NÚMERO 1

ENSAYOS
DEMOCRACIA
DIGITAL

PRIVACIDAD E INTERNET:

DESAFÍOS PARA LA DEMOCRACIA BRASILEÑA

DENNYS ANTONIALLI
FRANCISCO BRITO CRUZ

PLATAFORMA DEMOCRÁTICA
FUNDAÇÃO FHC
CENTRO EDELSTEIN

Realização

PRIVACIDAD E INTERNET:

DESAFÍOS PARA LA DEMOCRACIA BRASILEÑA

DENNYS ANTONIALLI
FRANCISCO BRITO CRUZ

Plataforma Democrática (www.plataformademocratica.org) es una iniciativa del Centro Edelstein de Pesquisas Sociais y de la Fundação Fernando Henrique Cardoso, dedicada al fortalecimiento de las instituciones democráticas y de la cultura en América Latina, a través del debate pluralista de ideas acerca de los cambios en la sociedad y la política en la región y en el mundo.

Colección: Ensayos Democracia Digital
Dirigida por Bernardo Sorj (Centro Edelstein de Pesquisas Sociais) y Sergio Fausto (Fundação Fernando Henrique Cardoso)

Privacidad e Internet: desafíos para la democracia brasileña
Texto no 1, Marzo de 2017
Dennys Antonialli y Francisco Brito Cruz

Edición de la Fundación FHC/Centro Edelstein, 2017
Imagen de Portada: Lisia Lemes

ÍNDICE

1. Sumario Ejecutivo

1. La tecnología y, de manera singular, Internet, han pasado a intermediar en gran parte de las actividades de la vida cotidiana, trátese de relaciones establecidas entre usuarios de Internet y el sector privado, o de relaciones establecidas entre los ciudadanos y el sector público;

2. Internet ha agregado desafíos adicionales a la protección de la privacidad de los usuarios, en razón de que impulsa la utilización de sofisticados y silenciosos mecanismos de recolección y tratamiento de datos personales;

3. La publicidad conductual constituye parte de la base de modelos de negocio que han gozado de amplia adopción por parte de las empresas del sector de Internet, lo cual permite ofrecer el servicio de manera gratuita, aunque a la vez, potencia la exposición de los usuarios de la red a actividades de recolección de datos personales;

4. La estructura globalizada de la red implica la transferencia internacional de datos personales por parte de actores del sector privado, superponiendo modelos regulatorios diferentes, hecho que genera dificultades de compatibilización;

5. La existencia de estos complejos bancos de datos de usuarios de Internet y la multiplicación de datos y registros respecto de ellos

también despierta el interés de los Estados, que comienzan a ver en esta información una posibilidad de incrementar sus capacidades de vigilancia y de eficiencia en la gestión pública;

6. Las prerrogativas de acceso a datos de usuarios y la facilidad de captación de datos y registros referentes a la vida de los ciudadanos exigen de respuestas regulatorias que garanticen la privacidad de los mismos, existiendo el riesgo de que el incremento de las capacidades de vigilancia de los Estados inhiba el ejercicio de las libertades públicas;

7. En lo que respecta a las relaciones establecidas con el sector privado, el ordenamiento jurídico brasileño no cuenta con un marco regulatorio completo, capaz de brindar respuestas y limitaciones precisas para las actividades de recolección y tratamiento de datos personales, siendo importante que se brinde atención a las propuestas legislativas que están siendo actualmente debatidas en el Congreso Nacional;

8. En lo que respecta a las relaciones establecidas con el sector público, aunque el Marco Civil de Internet haya establecido algunos de los derechos de los usuarios, tales como la protección de la privacidad y la libertad de expresión, con el requisito de orden judicial para la provisión de ciertos tipos de registro, la aplicación de estas garantías de parte de los tribunales debe ser efectuada con rigor, existiendo el riesgo de que se estiren mucho las prerrogativas de acceso a datos de usuarios por parte de las autoridades, lo cual atenta contra el derecho a la privacidad;

9. La inexistencia de regulación específica en relación a las actividades de recolección y tratamiento de datos personales tanto por parte del sector privado como del sector público deja a los ciudadanos brasileños muy expuestos a violaciones de su privacidad, sin soluciones efectivas para la responsabilización de los actores que incurrieren en tales violaciones.

2. Introducción

Ya hacia 1890, *Warren* y *Brandeis* llamaban la atención en su artículo "The right to privacy" acerca de los riesgos que entrañaban las nuevas tecnologías, en particular en el campo fotográfico[1]. El poder de capturar y eternizar imágenes le había abierto camino a formas más invasivas de intromisión en la vida privada, haciendo posible compartir registros de momentos vividos por otras personas. La vida ajena pasó a ser, desde entonces, blanco de escrutinio público y debate político; particularmente en el caso de aquellas personas que, por cualquier tipo de razón (económica, política o social), consiguiesen una posición destacable, circunstancia que los arriesgaba a una constante "flagrancia" y los convertía en noticia habitual de los periódicos, lo cual, en la visión de los autores, conllevaba serios desafíos a su derecho a la privacidad.

Más de cien años después, la posibilidad de compartir imágenes y videos de manera irrestricta continúa representando una amenaza a la privacidad. Esta amenaza adquirió nuevas dimensiones, tanto con la llegada de tecnologías y dispositivos de captación de imágenes mucho más sofisticados, como los drones[2], como con la multiplicación de espacios y plataformas en los cuales tales contenidos pueden ser replicados, generando, incluso, nuevas formas de exposición y de violencia. La difusión no consentida de imágenes

íntimas, fenómeno que pasó a conocerse como "pornografía de venganza" (revenge porn), por ejemplo, ha constituido la causa de situaciones graves de abuso y violencia que, en los casos más extremos, llevaron a las víctimas al punto de cometer suicidio.3 De forma similar, la múltiple replicación de estos tipos de registro y la facilidad de encontrarlos con herramientas de la red, permitió que surja un debate complejo respecto del llamado "derecho al olvido", a partir del cual los usuarios podrían demandar la remoción de noticias o contenidos, o su respectiva desindexación de los buscadores de Internet, es decir, impedir que tales contenidos aparezcan como resultados de búsqueda.

Más allá de los dispositivos de captura y de la posibilidad de compartir imágenes, fue el surgimiento de los computadores y, más tarde, de Internet, lo que exigió una redefinición de la agenda de investigación en torno del derecho a la privacidad. A partir del momento en el que comenzó a ser posible la recolección y el tratamiento automatizado de datos personales, creció el interés por parte de empresas y Estados por explotar las potencialidades de estos nuevos tipos de recursos tecnológicos. Del lado de las empresas, la posibilidad de construcción de perfiles detallados de los hábitos y preferencias de usuarios[4] y el desarrollo de algoritmos predictivos (los algoritmos predictivos son modelos matemáticos capaces de realizar inferencias sobre hábitos y preferencias de los usuarios, generalmente utilizados como respaldo para los procesos de toma de decisiones automatizadas)[5] permitió reconsiderar las formas de aproximación y de interacción con los consumidores, además de abrir camino a nuevos modelos de negocio, en particular a aquellos basados en la publicidad conductual. Del lado de los Estados, la posibilidad de ampliación del aparato de vigilancia y control de los ciudadanos ha sido considerada una exigencia para la optimización de la seguridad pública, y una alternativa para el perfeccionamiento de los mecanismos de gestión.[6]

En dicho sentido, la interacción de los ciudadanos tanto con el sector público como con el sector privado, pasó a ser intermediada por la tecnología. Esto tiene repercusiones significativas, no sólo para su privacidad, sino también para su propia experiencia democrática. Existiendo registros que revelan características tan sensibles y detalladas respecto de su personalidad, el usuario está, por ejemplo, cada vez más expuesto al poder de manipulación que estos actores pueden ejercer.[7] La misma exposición puede constatarse respecto de los Estados, lo cual puede representar nuevas formas de control e interferencia en el espacio público y en el libre debate democrático. Valga como ejemplo que durante las manifestaciones políticas de 2013, fue revelada por la prensa la organización, por parte de las fuerzas policiales, de "Rondas Virtuales", a partir de las cuales se hacían barridos de perfiles de redes sociales de personas sospechosas, lo que culminó con la captura de más de 20 manifestantes en Río de Janeiro.[8]

En lo que respecta a la propaganda política, es válido decir que cada vez se la segmenta más en función de los perfiles de los electores, realizándose su producción en función de sus afinidades y preconcepciones. Existen estudios que demuestran, por ejemplo, que los electores pueden ser inducidos a votar por determinados candidatos que cuenten con características faciales semejantes a las propias. De acuerdo con las experimentaciones realizadas, la combinación sutil y prácticamente imperceptible de fotos de los electores con fotos de los candidatos (en composiciones generadas por computador) podría impactar en su elección política, particularmente cuando se trata de candidatos desconocidos.[9]

En conclusión, el desarrollo de estas nuevas tecnologías nos sitúa en un momento de inflexión histórica, en el cual la privacidad y la autonomía de los individuos, elementos clave para el libre ejercicio de sus libertades públicas, están siendo jaqueados por mecanis-

mos tecnológicos que permiten construir sistemas de bombardeo de información y de manipulación de sus susceptibilidades, tanto por parte del sector público como del privado, lo cual puede producir resultados temerarios para la sociedad democrática. El objetivo del presente artículo es el de presentar las principales tensiones en referencia al derecho a la privacidad que se observan *(i)* en la relación de los usuarios de Internet con las empresas; y *(ii)* en la relación entre ciudadanos y Estados, indicando, en ambos casos, cuáles son los principales modelos regulatorios adoptados en el mundo, con énfasis en las cuestiones y desafíos del caso específico de Brasil.

3. Ciudadanía intermediada: sector privado

Desde su apertura comercial, en 1993[10], Internet, además de la nítida revolución que representó para las formas de comunicación e interacción social, pasó a tomar lugar en un número cada vez mayor de actividades de la vida cotidiana. Desde transacciones bancarias hasta consultas médicas, la red transformó la dinámica de buena parte de las relaciones sociales y comerciales. Esto puede ser constatado en función del creciente número de dispositivos que se conectan a Internet, un movimiento al que se convino en llamar "Internet de las cosas": automóviles[11], aviones[12], aparatos de gimnasia[13], relojes[14] y hasta inclusive objetos como botellas de bebida (por ejemplo, las etiquetas de las botellas de whisky "Johnnie Walker Blue Label" serían capaces de detectar el momento en que la botella fue abierta y enviar notificaciones y mensajes interactivos al dispositivo móvil del consumidor registrado)[15]. Mucho más allá del simple hecho de estar presente en los computadores, Internet ha avanzado rápidamente hacia otras diversas áreas e instancias de la vida cotidiana.

En dicho sentido, en tanto que sean ejecutadas mediante dispositivos conectados a Internet, las relaciones entre ser humano y sector privado están cada vez más *intermediadas* por la tecnología.

Ryan Calo advierte sobre las tres principales consecuencias de esa interacción: *(i)* la posibilidad de que las empresas obtengan registros sobre las preferencias, formas de interacción y compromiso de los consumidores; *(ii)* la posibilidad de que se pueda interferir en la arquitectura de plataformas y dispositivos para influir en esa interacción; y *(iii)* la posibilidad de abordar a los consumidores de manera proactiva, en vez de esperar a que ellos busquen las ofertas o inicien el contacto con las empresas.[16]

De aquí se desprende que la recolección y el tratamiento de datos personales están en la base de estas relaciones, lo cual sirve de ayuda no sólo para el desarrollo de técnicas avanzadas de manipulación de tales datos (lo que se convino en llamar *big data*), sino también para el surgimiento de modelos de negocios calcados de la publicidad digital. El resultado de esto puede convertirse en una situación circular, en la cual las elecciones y hábitos de los usuarios determinan su contacto con ciertos contenidos publicitarios, lo que reforzaría estándares anteriores y restringiría el acceso de los individuos a alternativas u opciones más inesperadas o imprevisibles. Esto traería consigo una menor heterogeneidad para los estándares de consumo. Desde el punto de vista del acceso a la información y al conocimiento, se argumenta la ocurrencia de un fenómeno similar, con la creación de burbujas de interés, dentro de las cuales los usuarios tendrían menos contacto con opiniones divergentes.[17]

3.1. La monetización de datos personales como modelo de negocios

Muchos de los productos y servicios ofrecidos en Internet son gratuitos, o al menos, ofrecen una versión de acceso gratuito: redes sociales, *webmails*, plataformas para compartir imágenes y vídeos

u otras innumerables aplicaciones con funcionalidad variada, como juegos e integradores de informaciones.

La enorme mayoría de los modelos de negocios que hacen posible la oferta gratuita de productos y servicios está basada en la publicidad digital. Aunque la lógica sea fundamentalmente la misma que aquella que financia la producción de contenidos para parte de la prensa escrita y televisada, como la venta de espacios publicitarios para anunciantes, el ámbito digital sofisticó mucho la posibilidad de monetización de tales espacios, haciendo que los mismos sean también, con frecuencia, menos transparentes.

Esto es así porque, a partir de la recolección y tratamiento de datos personales, es posible segmentar a los usuarios por grupos de interés específicos, y, en consecuencia, direccionar los anuncios de forma más eficiente. En este sentido, cuantos más sean los usuarios, más valiosa es la empresa en su función de vehículo de difusión de anuncios. De la misma manera, cuanto más se sabe sobre el usuario, es decir, cuantos más datos de él han sido recolectados, mayor es el grado de precisión con el cual la empresa puede determinar la relevancia de los anuncios que le serán exhibidos y, consecuentemente, mayor es el valor que puede cobrarse por su exhibición.[18]

Por esta razón, la recolección de datos personales es una actividad silenciosa que se convirtió en praxis entre las empresas del segmento de Internet.[19] Muchas veces sin que él se entere, los hábitos y preferencias de navegación del usuario son monitoreados mediante la utilización de diversos mecanismos tecnológicos de recolección de datos, como las *cookies*. Las *cookies* son pequeños archivos que pueden ser enviados durante la comunicación establecida entre el dispositivo del usuario y el servidor de la página que está siendo visitada. Estos archivos no son otra cosa que identificadores, que hacen posible reconocer el dispositivo en función de visitas futuras y almacenan información sobre sus preferencias, por

ejemplo. Gracias a las cookies pueden agregarse ítems y mantenerlos en "carritos de compra" virtuales, o configurarse las preferencias de exhibición de una página para futuras visitas del usuario. Chris Hoofnagle comenta la evolución de estos archivos, destacando las principales diferencias entre ellos, clasificándolos en *flash cookies, evercookies, cookies* de terceros, *web beacons y fingerprinting*. El autor también demuestra que algunas de estas tecnologías de recolección han sido desarrolladas para actuar de manera persistente, inclusive ignorando preferencias expresas del usuario para no someterse a estas prácticas intrusivas. [20]

A partir del momento en el que las empresas consiguieron acceder a este tipo de información acerca de sus usuarios, han sido creados auténticos bancos de datos, repletos de información extremadamente reveladora sobre su personalidad, tal como las palabras clave buscadas, las páginas visitadas, las compras realizadas, los libros y las noticias leídas, la lista de amigos con los cuales mantiene mayor y menor contacto, y hasta incluso los lugares que visitó.[21] A eso también se le suman los archivos que pueden quedar almacenados en los servidores de las empresas (*cloud computing*) o los metadatos, a partir de los cuales también pueden realizarse inferencias importantes acerca del usuario.[22]

La segmentación de los usuarios en base a dichos datos e inferencias derivó en el desarrollo de complejos sistemas automatizados de ubicación y exhibición de anuncios, cuyo funcionamiento depende de mecanismos de "subastas". Inicialmente, estos mecanismos fueron desarrollados para los anuncios ofrecidos en buscadores como Yahoo! y Google. Básicamente, cada anunciante podría proponer un valor (oferta) para la exhibición de un determinado anuncio asociado a una palabra clave (término). A cada búsqueda realizada por el referido término, el buscador consideraba la oferta del anunciante en comparación con las ofertas de otros anunciantes asocia-

dos a la misma palabra clave, como en un sistema tradicional de subastas. Los resultados de búsqueda patrocinados (publicidades) eran, por entonces, exhibidos en orden decreciente, quedando en la cima el anuncio asociado a la oferta de mayor valor, y así sucesivamente. Los anunciantes cuyas publicidades recibiesen clics, pagaban el valor por el cual habían adquirido el compromiso (ofertas)[23].

Con el transcurso del tiempo, mecanismos similares fueron adoptados para determinar cuáles anuncios serían exhibidos para cada usuario. Esto significa que, por detrás de la exhibición de anuncios en casi todas las páginas web y plataformas de Internet, existe un complejo sistema automatizado de subastas, administrado por un conjunto de intermediarios, como agencias y redes de anunciantes ("Ad Networks"). Estos intermediarios promueven el vínculo entre los anunciantes, las plataformas y el usuario, en razón de que determinan cuáles anuncios serán exhibidos a cuáles grupos de usuarios.

Este proceso de segmentación e identificación de las preferencias de usuarios basado en la recolección y tratamiento de datos personales y ejecutado por una compleja red de intermediarios preocupa a los estudiosos del derecho a la privacidad por diversas razones, tales como: *(i)* la dificultad de concientizar a los usuarios sobre la utilización de tales mecanismos de recolección y de los actores involucrados en el proceso;[24] *(ii)* la insuficiencia de la noción de "consentimiento informado" que se busca alcanzar a través de las políticas de privacidad, y la imposibilidad del usuario de no consentir, cuya consecuencia directa es el hecho de no tener acceso al servicio, en algunas circunstancias;[25] *(iii)* la posibilidad de entrecruzamiento de informaciones entre diferentes bancos de datos, creando perfiles cada vez más completos;[26] *(iv)* la posibilidad de adopción de prácticas discriminatorias en Internet, con base en inferencias acerca del usuario;[27] (v) la posibilidad de manipulación del usuario en base a la información recolectada; [28] entre otras.

Estas cuestiones han sido encaradas y reguladas de maneras diferentes, en particular en lo relativo a los límites definidos para la recolección y tratamiento de datos personales, además de la posibilidad de transferirlos a terceros o a otros países. Las secciones siguientes presentan las principales características de los modelos adoptados en los Estados Unidos, en Europa y en Brasil.

Finalmente, vale recordar que, más allá de la vía normativa, es decir, del derecho, la propia arquitectura de Internet también puede servir como instrumento de regulación. Por ejemplo, pueden instalarse extensiones en el navegador del usuario que protejan su privacidad, impidiendo el envío de cookies. La propuesta de creación del "Do Not Track" en los Estados Unidos siguió esta concepción.[29] En la misma línea, el concepto de "*privacy by design*" fue concebido como un conjunto de principios que pregona la incorporación de mecanismos y opciones de configuración estándar que garanticen, mediante la tecnología, una experiencia de navegación menos intrusiva para la privacidad del usuario.[30]

Sin embargo, por más que estos mecanismos puedan empoderar al usuario y permitirle una mayor protección de su privacidad, independientemente de la adopción de un andamiaje jurídico de respaldo, el poder de "elección" de los usuarios es aún muy reducido en estos casos. Existen diversas páginas web que exigen la aceptación del envío de cookies para que sea posible la utilización de todas sus funcionalidades o la exhibición de todos sus contenidos, por ejemplo.

3.2. La privacidad y su protección: el modelo de los Estados Unidos

El modelo regulatorio adoptado en los Estados Unidos puede definirse como fragmentado y de autorregulación. En primer lugar,

fragmentado porque las leyes que tratan sobre el tema de la recolección y tratamiento de datos personales son solamente aplicables a sectores específicos y bien diversificados: existen leyes que regulan la recolección y tratamiento de datos financieros,[31] vinculados a la salud[32], a niños menores de trece años[33], o hasta incluso, al listado de filmes alquilados en videoclubes.[34]

Buena parte de estas leyes fue aprobada en respuesta a las crecientes discusiones respecto de la necesidad de cuidado de la privacidad frente al desarrollo de la tecnología, en particular, de las capacidades de procesamiento automatizado de datos por parte de los computadores.

Además de estas normativas sectoriales, existen también, para algunos casos específicos, legislaciones estatales aplicables[35] y leyes federales que tratan el tema de la recolección y uso de datos personales. Sin embargo, en el caso de las normas federales, que podrían ser más abarcadoras, su ámbito de aplicación quedó limitado a los órganos de la administración pública federal, como en el caso de la *Privacy Act of 1974*[36] y la *Freedom of Information Act* (FOIA).[37]

Fuera del alcance de estas legislaciones y de los segmentos alcanzados por ellas, la recolección y tratamiento de datos personales por parte de actores del sector privado no están reglamentados en el ámbito federal de un modo genérico, lo cual brinda una considerable discrecionalidad para aquellos que desean poner en práctica tales operaciones.

En consecuencia, queda bajo la competencia de la Comisión Federal de Comercio ("Federal Trade Commission") la investigación de prácticas "injustas o engañosas" en relación al consumidor en lo que respecta a su privacidad.[38] De acuerdo a lo entendido por la Comisión, básicamente, toda colecta y tratamiento de datos personales debe cumplir con los requisitos de *conocimiento y elección*.[39]

En otras palabras, esto equivale a afirmar que es posible realizar recolección y tratamiento de datos personales, siempre y cuando el usuario sea informado y cuente con alguna opción para evitar la práctica (mecanismos de ***opt-out***). Por la libertad que este sistema les brinda a las empresas para el diseño de sus políticas de privacidad, se acostumbra decir que está fundamentado en la autorregulación.[40]

En varias ocasiones se ha discutido la adopción de una legislación federal genérica que reglamente el tema en los Estados Unidos, imponiendo límites y reglas más concretas a la recolección y tratamiento de datos personales por parte de las empresas. En estas discusiones, sin embargo, prevalecen habitualmente los argumentos de que el modelo regulatorio actual es lo que garantiza la capacidad de innovación y competitividad de las empresas del sector de Internet.[41]

3.3. La privacidad y su protección: el modelo de la Unión Europea

El modelo regulatorio adoptado por los países de la Unión Europea es el legislativo; es decir, está basado en la aprobación de una ley. En él, en consecuencia, se adopta un régimen general de protección de datos personales, normalmente consustanciado en una ley genérica, que establece parámetros mínimos que deben ser respetados para la recolección y tratamiento de tales datos (leyes de protección de datos). En estos casos, por lo tanto, no hay una libertad irrestricta de la iniciativa privada para moldear e implementar sus políticas de privacidad. La fiscalización y control son en general efectuados por organismos especiales ("autoridades de garantía"), cuyas competencias y atribuciones también suelen estar definidos por las legislaciones.

En verdad, el modelo se consolidó en Europa después de la aprobación de la Directiva 98/46/CE, del 24 de octubre de 1995, que les impuso a todos los Estados Miembro de la Unión Europea la obligación de asegurar, en sus ordenamientos jurídicos nacionales, la protección del derecho a la privacidad en conformidad con los parámetros mínimos establecidos en la Directiva.[42]

Mucho antes de la aprobación de la Directiva, sin embargo, algunos países ya habían adoptado legislaciones en este sentido. Desde 1973, Suecia cuenta con una ley de protección de datos personales (*Datalagen*); Alemania también cuenta con una ley de protección del año 1977 (*Bundesdatenschutzgesetz*). Es interesante notar, en este sentido, que a partir de la aprobación de la Directiva, no sólo los demás Países Miembro de la Unión Europea pasaron a adoptar el modelo legislativo, sino que también lo hicieron muchos otros países de todo el mundo: al día de hoy, más de cien países cuentan con leyes de protección de datos personales.[43]

Parte de la razón por la cual el modelo legislativo ganó adherencia mundial se debe a una característica de la propia Directiva que, al regular la transferencia internacional de datos personales, autoriza su realización solamente "hacia terceros países que aseguren un nivel de protección adecuado".[44] Esto implicaría que las empresas de países localizados fuera de la Unión Europea que pretendiesen recolectar y transferir datos de ciudadanos europeos para su tratamiento, deberían demostrar un nivel adecuado de protección. El modo más simple de cumplir con eso sería, entonces, adoptar legislaciones que estuviesen alineadas sustancialmente con las exigencias de la Directiva, facilitando las operaciones de dichas empresas de fuera de la Unión Europea.

Para evaluar la adecuación de los niveles de protección adoptados en otros países de fuera de la región, la Directiva europea creó un "Grupo de Trabajo", cuyos resultados serán presentados a continuación.[45]

3.3.1. Dificultades de compatibilización: la transferencia internacional de datos

La existencia de los referidos modelos nacionales diferentes de regulación genera incertidumbre en las empresas del segmento de Internet que actúan a nivel global, que tendrían que respetar, de manera concomitante, distintos grados de protección brindados al derecho a la privacidad, en particular al considerar que las actividades de recolección y tratamiento de datos involucran, con frecuencia, la transferencia de tales datos entre distintos países. Dicha tarea exigiría no sólo un estudio detallado de las particularidades de cada ordenamiento jurídico, sino también la creación de un sistema de recolección de datos personales diferente para cada país, de acuerdo con la ubicación geográfica del usuario, determinada por su dirección de IP, por ejemplo. Considerando que prácticamente todos los sitios web realizan algún tipo de recolección de datos, la exigencia podría representar un obstáculo técnico y económico para que muchos de ellos pudieran establecerse.

Como hemos visto, en los Estados Unidos no existe una legislación de protección de datos que garantice el cumplimiento de los parámetros mínimos de protección exigidos por la Directiva europea 95/46/CE, lo cual generó un ***impasse*** en relación a la posibilidad de transferencia de datos entre ambas regiones. Sin la garantía de un nivel adecuado de protección, las empresas estadounidenses no podrían transferir datos de ciudadanos europeos hacia fuera de la Unión Europea, lo que convertiría en inviables a los modelos de negocios de muchas de las empresas de Internet que actúan en el mercado europeo.

Para salvar esta situación, el 21 de julio de 2000, el Grupo de Trabajo celebró un acuerdo bilateral con el Departamento de Comercio de los Estados Unidos, en función del cual las empresas estadou-

nidenses podrían declarar la adopción de niveles de protección de privacidad adecuados, es decir, en conformidad con las exigencias de la Directiva ("Safe Harbor").[46] Dicha declaración estaba basada en algunos principios[47], y era suficiente para incluir a las empresas en una lista, autorizándolas a transferir datos recolectados de ciudadanos europeos ("US-EU Safe Harbor List").[48]

Por ser de participación voluntaria y por basarse en la mera declaración de las empresas participantes, sin existir un sistema de verificación por parte del Departamento de Comercio, durante su vigencia, el sistema recibió diversas críticas.[49]

Poco más de quince años después de su entrada en vigor, el 6 de octubre de 2015, el acuerdo fue invalidado por la Corte de Justicia Europea por un caso que involucraba a un ciudadano austríaco, que cuestionaba la validez del acuerdo para la protección de su derecho a la privacidad. Según expresa el fallo, el acuerdo no puede ser considerado un mecanismo válido de "adecuación" a los niveles de protección exigidos por la Directiva para la transferencia de datos de ciudadanos europeos a los Estados Unidos.[50]

Habiendo quedado invalidado el acuerdo, Estados Unidos y la Unión Europea iniciaron las negociaciones para la elaboración de un nuevo sistema que permitiese la transferencia de datos entre ambas regiones. El 12 de julio de 2016 se anunció la aprobación de una versión reformulada del acuerdo ("Privacy Shield"). Comparado con el "Safe Harbor", es poco lo que cambió respecto del sistema de autodeclaración de las empresas, que continúan teniendo que certificar su "adecuación" a los niveles de protección europeos en base a los mismos siete principios anteriormente adoptados. La diferencia principal del acuerdo reside en la exigencia de mecanismos de fiscalización por parte del Departamento de Comercio de los Estados Unidos y de la Comisión Federal de Comercio respecto del cumplimiento de tales certificaciones, además de abrir espacio a formas más efi-

caces de reclamo y denuncias de violación por parte de los ciudadanos europeos.[51] Desde el 1 de agosto de 2016, el Departamento de Comercio de los Estados Unidos está aceptando las certificaciones en conformidad con el nuevo acuerdo.

Vale recordar que los acuerdos contemplados tienen vigencia solamente entre Estados Unidos y la Unión Europea, no existiendo mecanismos significativos y semejantes en relación a otros países. El tópico siguiente presenta las características de la reglamentación existente en Brasil.

3.4. La privacidad y su protección: hacia dónde va Brasil

En Brasil, la privacidad recibe respaldo constitucional en los incisos X y XII del artículo 5º de la Constitución Federal. Figuran como parte de los derechos de los brasileños la protección de la vida privada, de la intimidad, la inviolabilidad de la confidencialidad de la correspondencia, de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas (este último, accesible sólo en casos de investigaciones o procesos criminales debidamente justificados por ley). Sin embargo, para hacerse efectiva, esta protección constitucional requiere de una legislación que le brinde soporte, consolidando la protección genérica con reglas específicas de resguardo de la privacidad frente al complejo ecosistema empresarial de recolección y tratamiento de datos ya descripto.

A pesar de la vasta utilización de productos y servicios de Internet por parte de los brasileños –en especial, aquellos productos que tienen como núcleo de sus modelos de negocios la recolección y procesamiento de datos personales para el posterior direccionamiento de publicidad–, la legislación por debajo de la Constitución

es aún tímida. En este plano, las reglas existentes pueden ser encontradas en *(i)* leyes sectoriales dispersas, y *(ii)* en la Ley nº 12.965, del 23 de abril de 2014 ("Marco Civil de Internet"), acompañada del decreto que la reglamenta ("Decreto nº 8771, del 11 de mayo de 2016").

Algunas leyes sectoriales[52] incluyen ciertas disposiciones aplicables a Internet. En el área de telecomunicaciones, por ejemplo, la Ley General del sector establece la protección de la privacidad y la inviolabilidad de las comunicaciones como deberes a cumplirse por parte de las prestadoras, aunque sin adentrarse más específicamente en el asunto. Estas disposiciones generales de la LGT traen más dudas que soluciones en los casos más recientes que involucraron a las prestadoras de servicios de telecomunicaciones y al derecho a la privacidad. En estos casos[53], la legislación de defensa del consumidor y su sistema de fiscalización fueron los fundamentos que brindaron soporte a la acción de protección de la privacidad por parte del Poder Público.

Los casos más notables hasta el momento son el de notificación (y multa, al menos en uno de ellos) por parte del ministerio de Justicia (más específicamente, de la Secretaría Nacional del Consumidor, organismo que está a la cabeza del Sistema Nacional de Defensa del Consumidor) de la Oi y de Telefónica/Vivo, por acciones de recolección y tratamiento de datos de usuarios sin previa información o consentimiento. En el caso de la Oi, la situación incluyó la investigación de alianzas firmadas en 2010 entre la empresa británica Phorm, desarrolladora de un software que monitoreaba integralmente la navegación de los consumidores, y empresas de telecomunicaciones brasileñas. Se le aplicó a la Oi una multa de 3,5 millones de reales en este caso, por violar los derechos de información y privacidad de los consumidores. Más recientemente, hacia inicios de 2015, Telefónica/Vivo también fue notificada por el Ministerio de Justicia, por anunciar públicamente la implementación del servicio "Smart

Steps", que recolectaría informaciones de geolocalización de los teléfonos celulares de los clientes de la compañía para la generación de informes y análisis, posiblemente con fines de lucro económico.

En este contexto, la Secretaría Nacional del Consumidor ("SENACON") ocupa un papel relevante en las discusiones que involucran la protección del derecho a la privacidad en Brasil; en particular, por coordinar la fiscalización de las disposiciones del Código de Defensa del Consumidor utilizadas para controlar a las empresas que concentran intensa actividad de recolección y tratamiento de datos personales. Dicha tendencia se confirma por la preeminencia de esta agencia frente a las discusiones que culminaron en la Ley de Registro Positivo (de notable importancia en la discusión de la protección al consumidor) por un lado, y en su protagonismo dentro del Ejecutivo en el proceso de elaboración de un anteproyecto de ley de protección de datos personales, a ser tratado más adelante.

El Marco Civil de Internet (Ley 12. 965/2014), por su parte, concentra una serie de disposiciones de considerable importancia, relativas a la protección de la privacidad de los usuarios de Internet en Brasil.

El Marco Civil de Internet está considerado como paradigmático en términos de elaboración normativa, por haber sido el fruto de un proceso de intenso debate público fomentado por el Poder Ejecutivo entre 2009 y 2011. Durante este período, el Ministerio de Justicia, en alianza con la Fundación Getúlio Vargas, puso en línea una plataforma en Internet para recoger opiniones y fomentar el debate entre ciudadanos, empresas y organizaciones. El proceso culminó con la proposición de un proyecto de ley presentado ante el Congreso Nacional, y quedó reconocido como referencia internacional de participación multisectorial en la elaboración de reglas y directrices para la gobernanza de Internet. Ese proyecto de ley llevaba a la consideración del Poder Legislativo una serie de acuerdos que habrían

de resolver los temas más abordados en la plataforma de debates; puntualmente, la responsabilidad de las empresas de Internet por los contenidos generados por sus usuarios, la retención de registros de navegación por parte de tales empresas, y la neutralidad de red, asunto vinculado a las normas de gerenciamiento de la infraestructura de telecomunicaciones.[54]

Hubo que esperar hasta la etapa final de la tramitación del proyecto de ley en el Poder Legislativo (2012-2014) para que la recolección y tratamiento de datos personales por parte del sector privado fuera incluida en la discusión del Marco Civil de Internet. Esta inclusión tuvo como factor catalizador las revelaciones del exfuncionario de la Agencia Nacional de Seguridad (NSA) de los Estados Unidos, Edward Snowden. Al quedar en evidencia que sectores de la inteligencia estadounidense conseguían acceso legal (respaldado por orden judicial, tanto de carácter secreto, general o vinculada a asuntos de seguridad nacional) o forzado (a partir del acceso privilegiado a la infraestructura de cableado necesaria para el funcionamiento de tales servicios digitales en red) a los servidores de buena parte de las más grandes empresas de Internet. Snowden se adueñó de los titulares. El proceso se agudizó cuando sus revelaciones llegaron al más alto escalafón del gobierno federal: el ex agente confesó que hasta incluso el teléfono celular de la por entonces Presidente de la República, Dilma Rousseff, había sido espiado, así como también la red interna de la mayor empresa estatal del país, Petrobras.

El llamado "efecto Snowden" abrió una ventana de oportunidad política para que el texto del proyecto de ley fuese enmendado con reglas genéricas referidas a la protección de los datos personales de los usuarios brasileños de Internet. El Congreso Nacional, sensibilizado por las revelaciones, refrendó la idea, que fue adoptada por el diputado impulsor del proyecto, Alessandro Molon (PT-RJ, en la época). Como respuesta al espionaje estadounidense producido

por la emergencia del sector de Internet con base en ese país, el texto aprobado por el Congreso Nacional dispone que es necesario el consentimiento libre y expreso del usuario para la recolección de sus datos personales (art. 7º, IX), así como también exige que se brinde información clara y completa respecto del uso de los datos, el cual está permitido solamente para finalidades lícitas, explicitadas en contrato con los usuarios y que justifiquen su recolección (art. 7º, VIII). La ley estableció también que los ciudadanos pueden requerir a las empresas de Internet la exclusión definitiva de datos personales una vez finalizada la relación entre las partes.

Finalmente, ese "efecto" también fue responsable de la inclusión de reglas de "fiscalización". El artículo 11, agregado luego de una negociación entre el impulsor y el Ejecutivo, dispone que "*en cualquier operación de recolección, almacenamiento, guarda y tratamiento de registros, de datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de Internet en las que por lo menos uno de estos actos se lleve a cabo en territorio nacional, deberán ser obligatoriamente respetadas la legislación brasileña y los derechos a la privacidad, a la protección de los datos personales y a la confidencialidad de las comunicaciones privadas y de los registros*". La ley prevé, inclusive, sanciones que pueden ser aplicadas en el caso de violación de esta norma.[55]

Las reglas establecidas en el Marco Civil están muy distantes, sin embargo, del andamiaje establecido en las legislaciones generales de protección de datos normalmente adoptadas por el modelo legislativo europeo mencionado más arriba, tanto en términos legales como de fiscalización por parte del Estado. No existe pronunciamiento sobre una serie de cuestiones clave tratadas exhaustivamente por estos acuerdos normativos.

A pesar de ello, existen hace ya algún tiempo discusiones apuntando a la institución, en el ámbito nacional, de una Ley de

Protección de Datos Personales acompañada de su correspondiente sistema de fiscalización. Una propuesta de marco normativo fue incluida en la agenda del Ministerio de Justicia hacia 2011, en pleno auge de los mencionados escándalos involucrando a las prestadoras de servicios de telecomunicaciones y la recolección y tratamiento de datos personales. En ese año, el Ministerio promovió un debate público respecto de un anteproyecto de ley. Luego de que el Marco Civil hubiera monopolizado las discusiones entre los sectores interesados en la regulación del ambiente digital entre 2011 y 2014, el tema volvió al ruedo en 2015. Hacia comienzos del 2016, una nueva versión del anteproyecto fue llevada de nuevo al campo del debate público, en forma conjunta con una propuesta de decreto reglamentario del texto de Marco Civil de Internet.

El decreto resultante de este proceso, que lleva al número 8771/2016, determinó la primera definición de "dato personal" incluida en la legislación brasileña, inclusive luego de controversias acerca de que no se trataría de la forma legislativa más adecuada para incluir tal definición. Las definiciones de "dato personal" y de "tratamiento de datos personales" son las mismas que están presentes en las propuestas de leyes de protección de datos propulsadas por el propio Ministerio de Justicia y elevadas al Poder Legislativo.

La consulta pública respecto del anteproyecto derivó en una serie de cambios en el texto. Posiblemente, el cambio más significativo haya sido la inclusión del "legítimo interés del responsable del tratamiento de datos personales", como una hipótesis que autoriza el tratamiento de los datos, mecanismo criticado por organizaciones de la sociedad civil organizada y por los defensores de los derechos del consumidor[56]. El texto fue elevado al Legislativo, luego de la consolidación de este proceso de negociación encabezado por la SENACON, pasando a ser tramitado bajo el número 5276/2016. En el Congreso, sin embargo, ya existían otros dos proyectos propuestos

por parlamentarios, que también versaban sobre la materia, uno en la Cámara de Diputados y otro en el Senado. A pesar de su anexión a un proyecto de matices radicalmente diferentes (y más blandos) –el proyecto de ley nº 4060/2012–, es de particular importancia el hecho de que este proyecto de ley haya sido propuesto por el Ejecutivo.

Esto es así porque, por requisito de la Constitución Federal, es de iniciativa privativa del Presidente de la República la creación de órganos de la Administración Pública (Art. 61,§ 1º, e). En tal sentido, el proyecto 5276/2016 es el único que puede instituir un organismo específico para actuar en la fiscalización de las actividades vinculadas al derecho a la privacidad (tarea desempeñada por las autoridades de garantía en países que adoptaran el modelo legislativo).

A pesar de las divergencias respecto de los detalles administrativos de su estructura, la institución de una autoridad central federal e independiente de protección de datos personales constituyó un punto pacificador entre sectores radicalmente enfrentados durante la consulta pública –el sector privado y la sociedad civil–. Para las empresas, el recelo residía en que la legislación fuera aplicada de manera heterogénea y espontánea por parte de diferentes autoridades locales y regionales, lo cual elevaría el riesgo y su costo de adecuación a la regulación. Por su parte, la sociedad civil temía que la ley "no pegara", es decir, que la fiscalización no sucediese en caso de que no existiera un conjunto efectivo de técnicos dedicados al tema, así como una autoridad con poder de policía que pudiese aplicar sanciones.

Aún tratándose de un tema de actualidad y fruto de debate previo, los proyectos de ley que reglamentan la protección de datos personales tienen por delante un largo camino de tramitación. Este vacío normativo abre espacio para que algunas cuestiones lleguen al Poder Judicial sin que existan limitaciones específicas y pensadas para los dilemas agregados por las innovaciones tecnológicas. En di-

ferentes casos, los magistrados han adoptado concepciones dispares en relación a la aplicación de los dispositivos constitucionales, de las reglas genéricas del Marco Civil, o de las disposiciones "prestadas" por las leyes sectoriales.

Dos casos pueden servir como ejemplo para ilustrar la disparidad de los fallos emitidos por la Justicia. En el primero, el Tribunal de Justicia de Rio Grande do Sul (TJ-RS) dictaminó[57] que la venta de datos personales, como nombre, CPF (*NdelT: "Cadastro de Pessoa Física", código personal de identificación tributaria en Brasil*) o dirección, aún sin consentimiento, no es ilícita, en razón de que dichos datos no serían "sensibles". Según la interpretación del Tribunal, merecerían protección exclusivamente aquellos datos que pudieren generar actos discriminatorios, como "orientación política, religiosa o sexual". La falta de "comprobación de daño" derivada de la venta sirvió también como fundamento para la decisión.

En el otro extremo, el Ministerio Público Federal dio lugar a un pedido de bloqueo del sitio web "Tudo Sobre Todos", que llevaba a cabo una actividad muy similar a aquella del caso juzgado por el Tribunal de Justicia de Rio Grande do Sul: la comercialización de datos personales sin el consentimiento de sus titulares[58]. En la visión del magistrado del 1º Tribunal Federal de Rio Grande do Norte, la actividad es ilícita.

Los fallos, que tuvieron repercusión nacional, datan del mismo año (2015). Su disparidad suscita dudas relevantes respecto de la interpretación de la protección constitucional de la intimidad y de la vida privada en el contexto digital, particularmente frente a los riesgos asociados a nuevas técnicas de entrecruzamiento de bancos de datos y al uso de algoritmos.

4. Ciudadanía intermediada: sector público

En la sección anterior, se describió de qué forma los modelos de negocios basados en la publicidad digital, que incluyen la recolección y tratamiento de datos personales, repercuten en el resguardo del derecho a la privacidad. Además de ello, fueron presentadas las principales características de los modelos regulatorios adoptados para hacer frente a las relaciones establecidas entre usuarios y empresas, con énfasis en Brasil, que aún cuenta con escasas disposiciones en tal sentido. El objetivo de esta sección es el de ilustrar el modo en el cual la regulación de dichas cuestiones interfiere también de manera directa en la relación entre ciudadano y Estado, sumando nuevas formas de potencial violación de su derecho a la privacidad.

Las denuncias realizadas en junio de 2013 por Edward Snowden respecto del aparato de vigilancia implementado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) convirtieron en palpable y explícita la relación entre el desarrollo de técnicas de vigilancia masiva, por un lado, y el ecosistema de recolección de datos personales como parte de un modelo de negocios, por el otro. La construcción de repositorios con gigantesca cantidad de registros

de navegación, de preferencias, de fotos o de actividades en la red por parte del sector privado, despertó un enorme interés en el Estado. Conscientes de la existencia de talas bancos de información, los Estados comenzaron a demandar, cada vez más asertivamente, prerrogativas de acceso a tales informaciones, como respaldos importantes para los procesos de investigación y de persecución penal.

Al mismo tiempo, el propio Estado administra (en sus organismos y subdivisiones) una serie de bancos de datos potencialmente sensibles. La actividad administrativa está permeada por la necesidad de recolección y tratamiento de datos, un punto neurálgico en términos de eficiencia de las políticas públicas a escala. Ejemplos no faltan: el registro biométrico electoral y el banco de datos de historias clínicas del sistema público de salud indican que la informatización de las más diversas áreas llevó consigo dilemas propios del área de protección de datos personales al núcleo de la Administración Pública.

En dicho sentido, son dos los puntos de atención en lo que respecta al tema de la vigilancia del Estado y la protección de datos personales: *(i)* el aumento de las prerrogativas de acceso a datos de usuarios mantenidos por empresas; y *(ii)* el aumento de las posibilidades de recolección y tratamiento de datos personales por parte del propio Estado.

4.1. Antagonismo o cooperación: prerrogativas del Estado para el acceso a datos de los ciudadanos

La reciente ola de ataques y atentados terroristas en todo el mundo ha suscitado numerosas discusiones acerca de las necesidades de aumentar las capacidades de vigilancia de los Estados. En

Francia, el Estado decretó estado de emergencia, lo cual incrementó considerablemente las prerrogativas de investigación por parte de las autoridades.[59] En Alemania, se discuten reformas legislativas para acelerar los procesos de investigación.[60] En el Reino Unido, fue aprobada el 16 de noviembre de 2016 una de las legislaciones más agresivas del mundo en términos de vigilancia.[61] En los Estados Unidos, a partir de los ataques del 11 de setiembre, se adoptó el camino de una intensa reforma legislativa para fortalecer el aparato de vigilancia nacional, lo cual se consolidó particularmente con la aprobación de la "USA Patriot Act".[62]

Todas estas medidas tienen en común el hecho de apoyarse en el aumento de las prerrogativas de acceso a datos de usuarios de Internet por parte de las autoridades. Estos datos, hasta entonces concentrados en manos de las empresas, tal como ya se ha comentado, pasan a ser objeto de deseo de los Estados, que abogan por medidas más invasivas en nombre de la seguridad nacional.

En Brasil, más allá de la ausencia de un marco normativo que establezca reglas básicas en relación a la atención de la protección de datos de los ciudadanos por parte de los organismos estatales, existen estudios recientes que expresan la opacidad de la actividad de vigilancia emprendida por el Estado brasileño.[63] En líneas generales, el rigor de la ley parece surgir solamente en aquellas ocasiones en las que autoridades como la Policía y el Ministerio Público –respaldados en orden judicial– buscan acceder a datos de ciudadanos ante intermediarios privados. Este acuerdo está ejemplificado en las tablas de más abajo, que esquematizan los límites a la vigilancia sobre las comunicaciones y datos en Brasil, y las prerrogativas de acceso a tales datos instituidas en la legislación vigente:

Tabla 1: prerrogativas de acceso a datos por parte de autoridades[64]

VIGILANCIA DEL ESTADO BRASILEÑO SOBRE LAS COMUNICACIONES			
Fin/ Autoridad (es)	**Regulación de las Telecomunicaciones (ANATEL)**	***Law enforcement* (autoridades policiales, Ministerio Público, jueces y CPIs)**	**Inteligencia (ABIN)**
OBLIGACIONES DE GUARDA DE DATOS	Las resoluciones 426/05, 477/07 y 614/13 de ANATEL obligan a que datos relativos a la prestación de servicios de telefonía fija y móvil sean guardados por prestadoras por al menos 5 años y que datos relativos a la conexión a Internet sean guardados por proveedores por plazo mínimo de 1 año.	La ley 12.850/13 (art. 17) impone la guarda de "registros de identificación de los números de los terminales de origen y destino de las llamadas telefónicas" a empresas concesionarias de telefonía fija y móvil por 5 años. La Ley 12.965/14 (arts.13 y 15) impone la guarda de registros de conexión a Internet por 1 año a todos los proveedores de conexión y la guarda de registros de acceso a aplicaciones a proveedores de aplicaciones con fines económicos por 6 meses.	No existe obligación de guarda para fines de inteligencia.
ACCESO A DATOS GUARDADOS (informaciones registrales y metadatos)	En el ejercicio de poderes fiscalizatorios (art. 8, Ley 9472/97), ANATEL puede acceder a documentos fiscales, que contienen informaciones registrales e informaciones, por requisición a las prestadoras de servicio. Actualmente, existe desarrollo de infraestructura que permite acceso directo e irrestricto online, basado en art. 38 de la Resolución 596/12.	Según leyes 9.613/98 (art. 17-B) y 12.850/13 (art. 15), en el caso de informaciones registrales de usuarios de telefonía, puede realizarse acceso mediante simple requisición de autoridades policiales o Ministerio Público a las prestadoras. El acceso a registros telefónicos y otros metadatos generados por el uso de telefonía (localización) no poseen reglamentación legal específica: se accede mediante orden judicial para fines de producción de prueba. Por el MS 23452/RJ del STF, puede accederse a registros telefónicos también en el ámbito de CPIs. Según Ley 12.965/14, puede accederse a informaciones registrales de suscriptores de proveedores de conexión y de usuarios de aplicaciones de Internet mediante requisición de autoridades competentes (art. 10, § 3º). En el caso de registros de conexión a Internet y acceso a aplicaciones, puede accederse por orden judicial cuando hubiera fundados indicios de ocurrencia de ilícito y utilidad de los registros para la investigación o instrucción probatoria, con necesidad de determinación de período específico (art. 22).	Poderes de requisición y de requerimiento de datos de la ABIN inexistentes. Posibilidad de acceso indirecto por el Sisbin, en los términos de los arts.6, V y 6-A del Decreto 4.376/02.
ACCESO A COMUNICACIONES DOCUMENTADAS	Las resoluciones de ANATEL permiten acceso a grabaciones de llamadas a servicios de atención al cliente de prestadores de servicios de telecomunicaciones.	La ley 12.965/14 permite acceso a comunicaciones privadas registradas realizadas por aplicaciones de Internet por orden judicial (art. 7, III). Según RE 418.416-8/SC emitido por el STF, el pedido de búsqueda y captura legitima el acceso a datos almacenados en computadores.	Poderes de requisición y de requerimiento de datos de la ABIN inexistentes. Posibilidad de acceso indirecto por el Sisbin (arts.6, V y 6-A del Decreto 4.376/02).

INTERCEPCIONES	Prerrogativa de realización y competencia de requerimiento de intercepciones inexistentes.	Según ley 9.296/96, pueden realizarse intercepciones de comunicaciones telefónicas y de sistemas de informática y telemática mediando orden judicial, de oficio o por requerimiento de autoridad policial o del Ministerio Público, cuando hay indicios razonables de autoría o participación en infracción penal punida con pena de reclusión e indisponibilidad de otros medios de producción de prueba (arts. 1 y 2). La ley 12.965/14 permite intercepción de flujo de comunicaciones vía Internet en la forma de la Ley 9.296/96. Resoluciones del CNJ y del CNMP especifican criterios a observarse en pedidos y decisiones.	Prerrogativa de realización y competencia de requerimiento de intercepciones inexistentes. La ley 9.296/96 no extiende tales poderes a la ABIN. Posibilidad de cooperación por el Sisbin (arts.6, V y 6-A del Decreto 4.376/02).

Tabla 2: límites a las prerrogativas de vigilancia[65]

LÍMITES A LA VIGILANCIA SOBRE LAS COMUNICACIONES EN BRASIL	
DERECHOS	La Constitución Federal protege la libertad de expresión, la intimidad y la confidencialidad de las comunicaciones (art. 5º incisos IX, X y XI).
	Las leyes nº 9.472/97 (arts. 3º, V y IX, y 72) y nº 12.965/14 (art. 7º) garantizan los derechos a la confidencialidad de las comunicaciones y a la privacidad del uso de telefonía e Internet.
	No existen pruebas consagradas de aplicación uniforme en la jurisprudencia y en la doctrina, para la evaluación de la constitucionalidad de restricciones a tales derechos.
	El art. 5º, § 2º de la Constitución Federal dispone que los derechos y garantías expresados en ella no excluyen a otros derivados del régimen y de los principios por ella adoptados, o de los tratados internacionales de los que Brasil sea parte. Forman parte del bloque de constitucionalidad, sin embargo, sólo tratados y convenciones internacionales sobre derechos humanos aprobados en régimen equivalente al de enmiendas constitucionales, por el art. 5º, § 3º.
RECURSOS	En casos de violación a derechos, el ciudadano puede interponer ***habeas corpus*** o mandato de seguridad, previstos en la Constitución (art. 5º, LXVIII y LXIX), o iniciar acción ordinaria.
GARANTÍAS	La Constitución Federal garantiza el debido proceso legal, el contradictorio y la amplia defensa, y la presunción de inocencia (art. 5º, LIV, LV y LVII). El Código de Proceso Penal ordena que el juez observe los principios de adecuación, de necesidad y de proporcionalidad al ordenar producción de pruebas (art. 156). Lo mismo vale para la apreciación de pedidos de medidas cautelares de producción de pruebas (art. 282). La intimación del imputado debe siempre realizarse, "exceptuando casos de urgencia y de riesgo de ineficacia" (art. 282, § 3º).
	Según la Constitución Federal (art. 5º, LVI) el Código de Proceso Penal (art. 157), son inadmisibles las pruebas obtenidas por medios ilícitos, contrariando a la Constitución o a la ley. No pueden ser aprovechadas.
SANCIONES	El art. 10 de la Ley nº 9.296/96 criminaliza intercepciones ilegales y violación del secreto de justicia. Pena: reclusión de 2 a 4 años y multa.
	El art. 156-A del Código Penal criminaliza la invasión a dispositivo informático con el fin de obtener datos. Pena: detención de 3 meses a 1 año, y multa. Se de allí derivase acceso a contenidos de comunicación privada, la pena es de reclusión de 6 meses a 2 años, y multa.

De las tablas, vale destacar el conjunto de garantías establecidas por el Marco Civil de Internet, que consagró la exigencia de orden judicial para el acceso a datos de identificación de usuarios de Internet en Brasil (como registros de acceso a aplicaciones de Internet y registros de conexión).

Con la aprobación de la ley, lo que se esperaba era consolidar una aplicación rigurosa de esa criba jurídica, resguardando la privacidad de los usuarios de Internet, que solamente deberían ser identificados en circunstancias de fundados indicios de ocurrencia de acto ilícito y con motivada justificación de la utilidad de los registros solicitados para fines de investigación o de instrucción probatoria (art. 22).

La existencia de este filtro jurídico para la identificación de usuarios también tiene repercusión en la libertad de expresión, dado que si se considera que existe un derecho irrestricto y genérico de identificación de los usuarios de Internet por cualquier manifestación o contenido difundido en la red, se incrementan las posibilidades de intimidación y constreñimiento de los usuarios.

En tal sentido, además del rigor jurídico para sólo determinar la entrega de datos de identificación en el caso de cumplimiento de los requisitos mencionados más arriba, existe un importante papel que deben desempeñar los proveedores de aplicaciones de Internet (como Facebook y Google), y también los proveedores de conexión a Internet (como NET, VIVO y TIM). En ambos casos, cuestionar pedidos abusivos de datos de usuarios o recurrir contra fallos judiciales poco rigurosos puede ayudar a fomentar una cultura de valorización del derecho a la privacidad y, consecuentemente, del derecho a la libertad de expresión[66]. En relación a las prácticas y políticas de protección a datos de usuarios adoptadas por los proveedores de conexión a Internet de Brasil, el InternetLab realiza una evaluación anual a través del proyecto “Quem defende seus dados?” (¿Quién defiende

sus datos?), cuyos resultados pueden consultarse en la URL www.quemdefendeseusdados.org.br.

Luego de las elecciones de 2014 (y a partir de algunas lecturas respecto de que la composición del Congreso Nacional se habría convertido en bastante más conservadora en relación a la de los años anteriores[67]), las garantías establecidas por el Marco Civil, sin embargo, quedaron bajo ataque. Como puede notarse, en virtud de una serie de iniciativas realizadas en los últimos años, la agenda legislativa en esta área ha sido dominada por una ofensiva solicitando retirar obstaculizaciones de acceso a datos por parte de autoridades estatales y la ampliación de la obligación de la retención de información sobre los usuarios para futuras investigaciones.

La ofensiva puede ilustrarse a través de algunos ejemplos. La tramitación del proyecto de ley 215/2015 –al cual algunos sectores de la sociedad civil organizada llamaron "PL Espía"– por parte de la Comisión de Constitución, Justicia y Ciudadanía de la Cámara de Diputados, por caso, levantó el recelo de académicos del área[68], en razón de concentrar una serie de propuestas que incluían la obligación de recolección y guarda de datos registrales de usuarios y su disponibilidad sin mediar orden judicial por cualquier razón. La intención explícita de los parlamentarios era la facilitación de procedimientos de identificación de usuarios en virtud de la proliferación de "ofensas al honor" en Internet.

Esta misma preocupación impregnó los trabajos de la llamada Comisión Parlamentaria de Averiguación (CPI) de Crímenes Cibernéticos, creada también en la Cámara de Diputados. La CPI estaba afirmada en un requerimiento que hacía mención a una grave defraudación bancaria, y fue tribuna de una serie de discusiones que no necesariamente guardaban relación entre sí (como la militancia política virtual y el combate contra la pornografía infantil). Su informe final tomó el mismo camino que la tramitación del PL 215/2015:

reforzó iniciativas que modificaban el Marco Civil[69] para apartar del control judicial a la recolección de datos personales de usuarios de Internet junto con el sector privado[70].

Recientemente, el clima entre las autoridades de investigación y el Poder Judicial, por un lado, y las empresas proveedoras de aplicaciones de Internet, por el otro, se ha convulsionado. La retórica y el requerimiento de medidas judiciales disuasivas de carácter sumamente extremo (como los bloqueos de sitios web y aplicaciones, entre las que se destaca el sistema de mensajería *WhatsApp*) está expresando la incesante búsqueda de los bancos de datos mantenidos por tales intermediarios. Estos bloqueos están insertos en una compleja trama de *impasses* políticos y jurídicos[71], y derivan de diversos tipos de resistencias creadas por las empresas, tanto de orden técnico (como la adopción de sistemas de criptografía que no permiten la intercepción de mensajes) como jurisdiccional (bajo el argumento de que el dato solicitado estaría almacenado por otra persona jurídica de fuera del territorio nacional). Independientemente de la motivación –y, en consecuencia, de la razonabilidad– de las resistencias, los bloqueos han evidenciado un proceso de antagonismo entre ambos sectores, catalizado por la avidez de autoridades del Estado por el franqueamiento de acceso facilitado a cualquier información generada a través del uso de aplicaciones de Internet.

4.2. Eficiencia o vigilancia: recolección directa de datos por parte del sector público

Es propio de la actividad de la gestión pública el hecho de mantener información sobre el registro y la identificación de ciudadanos o sobre la utilización de servicios públicos. Datos de ese tipo

son los que permiten administrar los procesos electorales, o calcular y ajustar tarifas en el área de transportes, por ejemplo. En razón de ser el guardián de tales datos, el Estado debe velar para no comprometer su seguridad, previniendo eventuales derrames y accesos no autorizados de terceros, y crear mecanismos que impidan su utilización para finalidades no reglamentadas por ley.

En el caso de Brasil, no es difícil encontrar ejemplos que ilustren de qué manera la falta de una reglamentación sólida de protección de datos personales acaba haciendo posibles situaciones de manipulación inadecuada o no deseable de estos datos. En 2013, por ejemplo, la prensa brindó amplia cobertura a un acuerdo celebrado entre el Tribunal de Justicia Electoral y la firma Serasa Experian, autorizando el intercambio de datos registrales de los ciudadanos entre la Justicia Electoral y la empresa. En posesión de dicha información, en particular de aquella relativa a la filiación, la empresa podría enriquecer significativamente sus bancos de datos, que habrían de ser posteriormente comercializado. En la época, la enorme repercusión que alcanzó el caso obligó al Tribunal a rever el acuerdo, declarándolo cancelado poco tiempo después de su difusión.[72]

Otro ejemplo hace referencia a los datos generados a partir del uso de tarjetas como el "Billete Único", que permiten el pago anticipado de viajes en el sistema de transporte público en las metrópolis brasileñas. En San Pablo, la empresa pública responsable de la administración del servicio ni siquiera difundió su política de privacidad para la recolección y tratamiento de la información sobre los viajes de los usuarios, que bien puede revelar detalles del día a día de todos los usuarios de su sistema de transporte público.[73]

Otro caso que toca la cuestión involucra a los bancos de datos para la adquisición de medicamentos a bajo costo en el programa federal "Farmacia Popular". Este programa de descuentos permitió que empresas privadas de "gestión de programas de beneficios en

medicamentos" colectasen y almacenasen una serie de informaciones sensibles de ciudadanos sin la correspondiente organización o supervisión por parte de alguna autoridad.[74]

Como puede observarse, la discusión sobre la protección de datos establecida en el ámbito del sector público carga con una serie de particularidades. La obligatoriedad (o inevitabilidad) de provisión de ciertos datos (tales como los provenientes del uso de sistemas o servicios públicos ineludibles, como el de salud, el de transporte o el de previsión) es una de ellas, características que convierten a la recolección en significativamente diferente de los casos típicos del sector privado, marcados por la necesidad de obtención del consentimiento.

En dicho sentido, es importante la existencia de limitaciones claras que impidan la utilización de tales datos para fines diferentes a aquellos previstos originalmente. En el caso del Billete Único, por ejemplo, los datos sobre rutas y trayectos de los ciudadanos podrían constituirse en interesantes para la guarda municipal con fines de vigilancia, lo cual extrapolaría la finalidad de recolección de estos datos para gerenciar la cobranza de las tarifas por la utilización del sistema de transporte público.

El hecho de compartir datos entre diferentes órganos de la Administración Pública fue tema de reciente reglamentación en Brasil. El decreto nº 8789 del 1 de julio de 2016 regula el intercambio de bases de datos entre organismos y entidades federales. El decreto se respalda en que compartir datos sirve a la "amplificación de oferta de servicios públicos", "formulación y monitoreo de políticas públicas", "fiscalización de beneficios" y "mejora de la credibilidad de los datos" (art. 2º).

En tal sentido, abre camino a la utilización de técnicas de *big data* para mejorar la gestión pública y perfeccionar los mecanismos de fiscalización. Un ejemplo sería la posibilidad de entrecruzamiento

de datos de diferentes bancos de datos para su "confirmación", lo cual permitiría un mayor control sobre la concesión, pago o fiscalización de beneficios.[75] En el caso del programa Bolsa Familia (***NdelT: plan social brasileño de asistencia financiera a familias con necesidades básicas insatisfechas***), por ejemplo, esto ayudaría a combatir fraudes, siendo que haría posible la verificación del cumplimiento de los requisitos por el entrecruzamiento de datos, lo cual también fue informado por la prensa.[76]

Analizando los términos del decreto. Jacqueline Abreu llama la atención sobre la falta de mecanismos que resguarden la privacidad de los ciudadanos y garanticen la transparencia de las actividades. Para ella, "un programa de intercambio de datos no puede justificarse sólo en términos de eficiencia de la gestión del Estado, como lo ha hecho el gobierno hasta ahora. El programa debe instituir garantías a los individuos afectados".[77] Particularmente, ante la falta de una ley general de protección de datos personales en Brasil, Jacqueline Abreu concluye en que es preocupante que el decreto no se ocupe de tales cuestiones.

5. Conclusión

El derecho a la privacidad tiene múltiples intersecciones con el ejercicio de las libertades públicas. En tal sentido, es imposible disociar este derecho de las condiciones de vida y participación democrática de los ciudadanos, tanto en su interacción con el poder público como en sus interacciones sociales y/o de acceso a la información, cada vez más intermediadas por actores privados, propietarios y desarrolladores de plataformas como las redes sociales o los motores de búsqueda.

Desde el punto de vista de las relaciones establecidas con el sector privado, el presente artículo argumenta que: *(i)* la arquitectura de Internet permite que sean adoptadas técnicas no transparentes de recolección, tratamiento y usos de datos personales, lo que aumenta la vulnerabilidad de los usuarios frente a estos actores; *(ii)* las tecnologías de monitoreo y recolección de datos implican la transferencia irrestricta de datos a todo el mundo, exigiendo la adopción de modelos regulatorios que sean compatibles entre sí; *(iii)* el hecho de que los modelos de negocios que financian el ofrecimiento de productos y servicios gratuitos estén asentados justamente en la recolección y tratamiento de datos personales exige que sean establecidas limitaciones regulatorias para la realización de dicha actividad, bajo el riesgo de fragilizar la protección del derecho a la privacidad.

En este contexto, los desafíos para la realidad brasileña son los de: *(i)* aprobar un marco regulatorio de protección de datos personales, con el objetivo de establecer parámetros para las actividades de recolección, tratamiento y transferencias internacionales de datos ejecutadas por actores privados y que involucran a usuarios brasileños; *(ii)* promover la concientización de los usuarios en relación a los modelos de negocio adoptados por estas empresas, y de los impactos que eso le genera a su propia autonomía; y *(iii)* crear en las instituciones brasileñas, particularmente entre los miembros del Poder Judicial, una cultura de valorización del derecho a la privacidad, garantizando que la aplicación del eventual marco regulatorio adoptado haya de ser implementada con rigor.

Desde el punto de vista de las relaciones establecidas con el sector público , el presente artículo indica que: *(i)* Brasil está inserto en un contexto mundial de avance de propuestas invasivas de vigilancia, que apuestan al aumento de las capacidades de investigación y control del Estado en nombre de lo que cada gobierno considera como seguridad nacional; *(ii)* el Poder Público ha intensificado el uso de herramientas de recolección y tratamiento de datos personales para la ejecución de sus funciones en su papel de gestor público ,lo cual abre camino a nuevas formas de intercambio y uso de los datos y registros generados en tales actividades para fines de vigilancia y persecución criminal; y *(iii)* el aumento de estas prerrogativas de recolección y acceso a datos de usuarios mantenidos por actores privados amenaza las libertades democráticas, en razón de que hace posible un mayor control por parte del Estado.

En el citado contexto, los desafíos para la realidad brasileña son los de: *(i)* reglamentar la utilización de datos personales colectados por el propio Poder Público, estableciendo, inclusive, límites rigurosos al hecho de que se los comparta entre diferentes órganos de la Administración; *(ii)* preservar las garantías establecidas en el

Marco Civil de Internet, manteniendo la criba judicial como límite para la violación de la privacidad de los usuarios y el consecuente acceso a datos personales que estén en manos de actores privados; y *(iii)* promover una cultura de valorización del derecho a la privacidad como premisa para el ejercicio de las libertades democráticas, en particular en el ámbito de instituciones como el Poder Judicial, el Ministerio Público y la Policía.

6. Bibliografía

ABREU, Jacqueline de Souza, O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?, JOTA.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015.

ANDERSON, Chris, *FREE: The Future of a Radical Price*, New York: Hyperion, 2009.

ANTONIALLI, Dennys M. Indenizações por dano moral ameaçam liberdade para se fazer humor na Internet, Consultor Jurídico, 31/08/2016, disponible en http://www.conjur.com.br/2016-ago-31/dennys-antonialli-dano-moral-ameaca-liberdade-humor-internet.

_____."Watch your virtual steps: an empirical study of the use of tracking technologies in different regulatory regimes". *Stanford Journal of Civil Rights and Civil Liberties*, v. VIII, 2012.

BAILENSON, J. N.; IYENGAR, S.; YEE, N.; *et al*. Facial Similarity between Voters and Candidates Causes Influence. **Public Opinion Quarterly**, v. 72, n. 5, p. 935–961, 2008.

BRANDEIS, Louis / WAREN, Samuel, "The right to privacy", ***Harvard Law Review*** IV (1890).

BRASIL, Portal. **Governo coloca em prática ação para barrar fraudes no Bolsa Família**. Portal Brasil. Disponible en: <http://www.brasil.gov.br/cidadania-e-

justica/2016/07/governo-coloca-em-pratica-acao-para-barrar-fraudes-no-bolsa-familia>. Revisado el: 21 nov. 2016.

BRILL, Julie, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" (20.01.2014), <disponible en **http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf**, último acceso: 26.10.2016>.

BRITO CRUZ, Francisco, Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet, Universidade de São Paulo, disertación de máster, 2015.

BUTLER, Brandon. **BMW's vision for a world of connected cars**. Network World. Disponible en: <http://www.networkworld.com/article/3072687/mobile-wireless/bmw-s-vision-for-a-world-of-connected-cars.html>. Revisado el: 21 nov. 2016.

CALO, Ryan, Digital market manipulation, The George Washington Law Review, vol. 82, 2013.

CAVOUKIAN, Ann, Privacy By Design: The Seven Foundational Principles (2009), <disponible en **http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf** , último acceso: 26.6.2014>.

CRAWFORD, Kate / SCHULTZ, Jason, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

CRAWFORD, Susan / GOLDSMITH, Stephen, The Responsive City, Jossey-Bass, 2014.

EDELMAN et. al, Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords, The American Economic Review 97 1 (2007).

French lawmakers extend state of emergency after Nice attack. **Reuters**, 2016. Disponible en: <http://www.reuters.com/article/us-europe-attacks-nice-idUSKCN10009V>. Revisado el 21 nov. 2016.

GONÇALVES, Antonio Felipe de Almeida. **Balões para segurança da Olimpíada são destaque — Ministério da Justiça e Cidadania**. Disponible en: <http://www.justica.gov.br/sua-seguranca/grandes-eventos/imprensa/baloes-para-seguranca-da-olimpiada-sao-destaque>. Revisado el 19 nov. 2016.

GREENLEAF, Graham, Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) (June 16, 2013). UNSW Law Research Paper No. 2013-39.

GRUMAN, Galen. **Apple Watch: The Internet of things' new frontier**. InfoWorld. Disponible en: <http://www.infoworld.com/article/2608996/consumer-electronics/article.html>. Revisado el 21 nov. 2016.

HICKS, Jennifer. **Johnnie Walker Smart Bottle Debuts At Mobile World Congress**. Forbes. Disponible en: <http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/>. Revisado el 21 nov. 2016.

HOOFNAGLE, Chris Jay *et al*, Behavioral Advertising: The Offer You Cannot Refuse, Harvard Law and Policy Review 6, 2012.

JANSEN, Sue Curry. The Streisand Effect and Censorship Backfire. 2015. Disponible en: <http://sal.muhlenberg.edu:8080/librarydspace/handle/10718/2589>. Revisado el 19 nov. 2016.

Justiça Eleitoral repassa dados de 141 milhões de brasileiros para a Serasa - Política. Estadão. Disponible en: <http://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255>. Revisado el 21 nov. 2016.

LOVE, Brian / PICY, Emile, French lawmakers extend state of emergency after Nice attack, **Reuters**, 2016.

McDONALD, Aleecia M. / CRANOR, Lorrie Faith, ***The Cost of Reading Privacy Policies***, A Journal of Law and Policy for The Information Society 543, 544, 564 (2008).

PARISER, Eli. The filter bubble: what the Internet is hiding from you. London: Viking/Penguin Press, 2011.

RATLIFF, James D.; RUBINFELD, Daniel L. Online advertising: Defining relevant markets. **Journal of Competition Law and Economics**, v. 6, n. 3, p. 653–686, 2010.

SOLTANI, Ashkan, et al., *Flash Cookies and Privacy* (Working Paper, 2009), <disponible en **http://ssrn.com/abstract=1446862**. , último acceso: 20.10.2016>.

SOPRANA, Paula. *CPI de Crimes Cibernéticos "mutila" o Marco Civil da Internet?* Revista Época, 01/04/2016. Disponible en: **http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html**. Revisado el 18/11/2016.

SPTrans não divulga política de privacidade do bilhete único. CartaCapital. Disponible en: <http://www.cartacapital.com.br/sociedade/sptrans-nao-divulga-politica-de-privacidade-do-bilhete-unico-4526.html>. Revisado el 21 nov. 2016.

TORY. **Farmácia Popular: falta transparência sobre uso de dados médicos**. CartaCapital. Disponible en: <http://www.cartacapital.com.br/sociedade/farmacia-popular-falta-transparencia-sobre-uso-de-dados-medicos>. Revisado el 21 nov. 2016.

The Connected Aircraft: Beyond Passenger Entertainment and Into Flight Operations. Avionics Today. Disponible en: <http://interactive.avionicstoday.com/the-connected-aircraft/>. Revisado el 21 nov. 2016.

The Government just passed the most extreme surveillance law in history – say goodbye to your privacy. The Independent. Disponible en: <http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-investigatory-powers-act-a7426461.html>. Revisado el 21 nov. 2016.

TURNER, Zeke, Germans Reconsider Tough Privacy Laws After Terrorist Attacks, **Wall Street Journal**, 2016.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge

porn no Brasil. InternetLab: São Paulo, 2016.

Wahoo Fitness Announces GymConnect: Treadmill integration & control. Disponible en: <https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html>. Revisado el 21 nov. 2016.

What is the USA Patriot Web. Disponible en: <https://www.justice.gov/archive/ll/highlights.htm>. Revisado el 21 nov. 2016.

WIRTHMAN, Lisa, What Your Cellphone Is Telling Retailers About You, Forbes EmcVoice (16.12.2013) <disponible en **http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/** , último acceso: 21.10.2016>.

Notas

1. Cf. BRANDEIS, Louis / WAREN, Samuel, "The right to privacy", *Harvard Law Review IV* (1890).

2. La utilización de dispositivos como estos permite, por ejemplo, la captura de imágenes de alta resolución a la distancia, tal fuera el caso que involucró a la cantante Barbra Streisand, cuya casa fue, en 2003, sobrevolada y fotografiada por uno de estos aparatos. Al pretender impedir la difusión de las imágenes en periódicos y tabloides, la cantante acabó llamando más la atención sobre el asunto, impulsando aún más su popularización. Cf. JANSEN, Sue Curry / MARTIN, Brian, The Streisand Effect and Censorship Backfire, International Journal of Communication 9, 2015, p.656-671. Más allá de la invasión de la privacidad de personas públicas o famosas, estos dispositivos también asumieron uan importante aplicación en el campo de la vigilancia con fines de seguridad pública. Cf. GONÇALVES, Antonio Felipe de Almeida, **Balões para segurança da Olimpíada são destaque — Ministério da Justiça e Cidadania,** disponible en: <http://www.justica.gov.br/sua-seguranca/grandes-eventos/imprensa/baloes-para-seguranca-da-olimpiada-sao-destaque>, revisado el: 01 oct. 2016.

3. Cf. VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. O Corpo é o Código: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. InternetLab: São Paulo, 2016, p.2.

4. Cf. HOOFNAGLE, Chris Jay *et al*, Behavioral Advertising: The Offer You Cannot Refuse, Harvard Law and Policy Review 6, 2012.

5. Cf. Kate Crawford / Jason Schultz, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

6. Gran parte de la discusión sobre "ciudades inteligentes" pasa por cómo aprovechar los datos generados para mejorar la gestión de los espacios públicos urbanos. Cf. CRAWFORD, Susan / GOLDSMITH, Stephen, The Responsive City, Jossey-Bass, 2014.

7. Un estudio sugiere, por ejemplo, que los anunciantes de cosméticos y productos de belleza concentren sus esfuerzos publicitarios durante las mañanas de los días lunes, momento en el cual, de acuerdo con las conclusiones de la encuesta, las mujeres se sienten menos atractivas. Cf. CALO, Ryan. Digital Market Manipulation. The George Washington Law Review, vol. 82, 2013, p. 996.

8. Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Informe de investigación), disponible en: http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf, pp.35-36.

9. Cf. BAILENSON, Jeremy et. al. Facial similarities between voters and candidates cause influence. **Public Opinion Quarterly**, v. 72, n. 5, p. 935–961, 2008.

10. RATLIFF, James D.; RUBINFELD, Daniel L., Online advertising: Defining relevant markets, **Journal of Competition Law and Economics,** v. 6, n. 3, p. 653–686, 2010, p. 655. (esclareciendo que la apertura comercial de la red se debió a una nueva interpretación de las políticas de uso aceptable [Acceptable Use Policy] de la National Science Foundation, que hasta entonces sólo admitía su uso para propósitos relacionados a la investigación y a la educación).

11. Cf. BUTLER, Brandon, **BMW's vision for a world of connected cars,** Network World, disponible en: <http://www.networkworld.com/article/3072687/mobile-wireless/bmw-s-vision-for-a-world-of-connected-cars.html>, revisado el: 17 nov. 2016.

12. Cf. **The Connected Aircraft: Beyond Passenger Entertainment and Into Flight Operations**, Avionics Today, disponible en: <http://interactive.avionicstoday.com/the-connected-aircraft/>, revisado el: 17 nov. 2016.

13. Cf. Wahoo Fitness Announces GymConnect: Treadmill integration & control, disponible en https://www.dcrainmaker.com/2016/01/announces-gymconnect-integration.html, revisado el: 17 nov. 2016.

14. Cf. GRUMAN, Galen, **Apple Watch: The Internet of things' new frontier**, InfoWorld, disponible en: <http://www.infoworld.com/article/2608996/consumer-electronics/article.html>, revisado el: 17 nov. 2016.

15. Cf. HICKS, Jennifer, **Johnnie Walker Smart Bottle Debuts At Mobile** World Congress, Forbes, disponible en: <http://www.forbes.com/sites/jenniferhicks/2015/03/02/johnnie-walker-smart-bottle-debuts-at-mobile-world-congress/>, revisado el: 17 nov. 2016.

16. Cf. CALO, Ryan, Digital market manipulation, The George Washington Law Review, vol. 82, 2013, p. 1003–1005.

17. Cf. PARISER, Eli. The filter bubble: what the Internet is hiding from you. London: Viking/Penguin Press, 2011.

18. Cf. ANDERSON, Chris, FREE: The Future of a Radical Price, New York: Hyperion, 2009.

19. Una investigación realizada en 2009 indicaba ya que las 100 páginas web más visitadas en el mundo utilizaban cookies de recolección de datos personales, por ejemplo. Cf. SOLTANI, Ashkan, et al., *Flash Cookies and Privacy* (Working Paper, 2009), <disponible en **http://ssrn.com/abstract=1446862**. , último acceso: 20.10.2016>.

20. Cf. Chris Hoofnagle et al., "Behavioral Advertising: The Offer You Cannot Refuse", pp. 291-294.

21. Eso se hizo posible con la incorporación de mecanismos de posicionamiento geográfico en las aplicaciones de telefonía celular, por ejemplo. Cf. WIRTHMAN, Lisa, What Your Cellphone Is Telling Retailers About You, Forbes EmcVoice (16.12.2013) <disponible en **http://www.forbes.com/sites/emc/2013/12/16/what-your-cellphone-is-telling-retailers-about-you/** , último acceso: 21.10.2016>.

22. Un buen ejemplo de esto es el proyecto "Immersion", desarrollado por el MIT Media Lab, que demuestra cuanta información relevante puede ser colectada por la simple combinación entre los remitentes y los

destinatarios presentes en su bandeja de e-mail. Cf. https://immersion.media.mit.edu/

23. Cf. EDELMAN et. al, Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords, p. 245-246.

24. Cf. Solon Barocas / Helen Nissenbaum, On Notice: The Trouble with Notice and Consent Order 1–6 (2009) (Manuscrito no publicado), <disponible en http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf, último acceso: 26.10.2016>.

25. Cf. McDONALD, Aleecia M. / CRANOR, Lorrie Faith, *The Cost of Reading Privacy Policies*, A Journal of Law and Policy for The Information Society 543, 544, 564 (2008).

26. Cf. BRILL, Julie, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions" (20.01.2014), <disponible en http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf, último acceso: 26.10.2016>.

27. Cf. CRAWFORD, Kate / SCHULTZ, Jason, Big Data Due Process: Toward a Framework to Reddress Predictive Privacy Harms.

28. Cf. CALO, Ryan, Digital Market Manipulation, George Washington Law Review 82 (2014).

29. Para más información respecto del funcionamiento del mecanismo, cf. Jules Polonetsky / Omar Tene, "To track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising, Minnesota Journal of Law, Science and Technology 13 (2012), pp. 320-322.

30. Cf. CAVOUKIAN, Ann, Privacy By Design: The Seven Foundational Principles (2009), <disponible en http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf, último acceso: 26.6.2014>.

31. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 12 U.S.C. §§ 3401-3422.

32. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

33. Children's Online Privacy Protection Act of 1998, Pub. L. No. 106-170, 15 U.S.C.

34. Video Privacy Protection Act of 1998, Pub. L. 100-618, 18 U.S.C. §§ 2710-2711.

35. Un ejemplo es la ley de privacidad del estado de California. Cf. "The California Online Privacy Protection Act".

36. La legislación exige que los órganos de la administración pública federal recolecten solamente los datos estrictamente necesarios para el desarrollo de sus actividades, y que establezcan procedimientos para resguardar su seguridad, por ejemplo. Cf. 5 U.S.C. párrafo 552a(e)(1)-(5).

37. La legislación excluye la posibilidad de acceso del público a documentos que contengan información personal, como historias clínicas (5 U.S.C. párrafo 552(b) (6)) y registros vinculados con la seguridad pública (5 U.S.C. párrafo 552(b) (7)).

38. Cf. Seção 5 do "Federal Trade Commission Act".

39. Cf. Fair Information Privacy Principles, <disponible en **http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf**, último acceso: 26.6.2014>.

40. Para más detalles sobre la historia del desarrollo del régimen de autorregulación en los Estados Unidos, cf. Daniel Solove / Woodrow Hartzog, "The FTC and The New Common Law of Privacy", *Columbia Law Review* 114 (2014), pp.1-15.

41. Respecto del tema, cf. Marsha Blackburn, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade f the H. Comm. Of Energy and Commerce", 112th Cong. 4 (2012).

42. Cf. Artículo 1o de la Directiva 95/46/CE del Parlamento Europeo, del 24.8.1995. La Directiva 95/46/CE sufrió un proceso de reformulación, habiendo dado origen al Reglamento General de Protección de Datos Personales, aprobado el 27 de abril de 2016, que entrará en vigor el 25 de mayo de 2018. Para más detalles sobre el proceso de reforma de los parámetros regulatorios en la Unión Europea y los cambios más importantes a introducirse en 2018, cf. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

43. Es el caso, por ejemplo, de Canadá, México, Nueva Zelanda, Sudáfrica, Australia, Argentina, Colombia, Chile, etc. Para uma lista completa dos países que adotam legislações de proteção de dados pessoais Para un listado completo de los países que adoptaron legislaciones de protecciones de datos personales, cf. GREENLEAF, Graham, Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) (June 16, 2013). UNSW Law Research Paper No. 2013-39, <disponible en http://ssrn.com/abstract=2280875, último acceso: 26.10.2016>.

44. Cf. Artículo 25 de la Directiva 95/46/CE del Parlamento Europeo, del 24.8.1995.

45. Cf. Artículo 30, 1, b, de la Directiva 95/46/CE del Parlamento Europeo, del 24.8.1995.

46. Cf. US-EU Safe Harbor Frameworks, <disponible en **http://www.export.gov/safeharbor/eu/eg_main_018476.asp**.

47. El "Safe Harbor" elegía siete principios: notificación, consentimiento, acceso, seguridad, restricción de transferencias subsiguientes, limitación de finalidad y derecho de reparación.

48. La lista con las empresas participantes puede consultarse en: https://safeharbor.export.gov/list.aspx

49. Cf. Jules Polonetsky / Christopher Wolf, The US-EU Safe Harbor: An Analysis of the Framework's Effectiveness in Protecting Personal Privacy, Future of Privacy Forum (2013), <disponible en **http://www.futureofprivacy.**

org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf, último acceso: 30.10.2016>.

50. Cf. Corte de Justicia Europea, Caso C362/14, disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031

51. Cf. Privacy Shield Agreement, disponible en http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf

52. Referencia a las leyes del Registro Positivo (Ley 12.414/2011), el Código de Defensa del Consumidor (8.078/1990), y la Ley General de Telecomunicaciones (Ley 9.472/1997).

53. Fuentes: http://oglobo.globo.com/economia/defesa-do-consumidor/oi-multada-em-35-milhoes-por-invasao-de-privacidade-feita-por-velox-13348505 y http://www.justica.gov.br/noticias/ministerio-da-justica-notifica-telefonica-vivo-por-servico-smart-steps

54. Las afirmaciones referentes al proceso de elaboración y tramitación del Marco Civil de Internet pueden encontrarse en: BRITO CRUZ, Francisco, Direito, democracia e cultura digital: a experiencia de elaboração legislativa do Marco Civil da Internet, Universidade de São Paulo, disertación de máster, 2015.

55. La interpretación de estas sanciones ha causado amplia divergencia en los Tribunales brasileños. Los jueces y otros funcionarios del fuero penal han entendido que el incumplimiento de determinaciones judiciales abre espacio para requerir, por ejemplo, el bloqueo de las aplicaciones de Internet involucradas. Tal ha sido el caso de algunas de las recientes órdenes de suspensión de la aplicación de mensajería WhatsApp, impugnadas al Supremo Tribunal Federal en la ADPF 403 y en la ADI 5527.

56. Debate ejemplificado en la controversia entre el director de políticas públicas de Google Brasil, Marcel Leonardi, y la representante del "Coletivo Intervozes", Veridiana Alimonti, en sus comentarios sobre el tema durante la Semana Especial sobre Protección de Datos Personales

organizada por el InternetLab, cf. http://www.internetlab.org.br/pt/semana-especial-protecao-de-dados-pessoais/

57. Apelación TJ-RS nº 0208925-06.2014.8.21.7000.

58. Proceso nº 0805175-58.2015.4.05.8400.

59. Cf. LOVE, Brian / PICY, Emile, French lawmakers extend state of emergency after Nice attack, **Reuters**, 2016.

60. Cf. TURNER, Zeke, Germans Reconsider Tough Privacy Laws After Terrorist Attacks, **Wall Street Journal**, 2016.

61. Cf. The **Government just passed the most extreme surveillance law in history – say goodbye to your privacy**, The Independent, disponível em: <http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-investigatory-powers-act-a7426461.html>, revisado el 20 nov. 2016.

62. Cf. **What is the USA Patriot Web**, disponible en: <https://www.justice.gov/archive/ll/highlights.htm>, revisado el 20 nov. 2016.

63. Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Informe de investigación), disponible en http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

64. Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015. (Informe de investigación), disponible en http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

65. Cf. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys M. "Vigilância das comunicações pelo estado brasileiro e a proteção a direitos fundamentais" – Electronic Frontier Foundation / InternetLab, 2015.

(Informe de investigación), disponible en http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf

66. En investigación realizada por el InternetLab sobre libertad de expresión y contenidos humorísticos en Internet, se constató un desprestigio del derecho a la libertad de expresión respecto de otros derechos como el de honra e imagen, lo cual lleva atención sobre casos de identificación de usuarios de Internet por contenidos difundidos como forma de constreñimiento. Cf. ANTONIALLI, Dennys. Indenizações por dano moral ameaçam liberdade para se fazer humor na Internet. Consultor Jurídico, 31/08/2016, disponible en http://www.conjur.com.br/2016-ago-31/dennys-antonialli-dano-moral-ameaca-liberdade-humor-internet, revisado el 10 de diciembre de 2016.

67. De acuerdo al Departamento Intersindical de Asesoría Parlamentaria (DIAP). Fuente: Valor Económico, 2015, disponible en: **http://www.valor.com.br/politica/3843910/nova-composicao-do-congresso-e-mais-conservadora-desde-1964**, revisado el 20 nov. 2016.

68. InternetLab, 2015, disponible en: **http://www.internetlab.org.br/pt/noticias/pesquisadores-questionam-medidas-de-pl-sobre-crimes-contra-a-honra-na-internet/**, revisado el 18 nov. 2016.

69. Cf. SOPRANA, Paula. *CPI de Crimes Cibernéticos "mutila" o Marco Civil da Internet?* Revista Época, 01/04/2016. Disponible en: **http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-alterar-marco-civil-da-internet-no-brasil.html**. Revisado el 18/11/2016.

70. Otros proyectos y leyes aprobadas siguen la misma dirección, como la Ley Antiterrorismo (n. 13.260/2016, que establece que pueden ser considerados terroristas los ataques cibernéticos y, por lo tanto, sometidos a su régimen singular y extremo de persecución criminal) y el proyecto de ley del Senado Federal n. 730/2015, también versando sobre el retiro de exigencia de orden judicial para acceso a datos de usuarios

71. InternetLab. *Bloqueios.info*. Sitio web, 2016.

72. Cf. **Justiça Eleitoral repassa dados de 141 milhões de brasileiros para a Serasa - Política**, Estadão, disponible en: <http://politica.estadao.com.br/noticias/geral,justica-eleitoral-repassa-dados-de-141-milhoes-de-brasileiros-para-a-serasa,1061255>, revisado el 18 nov. 2016.

73. Cf. **SPTrans não divulga política de privacidade do bilhete único**, CartaCapital, disponible en: <http://www.cartacapital.com.br/sociedade/sptrans-nao-divulga-politica-de-privacidade-do-bilhete-unico-4526.html>, revisado el 19 nov. 2016.

74. Cf. TORY, F**armácia Popular: falta transparência sobre uso de dados médicos**, CartaCapital, disponible en: <http://www.cartacapital.com.br/sociedade/farmacia-popular-falta-transparencia-sobre-uso-de-dados-medicos>, revisado el 19 nov. 2016.

75. Cf. ABREU, Jacqueline de Souza, **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, JOTA, disponible en: <http://jota.info/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro>, revisado el 19 nov. 2016.

76. Cf. BRASIL, Portal, **Governo coloca em prática ação para barrar fraudes no Bolsa Família**, Portal Brasil, disponible en: <http://www.brasil.gov.br/cidadania-e-justica/2016/07/governo-coloca-em-pratica-acao-para-barrar-fraudes-no-bolsa-familia>, revisado el 19 nov. 2016.

77. Cf. ABREU, Jacqueline de Souza, **O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?**, JOTA, disponible en: <http://jota.info/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-78916-um-frankenstein-de-dados-brasileiro>, revisado el 19 nov. 2016.