cet.la
Centro de Estudios de Telecomunicaciones de América Latina

ACCESO, USO Y PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

'diseños metodológicos y teóricos'

Amanda Espiñeira Lemos

Serie Working Papers cet.la Nº 2019/07
Centro de Estudios de Telecomunicaciones de América Latina

www.cet.la | @latam_digital
Rambla de Rep. de México 6125 Montevideo (Uruguay) CP 11400 +598 26 04 22 22 / 5401 contacto@tel.lat

Serie Working Papers cet.la

Nº 2019/07

Acceso, uso y protección de datos personales en América Latina:

'diseños metodológicos y teóricos'

Amanda Espiñeira Lemos[1]

Acceso, uso y protección de datos personales en América Latina: diseños metodológicos y teóricos es un *working paper* publicado por el Centro de Estudios de Telecomunicaciones de América Latina en julio de 2019, en el marco de su Programa Junior Fellowships para jóvenes investigadores.

Incluye referencias bibliográficas.

[1] Amanda Espiñeira es estudiante de maestría en derecho de la Universidad de Brasilia (UNB), becaria CAPES. Abogada. Licenciada en Derecho por la Universidad Federal de Bahía (UFBA) y miembro de Grupos de investigación del Observatorio de Políticas Públicas (GEOPP), y del Grupo de Estudio de Derecho de las Telecomunicaciones (GETEL). Participó como becaria de iniciación científica financiada con recursos del CNPq, y como monitora de las disciplinas de Sociología Jurídica en la UFBA y Derecho Constitucional en la UNB. Trabaja en investigación principalmente en los siguientes temas: Derecho constitucional, Regulación de internet, Políticas Públicas, Derecho a la Comunicación y Propiedad Intelectual. Realizó esta Investigación en el marco del Programa Junior fellowship cet.la 2019 con el acompañamiento de Andrés Sastre Portela.

Las opiniones publicadas en este documento son responsabilidad exclusiva del autor, y no corresponden necesariamente con la posición oficial de ASIET, del cet.la, o de las empresas y universidades asociadas a estos organismos.

Resumen

El uso de datos si torna cada vez más importante por el desarrollo de una economía global cada vez más digitalizada. La monetización de eses datos hace que su protección sea necesaria para los usuarios de la red. Ante las transacciones transfronterizas si piensa modelos regulatorios para resolución de conflictos. El objetivo principal del artículo es señalar los asuntos derivados del tratamiento de datos personales en la economía digital, cuáles son los problemas que se han generado y proponer posibles soluciones, partiendo de los contornos institucionales de la gestión de datos en el ecosistema digital, con las leyes y autoridades de protección de datos en América Latina. Desde el punto de vista metodológico se hace una investigación cualitativa con revisión bibliográfica. Además, se hace un levantamiento preliminar de las realidades de protección de datos de los países de América Latina. Se propone la implantación de un Mercado Digital Latino Americano y para eso la creación de una Carta de Derechos sobre el tema para la región.

Keywords: protección de datos personales; modelos regulatorios; América Latina; economía de datos.

1. Introducción

Internet ha servido para favorecer y perfeccionar los sistemas de interacción social, teniendo un gran impacto en la esfera económica, dada cuenta del vasto flujo de datos a escala global que ha transformado significativamente la velocidad de las transacciones financieras y en consecuencia la acumulación de capital.

Además, ha posibilitado la creación de nuevos modelos de negocio basados precisamente en el uso de dichos datos. A pesar de que la preocupación por la protección de los datos personales no es un tema reciente, sólo después de que aconteciesen una serie de episodios de fuerte impacto a nivel mundial, se empezó a generar un cierto consenso sobre la importancia de dicha protección (Veronese & Cunha, 2017).

Lo que cambió después de estos hechos fue el paradigma de la protección, con la adopción de un modelo de *risk base approach*, centrado no sólo en establecer medidas preventivas y punitivas después de la violación de derechos, sino también en la preocupación de incorporar principios y mecanismos de *accountability*, entendidos como el seguimiento y el control por parte de la sociedad en relación con la cuestión de la gobernanza de Internet.

La preocupación por el tratamiento de datos personales por parte del poder público también emerge tras el episodio que involucró a Edward Snowden y la divulgación de datos de la NSA - *National Security Agency*, la Agencia de Seguridad Nacional de los Estados Unidos de América. Este caso, de 2013, reveló la existencia de programas de vigilancia utilizados para monitorear globalmente a la población.

Más recientemente, en 2015-2016, el escándalo de *Cambridge Analytica* reforzó la relevancia de acelerar el proceso regulatorio, demostrando cómo la desprotección de datos personales impacta no sólo la vida de un ciudadano, sino de toda una colectividad y lo que se entiende por sistema democrático (Silveira & Froufe, 2018, P. 14).

A pesar de la forma en que la protección de la privacidad se implementa depende de las diferentes jurisdicciones y actores sociales que influyen en ese proceso, como el mercado y otros reguladores, "la necesidad de buscar un mínimo contenido común para el derecho a la privacidad es más que un ejercicio puramente académico, es una necesidad real ante el incremento en el flujo de información en los últimos años " (Doneda, 2006, P. 85-86). La necesidad de realizar este *paper* se debe sobre todo a que el potencial de recolección, procesamiento y utilización de datos personales ha crecido considerablemente con el avance de las tecnologías de la información repercutiendo en los modelos regulatorios de protección de los datos personales en el proceso económico y en las relaciones comerciales contemporáneos.

En este sentido, en un escenario en que cerca de 122 países tienen legislación sobre el tema (Banisar, 2019), la regulación se torna cada vez más incuestionable ante las pérdidas económicas y de inversión para el país generadas por la ausencia de leyes de Protección de Datos. Siendo un requisito imprescindible además para convertirse en un país miembro de la OCDE - Organización para la Cooperación y el Desarrollo Económico.

Varios países de América Latina poseen legislaciones nacionales sobre protección de datos personales y tienen autoridades que aseguran esa protección. En Brasil, por ejemplo, se sancionó recientemente la Ley General de Protección de Datos (LGPD) el 14 de agosto de 2018, con entrada en vigor prevista para febrero de 2020, 18 meses después de la sanción. La aprobación de la Ley, sin embargo, contó con algunos vetos, entre ellos las disposiciones enfocadas a crear la Autoridad Nacional de Protección de Datos (ANPD), que llevó la edición de la Medida Provisoria n. 869, de 2018, aprobada en el Congreso Nacional brasileño con una Autoridad vinculada a la Presidencia de la Republica.

La preocupación y la discusión sobre el tema en el resto de los países latinoamericanos ha hecho que varios países hayan adoptado legislaciones y creado autoridades de protección de datos. Seis países de América Latina[2] tienen ya autoridad de protección de datos y en ellos se centra parte del foco de la investigación. Chile no tiene su Autoridad todavía, está en desarrollo, junto a un proyecto de nueva ley de protección de datos en discusión, pero por tener una ley de protección de privacidad desde 1999 si incluye en la investigación. El Salvador y otros países también están desarrollando la implementación de la Ley como Brasil.

De esta forma, las preguntas que guían la investigación son: ¿Cuál es la situación legal de los siete países analizados en materia de protección de datos (los seis con Autoridad y Chile)? ¿Cuáles son los temas principales tratados en los modelos regulatorios de protección de datos en los países de América Latina? ¿Cómo los datos influyen en la economía digital en el contexto regional latinoamericano? Otras cuestiones se refieren a las prácticas culturales y su relación con las acciones de protección de datos: ¿Existe una cultura de protección de datos personales en América Latina? ¿Qué buenas propuestas regulatorias hay en la región?

El objetivo principal del artículo es señalar los asuntos derivados del tratamiento de datos personales en la economía digital, cuáles son los problemas que se han generado y proponer posibles soluciones, partiendo de los contornos institucionales de la gestión de datos en el ecosistema digital, con las leyes y autoridades de protección de datos en América Latina.

La investigación comprende la relación existente entre las culturas locales en lo que se refiere a la regulación de la protección de datos personales y de información. Este objetivo deriva de una duda acerca de las diferencias sociales que pueden existir en los diversos países cuando tratamos conceptos tan generales como privacidad, datos personales y vida privada.

Desde el punto de vista metodológico se hace una investigación cualitativa con revisión bibliográfica. Además, se hace un levantamiento preliminar de las realidades de protección de datos de los países de América Latina.

Esta metodología busca abarcar una "red conceptual de atributos jurídicos, cuya realidad depende de indicadores de orden normativo (base legal), de orden concreto (implantación de la legislación), de orden institucional (papel de los actores involucrados) y de orden prospectivo (tendencia hacia el futuro)" (Aranha, 2011, p. 17). En este sentido, la preocupación por la dificultad de desmembramiento de los institutos jurídicos en sus efectos prácticos y su necesaria contextualización nacional, es decir,

[2] México, Argentina, Uruguay, Perú, Colombia y Panamá

la preocupación por el "trasplante de prácticas reguladoras nacionales para cuerpos políticos dotados de modelos socioeconómicos, políticos y jurídicos distintos" (Aranha, 2011, p.4).

Este trabajo se divide en tres partes. La primera tiene como título “Derechos de privacidad y papel de las autoridades de datos personales en América Latina”, donde se hace un breve mapeo de propuestas regulatorias actuales. En esta parte se apuntan los principales ejes de discusión: el manejo de información personal; las políticas de consentimiento y el flujo transfronterizo de datos. La segunda parte trata las bases de gestión de datos en el ecosistema digital. Dividiéndose en tres subpartes: (a) el uso y manejo de los datos en la economía; (b) la responsabilidad de intermediarios, frente a delitos de odio en la red y en casos de *fake news* en procesos electorales; (c) la neutralidad de plataformas con el uso comercial de algoritmos y los problemas de competencia que de ello se deriva, tratando propiamente de la competencia con el acceso a los datos y los sistemas operativos. En el tercero tópico tenemos propuestas de regulación, hacia una armonización regional y la creación de reguladores independientes. Después en las conclusiones y recomendaciones tenemos también apuntes para una Carta de Derechos en la red, basada en modelos que existen desde IGF y desde el sector privado.

2. Derechos de privacidad y papel de las autoridades de datos personales en A. Latina.

A partir del contexto regulatorio brevemente descrito, así como las cuestiones y los objetivos que orientan la presente investigación, se elige trabajar con conceptos clave, los cuales orientan la visión sobre la privacidad, datos personales, territorialidad, la implementación de los marcos regulatorios en la región América Latina sobre protección de los datos personales, así como los desafíos que se plantean para la creación y actuación de una Autoridad de Protección de Datos.

Stefano Rodotà (2008) trae la idea de funcionalidad de la privacidad, al considerar que no es, hoy, una pura expresión de una necesidad individual, pero su colocación debe estar inserta en el marco de la nueva "ciudadanía electrónica" y conceptúa el derecho de la privacidad como “el derecho de mantener el control sobre las propias informaciones” (Rodotá, 2008, p.92). Cada vez más las personas son conocidas como sujetos públicos por medio de los datos que nos conciernen.

No obstante, al depender de factores subjetivos tales como el tiempo y el lugar, la privacidad no debe ser considerada como un derecho subjetivo. Una de las razones para ello es la dificultad para poder encuadrar la privacidad en una concepción coherente y unitaria (Doneda, 2006). Antes, debe ser vista como una situación subjetiva compleja, cuya tutela depende del sopesamiento de situaciones concretas de su aplicabilidad (Solove, 2008).

Comprender cómo las normas técnicas, políticas, económicas y sociales son articuladas es fundamental para entender quiénes son los principales actores de ese proceso de transformación y cómo interactúan (Brouseeau, Marzouki, Méadel, 2012). Las autoridades nacionales de protección de datos (APD), actores centrales en asegurar dicha protección, enfrentan una tarea difícil para cumplir su misión y actuando como responsables de esos derechos. Se entiende la actuación de las APD como instrumentos adecuados para permitir el desarrollo de las diferentes vertientes de economía basada en datos, tales como el comercio electrónico, al mismo tiempo que se garantiza la protección de los datos personales de los usuarios de Internet y se hace frente al problema de la responsabilidad de los intermediarios técnicos con el fin de

destacar la especificidad del enfoque europeo que se construye en torno a un objetivo fundamental que es el equilibrio entre una lógica de mercado y las preocupaciones de los ciudadanos. (Blandin, 2001).

2.1 Breve mapeamiento y propuestas regulatorias actuales

La actualidad y relevancia del tema cuenta también con la entrada en vigor del Reglamento 679/2016, conocido como Reglamento General sobre Protección de Datos en la Unión Europea (RGPD) el 25 de mayo de 2018, aprobado en abril de 2016 por el Consejo Europeo, no sólo en los Estados miembros de la Unión Europea directamente, sino globales sobre la protección, el tratamiento y la comercialización de los datos personales, así como la reestructuración de modelos antes regulados por la Directiva 95/46 / CE.

Se destaca que el Tribunal de Justicia de la Unión Europea a partir del caso Lindqvist ya presentaba el debate sobre el uso de datos personales en Internet antes de que el debate del RGPD se iniciara en 2012. Todo este escenario se encuentra en dirección a la conformación del denominado del Mercado Único Digital en la UE. El RGPD por ser un Reglamento, es directamente aplicable a todos los estados miembros de la UE, vincula a cualquier organización que ofrezca bienes o servicios que recopilen datos personales relacionados con la UE, a diferencia de la antigua Directiva.

Roger Kelemen (2011) presenta la perspectiva de que la estructura institucional fragmentada de la UE y la prioridad dada a la integración del mercado generaron incentivos políticos y presiones funcionales que llevaron a los formuladores de políticas de la UE a promulgar normas detalladas, transparentes y judicialmente aplicables.

A pesar de poseer principios e instrumentos similares a los de la Directiva 95/46, el RGPD presenta un cambio de paradigma en lo que se refiere a la obligación y responsabilidad de las organizaciones involucradas. Las principales innovaciones del RGPD son el Principio de la Responsabilidad Proactiva, que impone al responsable del tratamiento de datos la adopción de medidas técnicas adecuadas y pone el foco en el riesgo, según el cual las medidas a ser adoptadas deben ser proporcionales al riesgo que eventuales infracciones representan a los derechos y libertades fundamentales. El RGPD establece medidas sancionadoras y también un deber de diligencia y de buena gestión para los entes responsables del tratamiento de datos personales

El derecho europeo a la protección de datos personales se basa en tres pilares principales: las obligaciones por parte de aquellos que manejan datos privados, los derechos de los usuarios y el papel de las autoridades de protección de datos (APD). Las APD pueden considerarse como uno de los tres pilares de la protección de datos demuestra su importancia en la UE. Así, los poderes de las APD se definen sólo de manera general. Estas competencias se agrupan en categorías básicas como: poderes de investigación, poderes de intervención, poderes para involucrarse en procesos judiciales y escuchar reclamaciones.

Además, una APD debe ser preceptivamente consultada por los legisladores nacionales cuando elaboran reglamentos o medidas administrativas relacionadas con la protección de datos. Además, ante la importancia de la circulación transnacional de datos y de la relevancia económica de ese intercambio comercial que expande jurisdicciones y, por lo tanto, de la generación de conflictos transfronterizos a

resolverse, las APD se sitúan como esenciales en la solución de estos casos, precisamente por la cooperación internacional existente demostrada (Giurgiu, Larsen, 2016).

La adopción del Reglamento General sobre protección de datos no tiene la intención de frenar la innovación, sino precisamente generar confianza en los usuarios sobre el tratamiento que dan aquellas empresas que tomen sus datos.

En el marco de América Latina, Brasil asumió un papel destacado en relación a la regulación de Internet con la aprobación del Marco Civil de Internet (Ley nº 12.965/2014) y posteriormente con la publicación del Decreto Regulatorio nº 8.771/2016. El protagonismo brasileño en la aprobación del Marco Civil de Internet y el proceso participativo de construcción de esa ley impulsaron el debate entre las diversas partes afectadas por la regulación de la red en el país.

Paulatinamente, se fue estableciendo una tendencia a la regulación de Internet en Brasil, encabezada inicialmente por diversos proyectos de ley propuestos con el propósito de reglamentar la red de forma punitiva. Así, en 1999, se propuso el PL nº 84/99 conocido como Proyecto de Ley Azeredo, para tipificar conductas realizadas mediante uso de sistemas electrónicos, digitales o similares. La propuesta fue duramente rebatida por sectores de la sociedad y culminó en la elaboración de otro proyecto, el PLC nº 21/2014, que generó el MCI, que fue aprobado tras intensos debates en el Congreso Nacional, a partir de una construcción participativa, estableciendo principios, garantías, derechos y deberes para el uso de Internet en Brasil (Radomsky y Solagna, 2016). En 2016, también tras una consulta pública a la sociedad, se estableció su Decreto Regulador.

Desde entonces, varios proyectos de ley han sido presentados sobre diversos temas relacionados con Internet, entre ellos la protección de datos personales, teniendo la privacidad en la red como fondo central, con la Ley General de Protección de Datos (LGPD) el 14 de agosto de 2018, en período de vacancia. La aprobación de la Ley se hizo sin la Autoridad Nacional de Protección de Datos (ANPD), que compone la edición de la Medida Provisoria n. 869, de 2018, aprobada en el Congreso brasileño en mayo de 2019 con una Autoridad vinculada a la Presidencia de la Republica, no independiente como determina las directrices de OCDE, pero con la promesa de rever ese modelo en dos años y crear una autoridad autónoma.

La protección de datos personales también retoma la protección de la dignidad de la persona en que los derechos de privacidad son derechos fundamentales, tomando como referencia el artículo 12 de la Declaración Universal de los Derechos Humanos. La superación del derecho a la privacidad como una tutela de índole sólo patrimonial, frente a ese escenario en que es encarado como un derecho fundamental, y el establecimiento de nuevos mecanismos e institutos para posibilitar la efectiva tutela de los intereses de la persona, es decir, la protección de la privacidad hizo, por lo tanto, que de ella derivase una disciplina de protección de datos personales.

Argentina sancionó en 2000 la Ley n. 25.326 (Argentina, 2000), que trata en su artículo 29 del órgano administrativo de control de los datos. El contenido de la ley se basó bastante en la Ley francesa n. 78-17, de 6 de enero de 1978 (Francia, 1978). Esa ley surgió como respuesta a la recomendación hecha por el entonces Consejo para la Consolidación de la Democracia, que señalaba la conveniencia de

consagrar el derecho a la libertad, principalmente con el objetivo de evitar que la democracia fuera afectada por los avances de la tecnología de la información y de registro de datos.

En Argentina se está debatiendo nuevos proyectos de protección de datos y responsabilidad de intermediarios. Este proyecto de ley de responsabilidad de intermediarios se debatió por última vez en noviembre 2018. En la actualidad se encuentra en suspenso puesto que ha recibido muchas críticas por la responsabilidad irrestricta que otorgaba a las grandes plataformas y a reclamos sobre protección de derechos de autor que algunos sectores entienden se estarían vulnerando.

Uruguay aprobó en 2008 la Ley n. 18331, de11 ago. 2008, en el artículo 32 existe la previsión de un Consejo Consultivo (Uruguay, 2008).

México, por su parte, tiene una Ley Federal de Protección de Datos Personales en Poder de Particulares, vigente desde el 6 de julio de 2010 (México, 2010) y su reglamento, en vigor desde el 22 de diciembre de 2011. La Autoridad es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Existen otros países latinoamericanos que han desarrollado legislaciones específicas: Chile que posee la Ley 19.628/1999 y está usando los reglamentos europeos además de la RGPD como modelos para la creación de la Agencia de Protección de Datos Personales; Perú con la Ley n. 29.733, de 2011 y la Autoridad Competente (Peru, 2011); y Colombia, Ley n. 1581/2012, Ley General de Protección de Datos Personales y el Decreto n. 1.377/2013, además de la Delegación para la Protección de Datos Personales (Colombia, 2018). Panamá tiene una Autoridad Nacional de Panamá de Transparencia y Acceso a la Información y está aprobando una ley específica.

El mapeo regulatorio mundial de 2018 demuestra el crecimiento del número de países que pasaron a adoptar una legislación sobre protección de datos personales si se compara con el mismo mapeo en 2016 (Banisar, 2016, Banisar, 2018). Y si comparado a 2014 se nota que hasta 2016 ese crecimiento no fue tan expresivo.

Figura 1. Protección integral de datos nacional / leyes de privacidad y proyectos de ley (BANISAR, 2014).

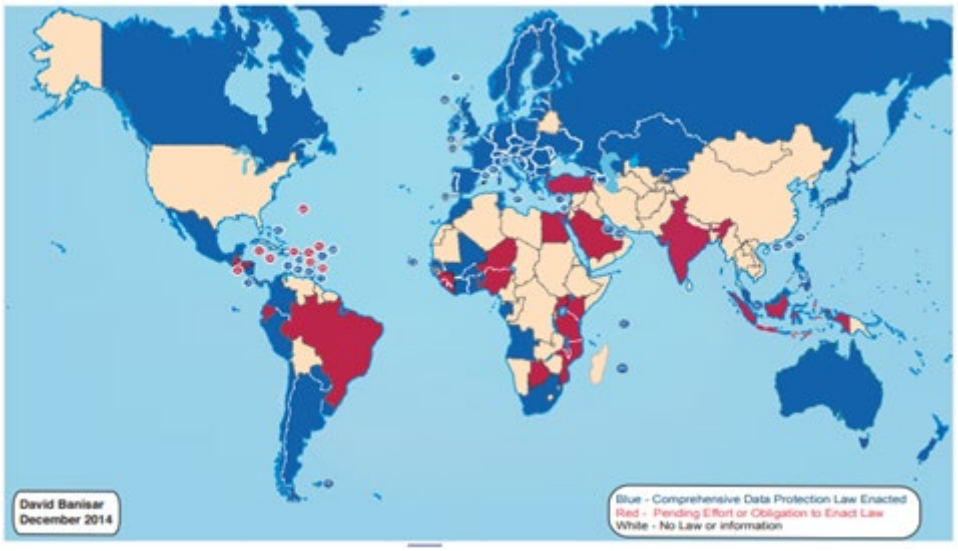


Figura 2. Protección integral de datos nacional / leyes de privacidad y proyectos de ley (BANISAR, 2016)

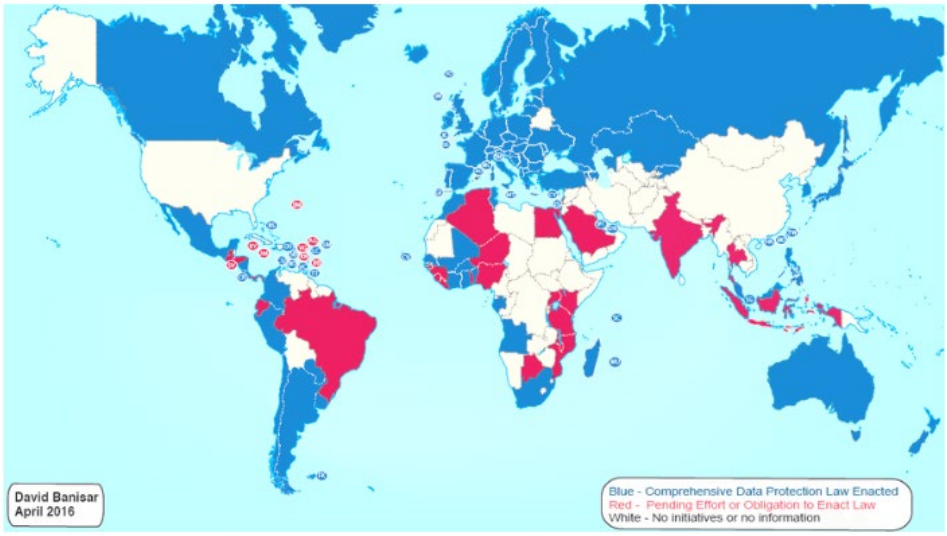
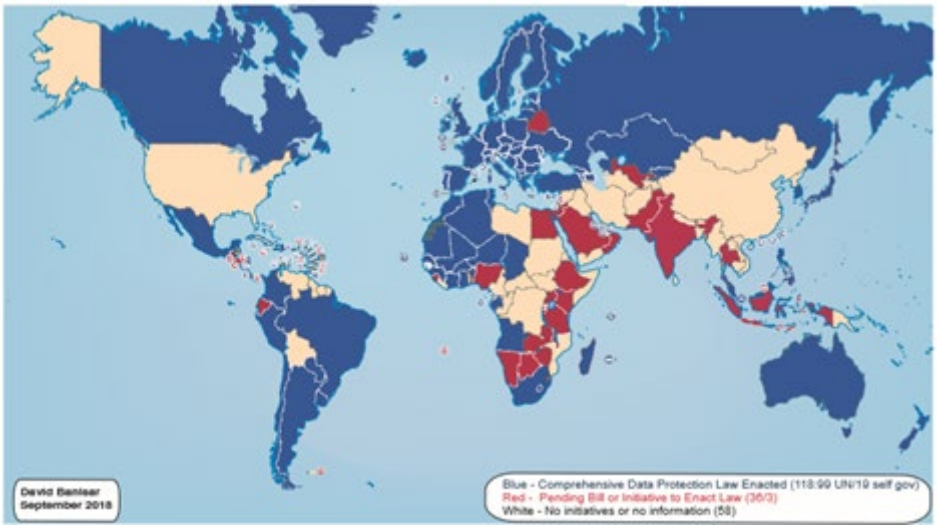
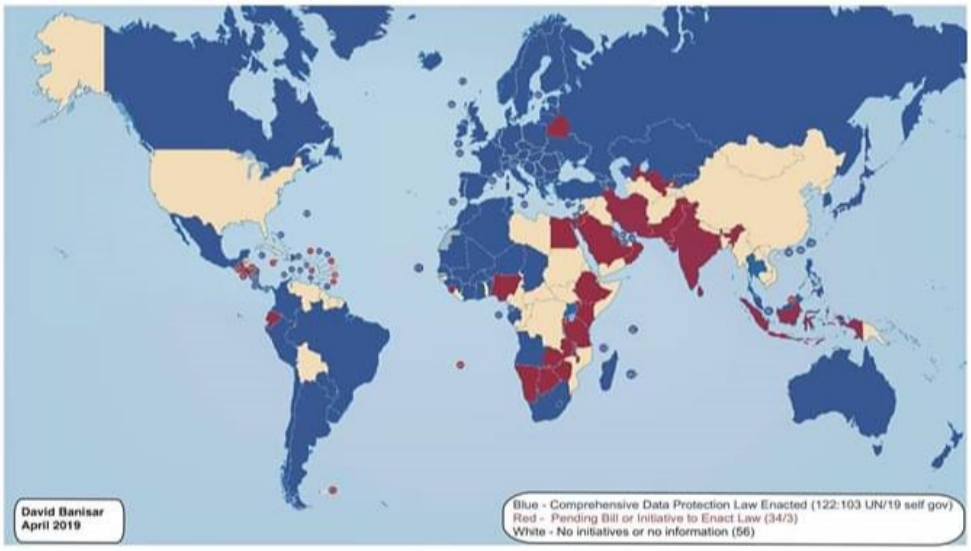


Figura 3. Protección integral de datos nacional / leyes de privacidad y proyectos de ley (BANISAR, 2018)



En 2018, gran parte de los países de América Latina ya tenían una legislación aprobada (muchas veces en período de adecuación antes de la aplicación están con leyes en proceso de aprobación), otros se encontraban con iniciativas de proyectos de ley y solo algunos pocos no se ocupan del asunto como Bolivia (quien ha presentado un proyecto de ley en Julio de 2019), Venezuela, Guyana, Suriname y Cuba.

Figura 4. Protección integral de datos nacional / leyes de privacidad y proyectos de ley (BANISAR, 2019)



En el próximo capítulo se tratan los tres principales aspectos de discusión cuando se habla de protección de datos personales.

2.2. Principales ejes de discusión: manejo de información personal, políticas de consentimiento y flujo transfronterizo de datos

Cuando se habla de protección de datos personales, hay que tener en cuenta en primer lugar que vivimos en una sociedad hiperconectada en que los datos son uno de los principales bienes para el desarrollo de una economía global cada vez más digitalizada. Para que los modelos de negocio basados en datos funcionen, se tiene que hacer manejo de la información personal de los usuarios de los servicios ofrecidos por la red. En una segunda etapa estos datos se les dan un uso comercial a través de un flujo entre organismos, empresas, instituciones, donde en muchas ocasiones resulta transfronterizo porque involucra no sólo el territorio en que el dato fue generado, o tratado, migrando a otro territorio y pasando a ser por tanto un flujo internacional. En este sentido, gran parte de las regulaciones que se han desarrollado abordan un capítulo con disposiciones sobre transferencia internacional de datos.

A pesar de la conciencia de que lo cotidiano y la personalidad de las personas se construye a partir de los datos en la era digital,

> sin embargo, muchas veces, pasa desapercibido por los usuarios, que no se dan cuenta del rastro digital que producen sobre sí mismos. Los datos producidos, no raramente, se almacenan durante un largo período de tiempo. El control de este rastro se ha convertido en un problema tecnológico y social, ya que de su análisis es posible obtener informaciones sobre el comportamiento, las preferencias y necesidades personales de una determinada persona e incluso prever sus acciones futuras (Magrani, Oliveira, 2019, p.338; Sjöberg, 2016).

Esto se refleja en el consentimiento y sus políticas, la mayoría de las veces expresadas en términos y condiciones previas a la contratación de un servicio, que ni siquiera son leídos por quien hace uso del mismo. La discusión sobre la validez del consentimiento como se inicia con la preocupación del tratamiento que se da a los datos no sólo por el Poder Público, sino también por los agentes privados que lucran con ese bien. (Bioni, 2019).

La protección individual de los propios datos se interpreta en muchas regulaciones como autodeterminación informacional, y la autonomía de la voluntad de los individuos con su "consentimiento informado, libre, expreso, específico o inequívoco" construye modelos regulatorios en los que el consentimiento es el elemento central de una regulación de la privacidad de los datos personales (Montelene, Le Métayer, 2009, Schartz, 1999).

Bioni (2019), sin embargo, cree ser una visión limitada y una "comprensión reduccionista del contenido de lo que se debe referir autodeterminación informacional" (p.137) y para ello es necesario reevaluar esa estrategia regulatoria, ampliando la idea de consentimiento. Esta limitación se debe a que el flujo de datos es bastante volátil y su minoración pasa por diversos actores. Así, para que pudiera gestionar su información personal el usuario, debería tener conciencia acerca del trayecto de ese flujo.

El flujo transfronterizo de datos, o sea el movimiento de datos personales a través de fronteras nacionales, es esencial para el comercio en el mundo electrónico. A pesar de que su uso es cada vez más común para el desarrollo comercial, crece también la necesidad de cooperación en cuestiones procesales y de investigación.

Así, lo más importante y el desafío para regulaciones transfronterizas es comprender como manejar ese flujo sin afrontar derechos y garantías protegidos en un determinado país y no regulado en otro, o mismo con leyes que tratan de protecciones de maneras distintas. Sobre todo, porque uno de los obstáculos para garantizar ese flujo es exactamente la regulación que se hace de la protección de datos, de esta forma por ejemplo para tener autorización de la OCDE para ejercer relaciones comerciales que impliquen el uso transfronterizo de datos, los países involucrados deben contar con una protección equiparable.

3. Bases del manejo de datos en el ecosistema digital

Los Intermediarios (proveedores de contenido) necesitan saber cada vez más de sus clientes, para mejorar su modelo de negocio y que este tenga mejores resultados. Este mayor conocimiento se obtiene a través del análisis exploratorio de los datos a los que tienen acceso, ya sean provenientes de sus clientes, proveedores, competidores, pero este análisis de datos puede y normalmente invade la privacidad de los involucrados.

3.1 Ejes de la economía de datos: uso y manejo comercial de algoritmos

En la economía de datos, hay relaciones plurilaterales, en que un servicio es ofrecido al usuario de forma que no tiene que aportar una cantidad pecuniaria por él, como los modelos tradicionales de negocio, en una relación binaria (consumidor y proveedor). El acceso "gratuito" se deriva de la cesión de los datos personales de esos usuarios, consumidores, a cambio del uso del servicio, donde el proveedor se beneficia con una publicidad dirigida conductual (Bioni, 2019, página 25). El concepto

"*zero-price advertisement business model*" utilizado por Katherine Strandburg (2013, p.86) define ese tipo de modelo de negocio.

Este modelo de negocio que se hace a partir de la información personal y actividades del individuo se basa en la minería de datos, que consiste en extraer conocimiento a partir de un dato bruto, en la inteligencia de búsqueda y en el aprendizaje de la máquina y el uso de Inteligencia Artificial.

Los datos son alimentados por los usuarios con su información personal, gustos, preferencias, acciones. Para tratar un dato considerado "bruto" se utiliza *matching* y *targeting*, o sea, los *data brokers* tratan los datos (*data analytics)*, cruzando las informaciones y haciendo direccionamiento de la publicidad. (Bioni, 2019, p. 31).

También existe el Quality of Service (QoS), que consiste en priorizar algunas clases de "datos", en que una transmisión de datos recibe preferencia de entrega en relación a otras transmisiones (Caruana, 2002). Es un elemento necesario para el Protocolo IP, sin embargo, muchas veces es utilizado como argumento del proveedor para hacer la inspección de paquetes, violando la privacidad.

> Es útil para la gestión de la red, manteniendo una Calidad de servicio (QoS) con optimización de contenido (que trata diferentes tipos de tráfico de acuerdo con proporcionar QoS requerida), distribución de aplicaciones y balanceo de carga; También contribuye a la red, seguridad y análisis forense, detectando y eliminando paquetes potencialmente dañinos que intentan entrar o salir de la red. Otras aplicaciones de DPI incluyen visibilidad de la red, perfiles de usuarios, políticas de derechos de autor. La censura o regulación del contenido. La inspección profunda de paquetes no es solo una herramienta poderosa para la detección de anomalías de red, pero también puede usarse en la gestión de ancho de banda, publicidad y filtrado de contenido de derechos de autor. Sin embargo, se puede usar con propósitos incorrectos, como interferir dentro de la neutralidad de la red o permitir vigilancia gubernamental e invasión de la privacidad. (Rodrigues *et.al*., 2017, p.3)

Los grandes *players* de Internet, son los que poseen el monopolio del comercio electrónico con el modelo de negocio basado en los datos. En ese sentido hay dos otros aspectos relevantes a debatir cuando se habla del manejo de datos: la responsabilidad de los proveedores, la competencia y poder que ellos tienen de decisión de los procesos y contenidos en la red.

3.2 Responsabilidad de intermediarios: frente a delitos de odio en la red y en casos de fake news en procesos electorales

Las plataformas no deberían ser responsabilizadas por todo lo que es compartido por sus usuarios. Sin embargo, ¿cómo deben actuar frente a situaciones de violación de derechos? ¿Debe tener alguna responsabilidad? ¿Y cuánto involucra delitos de odio en la red? ¿Y en casos de *fake news* en procesos electorales? ¿Debería requerirse la necesidad de una decisión judicial previa para la retirada de contenidos o el filtro debe ser automático? ¿Esa responsabilidad debe ser objetiva a lo subjetivo? ¿Se extiende la esfera penal o se restringe al ámbito civil? ¿La responsabilización inhibe la innovación y la explotación de ese modelo de negocio (que analizan los contenidos para su publicidad)? ¿Sería una barrera económica para los intermediarios?

Las plataformas están rentabilizando las *fake news*, los delitos de odio desde el sentido de que al generarles tráfico y actividad están lucrándose económicamente, entonces por eso hay que plantearse también si tienen una responsabilidad sobre lo que sucede. Además, por la escasa competencia que hay se hace más importante si cabe juzgar esa responsabilidad.

La responsabilidad de los intermediarios tiene que ver con la libertad de expresión de los usuarios y acceso a información, aliado a las consecuencias de los discursos utilizados en Internet (Mackinnon et.al, 2014). La mayor preocupación se refiere a las remociones de contenido abusivo y indebido (*overblocking)*. Sin embargo, cuando se trata de contenido racista, antisemita, homófobo, misógino, discriminatorio de cualquier naturaleza (los chamados "*hate speechs*") o mismo de pornografía infantil hay que discutir los límites de la libertad de expresión y ser capaces de legislar de forma responsable.

El estudio de la UNESCO concluye que hay algunas categorías comunes cuando si habla de responsabilidad de usuarios: "Necesidad y proporcionalidad en la restricción de contenido; La naturaleza transnacional de Internet pone límites particulares al espacio operativo para los intermediarios; La variedad de actores involucrados crea incertidumbre sobre el contenido permitido" (Mackinnon et.al, 2014, p.183). Existen incluso cuestiones de género, que cuando se presenta violencia esas plataformas podrían ser mecanismos de denuncia de acoso sexual y explotación.

En Brasil el artículo 18 del Marco Civil de Internet atribuye como regla la ausencia de responsabilización por los proveedores de conexión (ISPs). Y a los proveedores de aplicación en el 19 atribuye una responsabilidad subjetiva y posibilita que la retirada de contenido de la red preceda autorización judicial. En los párrafos siguientes hay excepciones como derechos autorales y conexos.

Se utiliza el modelo de notificación y retirada, utilizado mayoritariamente, como en los EE.UU. en los casos de violación de derechos de autor (Digital Millennium Copyright Act), en Canadá y en la Unión Europea (Directiva de Comercio Electrónico) contraposición al modelo que determina que el intermediario actúe proactivamente en la remoción de contenido, como en el caso de Venezuela[3].

En Argentina hay un Proyecto de Ley, publicado en 20 de octubre de 2016 por la orden del día n.824 del Congreso para regular la responsabilidad de los Proveedores de Servicios de Internet, a efectos de garantizar la libertad de expresión y el derecho a la información, sin dejar de preservar los derechos al honor, a la intimidad y a la imagen, con el mismo modelo de *notice and takedown*. Solo hay responsabilidad de los proveedores mediante orden judicial.

Ese modelo parece ser más razonable por garantizar la libertad de expresión y evitar bloqueo y remoción indebida de contenido. Por un lado, en muchas ocasiones es fundamental una remoción ágil, pero si esta no se hace bien puede convertirse en un arma contra la libertad de expresión. La responsabilidad pasa a ser del Judiciario donde hay un proceso de contradictorio y defensa.

La cooperación entre Gobierno y las empresas puede ser apuntada como una manera de solución de conflictos. Macron en su discurso en IGF 2018[4] presento un ejemplo de este tipo de cooperación para ser aplicado por Francia junto a Facebook. "Facebook acogerá una delegación de reguladores

[3] http://dissenso.org/intermediarios-de-internet-e-liberdade-de-expressao-o-mapa-da-busca-de-um-delicado-equilibrio-regulatorio/
[4] https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron

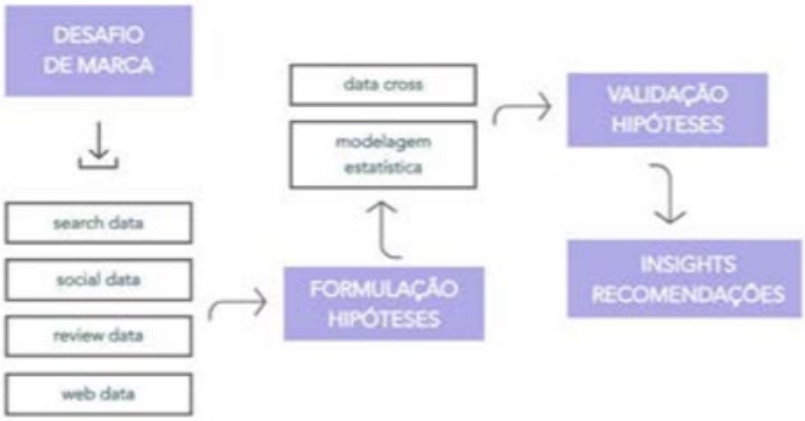
franceses, con los expertos de la plataforma, para desarrollar propuestas conjuntas, precisas y concretas sobre la lucha contra el odio o el contenido ofensivo".

La responsabilidad de intermediarios también se presenta en momentos electorales. El debate pasa por el microdireccionamiento de gustos y tendencias que generan manipulaciones como estrategia de captar electores en las elecciones. Los datos de los ciudadanos recolectados muchas veces legalmente en las redes sociales, retoma el caso de la *Cambridge Analytica* en las elecciones de México y de Estados Unidos que eligieron Trump. Se tiene aún el caso de las elecciones brasileñas y el papel de las redes. La discusión también atravesó el uso de *fake news* con el envío de mensajes masivos por WhatsApp (SANTOS, et.al, 2018). Propuestas de leyes que pueden cercenar la libertad de expresión han sido realizadass, trayendo nuevos desafíos regulatorios que se presentan junto a ese escenario.

La colección para trazar estrategias eficaces y captar al ciudadano no es solo en las redes sociales, sino si cruzan los datos con bases públicas, como de investigación de estadística de la población, los organismos del consumidor, lo que permite el *targeting* de los datos. La psicometría es la nueva técnica utilizada para realización de marketing político, que utiliza de una evaluación psicológica de los datos para identificar los deseos y comportamiento de los electores, publico-objetivo de la propaganda política, a fin de promover mejoras en sus perfiles (Santos, et.al, 2018, p.57).

El proceso de "*consuming insight*", es decir, de uso de todos los datos generados por el consumidor para dar lugar a una dirección e *insights* de marketing, realizado por las empresas y utilizado por partidos electorales, involucran el enriquecimiento de la base de datos y el modelaje de los datos, como se muestra en la Figura 5 a continuación. (Santos, et.al, 2018, p.59).

Figura 5. Ilustración del "*consuming insight*" (SANTOS, et.al, 2018, p.60).



El análisis de esos anuncios y propagandas permite verificar el alcance y mejorar el servicio se retroalimentando. Ese proceso tiene que ver con el uso y manejo de algoritmos del tópico 2.1 pero no solo para fines comerciales, sino aliñando ese compartir de datos con o proceso decisorio democrático de las elecciones y la perpetuación de valores de una sociedad con elementos de ciudadanía. Ese asunto lleva a cuestionamientos sobre el poder y las competencias que las grandes empresas manipuladoras de datos tienen, aspecto a ser abordado no próximo tópico.

3.3. Competencia: acceso a los datos y sistemas operativos

Tenemos que reflejar cómo aquel que tiene el acceso a los datos y sobre todo si es de manera de cuasi monopolio tiene un poder de decisión y de mercado muy elevado. Ellos deciden cómo y en qué condiciones se da acceso a esos datos eligiendo en muchas ocasiones ganadores y perdedores. Siendo, por tanto, uno de los problemas de competencia es la elección de ganadores y las brechas invisibles de entrada al mercado.

La falta de regulación en la red implica que unas pequeñas empresas (casi todas norteamericanas) tengan un oligopolio donde la innovación o los nuevos entrantes en muchos casos o bien son eliminados o por el contrario se les compra la iniciativa. La cuestión de la falta de competencia en el ecosistema que afecta también a la libertad de expresión y la concentración en manos privadas de la decisión sobre lo que se publica o se promociona. La autorregulación en exclusiva desde el sector privado permite que esas empresas creen los algoritmos y decidan los contenidos vehiculados, el uso de los datos y la venta para intereses puramente económicos, sin preocupaciones con los datos de los usuarios.

El intercambio de datos entre distintas jurisdicciones, ya que gran parte de las empresas son extranjeras y se encuentran deslocalizadas en un país en concreto, presenta la disyuntiva de cómo proteger los datos en países con legislaciones, derechos y regulaciones distintas- Por poner un ejemplo reciente de manejo y compartición de datos en diferentes jurisdicciones dentro de una misma empresa podemos mencionar a las compañías de pedido de comida a domicilio, que crecen bastante en toda América Latina como *IFood, Rappi, Ubereats, Glovo*, las mismas si bien tienen sede en un país latinoamericano concreto operan en varios, teniendo que importar los datos de sus clientes de otros países. Por un lado, si esto no fuera permitido el negocio no sería viable, pero debemos asegurarnos por el otro lado, la protección y seguridad de datos tan personales de clientes que migran de una legislación a otra. Hay que permitir ese flujo, pero debemos asegurar que se protegen los datos personales con la armonización regional y entidades supranacionales de protección.

Un Mercado Único Latinoamericano como el Mercado Europeo sería una buena salida posterior a la armonización de legislaciones, que sería un paso previo para eso. Todavía, para la implementación de la propuesta sería necesaria una adaptación al contexto de América Latina, frente a cuestiones de disparidades socioeconómica de los países, grandes diferencias culturales y dimensiones geográficas no tan equivalentes, cuando se habla de Brasil, por ejemplo. Un paso antes de hacer esa unificación tiene que ver con el fortalecimiento de las legislaciones internas de las Autoridades de Protección de Datos dentro de patrones internacionales como los de la OCDE para el comercio internacional.

4. Propuestas de regulación

El estudio sobre la regulación de Internet surgió como el esfuerzo requerido y los retos que los avances tecnológicos propuestos, especialmente teniendo en cuenta la pluralidad de intereses relacionados con Internet y el carácter innovador de este medio (Dutton, 2013). Es importante comprender que las regulaciones son más estrictas para los medios y servicios tradicionales y más flojos para los nuevos servicios surgidos de Internet. Esto plantea la cuestión de cómo regular estos nuevos servicios para poner orden, centrándose en el marco del análisis jurídico de las innovaciones, no sólo en el derecho positivo (Blandin, 2013). Se destaca la importancia del diálogo de varias áreas del conocimiento para comprender de forma eficiente los temas de la Regulación de Internet, en especial de los datos personales y de la privacidad. Los objetivos de la regulación del contenido pueden ayudar a redefinir algunos aspectos de la regulación de la red (Blandin, 2006).

Del mismo modo que no existe un consenso sobre una sola teoría de la regulación de Internet, cada país puede adoptar una visión de Internet, y un modelo para la comprensión de su regulación dependerá en buena parte de esta el desarrollo de Internet en cada país (Kurbalija; Gelbstein, 2005).

La idea de entender la modulación legal discutido en este trabajo es importante, no la coerción y el punto de vista estricto de la ley, sino porque se crea un entorno favorable para el desarrollo de la ciencia y la tecnología, teniendo en cuenta la armonización de la protección de datos personales derechos fundamentales de la libertad de expresión y el derecho a la información. Estos son los aspectos científicos que se enfrentan en la construcción del modelo de regulación de América Latina en el campo y entender los otros entornos institucionales políticos, legales y tecnológicos detrás pueden ayudar a superarlos. “Los diferentes instrumentos de regulación son producto de estos procesos de gobernanza que pueden ser más o menos participativos. El objetivo de la regulación es mantener en equilibrio y garantizar el correcto funcionamiento de sistemas complejos” (Belli, 2019, p.48)

Hoy, hay dos modelos existentes de ver la Internet, como bien puntualiza Macron en su discurso de apertura en el Foro de Gobernanza de Internet 2018, ocurrido en París: "hay una forma de Internet de California, y hay un Internet chino". Esos dos modelos poseen concepciones regulatorias distintas, el primero se centra en la autorregulación y en juego de intereses privados de los grandes jugadores y empresas globales dominantes. Está inserta en un contexto de democracia y en teoría hay la posibilidad de control de los datos personales por parte de sus usuarios, cuya práctica y profundidad de esa autodeterminación de los datos pueden ser debatidas. Entretanto, según Macron, precisamente este modelo tampoco es democrático, precisamente por la ausencia de controles a la voluntad de las empresas privadas, los ataques a la democracia y la ausencia de regulación estatal

Frente al modelo californiano, el modelo chino, donde el Estado posee un papel fuerte de vigilancia y de filtro de contenidos, con el desarrollo de elementos técnicos no orientados a la seguridad del usuario, sino para perfeccionar ese control estatal. El propio gobierno dibuja innovaciones y propone regulaciones que legitiman esas prácticas de control.

La autorregulación como modelo regulatorio encuentra el obstáculo de la concentración de poder en corporaciones internacionales, de plataformas y aplicaciones, lo que dificulta el debate plural y diverso de ideas y una Internet abierta.

Las regulaciones autoritarias tampoco parecen ser una buena solución por la violación de principios y derechos esenciales a la comunicación, la libertad de expresión y el uso de Internet en su total potencialidad.

> es importante destacar que las diferentes herramientas de regulación de Internet pueden ser de origen pública, como las convenciones internacionales, las leyes, los reglamentos y las decisiones tomadas para los tribunales y las agencias nacionales, sino que pueden tener también naturaleza privada. En este último caso, la regulación privada puede ser de tipo contractual, como los términos y condiciones que definen las reglas de utilización de plataformas web, aplicaciones móviles y redes de acceso Internet, o pueden ser de tipo técnico, como los algoritmos, los estándares y los protocolos que definen la arquitectura de software y hardware que determinan lo que los usuarios pueden o no pueden hacer en el ambiente digital (Belli, 2019, p.49)

Lo que se llama "*smart regulation*" es hoy visto como una de las alternativas más viable, y como una tercera vía a esos dos modelos polarizados que concentran poder en el Estado o en las grandes empresas. Se trata de un modelo basado en el multistakeholderismo, con la preservación de los derechos de los usuarios, el mantenimiento de una internet democrática y el respeto a convenciones internacionales de derechos. Así, se busca que la regulación no sea un obstáculo a la innovación, que sea un incentivo al desarrollo de *start-ups* y empresas locales, respetando la privacidad y los derechos de los ciudadanos.

En este escenario, otro elemento importante en lo que se refiere a América Latina, por ser una región históricamente marcada por desigualdades diversas, es que el modelo regulatorio busque el fortalecimiento de iniciativas de concientización y educación tecnológica, a fin de ampliar la inclusión digital y la calidad de acceso de los ciudadanos. Así se presenta en los dos tópicos siguientes propuestas de Regulación cooperativa hacia una armonización regional y por medio de un regulador independiente.

4.1 Hacia una armonización regional

Debemos hacer referencia a la necesidad de una armonización regulatoria a nivel regional que permita que la red siga siendo abierta y competitiva. También debemos reflexionar sobre la necesidad de eliminar las asimetrías impositivas entre aquellos que componen el ecosistema digital.

En eso sentido, comenzamos a ver ejemplos como el de Francia de cobrar impuestos a los GAFA (Google, Amazon, Facebook, Apple) desde la óptica de que mejor avanzar hacia un acuerdo global y no que cada país apueste por su propia regulación y actividad impositiva. El Mercado Único Latinoamericano se inserta como una propuesta dentro de ese equilibrio entre los países de la región.

Aquí se apunta la iniciativa de OCDE[5] de reformas al sistema tributario internacional para frenar la elusión fiscal por parte de empresas multinacionales, o sea la erosión de la base imponible y el traslado de beneficios (BEPS). Ese fenómeno ocurre por la existencia de lagunas o mecanismos no deseados

[5] https://www.oecd.org/newsroom/la-ocde-presenta-los-resultados-del-proyecto-beps-de-la-ocde-y-el-g20-para-su-discusion-en-la-reunion-de-los-ministros-de-finanzas-del-g20.htm

entre los distintos sistemas impositivos nacionales de los que pueden servirse las empresas multinacionales, con el fin de hacer "desaparecer" beneficios a efectos fiscales. Esas medidas de OCDE sirven para mejorar la coherencia de los estándares impositivos internacionales, reforzar su focalización en la sustancia económica y garantizar un entorno fiscal de mayor transparencia.

4.2 Hacia un regulador independiente

Otra propuesta regulatoria seria la creación de un regulador independiente en Latino América, como una Autoridad de Protección de Datos, pero más general para todos los sujetos de Internet. Ese regulador inicialmente debería ser país por país, compuesto por un modelo multisectorial. Después se haría un centralizado, regional, que se compondría de esos agentes de los reguladores de todos los países y conocería las particularidades de la región uniformizando las directrices y leyes, trayendo más transparencia a los procesos decisorios y regulatorios. Si propone aún un modelo multisectorial de actores desde sociedad civil, empresas, gobierno y órganos de investigación.

Como la propuesta del Parlamento Británico (Inglaterra, 2019), el regulador independiente tendría estatutaria para supervisar las empresas de tecnología; esto creará un regulador de sistema para contenidos online que es eficaz para las industrias offline también. Así debe tener la capacidad para iniciar procesos judiciales contra ellos, con el propósito de aplicar penas cuando del incumplimiento de las leyes y directrices, o sea debe tener el poder de *enforcement* para cumplir sus recomendaciones.

5. Conclusiones

Los temas principales para tratar en modelos regulatorios de protección de datos en los países de América Latina parten del manejo de información personal, y flujo transfronterizo de datos. O sea, de la importancia que los datos tienen en la economía contemporánea, digital. Así tratar de políticas de consentimiento y responsabilidad de intermediarios, en casos de discurso de odio y uso de datos para elecciones es demasiado importante cuando se piensa en la regulación del tema en Latinoamérica.

La cultura de protección de datos personales en América Latina está creciendo y cada vez más si debate el tema, no solo con regulaciones nacionales como un debate regional entre países, ya que los datos son interconectados y el beneficio que genera el compartirlos. Importante apuntar que por más que existan *standarts* regulatorios regionales generales, la incorporación por cada uno de los países se adapta a su contexto institucional y local.

Como propuestas regulatorias se ha avanzado lo que se ha denominado llamar "*smart regulation*", un modelo basado en el multistakeholderismo. Dentro de esa propuesta podemos tener dos modelos de autoridad responsable: hacia una armonización regional /mundial y hacia un regulador independiente. La primera refuerza la regulación local con una interconexión entre los órganos de los países de América Latina. La segunda propone algo como un órgano supranacional que partiría de cada país, haciendo propuestas de normas integradas. Además, se propone la implantación de un Mercado Digital Latino Americano, para eso sería imprescindible la creación de una carta de derechos, que en los próximos apuntes si diseña alguna idea.

La Carta de Derechos de Internet, una propuesta desarrollada en el marco de las iniciativas de las Naciones Unidas sobre la sociedad de la información y que ha sido consolidada a través del trabajo de diversos grupos, "*dynamic coalizations*" que han encontrado formas de unificación y métodos comunes, que se manifestaron en los Foros de Gobernanza de Internet promovidos en estos últimos años por la propia ONU. (Rodota, 2015, p.2)

"El refuerzo institucional de la libertad en su nueva dimensión no puede valer sólo contra la intromisión de los Estados. Debe proyectarse también sobre los nuevos "Señores de la Información" que, a través de las gigantescas colectas de datos, gobiernan nuestras vidas. "(Rodota, 2015, p.1)

Además de la Carta de Derechos, lanzada en el IGF 2010 en Vilnius, Lituania, hay también diez Principios Poderosos ("Ten Punchy Principles"), con valores orientadores para la Carta lanzados en 2011 por la Coalición Dinámica para Derechos y Principios de Internet. Todos esos documentos están en: http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_booklet_brazilian-portuguese_final_v2.pdf

En ese mismo sentido hay también un Manifiesto de Telefónica que habla de Principios “por un nuevo pacto digital” (https://www.telefonica.com/manifesto-digital/), los retos de ese Manifiesto son: “Conectar las vidas digitales”; “Reformar las políticas sociales e fiscales para as sociedades digitales”; “Generar confianza nos datos”; “Incentivar plataformas más equitativas y algoritmos responsables”; y “Modernizar los derechos y las políticas”. Esos capítulos presentan buenos apuntes para la regulación de Internet propuesta en este *paper*.

Así apunta-se la necesidad de construir una Carta de Derechos para uso de datos personales en América Latina, teniendo en cuenta la salvaguardia de la seguridad de los usuarios, con la protección contra riesgos de divulgación sin consentimiento, en consecuencia, la limitación de uso con especificación de propósito de uso de los datos. La transparencia y acceso a los algoritmos de procesamiento, a lo ruta que el dato pasa, las informaciones de quién controla, son otros dos derechos principiologicos a seren asegurados en esa carta.

Referencias

Argentina. **Protección de los datos personales, Ley 25.326**, 30 out. 2000. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm. Acceso em: 14 out. 2018.

Argentina. **Protección de Datos Personales. In: Investigaciones** 1, p. 121. Secretaria de Investigación de Derecho Comparado. Corte Suprema de Justicia de La Nación. República Argentina, 1998.

Aranha, Márcio Iorio. Diálogo político-jurídico na comparação de modelos regulatórios de comunicação. **Revista Brasileira de Políticas de Comunicação**, v.1, p. 1-20, 2011.

Associacion por Derechos Civiles; Intervozes; Observacom Pronunciamiento Latinoamericano de la Sociedad Civil. **Una perspectiva latinoamericana para construir una regulación democrática que limite el poder de las grandes plataformas y garantice la libertad de expresión en internet**.

Banisar, D. **National Comprehensive Data Protection/Privacy Laws and Bills 2014**. Article 19: Global Campaign for Free Expression. 2014. Disponible en: https://www.researchgate.net/publication/256011932_National_Comprehensive_Data_ProtectionPrivacy_Laws_and_Bills_2014_Map

_____. **National Comprehensive Data Protection/Privacy Laws and Bills 2016**. Article 19: Global Campaign for Free Expression. 2016. Disponible en: https://www.researchgate.net/figure/National-Comprehensive-Data-Protection-Privacy-Laws-and-Bills-2016-Banisar-2016_fig1_311495321

_____. **National Comprehensive Data Protection/Privacy Laws and Bills 2018**. Article 19: Global Campaign for Free Expression. 2018. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

Banisar, D. **National Comprehensive Data Protection/Privacy Laws and Bills 2019**. Article 19: Global Campaign for Free Expression. 2019.

Belli, Luca. Gobernanza y regulaciones de Internet: una presentación crítica. In.: Belli, Luca; Cavalli, Olga (Org.). **Governanza y Regulaciones de Internet en América Latina: análisis sobre infraestructura, privacidad, ciberseguridad y evoluciones tecnológicas em honor de los diez años de la *South School on Internet Governance***. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2019.

Bioni, Bruno R. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

Blandin, Annie. Du droit des telecommunications au droit des communications electroniques: quel changement de module? **Ann. Télécommun**., 61, n ° 7-8, 2006.

_____. La télévision sans frontières avec Internet:interactions et ordres juridiques. **La Revue des Sciences de Gestion**. Direction et Gestion. n 263-264, 2013/5, p. 117-123.

_____. **L'Union Europeenne Et Internet**. Publications Du Cedre. Apogee, 2001.

Brouseeau; Eric (ed.); Marzouki, Meryem (ed.); MÉADEL, Cécile (ed.). **Governance, regulations, and powers on the Internet**. Cambridge: Cambridge University Press, 2012.

Colômbia. **Delegatura para Protección de Datos Personales**. Disponible en: http://www.sic.gov.co/delegatura-para-la-proteccion-de-datos-personales. Acceso em: 1 nov. 2018.

Doneda, Danilo. **Da privacidade à proteção de datos pessoais**. Rio de Janeiro: Renovar, 2006.

Dutton, William H. (ed.). **The Oxford handbook of Internet Studies**. Oxford: Oxford University Press, 2013.

Francia. **Loi nº 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 jan. 1978.** Disponible en: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460. Acceso em: 14 out. 2018.

Giurgiu, Andra; LARSEN, Tine A. Roles and Powers of National Data Protection Authorities. 2 Eur. **Data Prot. L. Rev**. p.342-352, 2016.

Inglaterra. **Disinformation and 'fake news': Final Report**. Eighth Report of Session 2017–19. House of Commons. The Digital, Culture, Media and Sport Committee, 2019.

Kelemen, Roger Daniel. **Eurolegalism**: The Transformation of Law and Regulation in the European Union. Harvard University Press, 2011.

Kurbalija, J.; Gelbstein, E. **Governança da Internet** – questões, atores e cisões. Tradução Renato Aguiar. DiploFoundation/RITS. Rio de Janeiro, 2005.

Mackinnon, Rebeca; Hickok, Elonnai; BAR, Allon, LIM, Hae-in. **Fostering Freedom Online: the role of internet intermediaries**. UNESCO, Internet Society, 2014.

Magrani, Eduardo.; Oliveira, Renan Medeiros. Big Data somos nosotros: nuevas tecnologías y gerenciamiento personal de datos. In.: Belli, Luca; Cavalli, Olga (Org.). **Governanza y Regulaciones de Internet en América Latina: análisis sobre infraestructura, privacidad, ciberseguridad y evoluciones tecnológicas em honor de los diez años de la *South School on Internet Governance***. Rio de Janeiro: Escola de Direito da Fundação Getúlio Vargas, 2019.

México. **Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 5 jul. 2010.** Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010. Acceso em: 1 nov. 2018.

Milanes, Valeria *et.al*.. **El sistema de protección de datos personales em América Latina:** Oportunidades y desafíos para los derechos humanos. Volumen I Asociación por los Derechos Civiles, Diciembre 2016.

Monteleone, Shara; Le Métayer, Daniel. Automated consent through privacy agents: Legal Requirements and technical architecture. **Computer Law & Sexurity Review**. 25, 2009.

Peru. **Ley de Protección de datos personales, 3 jul. 2011**. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf. Acceso en: 1 nov. 2018.

Radomsky, G; Solagna, F. Marco Civil da Internet: abrindo a caixa-preta da agenda de uma política pública. **Liinc em Revista**, Rio de Janeiro, v.12, n.1, p. 57-71, maio 2016. Disponible en: http://dx.doi.org/10.18617/liinc.v12i1.867. Acceso en: 20 abr. 2019.

Rodotà, Stéfano. **A vida na sociedade da vigilância** – A privacidade hoje. Rio de Janeiro; São Paulo: Renovar, 2008.

_____. Por que é necessária uma Carta de Direitos da Internet?. Trad. Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**. Rio de Janeiro, a. 4, n. 2, jul.-dez./2015.

Disponível em: http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/

Rodrigues, G.A.P. Albuquerque, R. de O.; Gomes F.E.; Timóteo, R.; Junior, G.A.O.; Villalba, L.J.G; KIM, T.H. Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection. **Appl. Sci.** 2017, 7, 1082; doi:10.3390/.

Santos, Bruna; Varon, Joana. **Data and Elections in Brazil 2018 a research by Coding Rights for Tactical Technology Collective**, Published as Country Report of the Project 'personal data and political influence', available at "our data, our selves". Rio de Janeiro, October, 2018.

Schartwz, Paul M. Privacy and democracy in cyberspace. **Vanderbilt Law Review**, v.52, p.1658, 1999.

Silveira, Alessandra; Froufe, Pedro. Do mercado interno à cidadania de direitos: a proteção de datos pessoais como a questão jusfundamental identitária dos nossos tempos. **UNIO - EU Law Journal**. Vol. 4, No. 2, jul. 2018, p 4-20.

Sjöberg, M. et al. Digital Me: Controlling and Making Sense of My Digital. Footprint. In: GAMBERINI, L. et al (Eds.). **Symbiotic Interaction: Lecture notes in computer science**, 2016, pp. 155-156. Padua, Italy: Springer.

Strandburg, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. **University of Chicago Legal Forum**: Vol. 2013, Article 5, 2013. Disponible en: https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/5

Tanús, Gustavo Daniel. **El artículo 24 de la Ley 25.326 de proteccion de los datos personales**. Jornadas Argentinas de Informática e Investigación Operativa (JAIIO) organizadas por la Sociedad de Informática Operativa (SADIO). Buenos Aires, 2001.

Torrez, Jeannette, *et.al*. **Políticas de Protección de Datos Personales en las Empresas de Telecomunicaciones**: Estudios de casos de Argentina, Brasil, Chile y México. Volumen II. Asociación por los Derechos Civiles, Diciembre 2016.

Uruguai. **Ley n. 18331, 11 ago. 2008**. Disponible en: https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n°-18331-de-11-de-agosto-de-2008.html. Acceso em: 1 nov. 2018.

Veronese, A.; Cunha, M. Desafios do comércio eletrônico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de datos pessoais e cooperação regulatória internacional. **UNIO - EU Law Journal**. v. 4, n. 2, jul. 2018, p 73-89.