Revista de Derecho Privado
ISSN: 0123-4366
ISSN: 2346-2442
Universidad Externado de Colombia

RÍOS, CAROLINA

La influencia sobre el comportamiento y la 'asetización' de la privacidad como asunto contemporáneo que concierne a la regulación del comercio de dispositivos electrónicos*

Revista de Derecho Privado, núm. 39, 2020, Julio-Diciembre, pp. 263-299
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/01234366.n39.11

Disponible en: https://www.redalyc.org/articulo.oa?id=417564980010

La influencia sobre el comportamiento y la 'asetización' de la privacidad como asunto contemporáneo que concierne a la regulación del comercio de dispositivos electrónicos*

Carolina Ríos**

Resumen. Estudios y eventos recientes revelan la instrumentalización de datos personales para influenciar masivamente el comportamiento humano, mediante la diseminación de una arquitectura de dispositivos inteligentes de extracción y digitalización de experiencias privadas con fines comerciales. Dicho fenómeno, denominado por este estudio *asetización de la privacidad*, expone vacíos en regulación sobre los mercados conductuales y los llamados *bundled goods*. Además, este documento analiza

* Fecha de recepción: 7 de febrero de 2020. Fecha de aceptación: 27 de abril de 2020.
Para citar el artículo: Ríos, C., "La influencia sobre el comportamiento y la 'asetización' de la privacidad como asunto contemporáneo que concierne a la regulación del comercio de dispositivos electrónicos", *Revista de Derecho Privado*, n.º 39, julio-diciembre 2020, 263-299, doi: https://doi.org/10.18601/01234366.n39.11.
Este artículo hace parte de la investigación doctoral sobre la configuración de nuevos activos digitales en la contemporaneidad y el análisis de un asunto legal que la autora denomina "*asetización* de la privacidad", analizado desde las perspectivas del derecho internacional y comparado. Como se verá más adelante, el concepto de *asetización de la privacidad* busca describir el problema asociado al incremento progresivo de las presiones comerciales sobre valores legales de estatus constitucional, especialmente el derecho a la privacidad, la protección de datos personales y otras libertades fundamentales conexas, como resultado de estrategias de negocio globales que configuran la vida humana y la privacidad del individuo como un activo emergente.

** Korea University, Trade Law Center, School of Law, Seúl, Corea del Sur; investigadora asociada y candidata a doctora en Derecho Internacional. Abogada y Magíster en Asuntos Internacionales, Universidad Externado de Colombia, Bogotá, Colombia. Contacto: driosflorez@hotmail.com. Orcid: 0000-0003-0823-3004.
Este artículo está dedicado al apreciado profesor Jae-Hyung Lee, con quien estaré siempre agradecida por tener el honor de ser su pupila, así como por su guía y apoyo incondicionales durante todos estos años de estudio de doctorado en la Universidad de Corea. Así mismo, quiero agradecer a la Universidad Externado de Colombia por su interés en mi investigación, y por brindarme el espacio y la oportunidad de publicar en Colombia el resultado de mis investigaciones doctorales en Asia.

las legislaciones de la Unión Europea y Corea para concluir que incluso regulaciones más comprensivas requieren desarrollos legales adicionales para restringir el impacto de técnicas de inteligencia computacional y los mercados conductuales sobre valores jurídicos fundamentales.

PALABRAS CLAVE: 'asetización' de la privacidad, datos comportamentales, mercados de datos, protección de datos personales, dispositivos inteligentes, inteligencia artificial, *machine learning*, influencia comportamental.

The Influence on Human Behavior and the "Assetization" of Privacy as Contemporary Issue Concerning the Regulations of Trade on Electronic Devices

ABSTRACT. Recent studies and events disclose the instrumentalization of personal data as mean to influence behavior at scale, and the dissemination of a pervasive infrastructure of machine intelligence designed to extract and digitalize human experiences towards commercial purposes. This study describes the issue as the *assetization of privacy* and seeks to expose a legal vacuum concerning behavioral markets and the so-called *bundled goods*. The document analyzes the subject from the Europe Union and Korea perspectives, and concludes that even most comprehensive legislations require additional legal developments to restrict the impact of computational intelligence techniques and behavioral markets upon fundamental legal values.

KEYWORDS: "assetization" of privacy, behavioral data, personal data protection, internet of things, data markets, artificial intelligence, machine learning, influence on behavior.

You are intended to be in the feeling of being served, you are intended to be saturated with convenience, so then, you will not notice, and you will not complain, and all this shadow operation will remain hidden, because you will not ask questions, because you are so busy being entertained[1].

1 Entrevista con S. Zuboff en VPro Documentary, "Zuboff, on Survaliance Capitalism" [en línea], 12, 2019, [minutos 19:24 a 19:48], disponible en [www.youtube.com/watch?v=hIXhnWUmMvw] [consultado el 20 de enero de 2020].

Introducción

Internet, también llamado la tecnología de propósito general de nuestra era, ha facilitado la transformación y reorganización del comercio internacional y ha convertido corporaciones como Alphabet, Amazon, Apple, Facebook, Microsoft y Alibaba en compañías de influencia global[2]. No obstante, la capacidad de estas compañías de articular estrategias globales yace en la maximización del ciclo económico de los datos personales, gracias a la adopción sistemática de técnicas de inteligencia computacional de extracción y digitalización de datos personales y, en especial, comportamentales.

Estudios académicos y eventos recientes revelan la intensificación de métodos de extracción y análisis de datos personales sobre el comportamiento humano, a través de la diseminación calculada de una arquitectura de dispositivos inteligentes que capturan y digitalizan las experiencias del individuo y las convierten en materia prima comercializable en los llamados mercados futuros[3].

Paralelamente, las estadísticas revelan que en el 2020 el negocio de análisis de los llamados *big data* espera alcanzar 274 billones de dólares en ganancias[4], mientras que la industria del llamado "internet de las cosas", principal mecanismo de extracción de datos comportamentales, calcula que para el 2025 alrededor de 76 billones de dispositivos electrónicos se conectarán alrededor del mundo[5]. Dispositivos de extracción incluyen computadores, tabletas y teléfonos inteligentes, así como nuevos productos *físicos* que incorporan asistentes de inteligencia artificial, como Alexa, Siri, Google Assistant, Bixby y Cortana, o productos convencionales como televisores, refrigeradores, automóviles, cámaras y juguetes infantiles[6], articulados a sensores de extracción de datos.

2 Véase *Statista*, "The 100 largest companies in the world by market value in 2019", 8, 2019, disponible en [www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/] [consultado el 25 de enero de 2020]; *Statista*, "The most profitable companies in the world", 11, 2019, disponible en [www.statista.com/chart/17545/worlds-most-profitable-companies/] [consultado el 25 de enero de 2020]; *The Economist*, "The world's most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules", 5, 2017, disponible en [www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data] [consultado el 7 de octubre de 2019].

3 Véase Zuboff, S, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, London, Profile Books, 2019, 8.

4 International Data Corporation, "IDC forecasts revenues for big data and business analytics solutions will reach 189.1 billion this year with a double-digit annual growth through 2022", 4, 2017, disponible en [www.idc.com/getdoc.jsp?containerId=prUS44998419] [consultado el 10 de octubre de 2019]; véase también, *Statista*, "The big business of big data" 06, 2019, disponible en [www.statista.com/chart/18328/big-data-business-analytics-revenue/]] [consultado el 10 de octubre de 2019].

5 *Statista*, "Internet of things – Number of connected devices worldwide 2015-2025", 12, 2019, disponible en [www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/] [consultado el 20 de octubre de 2019).

6 Barbie Talks, o también llamada Barbie Dreamhouse, relaciona la asociación comercial entre Mattel y ToyTalk para producir y comercializar juguetes infantiles que incorporan micrófonos y sistemas de inteligencia artificial. Véase *Forbes*, "Barbie wants to chat with your child, but it is big data listening

En el ámbito tecnológico, los datos comportamentales denotan la digitalización de las huellas que el comportamiento humano refleja, no solo en actividades en línea[7], sino también en la *interacción* del individuo con dispositivos electrónicos, como los señalados. Dichas estelas comportamentales representan un recurso valioso para la industria de las tecnologías de la información, en la medida en que habilitan la inferencia de los caracteres más íntimos de la persona humana y su psiquis, tales como sentimientos, ideas políticas, preferencias, temores y demás aspectos de la individualidad humana[8]. De esta forma, estas corporaciones incrementan exponencialmente la eficacia de sus estrategias comerciales.

La presente investigación denomina el asunto la *asetización de la privacidad*. Este concepto busca describir el problema asociado al incremento progresivo de las presiones comerciales sobre valores legales de estatus constitucional, especialmente el derecho a la privacidad, la protección de datos personales y otras libertades fundamentales conexas, como resultado de estrategias de negocio globales que configuran la vida humana y la privacidad del individuo como un activo emergente.

Desde el punto de vista del derecho, dicha *asetización* concierne problemáticas multidimensionales, relacionadas con la carencia de límites legales sobre el modelo imperante de extracción y monetización de datos personales y comportamentales, como consecuencia de la diseminación, precariamente regulada, de redes globales de dispositivos electrónicos que incorporan sensores conectados al internet, comúnmente llamados "dispositivos inteligentes", o *bundled goods*[9].

Como hipótesis central, este estudio afirma que la carencia de límites legales y estándares de conducta sobre la extracción de datos personales y comportamentales ha favorecido la consolidación de prácticas comerciales ilegítimas y abusivas en torno a la privacidad y el tratamiento[10] de dichos datos, así como el surgimiento de mer-

in?", 12, 2015, disponible en [www.forbes.com/sites/bernardmarr/2015/12/17/barbie-wants-to-chat-with-your-child-but-is-big-data-listening-in/#725508292978] [consultado el 15 de enero de 2020]; *The New York Times*, "Barbie wants to get to know your child", disponible en [www.nytimes.com /2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html] [consultado el 15 de enero de 2020].

7 Los datos comportamentales refieren el comportamiento "digital o virtual" del ser humano, capturado y digitalizado a lo largo de descargas de aplicaciones, visitas a sitios virtuales, juegos electrónicos o virtuales, fotografías, aplicaciones de localización, compras o consultas virtuales, *likes*, emoticones, comportamientos en redes sociales, o más recientemente, datos de voz.

8 Véase GOLBECK, J. & ROBLES, C., "Predicting personality with social media", *IEEE Third International Conference on Social Computing*, 2011, 149-156; QUERCIA, D., "Our twitter profiles, our selves; predicting personality with twitter." IEEE third international conference on social computing, 2011, 180-85; *The Yorker*, "We know how you feel. Computers are learning to read emotions and the business world can't wait", 1, 2015, disponible en [www.newyorker.com/magazine/2015/01/19/know-feel] [consultado el 20 de enero de 2020].

9 LÓPEZ, J. & JOUANJEAN, M., "Digital trade, developing a framework for analysis" [en línea] OECD Trade Policy Papers, n.º 205, 2017, 6, disponible en [www.researchgate.net/publication/319667734_Digital_Trade_Developing_a_Framework_for_Analysis] [consultado el 10 de septiembre de 2020].

10 Véase el artículo 4.2 del Reglamento General de Protección de Datos, *Diario Oficial de la Unión Europea* (actos legislativos), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo,

cados que *asetifican* la intimidad y la psiquis del individuo. Este contexto, por tanto, dispone presiones multidimensionales sobre los desarrollos legislativos contemporáneos en torno a la diseminación del denominado internet de las cosas (*internet of things*) y las plataformas digitales que dichos dispositivos relacionan.

Desde una perspectiva académica, estudios recientes enfatizan la relevancia contemporánea del asunto, entre los cuales se resaltan las investigaciones de Constantiou y Kallinikos[11], Wu[12], Williams[13], Zuboff[14] y otros expertos[15], quienes coinciden en

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 (Reglamento General de Protección de Datos), disponible en [www.boe.es/doue/2016/119/L00001-00088.pdf] [consultado el 25 de enero de 2020].

11 Constantiou, I. y Kallinikos, J. "New games, new rules: big data and the changing context of strategy", *Journal of Information Technology*, n.º 30, 2010, 44-57. En este artículo, sus autores exploran el futuro epistemológico de los llamados *big data*, como una caja negra en la que permanecen irresueltos diversos temas centrales para la sociedad. Una sociedad en la que las experiencias humanas del día a día, se convierten en objetivo de estrategias comerciales implementadas por las corporaciones de análisis de los *big data* y el internet.

12 Wu, T., *The attention merchants. The epic scramble to get inside our heads*, New Your City, Vintage Books, 2017. En este libro el autor expone problemáticas fundamentales para la sociedad actual relacionadas con una industria que se alimenta y cultiva masivamente la retención de la atención del ser humano como modelo de negocio. Esta industria, liderada por los llamados "comerciantes de la atención", se dirige particularmente a influenciar nuestras decisiones y consumo a "control remoto", con profundas consecuencias en nuestra naturaleza cognitiva y social.

13 Williams, J., *Stand out of light, freedom and resistance in the attention economy*, United Kingdom, Cambridge University Press, 2018. De forma similar al texto anterior, en este libro su autor sienta una reflexión sobre cómo la era digital avanza sobre la posesión y manipulación de la atención humana como un recurso limitado, sobre el cual las compañías de la internet desarrollan una álgida competencia basadas en la explotación de las susceptibilidades del cerebro humano. De igual manera, el autor enfatiza sobre cómo la forma en la que la sociedad responda a dichos retos determinará también cómo se definirán en el futuro los asuntos morales y políticos.

14 Los estudios de Zuboff sobre el tema se encuentran compilados a lo largo de varios escritos como "In the age of smart machines", en Hangs, C., *Technology and Values: Essential Readings*, Wiley-Blackwell 2010; "Big others: surveillance capitalism and the prospects of an information civilization", en *Journal of Information Technology* (2015), 30, 75-89; y, más recientemente, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, London, Profile Books, 2019. Este último es quizá uno de los estudios más destacados y comprensivos realizados a la fecha sobre el asunto. En este último libro, la profesora emérita de la escuela de negocios de la Universidad de Harvard expone de forma detallada el producto de las investigaciones que por décadas ha conducido sobre el avance de lo que ella denomina la *era de la vigilancia capitalista*, en la que expone diversos ejemplos y reflexiones sobre los mercados comportamentales, los excedentes comportamentales y la forma en que actualmente compañías como Google lideran un sistema de explotación de la libertad y la autonomía del individuo, con fines económicos y privados.

15 Véase Jesus College Cambridge University, "Intellectual Forum: is tech making us miserable?" [en línea], 03, 2019, disponible en [www.youtube.com/watch?time_continue=13&v=1TXej5YMbvg] [consultado el 17 de octubre de 2019]. En este foro, diversos expertos del Jesus College de la Universidad de Cambridge reflexionan sobre la idea de desarrollo occidental aparejada al avance tecnológico y sobre la forma en la que dicho avance dispone riesgos fundamentales y sin precedentes sobre la salud, el bienestar y el sentido de pertenencia del individuo. Así mismo, los conferencistas sientan diversas opiniones sobre los cambios requeridos para establecer una relación con la tecnología en la que el humano prevalezca como valor central.

describir este fenómeno como un nuevo régimen que instrumentaliza[16] y mercantiliza[17] el comportamiento del individuo con fines comerciales. No obstante, estas contribuciones académicas aún no han sido utilizadas en el análisis particular de regulaciones sobre la protección de datos personales, la privacidad y los valores jurídicos que involucra el comercio de los denominados *bundled goods*, así como su diseminación, asunto que permanece precariamente regulado por las legislaciones domésticas alrededor del mundo, y relativamente inexplorado por la literatura jurídica actual.

En atención al contexto previo, este documento tiene por objetivo demarcar una reflexión sobre los mercados conductuales y la precariedad de los desarrollos legislativos actuales en torno a los límites legales necesarios para preservar los valores jurídicos y las libertades fundamentales amenazados con la diseminación de los llamados *bundled goods*. Metodológicamente, dicho objetivo se aborda a lo largo de tres grupos de evaluación: primero, a través del análisis de la relevancia del tema desde la literatura académica propuesta, las estadísticas y algunos de los eventos recientes con mayor relevancia en el asunto; segundo, en el ámbito internacional, mediante la exploración de algunos de los tratados existentes; y, tercero, desde el derecho comparado, a través del análisis de los desarrollos legislativos sobre la protección de datos personales codificados por la Unión Europea y Corea del Sur, considerados alrededor del mundo los más comprensivos en la materia. A lo largo de estos tres grupos de estudio, las fuentes utilizadas se estudian con métodos de análisis e interpretación documental.

Cuatro secciones conforman el cuerpo de este documento. La primera sección presenta sucintamente las principales contribuciones académicas sobre el objeto de estudio e introduce algunas reflexiones sobre la contemporaneidad social y jurídica del tema desde las estadísticas y algunos eventos relevantes. La segunda sección contextualiza el análisis jurídico del tema desde los modelos de regulación multilaterales más relevantes y disponibles en la actualidad, así como su énfasis de cara a la problemática central del estudio. La tercera sección expone el estudio comparado del Reglamento General de Protección de Datos de la Unión Europea (RGPD), y el marco jurídico de Corea del Sur sobre la protección de la información personal, ambos identificados entre los desarrollos legales más comprehensivos del mundo sobre la materia. Finalmente, la cuarta sección puntualiza las conclusiones y los principales hallazgos del estudio.

Este artículo concluye que la extracción de datos comportamentales y sus mercados asociados denotan un asunto contemporáneo que supera la regulación sobre la extracción y utilización de datos personales necesarios para el mejoramiento de bienes y servicios digitales, para configurar un problema multidimensional que relaciona la vigilancia y el control del comportamiento del ser humano como práctica comercial ilegítima, que contraría valores jurídicos, libertades y derechos fundamentales que

16 ZUBOFF, *op. cit.*

17 WU, *op. cit.*

están en la base del Estado de derecho y el orden democrático. En consecuencia, la regulación de los mercados comportamentales refiere asuntos de relevancia central para múltiples ámbitos del derecho moderno y la necesidad de articular diversos regímenes legales, como el derecho comercial y el derecho internacional de los derechos humanos, a fin de ampliar las bases jurídicas de que disponen los estados y sus legisladores para diseñar marcos legales más comprehensivos, capaces de garantizar la protección de bienes jurídicos de naturaleza esencial para el derecho y la sociedad contemporáneos.

I. La influencia sobre el comportamiento como asunto contemporáneo que concierne al derecho moderno

Actualmente firmas como Apple, Microsoft, Amazon, Alphabet (compañía matriz de Google), Facebook y Alibaba son consideradas las compañías más rentables y de mayor influencia en el mundo[18]. No obstante, dicha influencia global radica, particularmente, en estrategias comerciales de apropiación de datos comportamentales y la maximización del ciclo económico de ellos. Por tanto, la adquisición de datos personales y la disponibilidad de nuevas fuentes de extracción materializan una preocupación y un objetivo centrales para las corporaciones de las tecnologías de la información y la economía comportamental que ellas representan. Este contexto ha transformado la privacidad del individuo en campo de confluencia de una disyuntiva de intereses entre las corporaciones, sobre regulaciones flexibles que faciliten el acceso y la movilidad de datos[19] y la sociedad, sobre la protección de libertades y derechos individuales y colectivos.

De acuerdo con el artículo 4.2 del Reglamento General de Protección de Datos de la Unión Europea, marco jurídico brevemente analizado en la tercera sección de este documento, el tratamiento de datos personales implica

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como

18 Véase *Statista*, *op. cit.*; *The Economist*, *op. cit.*

19 Este asunto es también concebido como la agenda de política pública que lidera la llamada Internet Association, asociación comercial conformada solo por compañías globales como Google, Facebook, Microsoft, Amazon, Twitter y 37 compañías más. De acuerdo con los postulados de la asociación, como se lee en la sección introductoria de su sitio virtual, su misión busca "Foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies. Internet Association works to ensure legislators, consumers, and other stakeholders understand these benefits". Para más detalles sobre el contenido de esta agenda respecto de la liberalización del comercio, véase BSA, The Software Alliance, "Lockout, how a new way of protectionism is spreading through the world's faster growing it markets- and what to do about it"; BSA, The Software Alliance, "Powering the global digital economy. A trade agenda to drive growth"; Google, "Enabling trade in the era of information technologies. Breaking down barriers to the free flow of information", 2015. Véase también [https://internetassociation.org].

> la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Sin embargo, no existe una definición legal precisa sobre qué debe entenderse por "datos comportamentales" y su tratamiento. A pesar de la carencia de definiciones legales sobre los datos comportamentales y los mercados asociados[20], la existencia y el uso de estos devienen de estudios en el campo de la ciencia de la computación[21], los *big data*[22] y las estrategias de gestión de la innovación tecnológica, que definen los datos comportamentales como la digitalización de las huellas que el comportamiento humano refleja en la *interacción* del individuo con dispositivos electrónicos como tabletas, teléfonos inteligentes, asistentes de inteligencia artificial o productos convencionales que incorporan sensores conectados a internet.

Dichas estelas comportamentales representan un recurso valioso para la industria de las tecnologías de la información, en la medida en que habilitan la inferencia de los caracteres más íntimos de la individualidad, personalidad y psiquis humana[23]. De esta forma, estas corporaciones incrementan exponencialmente la eficacia de sus estrategias comerciales. Por tanto, diversos sectores económicos reportan la consolidación progresiva de un mercado ávido de la exploración[24] y explotación[25] del enorme potencial comercial que yace en los datos digitales sobre la información comportamental del ser humano y sus preferencias, así como estudios que además dan cuenta de la precisión y eficacia del uso comercial de protocolos automatizados[26]

20 Véase World Bank Group, "Data driven development. information and communication for development" [en línea], 2018, disponible en [www.worldbank.org/en/topic/digitaldevelopment/publication/data-driven-development] [consultado el 20 octubre de 2019], 51-68.

21 Bond, R. *et al*., "A 61-million-person experiment in social influence and political mobilization", *Nature*, n.º 7415, 2012, 295-98; Lyons, E. *et al*., "Behavioral change techniques implemented in electronic lifestyle activity monitors: a systematic content analysis", *Journal of Medical Internet Research*, n.º 8, 2014; Majid, S., "Message factors that favorably drive consumers' attitudes and behavioral intentions toward social networking and media platforms", *University of Plymouth Journal*, 2019.

22 Para el Banco Mundial, el concepto de *big data* se entiende de la siguiente forma: "The term 'big data' thus captures not only the large volumes of data now available, but also the accompanying process and technologies for collecting, storing and analyzing it", *ibid*., 33.

23 Véase Golbeck, *op. cit*.; Quercia, *op. cit*.

24 World Bank, *op. cit*., 22.

25 Para el Consejo de Derechos Humanos de las Naciones Unidas, "Some business, including the largest corporations, increasingly rely on the exploitation (collection, processing, repurposing and sale) of personal information, often without ensuring adequate transparency and informed consent of the individuals concerned". Véase Human Rights Council, "Report of the Special Reporteur on the Right to Privacy", 03, 2018, a/hrc/37/62, 6.

26 Protocolos automatizados relacionan, por ejemplo, el desarrollo de juegos de realidad aumentada, como Pokémon Go, Harry Potter Wizard Unit, the Walking Dead, también llamados *lure modules*. Otros protocolos se encuentran también en lentes de realidad aumentada tales como Google Glass y Orion, producto de la asociación entre Facebook y Luxottica para desarrollar lentes Ray-Ban de rea-

para predecir e influenciar el comportamiento de consumidores, en un contexto real, en el presente y hacia el futuro[27].

A. La influencia sobre el comportamiento y la literatura académica

Conforme a estudios académicos recientes[28], la intensificación del uso y la digitalización de datos personales responde a la evolución de los llamados "mercados futuros", y su articulación con estrategias dirigidas a consolidar la diseminación de dispositivos electrónicos para garantizar el acceso masivo y constante de las grandes corporaciones de las tecnologías de la información a nuevas y más precisas fuentes de extracción de datos personales e información comportamental.

Conforme a los estudios de Wu, el interés de las corporaciones del internet en la consolidación de nuevas y más variadas fuentes de extracción de datos personales e información comportamental correlaciona estrategias de expansión de una arquitectura de propósito dirigido, que integra sistemas de inteligencia computacional y algoritmos para capturar la atención humana[29], digitalizar el comportamiento, y transformarlo en materia prima[30] comercializable en los llamados "mercados conductuales". Dicha *asetización* es particularmente denominada por Zuboff el "excedente de datos comportamentales" o *behavioral surplus*[31].

Zuboff describe el excedente de datos comportamentales como el comportamiento humano representado en unidades observables y medibles, que una vez digitalizado es almacenado por las corporaciones de las tecnologías de la información, para su consiguiente comercialización e incorporación dentro de estructuras complejas de control y modificación del comportamiento con fines comerciales[32]. Fenómeno así mismo descrito por la autora, como el nuevo régimen de la "vigilancia capitalista" o *surveillance capitalism*[33].

En este orden de ideas, Wu concibe este problema como el régimen de la industria de la atención o *attentional industry*[34], mientras que otros autores, como Williams, desarrollan el problema desde una dimensión articulada a una industria que tiene como

lidad aumentada. Véase CNBC "Facebook working on smat glasses with Ray-Ban code name Orion", disponible en [www.cnbc.com/2019/09/17/facebook-enlists-ray-ban-maker-luxottica-to-make-orion-ar-glasses.html] [consultado el 15 de enero de 2020].

27 Véase Bond, *op. cit.*; Lyons, *op. cit.*; Majid, *op. cit.*

28 Véase Wu., *op. cit.*; Zuboff, *op. cit.*; Williams, *op. cit.*

29 *Ibid.*, Wu, *op. cit.*, 7.

30 World Bank Group, *op. cit.*

31 Véase Zuboff, *op. cit.*

32 *Idem.*

33 *Idem.*

34 Wu, *op. cit.*, 7.

propósito esencial la modificación predeterminada de patrones comportamentales individuales, la que, a su juicio, busca diseñar usuarios, no productos[35].

B. La 'asetización' de la privacidad desde las estadísticas globales

Tres hechos estadísticos son particularmente relevantes en el análisis que ocupa al presente estudio:

Primero, la rápida expansión global de dispositivos de internet de las cosas: Conforme a los reportes estadísticos, en el 2019, un total de 23 millones de dispositivos electrónicos fueron conectados alrededor del mundo, cifra que, según los pronósticos, podría alcanzar 76 billones de dispositivos conectados en solo cinco años más[36].

Segundo, el crecimiento exponencial del negocio del análisis de datos a escala o *big data*: Conforme a las estadísticas, en el 2019 el análisis comercial de datos obtuvo ganancias anuales de alrededor 189 billones de dólares[37], cifra que podría representar 274 billones de dólares en el 2020[38]. Paralelamente, desde el 2017 los medios han anunciado repetidamente el ascenso de los datos como el recurso más valioso del siglo XXI[39].

Tercero, la publicidad en línea, los motores de búsqueda y la tercerización de datos como principal fuente de ganancias para las corporaciones de las tecnologías de la información: Este tercer aspecto se encuentra estrechamente relacionado con el rápido ascenso y expansión global de compañías como Google, Facebook y las llamadas "compañías del internet" o "compañías en línea", las cuales fundan su éxito en la diseminación y diversificación de motores de búsqueda, publicidad en línea y la tercerización de datos, su principal fuente de ingresos y modelo de negocio altamente rentable[40].

Además, es importante enfatizar en tendencias comunes identificables entre las grandes corporaciones del internet. Por ejemplo, compañías como Apple, Facebook, Google, Amazon, Samsung, Microsoft y Alibaba prevalecen como los repositorios

35 WILLIAMS, *op. cit.*, 10.

36 *Statista*, "Internet of Things - number of connected devices worldwide 2015-2025", 11, 2019, disponible en [www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/] [consultado el 20 de octubre de 2019].

37 *Statista*, "The big business of big data", *cit.*

38 International Data Corporation, *op. cit.*

39 CBC News, "Data is the new oil: your personal information is now is the world's most valuable commodity", 08, 2017, disponible en [www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677] [consultado el 7 de octubre de 2019]; *The Economist*, *op. cit.*

40 *Statista*, "Market capitalization of the biggest internet companies worldwide as June 2019", 9, 2019, disponible en [www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/]; *Statista*, "Facebook annual revenue from 2009 to 2019", 2, 2020, disponible en [www.statista.com/statistics/268604/annual-revenue-of-facebook/] [consultado el 3 de febrero de 2020].

privados de datos personales más grandes del mundo[41], mientras que cada una de estas compañías dispone de una versión propia de dispositivos domésticos de inteligencia artificial, como Alexa (Amazon), Siri (Apple), Google Assistant (Google), Bixby (Samsung), AliGenie (Alibaba) y Cortana (Microsoft). No obstante, existe un marcado interés de dichas corporaciones en incursionar en sectores cada vez más extensos relacionados con la incorporación de sistemas inteligentes y sensores a lo largo de una amplia gama de nuevos productos y servicios[42].

C. La 'asetización' de la privacidad como fenómeno identificable en hechos recientes

Durante el 2017 y el 2018, algunos eventos de alcance global revelaron el avance de prácticas comerciales relacionadas con la tercerización y monetización de datos comportamentales a través de mercados de datos, así como el ascenso y diseminación global de estrategias de vigilancia, control y manipulación masiva del comportamiento humano en el ámbito político.

En el 2017, medios de comunicación europeos revelaron la existencia del arreglo contractual entre la firma de análisis de datos Cambridge Analytica y la campaña política *Leave.EU*[43], firmado con el fin de utilizar herramientas de análisis de datos comportamentales y técnicas de persuasión individuales y colectivas, con el fin de intervenir e influenciar el resultado del referendo europeo del 2016[44]. Con base en dicho acuerdo, durante el 2015 y el 2016 Cambridge Analytica adquirió, analizó y procesó información contenida en el perfil personal de millones de usuarios de Facebook, para inferir el perfil sicológico de los votantes europeos y construir una

41 *Privacy*, "Here's what the big tech companies know about you", 11, 2018, disponible en [www.visualcapitalist.com/heres-what-the-big-tech-companies-know-about-you/] [consultado el 13 de abril de 2018]; World Bank Group, *op. cit.*, 80.

42 Véase *The New York Times*, "Google to store and analyze millions of health records", 11, 2019, disponible en [www.nytimes.com/2019/11/11/business/google-ascension-health-data.html] [consultado el 5 de enero de 2020]; *Forbes*, "Key milestones of waymo Google's self'driving car", 11, 2018, disponible en [www.forbes.com/sites/bernardmarr/2018/09/21/key-milestones-of-waymo-googles-self-driving-cars/#46cb350d5369] [consultado el 13 de enero de 2020]; *Forbes*, "Barbie wants to chat with your child, but it is big data listening in?", 12, 2015, disponible en [www.forbes.com/sites/bernardmarr/2015/12/17/barbie-wants-to-chat-with-your-child-but-is-big-data-listening-in/#725508292978] [consultado el 15 de enero de 2020]; *Medium*, "Alibaba is developing self-driving cars", 4, 2018, disponible en [https://medium.com/self-driving-cars/alibaba-is-developing-self-driving-cars-e8a5c88f2cc7] [consultado el 20 de enero de 2020]; cnbc, "Facebook working on smart glasses with ray-ban code name Orion", *cit*.

43 Campaña política oficialmente fundada en el 2015 para apoyar el retiro del Reino Unido de la Unión Europea durante el referendo de junio del 2016.

44 *The Guardian*, "The great British Brexit robbery: how our democracy was hijacked", 5, 2017 [disponible en [www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy] [consultado el 25 de julio de 2019].

estrategia de "contagio social"[45], difundida de persona a persona, para influenciar y predecir la opinión de los votantes. Dicha estrategia se ejecutó mediante el diseño y distribución de contenido en línea, como noticias falsas, *cyberbullying*, "memes" y mecanismos similares planificados para exacerbar temores, crear confusión política, persuadir a los electores y finalmente modificar su decisión política[46].

Más tarde, en el 2018, los medios reportaron prácticas similares en torno a la campaña presidencial de Donald Trump, durante las elecciones presidenciales de Estados Unidos en el 2016. Conforme a los reportes, la campaña presidencial contrató a Cambridge Analytica para procesar más de cincuenta millones de perfiles personales de Facebook y desarrollar un programa de "guerra psicológica" o *psychological warfare tools*[47], con el fin de manipular el proceso de elección presidencial a favor del candidato[48].

Finalmente, investigaciones adicionales revelaron que durante varios años la misma firma de análisis de datos –propiedad de Peter Thiel, cofundador de PayPal e inversionista mayoritario de Facebook– fue contratada por diversos gobiernos y campañas para intervenir en el resultado de procesos políticos y electorales alrededor del mundo[49]. Según reportes recientes[50], Cambridge Analytica implementó instrumentos de guerra sicológica para predecir e influir exitosamente en más de cien elecciones en todo el mundo[51]. Algunos de los países y gobiernos involucrados incluyen a Italia, Chipre, Colombia, Ucrania, República Checa, Brasil, Argentina, India, Malasia, Tailandia, Filipinas, Indonesia, África del Sur, Kenya, Nigeria y México[52].

45 Estudios conducidos al interior de Facebook en el 2010 confirmaron la habilidad de influenciar el comportamiento humano a escala masiva, en el mundo real, mediante la instrumentalización de datos comportamentales. En dicho estudio, este fenómeno fue denominado "contagio social" o *social contagion*. Concretamente, el estudio demuestra la habilidad de ejercer una influencia directa en la expresión propia e individual de las personas fijadas como objetivo del experimento, a través del logro de un resultado concreto, en el mundo fáctico o real. Para más detalles sobre dicho estudio, véase BOND, R., op. *cit*., 295.

46 *Politico*, "Cambridge Analytica did works for Brexit groups, says ex-stuffer", 06, 2019, disponible en [www.politico.eu/article/cambridge-analytica-leave-eu-ukip-brexit-facebook/] [consultado el 17 de diciembre de 2019], VPro Documentary, ZUBOFF on Survaliance Capitalism, 12, 2019, disponible en [www.youtube.com/watch?v=hIXhnWUmMvw] [consultado el 20 de enero de 2020]. Para información un poco más detallada sobre el asunto, véase el interesante documental de Netflix *The Great Hack*, dirigido por Karim Amer y nominado al premio BAFTA como mejor documental (1, 2019).

47 *The Guardian*, "I' made Steve Bannon's phycological warfare tool': meet the data war whistleblower", 03, 2018, disponible en [www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump] [consultado el 5 de septiembre de 2019].

48 *The Guardian*, "Revealed: 50 million Facebook Profiles harvested for Cambridge Analytica in major data breach", disponible en [www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election] [consultado el 20 de julio de 2019].

49 *The Guardian*, "The great British Brexit robbery: how our democracy was hijacked", *cit*.

50 *The Guardian*, "Fresh Cambridge Analytica leak' shows global manipulation is out of control", 1, 2020, disponible en [www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation] [consultado el 10 de enero de 2020].

51 BBC News, "Cambridge Analytica: The data firm's global influence", 3, 2018, disponible en [www.bbc.com/news/world-43476762] [consultado el 20 de septiembre de 2019].

D. La 'asetización' de la privacidad como práctica comercial ilegítima

Una creciente preocupación global ha surgido en torno a la existencia y rápida diseminación de tecnologías dirigidas a la modificación del comportamiento humano, individual y colectivo, con fines comerciales, toda vez que dichas prácticas contradicen valores jurídicos esenciales del Estado de derecho, como el libre ejercicio de la autonomía del individuo, la privacidad y la democracia misma.

Como paradigma legal moderno, el derecho contemporáneo enfatiza sistemáticamente en la importancia de la libertad humana y la autonomía, individual y colectiva, como valores sociales y jurídicos supremos. Tanto en el derecho internacional público, a través del principio de *no intervención*[53]; en el derecho internacional de los derechos humanos, a través del reconocimiento de la protección del libre desarrollo de la personalidad y la autonomía individual[54]; y en el derecho privado, a través del ejercicio del consentimiento libre de vicios, el sistema jurídico busca preservar la libertad, no solo física, sino también de pensamiento y decisión del ser humano. Por tanto, no solo el uso de la fuerza, sino también todo acto de influencia, vigilancia, coacción, engaño o manipulación, directa o indirecta, sobre el comportamiento del individuo se consideran ilegítimos, arbitrarios y contrarios al derecho, en la medida en que niegan las libertades más básicas, y por tanto fundamentales, del ser humano[55].

En diversas declaraciones, organismos internacionales han expresado preocupación por la colección y el tratamiento masivo de datos personales, así como la carencia de regulaciones comprehensivas sobre el asunto. En el 2013, en la resolución 68/167, la Asamblea General de las Naciones Unidas indicó que la vigilancia, la colección arbitraria o ilegítima de datos personales, así como los "actos altamente intrusivos" sobre la privacidad, son también violaciones a los derechos a la privacidad y a la libre expresión. Por consiguiente, dichos actos contradicen los acuerdos y principios de una sociedad democrática[56].

En el 2018, en reporte anual sobre el derecho a la privacidad, el Consejo de Derechos Humanos de las Naciones Unidas enfatizó su preocupación por el incre-

52 *Quartz*, "Mapped: The breathtaking global reach of Cambridge Analytica's parent company", 3, 2018, disponible en [https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/] [consultado el 5 de septiembre de 2019]; BBC News, "Cambridge Analytica: The data firm's global influence", 3, 2018, disponible en [www.bbc.com/news/world-43476762] [consultado el 3 de septiembre de 2019].

53 Artículo 2.1, Carta de las Naciones Unidas.

54 Artículo 12, Declaración Universal de los Derechos Humanos.

55 Véase 1970 Declarations on principles of international law, friendly relations and cooperation among states in accordance with the charter of United Nations, adoptada por la Asamblea General de las Naciones Unidas en octubre de 1970 a través de resolución 26/25 (XXI).

56 United Nations General Assembly, "Resolution adopted by the general assembly on 18 december 2013, the right to privacy in the digital age", A/Res/68/167, par. 10; véase también Anderson, D., *A question of trust*, London, Crown Press, 2015, 93.

mento de prácticas comerciales entre las grandes corporaciones globales que utilizan la extracción, el tratamiento, reciclaje, reutilización y venta de información personal, como medios de explotación de datos personales, sin la existencia de medidas transparentes y sin el consentimiento informado de los individuos a quien dicha información concierne[57].

En el reporte anual del 2019, el comisionado especial de las Naciones Unidas sobre el derecho a la privacidad también expresó preocupación por los retos legales impuestos por las tecnologías emergentes[58] y los dispositivos inteligentes que recolectan datos personales. En referencia expresa a dispositivos de recolección de datos sobre la salud, el comisionado precisó que dichos dispositivos continuamente transmiten a las compañías de internet y otros terceros datos personales sobre la vida real de las personas, posicionando al cuerpo humano como datos, e incorporándolo como sujeto de procesamientos automatizados, que se llevan a cabo a través de sistemas de inteligencia artificial y *machine learning*[59].

Los estudios, estadísticas, hechos y pronunciamientos de la comunidad internacional hasta aquí plasmados permiten contextualizar el asunto desde una dimensión global y contribuyen a demarcar una reflexión alrededor de los mercados conductuales. Dicha reflexión expone no solo la contemporaneidad del tema y su relevancia jurídica, sino especialmente el impacto político y social generado por la carencia de límites legales sobre dichos mercados. A continuación, y en atención al contexto anterior, se introduce el análisis jurídico del tema desde los modelos de regulación multilaterales más relevantes sobre la protección de datos personales, disponibles en la actualidad.

II. Modelos multilaterales relativos al procesamiento de datos personales y la protección de la privacidad

Desde la perspectiva del comercio internacional, no existe un tratado común sobre la protección de datos personales, ni directrices o estándares particulares relativos al procesamiento de datos comportamentales. Los actuales desarrollos se encuentran extensamente fragmentados y especialmente limitados al diseño de marcos jurídicos sobre el comercio de servicios relativos al tratamiento de datos personales y

57 HUMAN RIGHTS COUNCIL, "Report of the Special Reporteur on the Right to Privacy", 3, 2018, A/HRC/37/62, 6.

58 Naciones Unidas ha reconocido la existencia de áreas grises en el tratamiento de datos personales, que conllevan múltiples retos regulatorios hacia el futuro. La UNCTAD ha afirmado que algunos análisis y procesos de toma de decisiones de los *big data* incorporan reglas y algoritmos no públicos o transparentes, e involucran asuntos relativos a la privacidad que permanecen mayoritariamente no resueltos. Véase UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, "Data protection regulation and international data flows: Implications for Trade and Development", United Nations, 2016.

59 HUMAN RIGHTS COUNCIL, "Right to privacy. Report of the special rapporteur on the right of privacy", 2, 2019, HRC/40/63, par. 25.

su movimiento transfronterizo, mas no concernientes al comercio de los llamados *bundled goods*[60]. De tal suerte que la diseminación de dispositivos inteligentes, su comercialización y disposición, así como su impacto sobre la privacidad y otros derechos conexos, permanecen como asuntos precariamente regulados en el campo internacional.

Los actuales desarrollos sobre la protección de datos personales pueden clasificarse en tres categorías. La primera incluye acuerdos que incorporan la protección de datos en el clausulado de capítulos sobre el comercio electrónico. La segunda abarca iniciativas de carácter facultativo que buscan guiar la operatividad del movimiento transfronterizo de datos, pero desde una dimensión no relacionada con preocupaciones particulares sobre los derechos humanos. Finalmente, la tercera categoría relaciona acuerdos e iniciativas multilaterales concernientes a la protección de los derechos humanos, y éstos como base jurídica esencial para determinar la legalidad de prácticas comerciales sobre los datos personales, así como la necesidad de adoptar medidas adicionales para su protección.

A. Tratados de libre comercio

Dada la naturaleza comercial de este primer grupo, el libre movimiento de datos prevalece como principio general[61], mientras que las limitaciones o restricciones a su movimiento refieren el desarrollo de medidas domésticas en la implementación interna del tratado que corresponda y conforme a las áreas políticas reservadas como derecho soberano de los estados parte. Así mismo, es importante notar que el carácter vinculante de estos acuerdos, los cuales conciernen de manera exclusiva la liberación del comercio entre los estados parte, los hace más efectivos que otros tipos de tratados, toda vez que incorporan cláusulas de obligatorio cumplimiento, así como sistemas propios de resolución de conflictos y disputas entre sus miembros.

Acuerdos relevantes incluyen el Tratado Integral y Progresivo de Asociación Transpacífico (Comprehensive and Progressive Agreement for Trans-Pacific Partnership [CPTPP]), antiguamente conocido como Acuerdo Transpacífico de Cooperación Económica (TPP, por sus siglas en inglés [Trans-Pacific Partnership]), el acuerdo entre Estados Unidos, México y Canadá (USMCA), también denominado el nuevo NAFTA, y el acuerdo entre Corea del Sur y Estados Unidos (KORUS), así como el tratado entre la Unión Europea y Estados Unidos, llamado también Acuerdo de Asociación Transatlántica sobre Comercio e Inversión (TTIP).

60 López, J., & Jouanjean, M., *op. cit.*, 6.

61 Véase, por ejemplo, Comprehensive and Progressive Agreement on Transpacific Partnership, CPTPP, capítulo 14, sobre comercio electrónico; APEC Privacy Protection Guidance, parágrafos 28 al 44; véase también otras referencias en G20's "Leaders declaration building consensus for fair and sustainable development", 2018, recital 9.

B. Declaraciones y acuerdos de naturaleza facultativa

Este grupo relaciona las declaraciones y los acuerdos de naturaleza facultativa para el diseño de estándares y principios internacionales sobre el tratamiento de datos personales y su movimiento transfronterizo. En ocasiones los estándares establecidos en estos acuerdos son también incorporados en acuerdos de carácter comercial; no obstante, la carencia de obligatoriedad de este tipo de tratados los traduce en mecanismos inapropiados para la efectiva ejecutoriedad y observancia de los estándares, principios y reglas que ellos contienen.

Instrumentos relevantes incluyen, por ejemplo el marco de privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC, por su sigla en inglés), así como las reglas de la misma organización sobre la privacidad en el movimiento transfronterizo de datos personales, los cuales buscan proporcionar guías y direcciones a los negocios establecidos dentro de las economías de la APEC, sobre aspectos comunes relacionados con la privacidad y formas legítimas de conducir negocios que afectan dicha privacidad[62]. Dentro de la guía se encuentran principios tales como la prevención del daño, la transparencia, la proporcionalidad, el consentimiento y los usos legítimos[63]. Se trata de principios también consagrados de forma semejante en otros instrumentos internacionales, tales como la guía sobre la privacidad de la OCDE y la Convención sobre la Seguridad Cibernética y la Protección de los Datos Personales de la Unión Africana.

C. La protección de los datos personales como derecho fundamental

Esta última categoría se encuentra referida a los acuerdos que abordan el asunto desde la perspectiva del derecho internacional de los derechos humanos. En esta categoría se destacan los desarrollos de la Organización de las Naciones Unidas (ONU) a través de medidas de alto nivel, el proyecto de la Organización de Estados Americanos (OEA) sobre los llamados "principios sobre la protección de los datos personales", así como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, acuerdo regional analizado de manera separada en la tercera sección de este documento.

La perspectiva de las Naciones Unidas sobre la materia requiere mención especial, toda vez que el tratamiento nacional de datos personales, su movimiento transfronterizo, así como su procesamiento fuera del territorio en el que se encuentran los sujetos de datos se consideran asuntos que conciernen al derecho internacional de los derechos humanos, y éste, marco jurídico necesario para evaluar la legalidad y legitimidad de las prácticas comerciales involucradas[64].

62 Véase ASIA PACIFIC ECONOMIC COOPERATION (APEC), "Privacy framework", Singapore, 2005, 4.

63 *Ibid*., 11-28.

64 Véase UNITED NATIONS GENERAL ASSEMBLY, *op. cit*., p. 10; UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *op. cit*., 24.

Las Naciones Unidas advocan por la necesidad de modular prácticas comerciales relativas al tratamiento de datos personales en torno a criterios multilaterales fijados mediante acuerdos de carácter consuetudinario, como el artículo 12 de la Declaración Universal de los Derechos Humanos, que reconoce la privacidad como derecho humano fundamental; el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; igual que el artículo 1.º del Pacto Internacional de Derechos Económicos, Sociales y Culturales[65], relacionados con el derecho a la privacidad y la libre determinación.

Además, la organización ha promovido el asunto a través de medidas de alto nivel. En el 2013, en reunión plenaria, la Asamblea General adoptó la resolución 68/167, sobre el derecho a la privacidad en la era digital, a través de la cual el órgano expresó preocupación sobre el impacto negativo que la colección de información personal y la vigilancia podría tener en el ejercicio de los derechos humanos fundamentales, en particular en relación con actividades llevadas a cabo a escala masiva.

En julio de 2015, a través de la resolución 28/16, el Consejo de las Naciones Unidas para los Derechos Humanos designó a un comisionado especial para el derecho a la privacidad, como experto independiente designado con la función de examinar y reportar periódicamente asuntos específicos sobre la materia[66], entre los cuales incluyó la evaluación periódica e independiente sobre los retos allegados con la adopción de nuevas tecnologías[67]. Más tarde, en octubre del 2018, la ONU adoptó los llamados "principios sobre la protección de la privacidad y los datos personales"[68], con el fin de establecer un marco básico para el procesamiento de datos personales dentro de su sistema, así como la armonización de dichos estándares en el interior de la organización[69].

En una tendencia similar, la OEA estableció un proyecto especial para el desarrollo de los llamados "principios sobre la protección de los datos personales", con base en el desarrollo del concepto de *habeas data*[70], con la finalidad de consolidar la adopción de quince principios básicos para el desarrollo y la promoción de instrumentos y mecanismos legales de protección dentro de su sistema. Dicho instrumento incorpora principios tales como propósito legítimo y justo, previo consentimiento, retención y usos limitados, protección especial sobre datos sensibles, entre otros.

65 United Nations General Assembly, *op. cit.*

66 United Nations Conference on Trade and Development, *op. cit.*, 24.

67 Véase también, United Nations Human Rights, Office of the High Commissioner, "Special rapporteur on the right to privacy", disponible en [www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx,] [consultado el 10 de octubre de 2019].

68 UN High-Level Committee on Management 36th Meeting, "Personal data protection and privacy principles", 10, 2018, disponible en [www.unsystem.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf] [consultado el 11 de octubre de 2019].

69 *Idem*.

70 Organization of American States, Inter-American Juridical Committee, "Privacy and data protection" 86th Regular Session, 3, 2015, 23-27, CJI/doc. 474/15 rev.2, disponible en [www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf] [consultado el 4 de octubre de 2019].

El análisis previo contribuye al diagnóstico del desarrollo actual del asunto en el ámbito multilateral, permitiendo observar, primero, el carácter fragmentario de las aproximaciones internacionales sobre la protección de la privacidad y los datos personales, la carencia de acuerdos vinculantes y específicos sobre la materia, así como la prevalencia de principios y estándares que, a pesar de su relevancia, limitan su ejecutoriedad en el ámbito doméstico. A continuación se presenta un estudio comparativo de las aproximaciones legislativas de la Unión Europea y Corea del Sur sobre la protección de datos personales y la privacidad, con el fin de profundizar en el análisis jurídico de la cuestión de los datos personales.

III. Modelos domésticos de regulación sobre el procesamiento de datos personales y la protección de la privacidad

Desde las regulaciones domésticas sobre el tratamiento de datos personales y la protección de la privacidad, los estándares nacionales y niveles de protección son asimétricos entre jurisdicciones. De acuerdo con la UNCTAD, el cincuenta y ocho por ciento de los estados alrededor del mundo, correspondiente a ciento siete países, ha implementado algún tipo de legislación para la protección de datos personales y la privacidad[71]. No obstante, el veintiuno por ciento de países carece de reglamentaciones básicas[72], mientras que el treinta y dos por ciento, que representa al menos sesenta y siete estados, aún no han establecido regulaciones mínimas esenciales para la protección de consumidores en actividades comerciales en línea[73].

Al respecto, los desarrollos legislativos de la Unión Europea y de Corea del Sur merecen mención especial, en consideración de su desarrollo, del nivel de protección definido y del establecimiento de procedimientos y estándares precisos, cuya ejecución es vigilada por autoridades especiales, creadas para tal fin.

A. La legislación de la Unión Europea sobre la protección de datos personales

La Unión Europea instituyó un enfoque propio y detallado respecto de actividades comerciales que involucran el procesamiento de datos personales, aproximación legislativa plasmada en el ampliamente conocido "Reglamento General de Protección de Datos" (RGPD)[74]. Esta legislación, considerada la más comprehensiva del mundo en

71 UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, "Data protection and privacy legislation worldwide", disponible en [https://unctad.org/en/Pages/DTL/STI_and_ICTS/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx] [consultado el 4 de septiembre de 2019].

72 *Idem*.

73 UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, "Online consumer protection legislation worldwide", disponible en [https://unctad.org/en/Pages/DTL/STI_and_ICTS/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx] [consultado el 4 de septiembre de 2019].

74 *Diario Oficial de la Unión Europea* (actos legislativos), *op. cit*., 15.

la materia[75], se estructura sobre la base de los derechos humanos y el orden constitucional de la Unión Europea[76]. En este contexto, la parte introductoria del reglamento, primer numeral, identifica sus bases constitucionales, tales como el artículo 8.° de la Carta de Derechos Fundamentales de la Unión Europea, el artículo 8.° de la Convención Europea de Derechos Humanos, y el artículo 16 del Tratado de Funcionamiento de la Unión Europea, todas estas, normas de carácter constitucional que reconocen la protección de los datos personales como un derecho fundamental.

Desde la perspectiva de la Unión, el tratamiento de datos personales, con fines comerciales[77], es considerado fuente de riesgos múltiples sobre los derechos humanos y las libertades fundamentales de la persona natural, connotación que confirma la necesidad de adoptar y ejecutar medidas restrictivas sobre prácticas económicas relacionadas con la colección, el tratamiento y la monetización de datos personales, dentro de su jurisdicción[78].

En particular, el recital 75 indica:

> Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, perdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.

En este contexto legal, los llamados "responsables y encargados del tratamiento" permanecen como los principales destinatarios de las obligaciones substantivas establecidas en la legislación, en particular los artículos 4.7 y 4.8, estándares extensibles

75 Mattoo, A., & Meltzer, J., "International data flows and privacy: the conflict and its resolution", *Journal of International Economy Law*, University of Oxford, 2018, 769-789, 770.

76 El reglamento consolida su estructura regulatoria y enfoque, articulando la regulación del procesamiento de datos personales con instrumentos legales constitucionales que conforman el ordenamiento jurídico de la Unión, tales como el artículo 8.º de la carta de derechos fundamentales de la Unión Europea; el artículo 8.º de la Convención Europea de Derechos Humanos; el artículo 16 del Tratado de Funcionamiento de la Unión Europea, así como las decisiones de la Corte de Justicia de la Unión Europea, como el caso Google Spain v aedp, 2014, ecr 317, mayo, 2014.

77 Véase el artículo 2.2 rgpd: "El presente reglamento no se aplica al tratamiento de datos personales: efectuado por los estados miembros (literal b), efectuado en el ejercicio de actividades puramente personales o domésticas (literal c), efectuado por autoridades competentes respecto a infracciones penales (literal d), etc.".

78 Dentro de las cláusulas del reglamento, el tratamiento de datos personales es definido como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (artículo 4.2 rgpd).

a responsables y encargados del tratamiento establecidos fuera del territorio de la Unión Europea[79].

Así mismo, el reglamento codifica principios[80] y derechos accionables[81], relevantes en el establecimiento de guías y estándares de protección en otros países, toda vez que la regulación de la Unión busca no solo lograr una protección comprensiva y armonizada entre sus miembros[82], sino también contribuir a la adopción de altos estándares sectoriales dentro de su territorio y fuera de él. Con dicho propósito, el reglamento establece mecanismos de certificación (artículo 42) y el cumplimento de ciertos códigos de conducta (artículo 40), aplicables a por compañías y corporaciones extranjeras (artículo 3.2), cuando el tratamiento de datos fuera del territorio de la Unión involucra a sujetos de datos ubicados dentro de su jurisdicción.

No obstante, el procesamiento de datos comportamentales y su excedente no son materia expresamente identificada o regulada por la norma europea. Dentro del reglamento no existe prohibición expresa sobre el uso de sistemas de inteligencia artificial para influenciar el comportamiento humano, ni la identificación de riesgos particulares respecto de la diseminación de bienes o dispositivos electrónicos de extracción y digitalización de datos comportamentales, así como tampoco sobre el escalamiento masivo de dichas técnicas. Por el contrario, el RGPD codifica afirmaciones que normalizan ciertas prácticas de análisis de datos comportamentales como operaciones por defecto. Por ejemplo, en las consideraciones del numeral 24 se establece:

> Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

79 RGPD, artículo 3.º: "El presente reglamento aplica al tratamiento de datos personales […], independientemente de que el tratamiento tenga lugar en la Unión o no". Además, el artículo 3.2 puntualiza: "El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes y servicios […] independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que éste tenga lugar en la Unión".

80 Según el artículo 5.º, RGPD, los principios sobre el tratamiento de los datos personales incluyen licitud, lealtad y transparencia, así como limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva.

81 Entre los derechos de los sujetos interesados se destaca el derecho de rectificación (art. 16), derecho al olvido (art. 17), derecho a la limitación del tratamiento (art. 18), derecho a la portabilidad de datos (art. 20), derecho a la oposición y las decisiones individuales automatizadas y la elaboración de perfiles (arts. 21 y 22), entre otros.

82 Véase RGPD, recitales 3, 53, 150 y 152.

A pesar de la carencia de regulaciones particulares sobre la materia, el RGPD contiene elementos jurídicos que contribuyen a la implementación de marcos de regulación más precisos para la protección de datos comportamentales a lo largo de las jurisdicciones de los estados miembros, como a continuación se enumeran:

Primero, en el artículo 4.°, el RGPD contiene una definición de datos personales que implícitamente incluye los datos comportamentales. El RGPD define los datos personales como toda información sobre una persona física, identificada o identificable, mediante uno o varios elementos de identificación, incluyendo "datos de localización o […] elementos propios de la identidad física, psíquica, económica, cultural o social de dicha persona", estos últimos, especialmente atinentes al ámbito de los datos comportamentales.

Segundo, el RGPD reconoce categorías de datos personales "particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales"[83], por lo cual requieren especial protección o el establecimiento de restricciones y disposiciones domésticas de carácter adicionales a las establecidas en el reglamento[84]. Conforme al reglamento, son datos sensibles la información relacionada con la etnicidad del sujeto (recital 51); las opiniones políticas, las creencias filosóficas, la vida y orientaciones sexuales (artículo 9.1); los datos biométricos (artículo 4.14); la información relativa a la condición de salud pasada, presente o futura, así como el estado mental y físico de la persona, sin consideración de la fuente de recolección (recital 35 y artículo 4.15); y la información relativa a menores de edad (recital 38).

A pesar de que el RGPD no identifica riesgos particulares sobre los datos comportamentales y la diseminación de dispositivos de internet de las cosas o *bunbled goods*, la naturaleza sensible de datos e información comportamental coleccionada a través de dichos dispositivos, tales como asistentes de inteligencia artificial, carros autoconducibles o dispositivos de salud, pueden justificar la adopción de medidas restrictivas respecto del diseño e instalación de dichos bienes.

Tercero, reglas relativas a la "elaboración de perfiles" reflejan una clara cercanía con los datos comportamentales. La elaboración de perfiles se conceptualiza en el artículo 4.4 como "toda forma de tratamiento automatizado de datos personales […] para evaluar determinados aspectos personales de la persona física, en particular para analizar o predecir aspectos relativos a […] preferencias personales, intereses, comportamiento o movimiento de dicha persona física". Por tanto, a través de la interpretación de dichas normas puede lograrse una protección extensiva sobre los datos comportamentales, a pesar de la carencia de menciones directas o expresas sobre estos.

Cuarto, el artículo 6.° del reglamento fija criterios para analizar la licitud del tratamiento, tales como el consentimiento informado (literal a) y la necesidad del

83 Para más detalles, véase recital 51, RGPD.

84 RGPD, recital 53.

tratamiento (literales b al f). Así mismo, el numeral cuarto de éste establece estándares relacionados con el llamado "tratamiento ulterior previsto", referido a los datos recolectados en adición a los requeridos para garantizar o mejorar el funcionamiento de dispositivos de internet de las cosas, particularmente relevantes respecto del excedente de datos comportamentales. Igualmente, los artículos 13.3 y 14.4 codifican requerimientos específicos sobre el tratamiento ulterior de datos personales realizado por responsables y encargados del tratamiento, así como por terceras partes.

Finalmente, y como quinto elemento, el artículo 35 exige la disposición de garantías adicionales en la adopción de nuevas tecnologías de análisis de datos, que "por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para las personas físicas". Estas garantías incluyen evaluaciones de impacto sobre las operaciones de tratamiento, prioritariamente requeridas en casos de tecnologías para elaboración de perfiles, el tratamiento a escala de categorías especiales de datos y la observación sistemática a gran escala (literales a, b y c, respectivamente)[85].

B. La legislación de Corea del Sur sobre la protección de información personal

Conforme a los datos estadísticos, Corea del Sur cuenta con una tasa de penetración del internet del 95 por ciento, clasificada como una de las más altas mundo[86]. Así mismo, el país se ubica como el primero en el mundo en términos de velocidad en internet móvil[87]. En consecuencia, en este país asiático la regulación del comercio electrónico y la protección de la información personal se consideran prioridad legislativa y sus desarrollos domésticos estimados como parte de los más comprehensivos y estrictos del mundo[88], con algunos estándares que incluso superan a los de la Unión Europea[89].

85 Véase el recital 91: "Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos".

86 *Statista*, "Countries with the highest internet penetration rate as January 2019", 2, 2019, disponible en [www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/] [consultado el 25 de enero de 2020].

87 SPEED TEST GLOBAL INDEX, "Global Speeds December 2019", 12, 2019, disponible en [www.speedtest.net/global-index] [consultado el 25 de enero de 2020].

88 Véase IAPP, "GDPR matchup: South Korea's personal information protection act", en [https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/] [consultado el 13 de octubre de 2020]; Thales, "South Korea's PIPA compliance", disponible en [www.thalesesecurity.com/solutions/compliance/apac/south-koreas-pipa] [consultado el 13 de octubre de 2019].

89 Véase LEAF, G. & PARK, W., "South Korea's Innovation in Data Privacy Principles. Asia Comparisons", *Computer Law and Security Review*, vol. 30, Issue 5, 2014, 492-505.

En Corea del Sur la protección de información personal se encuentra desagregada a lo largo de diversas regulaciones, algunas de ellas dirigidas a sectores específicos en consideración de la actividad económica o de su relación con el tratamiento intensivo de datos personales[90]. Conforme al artículo 1.° del decreto sobre la protección de la información personal (o PIPA, por sus siglas en inglés [Personal Information Protection Act]), la legislación relativa a la protección de información personal busca fortalecer los derechos e intereses de sus ciudadanos y la realización de la dignidad del individuo, mediante la protección de la privacidad respecto de la colección no autorizada de la información personal que a éste concierne, así como el abuso o usos ilegítimos de dicha información.

El referido PIPA es considerado la ley general de protección de información personal actualmente vigente en el país asiático. Así mismo, normas adicionales, como el llamado Communication Privacy Protection Act (CPPA), establecen regulaciones relevantes, como la tipicidad penal de actos relativos a la transmisión o recepción no consentidas por la parte interesada de cualquier sonido, palabra, símbolo o imagen, a través de cable, wifi, cables de fibra óptica o cualquier otro sistema electromagnético, incluyendo teléfonos o correos electrónicos (artículo 75).

Además, Corea del Sur ha implementado tres regulaciones especiales para algunos sectores y temas concretos:

Primero, la ley sobre la promoción de información y su protección respecto a la utilización de redes de comunicación, denominada Act on Promotion of Information and Communications Network Utilization and Information Protection[91], también llamada Network Act, que gobierna la protección de información personal administrada por proveedores de servicios de comunicación.

Segundo, el conjunto conformado por dos regulaciones financieras establecidas para la protección de la información financiera de clientes y consumidores en contra de su abuso o usos arbitrarios. La primera relativa al uso y protección de información

90 Así mismo, Corea del Sur ha establecido diversas comisiones y agencias, como autoridades competentes, en consideración a tema de legislación correspondiente. Así, por ejemplo, el Ministerio del Interior y Seguridad es encargado de conocer sobre los asuntos relacionados con el PIPA, mientras que la llamada Comisión para la Protección de la Información Personal es encargada de elaborar las políticas sobre protección de datos y evaluar, modificar o establecer leyes y medidas administrativas relacionadas con la materia. De igual forma, la Comisión de Servicios Financieros es encargada de la ejecución y el seguimiento del cumplimiento de la reglamentación contenida en la Credit Information Act, así como su interpretación formal. Véase *personal information protection commission*, artículo 7 PIPA. Para más información, véase *Personal information protection commission* [www.pipc.go.kr/cmt/main/english.do]; Financial service commission, disponible en [www.fsc.go.kr/eng/index.jsp]; otras entidades relevantes incluyen la agencia para la protección de datos en Corea, llamada Korea Internet & Security Agency (KISA) [www.kisa.or.kr/eng/main.jsp] y la llamada Korea Communication Commission, véase [https://eng.kcc.go.kr/user/ehpMain.do].

91 Véase Act on the promotion of information and communication networks utilization and information protection, disponible en [www.privacy.go.kr/eng/laws_view.do?nttId=8187&imgNo=2] [consultado el 10 de enero de 2020].

crediticia, denominado Use and Protection of Credit Informatión Act[92], comúnmente llamado Credit Informatión Act, y la ley sobre transacciones electrónicas finacieras, o Electronic Financial Transaction Act.

Tercero, Corea del Sur desarrolló una legislación especial sobre la protección de información personal respecto del uso de dispositivos de localización, a través de la ley Act on the Protection and Use on Location Information[93], comúnmente denominada Location Information Act. Esta regulación establece estrictas medidas sobre información relativa a la localización de individuos residentes en el país, materia regulada con particular atención y detalle, en consideración de la situación geopolítica del país en la región y sus tensiones con Corea del Norte[94].

Otros desarrollos de la política doméstica sobre la materia incluyen la guía sobre la de-identificación de datos personales, denominada *Guidelines for De-identification of Personal Data*[95], elaborada y publicada para formular estándares nacionales sobre técnicas comerciales de análisis de datos y su convergencia con desarrollos tecnológicos de los llamados *big data* y el internet de las cosas[96]. La de-identificación de datos personales se refiere a la eliminación de elementos identificadores del sujeto de datos, como un procedimiento que hace presumir el carácter no-personal de los datos en cuestión y autoriza su utilización, tan amplia como sea posible, sin ninguna restricción legal[97]. Consecuentemente, la guía presume como no-personales los datos que no identifican a una persona en específico, los datos sobre personas fallecidas, así como datos de corporaciones, personas jurídicas, grupos, múltiples individuos, u objetos[98].

La guía estipula la obligatoriedad de la de-identificación de "valores de atributos", tales como características individuales o físicas, económicas o profesionales, así como las características electrónicas contenidas en los datos que han de ser procesados, incluyendo *cookies*, registros sobre tiempos y fechas de ingreso a sitios virtuales, usos de servicios digitales, y teléfonos celulares, al igual que datos obtenidos a través del *global positioning systems* o GPS, entre otros[99].

92 Véase Use and protection of credit information act, disponible en [www.privacy.go.kr/eng/laws_view.do?nttId=8188&imgNo=3] [consultado el 10 de enero de 2020].

93 Véase Act on the protection, use, etc, of location information, disponible en [www.privacy.go.kr/eng/laws_view.do?nttId=8189&imgNo=4] [consultado el 10 de enero de 2020].

94 Véase YOON., J., "South Korea data localization shaped by conflict" [en línea], 2, 2018, *The Henry M. Jackson School of International Studies*, disponible en [https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/] [consultado el 15 de septiembre de 2019].

95 KOREA MINISTRY OF INTERIOR, KOREA FINANCIAL SERVICE COMMISSION, KOREA MINISTRY OF HEALTH AND WELFARE, MINISTRY OF SCIENCE, ICT AND FUTURE PLANNING, "Guidelines for de-identification of personal data, guide for de-identification standards and support / management system", disponible en [www.privacy.go.kr/eng/policies_view.do?nttId=8190&imgNo=1] [consultado el 15 de enero de 2020].

96 *Ibid*., 3.

97 *Ibid*., 7.

98 *Ibid*., 8.

99 *Ibid*., 10.

Cláusulas y definiciones similares a las establecidas en el RGPD se encuentran también plasmadas en la PIPA. Por ejemplo, definiciones sobre datos personales y titulares (artículo 2.º), datos sensibles (artículo 23), principios[100] y derechos accionables[101], consentimiento previo e informado (artículo 15), así como requerimientos especiales sobre evaluaciones previas en torno al impacto sobre la privacidad, como consecuencia de la implementación de nuevas tecnologías de análisis de datos o *big data* (*privacy impact assessment*, artículo 33 PIPA).

Al igual que el reglamento europeo sobre protección de datos personales, la normatividad surcoreana no relaciona elementos que conciernen expresamente los datos comportamentales, no obstante ésta contiene elementos relevantes sobre el asunto. Por ejemplo, restricciones expresas sobre los datos de identificación particular del individuo o *particular identification data* ("RRNs"), entendidos como los identificadores únicos asignados a cada persona natural, conforme al derecho y las leyes aplicables[102]. Así mismo, la normatividad surcoreana prohíbe expresamente la denegación de servicios o bienes como consecuencia del no-consentimiento del usuario sobre la colección de sus datos personales y su procesamiento, en adición al mínimo requerido[103], cláusula no expresamente contenida en la legislación de la Unión Europea.

C. Anotaciones pertinentes sobre ambas legislaciones

En síntesis, las regulaciones de la Unión Europea y Corea del Sur sobre la protección de datos y la información personal establecen modelos de regulación relevantes para analizar la implementación de marcos jurídicos que justifican la implementación de medidas domésticas necesarias para la protección de datos comportamentales y restricciones sobre los mercados relacionados, desde una perspectiva que relaciona la privacidad como derecho fundamental del individuo. No obstante, ambas legislaciones presentan vacíos importantes que dificultan una protección comprehensiva sobre el asunto. Por ejemplo, la carencia en el RGPD de sanciones penales en casos de violación graves a las normas sustantivas, o la falta de requerimientos sobre dicha

100 En el artículo 3.º del PIPA, Corea estableció principios básicos sobre la recolección y el tratamiento de información personal, similares a los establecidos en el RGPD, tales como transparencia, licitud del tratamiento, limitación de la finalidad del tratamiento, proporcionalidad, minimización de datos, limitación del plazo de conservación, entre otros.

101 En el artículo 4.º el PIPA establece como derechos fundamentales de los sujetos de datos el derecho de acceso a la información recolectada y procesada sobre sí mismo, el derecho a la rectificación de errores, así como el derecho a ser olvidado, derecho a la oposición al tratamiento de sus datos personales o a restringirlo, derecho al retiro del consentimiento previo, entre otros.

102 Se consideran datos de identificación particular el número de registro de residencia, el número de licencias de conducción, el número de pasaporte, así como los números de registro de extranjería, servicio militar y demás.

103 Según el artículo 16.2, "the personal information processor shall not deny the provision of goods or services to the data subjects on ground that they would not consent to the collection of personal information exceeding minimum requirement".

codificación en las regulaciones domésticas de los estados miembros. De igual modo, a pesar de estipulaciones expresas sobre el análisis de datos y la llamada "elaboración de perfiles", se observa la carencia de restricciones mayores sobre análisis de datos dirigidos a evaluar o predecir aspectos personales sobre el comportamiento o incluso el movimiento de la persona física, en atención a su naturaleza altamente intrusiva.

En el caso de la regulación surcoreana, también se observan lagunas legales similares. Por ejemplo, esta normatividad no contiene referencias expresas sobre la protección especial que requiere el procesamiento de datos a escala masiva, ni referencias sobre el desarrollo de perfiles o normas precisas sobre el tratamiento de datos personales para analizar o predecir la personalidad o el comportamiento del sujeto de datos.

En adición, en ninguna de las dos legislaciones se manifiestan preocupaciones particulares sobre riesgos respecto de derechos y libertades fundamentales originados en la diseminación e instalación masivas de dispositivos de internet de las cosas o *bundled goods*. Aspecto central respecto de la extracción a escala de datos comportamentales y el acceso de corporaciones privadas a dichos datos. Así mismo, no existen consideraciones ni normas particulares respecto de la implementación persistente y masiva de sistemas de inteligencia artificial, algoritmos o *machine learning*, relacionados con la extracción y digitalización de datos comportamentales.

Por el contrario, la exigencia de evaluaciones de impacto previas, a pesar de contribuir como medidas preventivas respecto de la identificación de efectos negativos sobre la privacidad y los derechos fundamentales que se originan con el uso de nuevas tecnologías, en ciertos casos dichas evaluaciones pueden no ser efectivas. Por ejemplo, respecto de tecnologías que por sus implicaciones a largo plazo deberían ser prohibidas legalmente, como es el caso de inteligencia computacional y algoritmos que escalan opiniones xenofóbicas o de grupos políticos radicalizados[104], al igual que algoritmos implementados en la adjudicación de justicia[105] o en estrategias de publicidad implementadas en procesos electorales.

Dichas preocupaciones reglamentarias, por tanto, requieren desarrollos posteriores e interpretaciones amplias sobre los principios, derechos e instrumentos codificados en ambas legislaciones, así como nuevas asociaciones substantivas entre regímenes jurídicos, necesarios para el desarrollo de marcos legales más comprehensivos en la reglamentación de los aspectos multidisciplinarios allegados con la implementación, sin precedentes, de sistemas de inteligencia computacional para el análisis de datos comportamentales.

104 Véase COVERT, D., "Radicalization and the Internet", monografía, 2018, University of Akron, disponible en [https://ideaexchange.uakron.edu/honors_research_projects/802/] [consultado el 13 de enero de 2020]; Daily Beast, "How YouTube Build a Radicalization Machine for the Far-Right", 12, 2018, disponible en [www.thedailybeast.com/how-youtube-pulled-these-men-down-a-vortex-of-far-right-hate] [consultado el 30 de enero de 2020].

105 Véase MARKOU, C., "*Ex machina lex*, the limits of legal computability" [en línea], Center for Business Research, University of Cambridge, Faculty of Law, 9, 2019, disponible en [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407856] [consultado el 10 de enero de 2020].

Finalmente, esta última sección contribuye a apreciar de una manera más precisa el asunto, en la medida en que ofrece un análisis sustantivo de los desarrollos legislativos de la UE y Corea del Sur, considerados los más comprensivos del mundo en el ámbito que atañe este documento. A partir del análisis de ambas normas y conforme al objetivo fijado por este documento, dicho análisis confirma que no obstante la existencia de avances significativos en la materia, incluso legislaciones más comprensivas como las arriba señaladas, aún carecen de elementos legales claros que develen el carácter jurídico esencial que relaciona los datos comportamentales, así como los riesgos que su análisis y procesamiento presentan sobre los derechos y libertades fundamentales del individuo.

Conclusión

Los mercados conductuales o *behavioral markets* han transformado los datos personales y comportamentales en un activo emergente, capitalizado y comercializado por las corporaciones de las tecnologías de la información, a través de estrategias que incrementan exponencialmente los resultados y ganancias de la explotación del ciclo económico de los datos personales. El asunto, por tanto, relaciona un fenómeno contemporáneo relativo a la monetización del comportamiento humano, a través de la diseminación de una arquitectura ubicua de inteligencia computacional que intensifica los medios de extracción de las experiencias del individuo, para digitalizarlos e incorporarlos al interior de estructuras que re-intervienen y manipulan las decisiones del individuo con fines económicos.

Este asunto es denominado e identificado en el presente estudio como la *asetización de la privacidad*, concepto que busca describir el incremento progresivo de presiones sobre valores legales de estatus constitucional, tales como la privacidad y las libertades fundamentales del ser humano. La expresión, además, busca referir conceptualmente la precariedad de los límites legales actuales sobre el modelo de extracción y monetización de datos personales, así como las deficiencias en el cumplimiento de obligaciones internacionales de los estados de adoptar marcos legales internos para regular prácticas que involucran riesgos significativos sobre el goce y libre ejercicio de los derechos humanos, las libertades del individuo y el imperio del Estado de derecho.

En un contexto global, el asunto relaciona la demanda creciente de nuevas y más precisas fuentes de extracción de datos comportamentales y la competencia asidua entre corporaciones globales por asegurar fuentes de extracción *in-house*. Este contexto involucra además la compleja disyuntiva que concierne al derecho contemporáneo respecto de la búsqueda de balance entre los intereses económicos de las corporaciones de las tecnologías de la información y el interés de la sociedad en la protección de valores sociales y jurídicos supremos, como la privacidad, la libre determinación y la democracia. Los datos comportamentales hacen parte integrante de la información que jurídicamente se considera personal, por su impacto esencial en la psiquis de la persona natural, su individualidad, así como su expresión colectiva.

A pesar del avance de algunas jurisdicciones en la adopción de marcos legislativos y estándares imperativos para la protección de datos personales y la privacidad, particularmente en la legislación de la Unión Europea y Corea del Sur, aún se identifican vacíos legales importantes en la mayor parte de jurisdicciones alrededor del mundo, por ejemplo, respecto de reglas y criterios precisos para determinar la legitimidad/ilegitimidad de la extracción de datos comportamentales que sobrepasan los requeridos para garantizar el funcionamiento de dispositivos inteligentes (de internet de las cosas) y tratamientos ulteriores de datos no previstos por la parte interesada.

Otros vacíos relacionan aspectos tales como: primero, control sobre la diseminación persistente de dispositivos de internet de las cosas o *bundled goods*. Segundo, la supervisión y el control sobre cláusulas contractuales entre proveedores de estos bienes y los usuarios de ellos. Tercero, la adopción incremental de inteligencia computacional para la extracción y el análisis de datos comportamentales, individuales, grupales y masivos o a escala. Cuarto, la protección de derechos no supeditada a la naturaleza nacional o extranjera de las fuentes de riesgo.

Finalmente, y como sugerencias, algunas consideraciones adicionales podrían resultar pertinentes:

Primero, los modelos económicos de "pago con datos personales" o "pagos con la privacidad" deben ser expresamente prohibidos por las regulaciones comerciales, o detalladamente regulados respecto del alcance y uso de dichos datos, por las compañías que proveen dichas transacciones económicas, así como las terceras partes involucradas, en consideración de las asimetrías de conocimiento e información, entre proveedores y usuarios, que imperan en el asunto.

Segundo, la inclusión de campañas publicitarias en el contenido de los juegos o dispositivos de realidad aumentada o *augmented reality* debe ser prohibida o estrictamente regulada por el derecho doméstico, dada su conexión con riesgos significativos de la influencia y manipulación sobre las decisiones de los usuarios. Así mismo, la protección de usuarios menores de edad es de especial relevancia en el asunto.

Tercero. Se deben establecer estrictas y variadas medidas de regulación respecto del clausulado de contratos sobre la adquisición, disposición, administración y mantenimiento de dispositivos de internet de las cosas, domésticos o personales, así como criterios legales sobre cláusulas abusivas que perpetúan la extracción y tercerización ilegítimas de datos a través de dichos dispositivos.

Cuarto, se requieren regulaciones domésticas precisas y estrictas para estandarizar límites sobre los llamados *targeted advertisement*. Dichas estrategias comerciales precisan una vigilancia y una regulación estrictas por los marcos de regulación internos y las autoridades domésticas, las cuales deben ser establecidas para dicho fin.

Quinto, la implementación masiva de sistemas de reconocimiento facial debe prohibirse por el derecho o estar estrictamente limitada, al igual que la tercerización de datos biométricos, en atención a su potencial impacto sobre la democracia y la libertad individual y colectiva.

Sexto, las normas domésticas deben asegurar el establecimiento de penas civiles y pecuniarias, así como privativas de la libertad en caso de serias violaciones a la normatividad sobre la protección de datos personales, derechos fundamentales o faltas en contra de la democracia, la paz o la estabilidad política interna, al igual que sobre violaciones que generen serios daños o riesgos en contra de la vida y la integridad física o mental de las personas naturales.

Referencias

Anderson, D., A *question of trust*, London, Crown Press, 2015.

Aaronson, S. & Leblond, P., "Another digital divide: the rise of data realm and its implications for the wto", *Journal of International Economic Law*, University of Oxford, n.º 21, 2018, 245.

Bond, R. *et al*., "A 61-million-person experiment in social influence and political mobilization", *Nature*, n.º 7415, 2012, 295-98;

Chander, A. & LeUyen, P., "Data Nationalism", *Emory Law Journal*, n.º 64, 2015, 677.

Cleverland, S., "Human Rights Sanctions and International Trade: A Theory of Compatibility", *Journal of International Economic Law,* University of Oxford, 2002, 133.

Constantiou, I. y Kallinikos, J., "New games, new rules: big data and the changing context of strategy", *Journal of Information Technology*, n.º 30, 2010, 44-57.

Covert, D., "Radicalization and the Internet" [en línea], monografía, 2018, University of Akron, disponible en [https://ideaexchange.uakron.edu/honors_research_projects/802/] [consultado el 13 de enero de 2020].

Fleuter, S., "The role of digital products under the wto: a new framework for gatt and gats classification", *Chicago Journal of International Law*, n.º 17, 2016, 153.

Gao, H., "Google's china problem. A case study on trade, technology and human rights under the gats", n.º 6 *Asian Journal of wto and International Health Law and Policy*, 2011, 349.

Gao, H., "Digital trade? The contrasting approaches of China and US to digital trade", n.º 21, *Journal of International Economic Law*, University of Oxford, 2018, 297.

GOLBECK, J. & ROBLES, C., "Predicting personality with social media", *IEEE Third International Conference on Social Computing*, 2011, 149-156.

HARRIS, R. & MOON, G., "GATT article xx and human rights: what do we know from the first 20 years", *Melbourne Journal of International Law*, n.º 16, 2015.

KELLY, K. *The inevitable*, New Your, Viking Press, 2016.

KENNETH, L. *et al*. (2016), *T-commerce*. *Business, Technology and Society*, 3.ª ed., United Kingdom, Pearson.

KENNEY, M. & ZYSMAN, J., "The rise of the platform economy*", Issues In Science and Technology*, 2016, 61.

LEAF, G. & PARK, W., "South Korea's Innovation in Data Privacy Principles. Asia Comparisons", *Computer Law and Security Review*, vol. 30, n.º 5, 2014, 492-505.

LESSIG, L., *Code and other laws in the cyberspace*, New York, Basic Books, 1999.

LESSIG, L., *Code version 2.0*, New York, Basic Books, 2006.

LYONS, E. *et al*., "Behavioral change techniques implemented in electronic lifestyle activity monitors: a systematic content analysis", *Journal of Medical Internet Research*, n.º 8, 2014.

MAJID, S., "Message factors that favorably drive consumers' attitudes and behavioral intentions toward social networking and media platforms", *University of Plymouth Journal*, 2019.

MARKOU, C., "*Ex machina lex*, the limits of legal computability", Center for Business Research, University of Cambridge, Faculty of Law, 9, 2019, disponible en [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3407856] [consultado el 10 de enero de 2020].

MATOO, A. & MELTZER, J., "International Data Flows and Privacy: The conflict and Its Resolution", *Journal of International Economic Law*, University of Oxford, 2018, 769.

MCDONALD, D. & STRERATFEILD, C., "Personal Data Privacy and the WTO", *Houston Journal of International Law*, n.º 35, 2014, 625.

McLachlan, C., *The Principle of Systemic Integration and Article 31(3)(c) of the Vienna Convention*, *International and Comparative Law Quarterly*, Cambridge University, 2008, 280.

Quercia, D., "Our twitter profiles, our selves; predicting personality with twitter", *ieee Third International Conference on Social Computing*, 2011, 180-85

Schultz & Ball, "Trade as a Weapon? The wto and Human Rights-Based Measures", *Deakin Law Review*, n.° 12, 2007, 42.

Schwab, K., *The fourth industrial revolution*, United States of America, Crown Business, 2017.

Sen, N., "Understanding the Role of the wto in International Data Flows: Taking the Liberalization of the Regulatory Autonomy Path?", *Journal of International Economic Law*, University of Oxford, n.º 21, 2018, 332.

Tapscott, D. *et al*., *Blockchain revolution*, New York, Portfolio Penguin, 2016.

Tauscher, C., "Understanding Platform Business Models: A mixed Methods Study of Marketplaces", n.º 36, Elsevier, 2018.

Van der Marel, E., "Disentangling the flows of data: Inside or outside the multinational company?", *Ecipe Occasional Papers*, n.º 7, 2015.

Williams, J., *Stand out of light, freedom and resistance in the attention economy*, United Kingdom, Cambridge University Press, 2018.

Wu, T., (2017), *The attention merchants. The epic scramble to get inside our heads*, New York, Vintage Books.

Wunsch, V., *The wto, the internet and trade in digital products, ec-us perspectives*, United States, Oxford University Press, 2006.

Yoon, J., "South Korea data localization shaped by conflict", 2, 2018, The Henry M. Jackson School of International Studies, disponible en [https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/] [consultado el 15 de septiembre de 2019].

Zuboff, S., (2019), *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, London, Profile Books.

A. Otras publicaciones

BSA, THE SOFTWARE ALLIANCE, "Lockout, how a new way of protectionism is spreading through the world's faster growing it markets- and what to do about it".

BSA, THE SOFTWARE ALLIANCE, "Powering the global digital economy. A trade agenda to drive growth".

Google, "Enabling trade in the era of information technologies. Breaking down barriers to the free flow of information", 2015.

HELBING, D. *et al*., "Will democracy survive big data and artificial intelligence?" [en línea], *Scientific American*, 2, 2017, disponible en [www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/] [consultado el 9 de enero de 2020].

IAPP, "GDPR matchup: South Korea's personal information protection act", disponible en [https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/] [consultado el 13 de octubre de 2020].

INTERNATIONAL MONETARY FUND (2018), "Money, transformed. The future of currency in a digital world", *Finance and Development*, 2018.

INTERNATIONAL MONETARY FUND, "Measuring the Digital Economy", 2018.

OECD, "Measuring digital trade: towards a conceptual framework", 2017.

SILVER, D., "Alibaba is developing self-driving cars", 4, 2018, *Medium*, disponible en [https://medium.com/self-driving-cars/alibaba-is-developing-self-driving-cars-e8a5c88f2cc7] [consultado el 20 de enero de 2020].

THALES, "South Korea's PIPA compliance", disponible en [www.thalesesecurity.com/solutions/compliance/apac/south-koreas-pipa] [consultado octubre 13 de 2019].

WORLD BANK GROUP, "Data driven development. Information and communication for development" [en línea], 2018, disponible en [www.worldbank.org/en/topic/digitaldevelopment/publication/data-driven-development] [consultado el 20 octubre de 2019].

WORLD ECONOMIC FORUM, "Personal data: the emergence of a new asset class", 2011.

WORLD TRADE ORGANIZATION, *World Trade Statistical Review 2018, 2019*.

B. Fuentes de prensa

BBC News, *Cambridge Analytica: the Data Firm's Global Influence*, 3, 2018, disponible en [www.bbc.com/news/world-43476762] [consultado el 3 de septiembre de 2019].

CBC News, "Data is the new oil: your personal information is now the world's most valuable commodity", 8, 2017, disponible en [www.cbc.ca/news/technology/data-is-the-new-oil-1.4259677] [consultado el 10 de octubre de 2019].

CNBC, "Facebook working on smart glasses with Ray-Ban code name Orion", disponible en [www.cnbc.com/2019/09/17/facebook-enlists-ray-ban-maker-luxottica-to-make-orion-ar-glasses.html] [consultado el 15 de enero de 2020].

Daily Beast, "How YouTube Build a Radicalization Machine for the Far-Right", 12, 2018, disponible en [www.thedailybeast.com/how-youtube-pulled-these-men-down-a-vortex-of-far-right-hate] [consultado el 30 de enero de 2020].

Forbes, "Barbie wants to chat with your child, but it is big data listening in?", 12, 2015, en [www.forbes.com/sites/bernardmarr/2015/12/17/barbie-wants-to-chat-with-your-child-but-is-big-data-listening-in/#725508292978] [consultado el 15 de enero de 2020].

Forbes, "Key milestones of waymo Google's self'driving car", 11, 2018, disponible en [www.forbes.com/sites/bernardmarr/2018/09/21/key-milestones-of-waymo-googles-self-driving-cars/#46cb350d5369] [consultado el 13 de enero de 2020].

International Data Corporation, "IDC forecasts revenues for big data and business analytics solutions will reach 189.1 billion this year with a double-digit annual growth through 2022", 4, 2017, disponible en [www.idc.com/getdoc.jsp?containerId=prUS44998419] [consultado el 10 de octubre de 2019].

Privacy, "Here's what the big tech companies know about you", 11, 2018, disponible en [www.visualcapitalist.com/heres-what-the-big-tech-companies-know-about-you/] [consultado el 13 de abril de 2018].

Quartz, "Mapped: the breathtaking global reach of Cambridge Analytica's parent company", 3, 2018, disponible en [https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/] [consultado el 3 de septiembre del 2019].

The Economist, "The world's most valuable resource is no longer oil, but data. The data economy demands a new approach to antitrust rules", 5, 2017, disponible en [www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data] [consultado el 7 de octubre de 2019].

The Guardian, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach", 3, 2018, disponible en [www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election] [consultado el 2 de octubre de 2019].

The Guardian, "The Great British Brexit Robbery: How Our Democracy was Hijacked", 5, 2017, disponible en [www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy] [consultado el 10 de octubre de 2019].

The New York Times, "Google to store and analyze millions of health records" 11, 2019, disponible en [www.nytimes.com/2019/11/11/business/google-ascension-health-data.html] [consultado el 5 de enero de 2020].

The New York Times, "Barbie wants to get to know your child", disponible en [www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html] [consultado el 15 de enero de 2020].

The Yorker, "We know how you feel. Computers are learning to read emotions and the business world can't wait", 1, 2015, disponible en [www.newyorker.com/magazine/2015/01/19/know-feel] [consultado el 20 de enero de 2020].

C. Documentos oficiales

G20's "Leaders declaration building consensus for fair and sustainable development".

General Assembly Resolution 68/167, "The right to privacy in the digital age", A/Res/68/167 (December 18, 2013).

HUMAN RIGHTS COUNCIL, "Report of the special reporteur on the right to privacy", 03, 2018, A/HRC/37/62, 6.

Organization of American States, Inter-American Juridical Committee, "Privacy and data protection", 86th Regular Session, 3, 2015, 23-27, CJI/doc. 474/15 rev.2.

UN HUMAN RIGHTS COUNCIL, "Report of the special rapporteur on the right of privacy", HRC/40/63 (February 2019).

United Nations Conference on Trade and Development (unctad), "Data protection regulation and international data flows: implications for trade and development", 2016.

United Nations, Human rights Council, The right to Privacy in the digital Age. Report of the Office of the united Nations Hight Commissioner for Human Rights, a/hrc/27/37 (June 2014).

D. Tratados y declaraciones multilaterales

apec, Privacy Protection Guidance.

apec, Marco de privacidad.

Asociación Transatlántica sobre Comercio e Inversión (ttip), Tratado entre la Unión Europea y Estados Unidos.

Comprehensive and Progressive Agreement on Transpacific Partnership (cptpp).

Convención sobre la seguridad cibernética y la protección de los datos personales de la Unión Africana

ocde Guía sobre la privacidad.

Tratado de Libre Comercio Estados Unidos, México y Canadá (usmca).

Tratado de Libre Comercio Corea del Sur y Estados Unidos (korus).

Tratado integral y progresivo de la asociación transpacífico (cptpp).

E. Legislación

Diario Oficial de la Unión Europea (actos legislativos), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 (Reglamento General de Protección de Datos).

South Korea, Act on the promotion of information and communication networks utilization and information protection, Amended by Act n.º 13520, Dec. 1, 2015.

South Korea, Act on the protection, use, etc, of location information, Act n.º 14224, May 29, 2016.

South Korea, Guidelines for de-identification of personal data, guide for de-identification standards and support/management system, June 30, 2016.

South Korea, Use and protection of credit information act, Act n.º 11845, May 28, 2013.

F. Datos estadísticos

SPEED TEST GLOBAL INDEX, "Global Speeds December 2019", 12, 2019, disponible en [www.speedtest.net/global-index] [consultado el 25 de enero de 2020].

Statista, "Countries with the highest internet penetration rate as January 2019", 2, 2019, disponible en [www.statista.com/statistics/227082/countries-with-the-highest-internet-penetration-rate/] [consultado el 25 de enero de 2020].

Statista, "Facebook annual revenue from 2009 to 2019", 2, 2020, disponible en [www.statista.com/statistics/268604/annual-revenue-of-facebook/] [consultado el 3 de febrero de 2020].

Statista, "Internet of things - Number of connected devices worldwide 2015-2025", 12, 2019, disponible en [www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/] [consultado el 20 de octubre de 2019].

Statista, "Internet of Things - Number of connected devices worldwide 2015-2025", 11, 2019, disponible en [www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/] [consultado el 20 de octubre de 2019].

Statista, "Market capitalization of the biggest internet companies worldwide as June 2019", 9, 2019, disponible en [www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/].

Statista, "The 100 largest companies in the world by market value in 2019", 8, 2019, disponible en [www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/] [consultado el 25 de enero de 2020].

Statista, "The big business of big data", 5, 2019, disponible en [www.statista.com/chart/18328/big-data-business-analytics-revenue/] [consultado el 10 de octubre de 2019].

Statista, "The most profitable companies in the world", 11, 2019, disponible en [www.statista.com/chart/17545/worlds-most-profitable-companies] [consultado el 25 de enero de 2020).

G. Videos en línea

Jesus College Cambridge University, "Intellectual Forum 'Is Tech Making Us Miserable?'", March 11, 2019, disponible en [www.youtube.com/watch?time_continue=13&v=1TXej5YMbvg].

VPro Documental, "Are self-driving cars the future?", 10, 2019 [minutos 33:08 a 34:01], disponible en [www.youtube.com/watch?v=5gyxjwersu8] [consultado el 12 de enero de 2020].

VPro Documentary, Zuboff on Survaliance Capitalism, 12, 2019 [minutos 19:24 a 19:48], disponible en [www.youtube.com/watch?v=hIXhnWUmMvw] [consultado el 20 de enero de 2020].