanto, juicios de valor sobre las opiniones de los demás, etcétera» (Sarlet, 2014, pp. 446-461).

En cuanto al derecho a la información, este también es protegido en la Constitución Federal de 1988, en su artículo 5, punto XIV; en la Ley de Acceso a la Información Pública de 2011; así como en la Convención Americana sobre Derechos Humanos de 1969 en el contenido del

artículo 13. Este derecho tiene como objetivo, en resumen, «buscar, recibir y difundir información e ideas de todo tipo, sin tener en cuenta los límites, ya sea verbalmente o por escrito, o en forma impresa o artística, o por cualquier otro proceso de su elección» (Convención Americana sobre Derechos Humanos, 1969, art. 13.1)[8].

Finalmente, los derechos de comunicación y opinión son intrínsecos y se amalgaman en la libertad de expresión. Por lo tanto, según lo previsto en el artículo 13, punto II del segundo capítulo de la Convención Americana de Derechos Humanos[9], el ejercicio de estos derechos no está sujeto a censura[10] previa. Sin embargo, la responsabilidad posterior por su violación y su uso excesivo puede regirse por la ley.

Las informaciones proporcionadas por personas/usuarios en contrataciones electrónicas[11] para obtener ciertos servicios genera nuevos contextos significativos. En cantidad y calidad, permiten una serie de usos secundarios rentables para los administradores de sistemas interactivos. Es decir, se puede vender información. Sin embargo, la disciplina de recopilar y procesar información no puede reducirse a su valor individual. Según Rodotà, «su verdadero tema es el papel del ciudadano en la sociedad informatizada, la distribución del poder vinculada a la disponibilidad de información y, por lo tanto, la forma en que se recopila y pone en circulación» (2008, p. 46).

8 «El derecho a informar, como un aspecto de la libertad de expresión del pensamiento, es un derecho individual, pero ya contaminado por un sentido colectivo, debido a las transformaciones de los medios, de modo que la caracterización más moderna del derecho a la comunicación, que se concreta especialmente en los medios de comunicación de masas, implica la transmutación del antiguo derecho de la prensa y la expresión del pensamiento a través de estos medios en derechos de carácter colectivo» (Silva, 2008, pp. 110-111).

9 «Artículo 13. Libertad de pensamiento y expresión. 1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas».

10 «La censura es la restricción previa a la libertad de expresión, lo que hace que, cuando hay una prohibición, se remita a la idea de un gobierno autoritario en el que se censura información que no se considera necesaria o favorable desde el punto de vista de los gobernantes» (Canotilho, Mendes, Sarlet & Streck, 2013, p. 275). Además, como «una característica inherente del derecho a la libertad de expresión, existe la presunción de inconstitucionalidad de todos los medios utilizados para llevar a cabo la censura, ya sea privada o pública» (Canotilho & Machado, 2014, p. 129).

11 «El contrato electrónico, a su vez, es la transacción legal bilateral que resulta de la reunión de dos declaraciones de voluntad y se concluye a través de la transmisión electrónica de datos. Generalmente consiste en la aceptación de una oferta pública disponible en Internet o una propuesta enviada al destinatario correcto por correo electrónico, que contiene al menos la descripción del bien y/o el producto ofrecido, el precio y las condiciones de pago» (Finkelstein, 2004, pp. 187-188).
Para Oliver Iteanu, el contrato electrónico «es la reunión de una oferta de bienes o servicios que se expresan de forma audiovisual a través de una red internacional de telecomunicaciones y una aceptación que se puede expresar a través de la interactividad» (Iteanu, 1996, p. 27).
En opinión de Semy Glanz, «un contrato electrónico es aquel que se suscribe mediante programas de computadora o aparatos con dichos programas. No requieren firma o requieren firma codificada o contraseña» (Glanz, 1998, p. 72).

La inmaterialidad de la información en red como recurso hace que las desviaciones hacia las prácticas totalitarias sean menos notorias. En efecto, dicho régimen puede surgir sin los signos que tradicionalmente lo acompañan, ya que la protección y la tutela de estos derechos trascienden la perspectiva individual y agudizan las sensibilidades sociales, estimulando la capacidad de reacción (Rodotà, 2008, p. 58).

Cuando la recopilación y el procesamiento de datos personales pueden sistematizar y amalgamar los preceptos del orden público, social y económico —como se identificó anteriormente, especialmente el derecho a la personalidad[12]—, podremos verificar la defensa y la protección eficaz de la dignidad y el ejercicio de la ciudadanía por parte de las personas físicas. Y, además se aplica la ley de protección al consumidor. Por lo tanto, en el caso de situaciones en las que el código de consumo es aplicable, se entiende que el diálogo de las fuentes tiene lugar, convirtiendo al consumidor en el mayor beneficiario de una u otra normativa.

Los límites impuestos a la recopilación y difusión de información en el escenario virtual-tecnológico tienden a encontrarse en las pautas de principios legales. En el escenario brasileño, estas disposiciones están reguladas por el artículo 6 de la LGPD. Una referencia importante que el legislador ha elegido presentar es el respeto a la buena fe. En sus términos objetivos, según lo previsto en el artículo 422 del Código Civil brasileño de 2002[13], se deben observar todas sus funciones y deberes adjuntos.

Aunque existe una disensión en la doctrina sobre el número y la delimitación de los elementos contenidos en cada una de las referencias enumeradas anteriormente, al menos tres son comunes y verificables en cada una. Con respecto a los deberes adjuntos, debe verificarse el deber de protección y cuidado, información y aclaración, y lealtad y probidad (Cordeiro, 2011). En cuanto a sus funciones, existe la interpretativa (artículo 113 del Código Civil), la de control (artículo 187 del Código Civil) y la integradora (artículo 422 del Código Civil) (Martins-Costa, 1999).

En virtud de esta última función, la aplicabilidad y la incidencia de la buena fe objetiva se asume en todas las fases contractuales. Así, tanto el agente de recopilación y procesamiento de datos como el interesado deben actuar en consecuencia para lograr el cumplimiento de esa relación obligatoria.

12 La personalidad se refiere a «una susceptibilidad a la propiedad de los derechos y obligaciones legales» (De Cupis, 2008, p. 19). Los derechos que se le atribuyen son «facultades legales cuyo objeto son los diversos aspectos de la persona del sujeto, así como sus extensiones y proyecciones» (França, 1983, p. 37).

13 «Artículo 422. Los contratistas están obligados a respetar los principios de probidad y buena fe al concluir el contrato y en su ejecución».

Además de la buena fe objetiva, el principio rector general de las relaciones privadas, el primer principio enumerado por la LGPD es el de propósito. En él podemos verificar la presencia de características consideradas, entonces, indispensables para la obtención del consentimiento necesario para el *data processing.*

Depende del agente de tratamiento definir las situaciones específicas a las que se asignarán los datos recopilados después del tratamiento. Esta conducta se materializa a través de la especificación, la cual supone indicar las categorías de datos que serán objeto de esa relación legal; de la explicitación, por la cual el agente de procesamiento de datos demostrará al interesado cómo, dónde y cuándo se realizará el procedimiento; y de la información, proceso por el cual se asegurará que el sujeto pasivo sepa la cantidad de información que se puede recopilar y almacenar en el dominio del sujeto activo.

Entre estas situaciones, la legislación prohíbe la posibilidad de tratamiento adicional de una manera incompatible con los propósitos inicialmente acordados. La condición del interesado no puede ser agravada, por regla general. Sin embargo, si el agente de tratamiento obtiene el consentimiento específico para esto, él/ella podrá aceptar las adiciones contractuales y permitir la recolección de acuerdo con los nuevos propósitos, de acuerdo con el artículo 9, § 2 de la LGPD[14].

El principio de adecuación prescribe que la exigibilidad de los datos que se recopilan y procesan está vinculada a la actividad del agente activo. Se vuelve verificable, por ejemplo, en una conducta en la que una institución financiera actúa como un agente de gestión mediante la recopilación de información financiera de sus clientes. Debido a que la actividad comercial adquiere su carácter de institución financiera, es justificable adoptar estrategias legales integradas para mejorar los servicios ofrecidos al cliente, a partir de la recopilación de datos relacionados con los gastos X, en el día A y en la hora Y.

Por el contrario, de conformidad con el artículo 5, II, de la LGPD, si la institución está recopilando datos tales como «creencias religiosas, opinión política, afiliación sindical u organización religiosa, filosófica o política, datos de salud o vida sexual, datos genéticos» intrínsecamente sensibles, fuera de su ámbito de línea de negocios, incluso si hay un consentimiento expreso del titular que autoriza dicha conducta, se puede

14 «Artículo 9 El titular tiene derecho a acceder fácilmente a la información sobre el procesamiento de sus datos —que debe estar disponible de manera clara, apropiada y abierta— en torno a, entre otras características previstas en la normativa para cumplir con el principio de libre acceso: [...] § 2 En caso de que se requiera el consentimiento, si hay cambios en el propósito del procesamiento de datos personales no compatibles con el consentimiento original, el controlador informará al titular con anticipación de los cambios del propósito, y el titular puede revocar el consentimiento si no está de acuerdo con las alteraciones».

verificar una afrenta al principio considerando su falta de disponibilidad y oponibilidad *erga omnes*.

Además, de acuerdo con el principio de necesidad, el agente de procesamiento debe justificar el motivo de sus acciones al interesado en esa relación contractual. Es justo dar razones específicas y objetivas por las cuales se recopilan datos. Y la ley es estricta en este sentido, considerando las autorizaciones y justificaciones genéricas que no delimitan correctamente el propósito y la objetividad de la conducta practicada allí por el agente activo[15].

La descripción del cuarto principio garantiza el libre acceso de los datos a su titular, previa solicitud. Como la legislatura no ha delimitado las modalidades de esta solicitud, ya sea judicial o extrajudicial, se entiende que puede aceptarse la aplicabilidad de ambas. En un primer momento, el procedimiento extrajudicial puede ser una forma efectiva de garantizar la eficacia principiológica que venimos discutiendo, ya que presenta un procedimiento menos solemne y más rápido en relación con el proceso judicial. Sin embargo, eso no significa que el propietario deba pasar por canales extrajudiciales solo para usar los canales judiciales más adelante. Debido al principio que señala que la protección judicial no puede obviarse, está clara la posibilidad del uso directo de los procedimientos judiciales. Pero, por supuesto, la directiva se refiere a una orientación más ligera y menos problemática, dado el escenario actual del poder judicial brasileño.

Con respecto al principio de calidad y transparencia, el legislador reprodujo el contenido de los principios de propósito, adecuación y acceso abierto con otros vocabularios. Como ya hemos hecho las consideraciones necesarias al respecto, solo hay un breve aspecto que discutir. Con relación a los secretos comerciales e industriales, tenemos la obligación de no hacer. En tal situación, en caso de que se verifique, el controlador puede denegar el acceso a los datos precisamente para cumplir con su obligación. Por lo tanto, si el titular persiste en el interés de verificar los datos, debe solicitarlos en el tribunal, para que el magistrado analice la situación y determine si necesario o no.

Los principios de seguridad, protección y responsabilidad son independientes, pero actúan juntos. Dado que tenemos la posibilidad de que el tratamiento se realice en medios materiales e inmateriales, existen amenazas efectivas de que pueden aumentar los costos de transacción del agente de tratamiento. La protección contra *hackers* informáticos, el entorno de acceso controlado, etcétera —en conformidad con el artículo 6, VII de la LGPD—, son ejemplos de situaciones y «medidas técnicas y

15 «Artículo 8, § 4 El consentimiento debe ser para fines específicos, y las autorizaciones genéricas para el procesamiento de datos personales serán nulas» (LGPD).

administrativas diseñadas para proteger los datos personales del acceso no autorizado y de la destrucción, pérdida, alteración, comunicación o difusión accidental o ilegal». En caso de que uno de estos eventos ocurra debido al incumplimiento del principio de protección incluido en la LGPD[16], el agente puede ser responsable de cualquier daño al interesado, de conformidad con los artículos 31-32 y 42-45 de la LGPD. En este caso, para evitar responsabilidad, además de las hipótesis legales descritas en los últimos artículos, de conformidad con el artículo 6, X, de la LGPD, el agente debe demostrar la adopción de medidas efectivas capaces de manifestar la observación y el cumplimiento de las normas de protección de datos personales, incluida la efectividad de dichas medidas.

Finalmente, el principio de no discriminación, previsto en el artículo 6, IX de la LGPD tiene una ontología vinculada a datos sensibles. Además, según el artículo 5, II, de la LGPD, bajo ninguna circunstancia el agente de procesamiento puede usar «datos personales sobre origen racial o étnico, creencia religiosa, opinión política, afiliación sindical u organización religiosa, filosófica o política, datos de salud o vida sexual, datos genéticos o biométricos» para discriminar al titular y proporcionarle servicios y productos a diferentes precios.

Entre los requisitos indispensables para realizar el procesamiento de datos se encuentra el énfasis del consentimiento. Primero, uno debe delimitar el aspecto conceptual de este término, pero tal tarea no es fácil. Se supone que un sujeto de derecho tiene autonomía para decidir y elegir sobre los aspectos de su vida. El ejercicio de este discernimiento como una herramienta singular desarrolla la autodeterminación como capacidad de practicar o no realizar un acto particular propuesto. Específicamente, en el campo legal, la aplicación del consentimiento se produce como un elemento constitutivo de la esfera empresarial. La externalización psíquica de este consentimiento, esta voluntad, este deseo, esta creencia en lograr algo y este fenómeno intencional es lo que pretende constituir un contrato. Un sujeto X solo vende bienes muebles o inmuebles porque tiene la intención de venderlos. A partir de criterios racionales sumados al discernimiento, el sujeto desarrolla una capacidad de ejercicio mental para elegir lo que quiere para su vida. Este aspecto se extiende incluso a derechos considerados muy personales, como la realización económica del derecho a la imagen. Un actor famoso o un sujeto famoso que aspira, desea, pretende hacer un uso económico de su imagen; quiere que ello suceda mediante la externalización psicológica de su voluntad en el aspecto práctico —lo que puede o no registrarse en un instrumento contractual—. Por lo tanto, el consentimiento se considera la llave maestra y el elemento indispensable para un

16 «Artículo 6, VIII – prevención: medidas tomadas para evitar daños por el procesamiento de datos personales».

negocio jurídico. Al principio, nadie puede ser parte de un contrato que no quiere. El contenido de las cláusulas contractuales debe ser compatible con las pautas psicológicas seguidas por el contratista, bajo pena de violación de su autonomía y de la buena fe objetiva. Así, el consentimiento adquiere un énfasis importante en el ejercicio del titular como persona. Su logro como el bien supremo está en la satisfacción y la realización del bien objetivado por su consentimiento, abstraído de su discernimiento y criterios racionales. En términos generales, por lo tanto, el consentimiento supone la externalización de la intencionalidad del individuo a través de actos de habla para el ejercicio y la práctica de un acto al que él o ella aspira. En consecuencia, el consentimiento para el procesamiento de datos solo se otorgará si el titular lo comprende y tiene la intención de otorgarlo.

El artículo 7 de la LGPD brasileña establece algunas hipótesis alternativas en las que el procesamiento de datos sería legítimo. Se entiende en este punto que, como la legislatura usó la conjunción disyuntiva «o» al final del ítem IX, si está configurada, cualquiera de las hipótesis presentes en otros ítems permitiría el procesamiento de datos, independientemente de si se acepta o no. Considérese lo siguiente: en una lectura hermenéutica, si la legislatura decidiera aplicar plenamente el consentimiento en las otras hipótesis prescritas en la normativa en cuestión, habría creado puntos en el ítem I, en lugar de crear otros incisos. O, más bien, habría incluido tal requisito en el encabezado del artículo. Además, utilizó la conjunción disyuntiva «o», en un contexto en el que podría haber limitado la hipótesis a la confección de la primera. Por esta razón, incluso si no hay consentimiento del titular, si se configura alguna de las hipótesis presentes en los puntos II a X, el procesamiento de los datos será legítimo, siempre que se respeten los demás principios legislativos.

El § 3 del artículo 7 de la LGPD prescribe que debe haber un propósito, buena fe e interés público que justifiquen la disponibilidad de datos para sus actividades. Aquí entramos en un camino conceptual estrecho: ¿qué se puede considerar un interés público?

Como el interés público tiene una amplia área de cobertura, también actúa junto con los derechos a la libertad de información a la libertad de expresión. En resumen, su concepto debería aplicarse también a dichas áreas y no solo a la administración pública. Sin embargo, aquí está el mayor problema. Como no hay consenso sobre la definición del interés público, dicho criterio quedará al arbitrio del magistrado, quien definirá en el caso concreto lo que puede ser considerado o no de interés público (Divino & Siqueira, 2017, p. 231).

Según Celso Antônio Bandeira de Mello, «el interés público debe conceptualizarse como el vínculo entre el interés público y el privado, proyectándose este último en ese, representando un ideal de bienestar

y seguridad como un conjunto de intereses individuales hacia los colectivos como miembros de la sociedad» (2009, p. 61).

Otro punto a destacar es la prescripción del § 4 del artículo 7 de la LGPD. Primero, el encabezado no prescribe el requisito de consentimiento. Este se enumera en la sección I. Segundo, ¿qué datos se hacen públicamente evidentes? ¿Las imágenes, la ubicación, las fotos y los videos colocados en una red social privada se consideran públicos o, al menos, publicitados? En nuestra opinión, depende. Existe la posibilidad de transformar un perfil social en una red privada. Al ingresar la información, uno elige la privacidad o la publicidad. Si es visible para todos sin restricciones, puede considerarse público. En la situación opuesta, donde solo los participantes que ingresan a esa red social pueden ver el contenido, no es posible considerarlos públicos, ya que su acceso está restringido. Nuevamente, el legislador deja a discreción del magistrado verificar el caso concreto.

Finalmente, las situaciones que corresponden a la transferencia de datos del controlador a otros controladores requieren el consentimiento específico del sujeto titular de los datos, bajo pena de nulidad. En esos casos, el transferidor asumirá los daños sufridos por la parte perjudicada.

Por lo tanto, el tema vinculado a la protección de los datos personales experimento un refuerzo y un enriquecimiento de la personalidad dirigido a la persona física. La atención se dirige al carácter polimórfico de la personalidad. La importancia de la consagración de derechos en el escenario virtual tiene como propósito permisible la efectividad y la consagración del interés de la persona considerada como el sujeto de los datos. El énfasis cambia hacia la autodeterminación informativa, reconociendo qué información debe usarse y divulgarse en esa relación contractual. Este, sin embargo, es el plano ideal. La praxis nos aporta consideraciones elementales que son indispensables para la comprensión social y legal del tema en discusión. Esto es lo que veremos a continuación.

III. RACIONALIDAD LIMITADA: REFLEXIONES ESCÉPTICAS Y ECONÓMICAS.

La protección de datos confidenciales aportados por la LGPD (artículo 11)[17] tiene como propósito evitar conductas discriminatorias contra el interesado. Su protección específica se debe precisamente a su ontología, ya que se relaciona con los derechos y libertades fundamentales del ser humano. En caso la recolección y el tratamiento tengan lugar de manera

17 «Artículo 11. El procesamiento de datos personales sensibles solo puede llevarse a cabo bajo las siguientes condiciones: I. – cuando el titular o su tutor legal consiente de manera específica y destacada para fines específicos».

indiscriminada, o en el resto de situaciones indicadas, pueden implicar riesgos significativos para los derechos que se ejercen.

Un aspecto importante se refiere al tratamiento de fotografías. Incluso cuando contenga información sobre el origen racial o étnico, las creencias religiosas, la opinión política, la afiliación sindical o la organización religiosa, filosófica o política, datos de salud o vida sexual, datos genéticos o biométricos (datos considerados sensibles), el tratamiento de las fotografías no se ajusta a las definiciones enumeradas en el dispositivo legal y, por lo tanto, se basa en la regla general.

Como norma, la legislación adopta una postura protectora y enumera dos situaciones en las que es posible procesar estos datos. La primera requiere, específica y prominentemente, el consentimiento del interesado para llevar a cabo el procesamiento de datos, siempre que el propósito esté delimitado (LGPD, artículo 11, encabezado, I). La segunda (LGPD, artículo 11, II, a-g) no requiere consentimiento, pero solo será aceptada en casos excepcionales[18]. Todas estas situaciones son enumeraciones exhaustivas y no permiten una interpretación amplia. Cualquier otra situación no mencionada aquí —o en la que el consentimiento del titular esté ausente o no se pueda verificar— evitará la acción del agente de tratamiento.

Una observación importante está contenida en el § 2 del artículo 11 de la LGPD. En el procesamiento de los datos realizados sin el consentimiento expreso del titular —«para cumplir con la obligación legal o reglamentaria del controlado», de conformidad con el artículo 16, I, de la LGPD; o «necesario para la ejecución de las políticas públicas previstas en las leyes y reglamentos o respaldados por contratos», según el artículo 7, III, de la LGPD—, resulta necesario, por determinación expresa del artículo 11, §2, de la LGPD, que «se dé publicidad a dicha renuncia de consentimiento, en los términos del punto I del art. 23 de esta Ley»[19].

18 «Artículo 11. El procesamiento de datos personales confidenciales solo puede tener lugar en los siguientes casos: I. – cuando el titular o su tutor legal consiente de manera específica y destacada para fines específicos; II. – sin dar el consentimiento del titular, en el caso de que sea indispensable para: a) el cumplimiento de la obligación legal o reglamentaria por parte del controlador; b) el procesamiento compartido de los datos necesarios para que la administración pública ejecute las políticas públicas previstas en las leyes o reglamentos; c) realizar estudios por un organismo de investigación, asegurando, siempre que sea posible, el anonimato de los datos personales sensibles; d) ejercicio regular de derechos, incluso por contrato y en procedimientos judiciales, administrativos y arbitrales, este último de conformidad con la Ley No 9.307, de 23 de setiembre de 1996 (Ley de Arbitraje); e) protección de la vida o seguridad física del titular o de un tercero; f) protección de la salud, exclusivamente, en un procedimiento realizado por profesionales de la salud, servicios de salud o autoridades de salud; o (redacción dada por la Ley N° 13853 de 2019) g) garantía de prevención de fraude y seguridad del titular, en los procesos de identificación y autenticación de registro en sistemas electrónicos, salvaguardando los derechos mencionados en el art. 9 de esta Ley y salvo que prevalezcan los derechos y libertades fundamentales del titular que requieren la protección de datos personales».

19 «Artículo 23. El tratamiento de datos personales por personas jurídicas reguladas por el derecho público al que se refiere el único párrafo del art. 1 de la Ley N° 12.527, de 18 de noviembre de 2011 (Ley de Acceso a la Información), se llevará a cabo para el cumplimiento de su propósito público,

Además, la mercantilización de datos sensibles está prohibida por el § 3 del artículo 11[20] de la LGPD (Divino, 2018). En caso de que se establezca un objetivo para la ventaja económica, las partes pueden acordar su prohibición y la autoridad nacional de protección de datos puede regular esta situación. Dicha conducta existe para evitar la venta y el intercambio de datos por posible discriminación institucional, social y política. Esta es la regla[21].

Sin embargo, la participación de las empresas en el campo de la recopilación y el procesamiento de datos en el panorama político no es algo sorprendentemente nuevo. Tras la formulación de políticas electorales, los especialistas en *marketing* entran en una nueva fase de operación: la identificación de valores, creencias, actitudes, comportamientos sociales y creencias políticas (incluidos los patrones de votación) de ciertos segmentos de la población, identificados por su distribución espacial y demográfica (Castells, 2009, p. 210). Hillary Clinton utilizó esta estrategia en 2008 a través de su jefe de campaña, Mark Penn. Penn demostró como —al buscar asociaciones estadísticas entre características demográficas, creencias, sesgos de los medios y comportamiento político— es posible dirigir la publicidad a cada grupo específico y explotar sus predisposiciones para una mejor

en la búsqueda del interés público, con el fin de ejecutar las competencias legales o cumplir con las atribuciones legales. I. – serán informados los casos en los que, en el ejercicio de sus poderes, procesan datos personales, proporcionando información clara y actualizada sobre la disposición legal, el propósito, los procedimientos y las prácticas utilizadas para realizar estas actividades en vehículos de fácil acceso, preferiblemente en sus sitios web".

20 «§ 3º La comunicación o el uso compartido de datos personales confidenciales entre los controladores con el fin de obtener una ventaja económica puede estar prohibida o regulada por la autoridad nacional, previa consulta con las agencias sectoriales del gobierno, dentro del alcance de sus competencias» LGPD (2018).

21 Una disposición elemental y problemática está contenida en el artículo 7, IX y en el artículo 10 de la LGPD: «Cuando sea necesario para satisfacer los intereses legítimos del controlador o de un tercero, excepto cuando prevalezcan los derechos y libertades fundamentales del titular que requiere la protección de datos personales», el procesamiento de datos puede realizarse en principio sin el consentimiento de su titular. Según lo prescrito por el artículo 10 de la LGPD, este interés solo puede basarse en expectativas legítimas y legales, que se observarán concretamente cuando se aplique la actividad. Entre ellos, la legislación estipulaba una lista ejemplar de qué tipo de actividades podrían considerarse de «interés del controlador»: «I. – apoyo y promoción de actividades de controlador; y II. – protección, en relación con el titular, del ejercicio regular de sus derechos o la prestación de servicios que lo benefician, respetando sus expectativas legítimas y los derechos y libertades fundamentales, de conformidad con los términos de esta Ley». Esta disposición crea una situación problemática sin expectativa de fines. En principio, si existe una justificación legal para la recopilación y el procesamiento de datos que se ajuste al interés subjetivo del controlador de datos, el sujeto de datos estará sujeto a dicha actividad sin muchas opciones, a menos que haya una violación patente de los preceptos y libertades fundamentales. Sin embargo, el legislador brasileño, al crear esta brecha, visualizó que esta hipótesis no podía ser tan abstracta y genérica. Así, indicó —en el artículo 10, §§ 1, 2 y 3 de la LGPD— que solo se pueden procesar los datos personales estrictamente necesarios para el propósito previsto. Además, el controlador tomará medidas para garantizar la transparencia del procesamiento de datos en función de su interés legítimo. Y, finalmente, según el artículo 10, § 3, de la LGPD, la autoridad nacional puede solicitar al controlador que informe sobre el impacto de la protección de datos personales cuando el procesamiento se base en su interés legítimo, sujeto a secretos comerciales e industriales. Sin embargo, todavía son situaciones en gran medida subjetivas, las cuales permiten la aplicación discrecional por parte del controlador de datos. El vínculo entre legalidad e ilegalidad será la única alternativa, en este caso, para que el interesado los proteja de acuerdo con los preceptos legalmente establecidos.

efectividad en el mensaje político (Castells, 2009, pp. 210-211). Pero ¿cómo se convierte esto en estrategia política?

> *That this sophisticated form of political marketing is a derivative of commercial marketing is a clear indication of the rise of the citizen-consumer as a new persona in public life. In fact, politicians and businesses use the same databases because there is an active commerce of data-selling which originated from the use of massive computer power applied to processing data from government and academic sources with the huge collection of data resulting from the invasion of privacy by credit-card companies, telecommunication companies, and Internet companies selling information about those of their customers (the majority) who, unaware of the fine print in their contracts, do not opt out of the companies' policy of selling their customers' data* (2008, pp. 211-212).

En 2016, el escenario se repitió en las campañas electorales de Donald Trump, quien contrató a la compañía Cambridge Analytica para ayudarlo en su *marketing*. La compañía británica le ofreció herramientas tecnológicas que podrían identificar a las personalidades del electorado estadounidense y, posteriormente, influir en su comportamiento. Cambridge Analytica podría ofrecerle aquello porque obtuvo acceso a la información personal y privada de más de cincuenta millones de usuarios de redes sociales Facebook y lo utilizó, sin tener autorización específica ello (Granville, 2018). Estos datos se obtuvieron a través de una investigación gestionada por Global Science Resarch (GSR), entidad fundada por Aleksandr Kogan, profesor de la Universidad de Cambridge, a través de *freelancers* de la Mechanical Turk, una plataforma de Amazon encargada de reclutar personas para realizar «tareas de inteligencia humana» (Davies, 11 de diciembre de 2015). La GSR ofreció una tarifa de entre 1 y 2 dólares para que los usuarios completen una encuesta en línea. Sin embargo, había dos restricciones: los usuarios deberían ser *turkers*[22] americanos; y deberían instalar una aplicación de Facebook para recibir su pago (Schwarts, 2018). De acuerdo con las políticas de privacidad y los términos de uso de esta aplicación, la GSR tendría acceso a todos los datos del usuario instalador, algo que está permitido por Facebook. Sin embargo, el procesamiento de estos datos para la venta es contrario a la política de las redes sociales. Así fue como surgió el escándalo en todo el mundo, llevando a que Facebook se devalúe 70 000 millones de dólares y a que Cambridge Analytica se declarase en bancarrota (Reuters, 2018; Solon & Laughland, 2018).

Y no son solo las empresas privadas las que trabajan en esta área. Las agencias gubernamentales asumen la posición de controlador y procesador de datos en la sociedad de vigilancia. Uno de los sistemas de

22 Los *turkers* son personas que tienen la tarea de hacer un trabajo repetitivo (como identificar imágenes pornográficas) y reciben una pequeña cantidad de dinero, alrededor de 1 a 15 centavos, como recompensa por su trabajo (Schwarts, 2018).

relevancia significativa es el Echelon (Tomizawa, 2013, pp. 4-5). Se trata de un sistema inicialmente diseñado en 1971 —con la participación conjunta de Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda— con el objetivo de interceptar las comunicaciones en todo el mundo. Según algunas hipótesis, este sistema consistía a principios de la década de 2000 en 120 satélites y 11 estaciones de satélite terrestres y podía interceptar aproximadamente el 90% de las comunicaciones de red. Otro sistema es Enfpol (Enforcement Police), el cual se originó en 1995 en Bruselas, destinado a las escuchas telefónicas masivas de llamadas telefónicas, de comunicación, internet y fax, bajo la justificación de la seguridad nacional y global contra actividades ilegales de las mafias y otras organizaciones criminales (Tomizawa, 2013, pp. 5-6).

Del mismo modo, desarrollado por el FBI especialmente para la creación de redes, existe el sistema Carnivore, el cual simplemente intercepta las comunicaciones individuales y en tiempo real de las operaciones virtuales en red (Tomizawa, 2013, p. 7). Innumerables, indefinidos y secretos son los recursos gubernamentales para la vigilancia de sus ciudadanos y el resto del mundo. Es por eso que los datos personales, no solo en la contratación electrónica, tienen un poder inmenso. Cualquier información, si se recopila y procesa de la manera correcta, puede darle a su titular la oportunidad de usarla como un recurso financiero o de otro tipo. Los datos personales, además de los posibles productos, tienen un poder informativo y gubernamental inconmensurable para el titular. Los peligros no son imaginarios.

El supuesto de múltiples funcionalidades aportadas por la tecnología se inserta en el desarrollo de los diversos momentos de un viaje en la vida de una persona. Su dimensión no es solo diacrónica, sino que —sincronizada también con la identidad del sujeto— rompe barreras y asume una posición interactiva continua entre humanos y máquinas. En cada momento, el contexto en el que la persona construye su camino y su referencia subjetiva y objetiva significativa cambia radicalmente. En una dimensión legal, esto no es diferente.

Especialmente en el campo del consumo, la discusión sobre la protección del consumidor en el comercio electrónico no es nueva, aunque tampoco es tan antigua. La referencia legislativa en el derecho extranjero responsable del reconocimiento de los contratos electrónicos como negocio legal se dio en la Ley Modelo UNCITRAL sobre Comercio Electrónico de 1996, en sus artículos 5 y 11[23]. En Brasil, la discusión tiene lugar a principios de la década de 2000, especialmente gracias a la

23 «*Article 5. Legal recognition of data messages information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.*
[…] Article 11. Formation and validity of contracts. (1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall

profesora Claudia Lima Marques (2004). Ya en ese momento, la autora imaginó la posibilidad de la existencia y la expansión de un espacio producido por internet expresado en redes de comunicación electrónica y de masas para ganar la confianza y elaborar mecanismos prácticos para los consumidores, así como para reconstruir la deconstruida dogmática contractual.

Las reflexiones sobre este tema son aparentemente infinitas. El carácter innovador de la tecnología destaca los cambios en la relación entre el ciudadano y el mercado de consumo. Esta descripción común de las características de una sociedad sometida a criterios informativos denota un crecimiento asombroso en su participación en el mundo virtual. Los contratos electrónicos operan la experiencia consumista en la sociedad de la red. Si se desea verificar cuál es el papel y la posición del consumidor en las relaciones contractuales electrónicas, el llamado *e-commerce*, sería un error analizarlos exclusivamente desde el aspecto teórico. Algunas consideraciones prácticas de carácter general deben señalarse para apoyar el presente argumento.

En relación al año 2018, el *e-commerce* cumplió una función latente en la interacción y la convergencia de medios para el servicio al cliente. Por ejemplo, en el Black Friday[24] las ventas de *e-commerce* rondaron los 2,600 millones de reales brasileños (R$), un 23% más que en 2017. Los pedidos en línea alcanzaron los 4,27 millones, un 13% más, mientras que el gasto promedio aumentó a R$ 608, un aumento del 8% en comparación con el año anterior. Además, el número de consumidores que utilizaron la plataforma digital para realizar al menos una compra fue de R$ 2,41 millones, un 9% más que en 2017 (Ebit|Nielsen, 2018b).

En el Cyber Monday[25], el lunes después del Black Friday, las ventas alcanzaron la marca de R$ 372 millones, un aumento del 20,7% en comparación con los R$ 308 millones vendidos en 2017. El número de pedidos superó los 750 mil (+ 4%) y el gasto fue de alrededor de R$ 494 (+ 15%). El total de 6,9 millones de pedidos consolidados entre este período (Black Friday + Cyber Monday) generó ingresos de R$ 3,92 mil millones, un aumento del 24%, a un costo promedio de R$ 568 (+ 9%) (Ebit|Nielsen, 2018a).

Considerando las experiencias y experimentos concretos del comercio electrónico, identificamos la influencia de una pluralidad de instrumentos utilizados para la satisfacción efectiva del consumidor. La organización de estructuras privadas en la formación de redes contractuales permite

not be denied validity or enforceability on the sole ground that a data message was used for that purpose».

24 Generalmente celebrado en noviembre, en esta fecha los proveedores de productos reducen el precio de sus productos y servicios para que se incremente su circulación y compra.

25 Destinado principalmente a la venta de productos electrónicos.

el acceso a la información y la prestación de servicios en línea a través de herramientas y procedimientos estructurados y diferenciados en nuevas perspectivas.

La relevancia del comercio electrónico y, en general, la dimensión económica, fomenta la transformación de internet en un lugar aséptico, donde el consumidor, ya sea adulto o niño, puede ingresar como quien ingresa a un gran centro comercial, un *shopping center* sin fronteras, sin el riesgo de desviar su atención hacia otra cosa que no sea la actividad consumista (Rodotà, 2008, p. 179). Sin embargo, nos enfrentamos a una situación compleja: desde el momento en que el uso comercial trasciende todas las demás formas de uso contractual, en virtud de su practicidad y conveniencia, el formato de internet y su propia naturaleza se transforman profundamente y emergen nuevas demandas y propuestas para regular este escenario. Para el proveedor de productos o servicios en el *e-commerce* es esencial la aceptación del consumidor para recopilar y procesar datos destinados a poder finalizar esa relación de consumo. Si el consumidor se niega, no podrá finalizar dicha relación, como se indicó anteriormente. Sin embargo, el consumidor puede, a través del apoyo de la LGPD y Código de Defensa del Consumidor, reclamar sus derechos ante los organismos proteccionistas correspondientes.

Prosiguiendo con la discusión, centrémonos ahora en la excepción del artículo 11 del LGPD, prevista en su párrafo 4, que fue reformulado por la Medida Provisional 869/2018. Dicha Medida insertó los ítems I y II. Se admite obtener ventaja económica en la hipótesis de la portabilidad de los datos, siempre que el interesado lo consienta; asimismo, cuando se requiere comunicación para la provisión adecuada de servicios de salud complementarios. Debe tenerse en cuenta que la descripción legal se refiere a datos personales sensibles con respecto a la salud. En teoría, los más afectados serán los hospitales privados, los profesionales libres y los planes de salud.

Sin embargo, resulta que el legislador pecó al postular una disposición tan genérica como la de la sección I. En primer lugar, los contratos de seguro o de salud son en gran medida contratos de adhesión. No hay posibilidad de discutir las cláusulas prescritas en los mismos. En segundo lugar, al aceptar los términos de este contrato, en teoría se obtendría el consentimiento del titular. Esto tiene una racionalidad limitada a lo que se prescribe allí. Es posible que el usuario ni siquiera haya leído el contrato o que no haya sido consciente de la asignación de estos datos; tal vez solo haya notado su carácter oneroso.

Es cierto que existen estrategias que se oponen a tales lógicas y estructuras organizativas legales, como los moldes contractuales electrónicos

contemporáneos. Estos, denominados *clickwrap*[26] o *point-and-click*, dificultan un análisis más preciso para verificar los requisitos anteriores. Sin embargo, la fuerza de estructuración de las nuevas tecnologías y su sinergia con la legislación deberían ser tales que faciliten esto, así como la creación de modelos contractuales específicos para la transferencia opcional de datos personales por parte del titular cuando se utiliza un servicio en particular. Lo que debe tenerse en cuenta, en primer lugar, es que el diseño del consentimiento como lugar del procesamiento de datos demarca algunas tendencias, principalmente principiológicas, que no fueron olvidadas por la ley. Por el contrario, se enumeraron en una sección específica.

El problema es qué hacer para obtener este consentimiento. Los modelos contractuales electrónicos actuales no favorecen esta práctica. Evidentemente, la simple actitud de hacer clic en un cuadro de diálogo y aceptar los «términos de servicio» y la «política de privacidad» no es algo que pueda equipararse a otorgar el consentimiento. De hecho, estudios empíricos como los de Obar & Oeldorf-Hirsch (2018); Reidenberg, Breaux, Carnor & French (2014); Strahilevitz & Kugler (2016); y Mcdonald & Cranor (2008) destacan que el consumidor / usuario /titular de los datos no comprende el contrato electrónico que se le proporcionó para su aceptación. Es decir, la lectura de este tipo de contrato, ya que contiene muchos rasgos técnicos, afecta la comprensión de los no-especialistas. Esto cuando llevan a cabo la lectura. La mayoría

26 «Como una forma particular de contratos de membresía, en el campo de la adquisición electrónica, es importante resaltar los llamados acuerdos *clickwrap* ("acuerdos *clickwrap*" o "acuerdos *point-and-click*"), generalmente sujetos al acuerdo del usuario del producto o servicio, que contiene cláusulas. Por lo tanto, su validez se basa en el acto de presionar el botón Aceptar (a menudo a través del mouse), manteniendo una gran similitud con las licencias retráctiles utilizadas en la comercialización del software, en el que la aceptación se produce en el abrir el paquete que contiene los soportes físicos donde se encuentra el programa» (Martins, 2016. p. 131).
Además, el término «clickwrap» proviene del término «*shrinkwrap*», que se utiliza para designar las compras de *software* realizadas en alta demanda. Su relación intrínseca con la propiedad intelectual adquiere gran relevancia en 1996, con el caso ProCD, Inc. v. Zeidenberg: «En ProCD, un fabricante de software de computadora (ProCD), compiló información de más de 3,000 directorios en una base de datos de la guía telefónica que contenía aproximadamente 95 millones de listas telefónicas (a un costo considerable) y desarrolló un motor de búsqueda para ser usado en conjunto con la base de datos. Con el fin de comercializar eficazmente el software, ProCD otorgó la licencia de la base de datos a diferentes precios: precios más altos para usuarios comerciales y precios más bajos para usuarios privados. Sin embargo, surgió un problema cuando Zeidenberg compró un paquete de usuario privado, pero ignoró la licencia, extrajo los listados e hizo que la base de datos estuviera disponible comercialmente a través de Internet por medio de su propio motor de búsqueda. ProCD demandó a Zeidenberg, alegando infracción de derechos de autor e incumplimiento del acuerdo de licencia retráctil» (Covotta & Sergeeff, 1998, p. 37). La importancia de esta jurisprudencia es la consideración de la posibilidad de la fuerza vinculante de las licencias *clickwrap* y *shrinkwrap*. Los términos allí descritos, de acuerdo con la decisión del tribunal de los Estados Unidos, son de carácter contractual y equivalen al principio de *pacta sunt servanda*. Es decir, lo acordado debe cumplirse. Esta posición trae serias consideraciones. Primero, debe entenderse que no existe una reducción teórica en el consentimiento para este tipo de acuerdo contractual. Si bien el consentimiento es un factor de intencionalidad, algo esencialmente de naturaleza subjetiva que está vinculado a la autonomía y la autodeterminación del titular, tanto *clickwrap* como *shrinkwrap* son acuerdos contractuales electrónicos en los que el titular usará estos métodos como una posible forma de expresar su consentimiento. Mientras que uno de estos momentos tiene un significado subjetivo, el otro adquiere una dimensión legal y formal.

de las veces, según los autores citados, el 74% de las personas ignora dichos términos y políticas.

Además, el consumidor/usuario del servicio está obligado a aceptar los términos que se le *imponen* o la contratación no será posible. Esta es otra crítica que debe ser considerada. Ahora, ¿cómo podemos hablar de libre consentimiento si el titular está obligado a renunciar? ¿Cómo podemos reclamar autonomía privada si el servicio prestado solo se realiza si se proporcionan los datos?

Así que, además del reconocimiento de los derechos individuales, las normas destinadas a regular la circulación de información en el ámbito virtual determinan y designan la autonomía privada como un requisito importante que debe estar presente en las situaciones enumeradas. Por lo tanto, la información obtenida, originalmente proporcionada, puede causar daños patrimoniales y extrapatrimoniales a su propietario si se usa incorrectamente (LGPD, artículos 31-32 y 42-45).

Se debe visualizar una solución legal para resolver este problema. Modestamente, en el siguiente apartado, sobre la base del principio de libertad contractual y autonomía privada, se propone una alternativa al modelo contractual electrónico contemporáneo.

IV. PROPUESTA PARA LA IMPLEMENTACIÓN DE LA AUTONOMÍA PRIVADA Y DE LA PROTECCIÓN DEL TITULAR DE DATOS EN RED

La autosuficiencia de las directrices de poder del gobierno para las relaciones digitales en la era tecnológica debe ser considera como parte de una estrategia más amplia. Si se usa en sus aspectos negativos, el sistema de vigilancia Big Brother de Orwell estará activo. La unidad de protección sistémica debe ofrecer una respuesta convincente desde la premisa de que todo debe tener un grado de transparencia. Esto introduce la imposibilidad de adoptar cláusulas generales y abstractas para favorecer al agente de tratamiento, ya sea público o privado.

Aunque la legislación requiere la provisión de información clara y actualizada sobre el pronóstico legal, así como el propósito, los procedimientos y las prácticas utilizados para la ejecución del procesamiento de datos personales por parte del gobierno, no se presenta la descripción del escenario enumerado en la LGPD como un discurso sólido, capaz de brindar seguridad legal al interesado en este tipo de relación contractual. Esto se debe a la modalidad contractual utilizada para la recopilación y el procesamiento de datos.

La aceptación de la verdad de las premisas (a) «el mundo está impulsado por la información» y (b) «la información es poder y dinero» supone

un paso hacia el desarrollo legal y la atención de las peculiaridades amalgamadas en los escenarios sociopolíticos y legales. Esto significa que no debemos renunciar a la protección de la privacidad. Tampoco debemos abandonar el concepto de identidad en favor del poder económico. Por el contrario. La ley debe analizar una situación empírica y ver cómo posicionarse frente a una construcción capitalista sólida para preservar un significado humanista frente al consumismo depredador.

Para superar estas situaciones, el criterio básico es la libertad de contratar. Se reconoce que los modelos contractuales electrónicos contemporáneos facilitan la relación entre el usuario y el proveedor de servicios. Sin embargo, se busca tomar distancia de la autosuficiencia tecnológica y del paternalismo legislativo, para evitar distorsiones pragmáticas y asumir una correcta dimensión técnica y legal del enfoque.

Con este fin, tenemos la intención de estipular que la recopilación y el procesamiento de datos solo se considerarán como un elemento de respeto legal —en el que la innovación tecnológica implica una innovación social— cuando permitan que el interesado acepte o no la política de privacidad sin penalizarlo. Veamos: en los últimos años hemos sido testigos del imperio del poder de la información. Ello ha producido una pérdida real de autocontrol, así como formas radicales y abundantes de expropiación y fragmentación, tales como las pautas de los casos Facebook y Cambridge Analytica. Si la descripción del nuevo panorama contractual electrónico se basa en el poder de la autodeterminación informativa y la libertad de contratación, la eficacia y la eficiencia de las leyes de protección de datos se verán significativamente mejoradas.

La dificultad de construir este marco institucional vinculante, en un contexto donde el sujeto de datos es el lugar y el foco de la relación legal, encuentra barreras en el propio sistema económico. No vale la pena que el proveedor de servicios califique esta posibilidad, porque la negativa del titular da como resultado situaciones menos rentables que aquellas en las que el proveedor podría beneficiarse mediante la recopilación y el procesamiento de sus datos.

Sin embargo, no podemos imaginar un escenario en el que la libertad de contratación y la autodeterminación informativa no sean elementos indispensables para el ejercicio de la personalidad y los datos personales. Esa directriz debe expresarse brevemente de la siguiente manera:

> *Usuario X ante los Términos de Servicio y Política de Privacidad: «Leí - No leí»; Estoy de acuerdo con la asignación de datos; No estoy de acuerdo con la asignación de datos».*

En el caso de aceptación, la contratación debe proceder normalmente, tanto para el controlador/operador como para el usuario. De lo contrario,

el proveedor no puede evitar el uso del producto o servicio debido al desacuerdo del interesado. Esta, entonces, es una instancia que se define como abusiva por no respetar la voluntad del usuario. La cuestión central, por lo tanto, se refiere al ejercicio de la posibilidad que el titular de los datos tiene y no a los datos recopilados mediante su voluntad.

Por lo tanto, se confirma que la privacidad, en este sentido actual, a pesar de su protección por la legislación de protección de datos, constituye un elemento frágil en vista de la posible ineficacia de estas regulaciones. Por el contrario, como un elemento estructurante fundamental de la ciudadanía de la sociedad de la información, la hipótesis de la libertad infinita y anárquica titulada por el poder de las grandes empresas de procesamiento de datos hace que la amenaza a la esfera personal sea inminente. Se busca, por ello, un equilibrio justo entre una visión aparentemente individualista de la privacidad y la satisfacción de las demandas sociales y del mercado. Pero la clave para prevenir la violación de estos derechos y la aparición de zonas problemáticas radica en reconocer y modificar el marco contractual electrónico actual.

V. CONCLUSIÓN

La tecnología está llena de promesas (Rodotà, 2008, p. 165). Todo lo discutido en este escrito apunta a situaciones aparentemente opuestas en el entorno contemporáneo. Si bien la reflexión basada en principios dirigida al desarrollo de los procesos de identidad individual y personal del usuario titular de datos de la red se centra en la expansión y protección del derecho a la privacidad, las reflexiones escépticas y económicas demuestran lo contrario.

Así, se adoptan instrumentos analíticos cada vez más precisos para actuar en la sociedad de la información. Las relaciones contractuales electrónicas, basadas en algoritmos, tienden a crear situaciones de poder e ignoran la dinámica legal reclamada por la sociedad y la legislatura. Las demandas de esta esfera ya están tratando de imponer limitaciones en internet y en su transformación progresiva incontrolada. Pero, debido a que es un gran espacio público, ¿cómo establecer límites donde no hay límites para delimitar? ¿Cómo limitar algo inmaterial?

Desde este punto de vista, si bien las tradiciones principiológicas creadas por la legislación desde inicios del siglo XX se encuentran en un amplio desarrollo, permanecer en este enfoque solo afectará a los juristas. El enfoque regulatorio no debe dirigirse a las fuerzas incontrolables de internet. Las fuerzas legislativas pueden redefinir el curso protector del espacio de libertad individual. No es suficiente afirmar la demanda de consentimiento expreso, informado y explícito, si la experiencia

contractual contemporánea no proporciona un sustrato fáctico para su realización.

Los protagonistas de esta extraordinaria relación virtual son la autodeterminación informativa y la libertad contractual. Son elementos formidables e íntimamente ligados ante el capitalismo depredador envuelto en su esfera. Por lo tanto, el uso de tecnologías informáticas debe continuar avanzando independientemente del consentimiento del usuario para recopilar y procesar datos. Existen dos contratos distintos: los términos del servicio y la política de privacidad. Una reacción —la más básica posible— sería su desvinculación. La coalición de estas modalidades contractuales constituye un exceso en la negociación del proveedor del servicio. Y, para complicar la situación de emergencia, es necesario aceptar ambos. Por lo tanto, se propone que el usuario elija ceder o no sus datos para que el resultado sea diferente en los próximos años.

Por lo tanto, si bien la legislación sigue un camino lento y arduo, se postula que su objeto debe basarse en la suposición de una carencia de suficiencia del usuario, y no solo en el exceso de potencia del controlador/operador. Cuando estas demandas son urgentes, como lo son hoy, la legislatura no puede cubrirse los ojos e ignorarla. Debe participar como protagonista a nivel internacional en la redacción de un tratado, requiriendo que las grandes empresas modifiquen su sistema contractual y permitiendo un ejercicio autónomo de la libertad contractual y la autodeterminación informativa.

REFERENCIAS

Albuquerque, J. (1995). Michel Foucault and the Theory of Power. *Tempo Social*, *7*(1-2), 105-110. doi: https://doi.org/10.1590/ts.v7i1/2.85209

Arendt, H. (2001). *Sobre a violência*. Río de Janeiro: Relume Dumará.

Bentham, J. (2000). *O panóptico*. Belo Horizonte: Autêntica.

Canotilho, J.J.G & Machado, J.E.M. (2014). Constituição e código civil brasileiro: âmbito de proteção de biografias não autorizadas. En A.P.G. Júnior & M.G.T. Santos (Eds.), *Constituição Brasileira de 1988: reflexões em comemoração ao seu 25º aniversário*. Curitiba: Juruá.

Castells, M. (2009). *Communication Power*. Nueva York: Oxford University Press.

Castells, M. (2017). *A sociedade em rede*. (Trad. R.V. Majer). São Paulo: Paz e Terra.

Cavalieri Filho, S. (2014). *Programa de responsabilidade civil*. São Paulo: Atlas.

Cordeiro. A.M. (2011). *Da boa fé no direito civil*. Coimbra: Almedina.

Covotta, B. & Sergeeff, P. (1998). ProCD, Inc. v. Zeidenberg. *Berkeley Technology Law Journal*, *13*(35), 35-54. doi: https://doi.org/10.15779/Z38408Q

Davies, H. (11 de diciembre de 2015) Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. Recuperado de https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Divino, S.B.S. (2018). A aplicabilidade do Código de Defesa do Consumidor nos contratos eletrônicos de tecnologias interativas: o tratamento de dados como modelo de remuneração. *Revista De Direito Do Consumidor*, *118*, 221-246.

De Cupis, A. (2008). *Os direitos da personalidade*. São Paulo: Quorum.

Divino, S.B.S. & Siqueira, L.A.V.C. (2017). O direito ao esquecimento como tutela dos direitos da personalidade na sociedade da informação: uma análise sob a ótica do direito civil contemporâneo. *Revista Eletrônica Do Curso De Direito Da UFSM*, *12*, 218-236. doi: https://doi.org/10.5902/1981369424579

Ebit|Nielsen, (2018a). *Com alta de 20,7%, Cyber Monday fecha temporada de descontos no e-commerce*. Recuperado de https://www.ebit.com.br/imprensa/cyber-monday

Ebit|Nielsen. (2018b). *E-commerce fatura 2,6 bilhões, alta de 23% na Black Friday em 2018*. Recuperado de https://www.ebit.com.br/imprensa/faturamento-total-blackfriday

Finkelstein, M.E. (2004). *Aspectos jurídicos do comércio eletrônico*. Porto Alegre: Síntese.

Foucault, M. (1989). *Microfísica do poder*. Río de Janeiro: Graal.

Foucault, M. (2004). *Vigiar e punir*. Petrópolis: Vozes.

França, R.L. (1983). Direitos da personalidade: coordenadas fundamentais. *Revista dos Tribunais*, *72*(567).

Glanz, S. (1998). Internet e contrato eletrônico. *Revista dos Tribunais, 87*(757), 70-75.

Granville, K. (2018) Facebook and Cambridge Analytica: what you need to know as fallout widens. *The New York Times*. Recuperado de https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Huxley, A. (1978). *Admirável mundo novo*. Porto Alegre: Globo.

Iteanu, O. (1996). *Internet et le droit: aspects juridiques du commerce électronique*. Paris: Eyrolles.

Maceira, I.P. (2015). *A proteção do direito à privacidade familiar na internet*. Río de Janeiro: Lumen Juris.

Marques, C.L. (2004). *Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico*. São Paulo: Revista dos Tribunais.

Martinez, P.D. (2014). *Direito ao esquecimento: a proteção da memória individual na sociedade da informação*. Río de Janeiro: Lumen Juris.

Martins-Costa, J. (1999). *A boa-fé no direito privado: sistema e tópica no processo obrigacional*. São Paulo: Revista dos Tribunais.

Martins, G.G. (2016). *Contratos eletrônicos de consumo*. São Paulo: Atlas.

McDonald, A. & Cranor, L (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3), 543-568.

Mello, C.A.B. (2009). *Curso de direito administrativo*. São Paulo: Malheiros.

Nery, A.L. (2010). Considerações sobre os bancos de dados de proteção ao crédito no Brasil. En N. Nery Junior & R.M. Nery (Coord.), *Doutrinas essenciais. Responsabilidade Civil. Direito fundamental à informação. Dever de informar. Informações cadastrais. Mídia, informação e poder. Internet*. São Paulo: Revista dos Tribunais.

Obar, J.A. & Oeldorf-Hirsch, A. (2018) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*.
doi: https://doi.org/10.1080/1369118X.2018.1486870

Orwell, G. (2009). *1984*. São Paulo: Companhia das Letras.

Paesani, L.M. (2014). *Direito e Internet: liberdade de informação, privacidade e responsabilidade civi*l. São Paulo: Atlas.

Reidenberg, J.R., Breaux, T., Carnor, L.F. & French, B. (2015). Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal*, *30*(39). doi: https://doi.org/10.2139/ssrn.2418297

Reuters. (2018). *Facebook has lost $70 billion in 10 days – and now advertisers are pulling out*. *Financial Post*, 26 de marzo. Recuperado de https://business.financialpost.com/technology/u-s-ftc-investigating-facebooks-privacy-practices

Rodotà, S. (2008). *A vida na sociedade da vigilância: a privacidade hoje*. Río de Janeiro: Renovar.

Sarlet, I.W. (2014). Direitos fundamentais em espécie. En I.W. Sarlet, L.G. Marinoni & D. Mitidiero (Eds.), *Curso de direito constitucional*. São Paulo: Revista dos Tribunais.

Schwarts, M. (2017). Facebook failed to protect 30 million users from having their data harvested by Trump Campaign affiliate. *The Intercept*. Recuperado de https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/

Silva, J.A. (2008). *Comentário contextual à Constituição*. São Paulo: Malheiros.

Solon, O. & Laughland, O. (2018). Cambridge Analytica closing after Facebook data harvesting scandal. *The Guardian*. Recuperado de https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say

Strahilevitz, L. & Kugler, M. (2016). *Is Privacy Policy Language Irrelevant to Consumers?* Coase-Sandor Working Paper Series in Law and Economics, 776. Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2838449

Tomizawa, G. (2013). Mecanismo disciplinar de Foucault e o panóptico de Bentham na era da informação. *ANIMA*, *4*(9).

Warren, S.D. & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220. doi: https://doi.org/10.2307/1321160

Jurisprudencia, normativa y otros documentos legales

Código Civil. Lei 10.406 del Congreso Nacional de Brasil. *Diário Oficial da União*, 10 de enero de 2002.

Constitución Federal de la República Federativa de Brasil. *Diário Oficial da União*, 5 de octubre de 1988.

Convención Americana sobre Derechos Humanos. Conferencia Especializada Interamericana sobre Derechos Humanos, Costa Rica, 22 de noviembre de 1969.

Declaración Universal de Derechos Humanos. Adoptada y proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948.

Directiva 95/46/CE. Directiva del Parlamento Europeo y del Consejo, del 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*, L 281 del 23 de noviembre de 1995, pp. 31-50. Recuperado de http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:31995L0046

Ley de Acceso a la Información Pública. Ley 12.527 del Congreso Nacional de Brasil. *Diário Oficial da União*, 18 de noviembre de 2011.

Ley General de Protección de Datos (LGPD). Ley 13.709 del Congreso Nacional de Brasil. *Diário Oficial da União*, 14 de agosto de 2018.

Ley Modelo UNCITRAL de Comercio Electrónico. Adoptada por la Asamblea General de las Naciones Unidas en su resolución 51/162 del 16 de diciembre de 1996. Recuperado de http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

Medida Provisional 869/2018. Medida que altera la ley 13.709, del 14 de agosto de 2018, sobre protección de datos. *Diário Oficial da União*, 28 de diciembre de 2018.

Recibido: 28/05/2019
Aprobado: 02/10/2019