

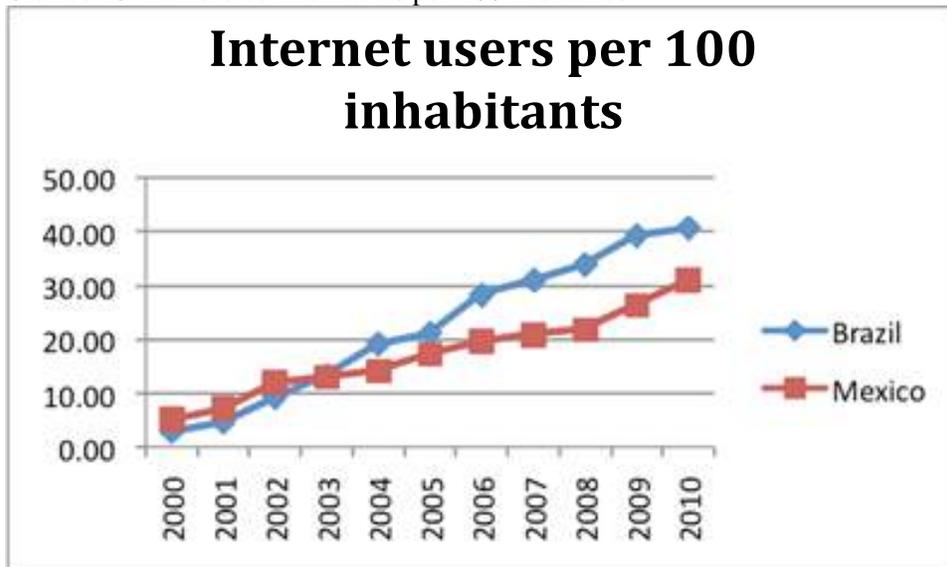
5. APARTADO ACERCA DE DATOS PERSONALES EN INTERNET

5.1 Introducción: El contexto de las condiciones de acceso a las TIC's en América Latina

Las condiciones de acceso y uso de las tecnologías de la información y de la comunicación difieren de manera sustancial en los países desarrollados y en el mundo en desarrollo. Mientras los primeros están preocupados por cuestiones relativas al uso de la red, en los últimos, la universalización del acceso sigue siendo un reto en la agenda de las políticas públicas de sus gobiernos.⁴⁰

Históricamente, El uso del internet en América Latina comienza en 1996 y evoluciona lentamente: en 1998, menos del 1% de la población estaba conectada (Hilbert, 2001), cifra que representaba a las personas con ingresos más altos. Desde este año, la participación latinoamericana en Internet comienza a ampliarse y evoluciona rápidamente, llegando a 9.9 millones en 2000, número que saltó para 60.5 millones en 2005⁴¹. El gráfico 13 presenta la evolución del número de internautas brasileños y mexicanos entre los años de 2000 y 2010:

Gráfico 13: número de internautas por 100 habitantes.



Este desarrollo fue acompañado por iniciativas del gobierno y por políticas de inclusión digital para desarrollar a la sociedad de la información. En Brasil dichas iniciativas eran asignadas al Ministerio de la Ciencia y de la Tecnología o al Ministerio de las Comunicaciones, como es el caso del “Programa Sociedad de la Información”, establecido en 1999 y del “Plan Nacional de Banda Ancha”, puesto en marcha en 2010.

Según la medición realizada por la *International Telecommunication Union* en 2008 (UIT, 2010), en los últimos años, Brasil y México han alcanzado niveles elevados de acceso y uso de las nuevas tecnologías que se llegaron a la mayoría de sus habitantes. Sin embargo, el posicionamiento de

⁴⁰ Una investigación de UNCTAD realizada en 2002 en 51 países revela las diferencias entre esos dos grupos de países en relación a las estrategias empleadas para el desarrollo de la sociedad de la información. La preocupación con la concienciación, entrenamiento y educación aparece de forma recurrente en los dos grupos. No obstante, los países desarrollados tienden a priorizar aspectos regulatorios y legales, mientras que los países en desarrollo priorizan el desarrollo de la infraestructura y la universalización del acceso (UNCTAD, 2002).

⁴¹ Datos de e-Marketer, disponibles en: www.emarketer.com/Reports/All?Latam_aug06.aspx.

estos países en el conteo mundial de desarrollo de las tecnologías de la información y de la comunicación⁴² muestra que todavía queda mucho por hacer: Brasil ocupa solamente el 60° lugar, aparece como el cuarto país en la mejor posición en el escenario latinoamericano, detrás de Argentina, Uruguay y de Chile —que aparecen en la 49ª, 50ª y 54ª posición, respectivamente— y por delante de México, que ocupa el 77° lugar. Con relación a la universalización del acceso⁴³, Brasil ocupa el 65° lugar; con relación al uso⁴⁴, el 54° y con respecto a las habilidades para el uso⁴⁵ de las nuevas tecnologías, el 61°.

Una de las consecuencias más inmediatas de este escenario es el nivel de las discusiones acerca de la regulación de la red en esos países. Por lo general, ellas todavía se muestran incipientes y o poco consolidadas, como es el caso del debate sobre la privacidad y de la recolección y del tratamiento de datos personales en América Latina.

i. Brasileños online

Según datos del Comité Gestor de Internet en Brasil (CGI.br, 2010) hoy, el 35% de hogares de Brasil poseen computadora y el 27% cuentan con acceso a Internet. Los datos muestran que la velocidad de las conexiones de internet en los hogares brasileños ha aumentado en los últimos tres años y que la principal motivación para acceder a la red es la comunicación (94%); seguida de la búsqueda de informaciones y del ocio (87% cada uno); de la educación (66%) y de los servicios financieros (17%). El correo electrónico fue la principal actividad desempeñada (80%), seguido de los servicios de mensajes instantáneos (74%) y de las redes sociales, como Orkut (70%).

La vivienda es el principal lugar de acceso a internet en el país: el 57% de los internautas usan la red desde sus hogares, mientras que el 34% utiliza las casas de acceso público, como los cibercafés. Es notable que en 2007 y 2008, el uso de estos establecimientos superaba a los accesos provenientes desde las casas, lo que muestra el importante papel desempeñado por los centros de acceso público a la inclusión digital en el país. Hoy, el 77% de los que utilizan este lugar lo hacen por no tener computadora en casa y el 72% por no tener conexión de internet. La diversión, la sociabilidad y los juegos en línea también aparecen como motivaciones para el uso de los cibercafés y fueron mencionados por el 40%, el 25% y el 20% de los internautas brasileños, respectivamente.

Algunas estadísticas están relacionadas a las prácticas de seguridad y acceso a datos personales. Del total de usuarios que usan internet en área urbana, un 20% identificó los dispositivos de seguridad, como contraseñas, registros, nombres de usuario y pruebas *anti-Spam* como una dificultad en el uso de la gestión de internet. Entre quienes han utilizado el internet, pero nunca han comprado productos por la red, un 29% señaló como uno de los motivos para no hacerlo la preocupación por la privacidad o seguridad y dijeron que se resistían a suministrar información o datos personales, como la tarjeta de crédito por internet. El 15% de la población que usa el internet mencionó la preocupación por la protección o la seguridad de sus datos como motivo para no usar el gobierno electrónico.

⁴²Para realizar esta medición, el informe se basa en un indicador denominado IDI (ICT Desarrollo Tecnológico), que considera diversos indicadores relacionados con el acceso, uso y habilidades en el manejo de tecnologías de la información y la comunicación. El primer y segundo grupo aparecen con un peso de 40 años, y por último, un peso de 20.

⁴³ El índice de acceso está dado por cinco indicadores: la proporción de hogares con computadoras, la proporción de hogares con acceso a Internet, acceso de banda ancha para los usuarios de Internet, la penetración de líneas telefónicas fijas y penetración de líneas telefónicas de celular (ITU, 2010)

⁴⁴ El índice de uso está calculado con base en el número de usuarios de Internet por cada cien habitantes, el número de suscriptores de banda ancha por cada cien habitantes y el número de abonados a Internet móvil de banda ancha por cada cien habitantes (ITU, 2010).

⁴⁵ El índice de habilidad está dada por la tasa de alfabetización de adultos y por la GER (Tasa bruta de matriculación) en la educación de los grados segundo y tercero (ITU, 2010).

ii. Mexicanos online

De acuerdo con la información disponible derivada de los estudios hechos por la *IWS Corporation* sobre América Latina y el Caribe que comprende 20 países; Brasil, es el país más poblado de la región (201 millones 103 mil 330 habitantes), concentra el mayor número de usuarios de Internet en la zona (75 millones 943 mil 600). La penetración de Internet en Brasil (37.8%) fue superior al promedio mundial (28.7%) y al promedio en la zona (34.5%).

México, el segundo país más poblado en América Latina (112 millones 468 mil 855 habitantes), es la segunda nación con el mayor número de usuarios de Internet en la zona (30 millones 600 mil). Sin embargo, el acceso de Internet en México (27.2%) fue inferior al promedio mundial (-1.5%) y al promedio en la zona (-7.3%).

En cuanto al acceso de Internet en la población, la más elevada se presentó en Argentina (64.4%); luego en Uruguay (52.8%); Chile (50%), Colombia (48.7%). Costa Rica (44.3%), Brasil (37.8%), Venezuela (34.2%), República Dominicana (30.5%) y Panamá (28.1%). Cabe destacar que México fue ubicado en la posición diez en la región.

Sin embargo, México es el país con el mayor número de usuarios de Facebook en América Latina (15 millones 37 mil 20). Su penetración fue establecida por la *IWS* en 13.4%. Ello se debe a que en 2010 fueron considerados 112 millones 468 mil 855 habitantes en el territorio nacional. La *IWS* omitió precisar el “índice Facebook” en México, el cual, de acuerdo con estimaciones asciende a 49.14%. Ello significa que de cada 10 usuarios de Internet, 5 son usuarios de Facebook. Debemos tener presente que la *IWS* estimó en 35% el “índice Facebook” en la región.

De acuerdo con los resultados obtenidos en *The Global Information Technology Report 2009-2010* (Foro Económico Mundial), México fue ubicado en la posición 78 de entre 133 países que fueron analizados. En el estudio correspondiente al periodo 2008-2009, en la posición 67. En el periodo 2007-2008, en el lugar 58 de 127 países analizados. De acuerdo con los resultados de los estudios realizados por el Foro Económico Mundial, en el periodo 2007-2010 México descendió 20 posiciones en materia de competitividad tecnológica. Los resultados obtenidos en determinados indicadores considerados en el estudio *The Global Information Technology Report 2009-2010* resultan sumamente reveladores. Por ejemplo, en “disponibilidad de las nuevas tecnologías” México fue ubicado en la posición 79; en materia de leyes relativas a las nuevas tecnologías, lugar 67; número de líneas telefónicas, 67; seguridad de los servidores de Internet, 60; accesibilidad al contenido digital, 87, ancho de banda, posición 80; teléfonos en el hogar, 108; tarifas ancho de banda, 73; tarifas de telefonía móvil, 79; tarifas de telefonía fija, posición 100; prioridad de las tecnologías de información y comunicaciones (*TIC*) para el gobierno, 96; contratación pública de productos de tecnología avanzada, 93; importancia de las *TIC* en la visión del gobierno del futuro, 74; suscripciones teléfonos móviles, 91; usuarios de Internet, 79; acceso de Internet en las escuelas, 77; capacidad de innovación, 80; grado de utilización de Internet en negocios, 78; éxito del gobierno en la promoción de *TIC*, posición 100. En materia de la calidad de la enseñanza de las matemáticas y las ciencias, México fue ubicado en el lugar 123.

De esta manera, y con base en los resultados de la *Global E- Government Survey 2010*, reporte anual que realiza la *United Nations Public Administration Network* –órgano de Naciones Unidas– para evaluar la efectividad de las estrategias y acciones emprendidas por los gobiernos en materia de e-gobierno, México fue ubicado en la posición 56. En el estudio correspondiente a 2008, en la posición 37. Es necesario puntualizar que un plazo de dos años México descendió 19 posiciones en el ranking mundial.

Ahora bien, es necesario mencionar que los principales estudios sobre los usuarios de Internet en México coinciden en advertir la existencia de una marcada brecha por género en el acceso a Internet. De acuerdo con lo asentado en el estudio de la AMIPCI, 55% son hombres y 45% mujeres. En cambio, de acuerdo con los resultados que arrojó el estudio del *WIP* en el capítulo dedicado a México, la distribución por género fue establecida así: 58% hombres y 42% mujeres. Asimismo, En México la mayoría de los usuarios de Internet son jóvenes: 61% de los usuarios tiene menos de 25 años –cifra sin considerar a los menores de 12 años–. Además 76% son menores a 32 años.

5.1.1. TIC's y protección de datos personales en América Latina

El escenario de desarrollo de nuevas tecnologías de información y comunicación, en particular de Internet, trae consigo un nuevo paradigma para la protección de datos personales. Por un lado, tenemos la facilidad de transportar, almacenar y procesar información, lo cual se acelera vertiginosamente junto con la evolución de las TIC's. Por otro lado, tenemos las características específicas del funcionamiento y arquitectura de Internet, que consisten, en última instancia, en la transferencia de archivos entre computadoras repartidas por todo el mundo, cuyo uso está estrechamente relacionado con prácticas de registro. En Internet, todo puede ser rastreado, almacenado, codificado y muchas de estas prácticas están asociadas, inclusive los protocolos de mantenimiento y operación de la red.

Esta nueva realidad nos lleva a la necesidad de regular las prácticas y los flujos de comunicación en este nuevo escenario. No obstante, en el bloque latinoamericano, sólo algunos países están más próximos al debate en torno a la protección de datos personales, sea en espacios académicos o jurídicos. Chile fue el primero en tener una ley consolidada sobre el tema (19.628), seguido por Argentina (25.326), que se destaca por ser el único país en el grupo cuya legislación es reconocida como adecuada por los estándares de la Unión Europea. En Uruguay, surgió una ley específica sobre el tema en el año 2004, siendo derogada con la publicación de la nueva ley en 2008 (18.331). Y en Colombia el debate sobre el tema es más reciente, aunque el país ya tiene una ley para proteger los datos personales (Nougrères et al., 2008).

En México, es en el año de 2010 cuando se aprueba la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), la cual tiene como finalidad regular su tratamiento legítimo, controlado e informado. Como se ha señalado para el caso de los CCTV y de la cédula de identidad, en un contexto de desarrollo de las tecnologías de información y comunicación, la LFPDPPP se ha presentado como una necesidad y diversos sectores de la sociedad y del ámbito público señalaron la necesidad de conformar esta regulación frente a la ausencia de está.

En este sentido, la ley llega a fortalecer la incipiente normatividad que regula el acceso a la información y la protección de datos por parte de las autoridades y reconoce como sujetos regulados a las personas físicas o morales de carácter privado, tales como empresas, comercios, escuelas particulares, etcétera; pero exceptúa de su aplicación a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y a las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Lo anterior en virtud de que la Ley para Regular las Sociedades de Información Crediticia establece un procedimiento jurídico específico para la protección de la información de las personas físicas y morales con motivo de la recopilación, manejo y entrega o envío de información relativa a su

historial crediticio, de operaciones crediticias y otras de naturaleza análoga.

Desde un punto de vista legal la LFPDPPP está orientada a:

- garantizar la privacidad de las personas, es decir, debe proteger la información particular o propia de aquello que se realiza a la vista de pocos.
- Constituir el derecho a la autodeterminación informativa, el cual consiste en reconocer a los individuos la libertad para que puedan saber qué información ha sido anotada, archivada, empleada o retransmitida por cualquier método; quién, cuándo y con qué fin se hizo.

En otras palabras, establece un cauce procesal para que los individuos gocen de protección jurídica respecto al tratamiento de su información personal, pues su automatización e informatización, además de suponer un riesgo a su vida privada, conlleva el uso, divulgación o almacenamiento de datos personales, por cualquier medio.

El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Finalmente establece una serie de principios y derechos, cuyos límites para su observancia y ejercicio, son: la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Con esta Ley, el gobierno federal en México ha pretendido regular algunas de las principales acciones que en materia de seguridad está llevando a cabo, tales como la proliferación de video vigilancia y la implementación de una cédula de identidad de carácter único. La ley también supone un avance en la regulación informática, aunque, como se referirá más adelante, la discusión en este ámbito no es muy frecuente debido, en alguna medida, a la amplitud de problemáticas que pueden ser derivadas del tema de Internet.

Entre los países económicamente más importantes de América Latina, Brasil es el único que aún no cuenta con una ley para proteger los datos personales. Hoy día, hay tres principales marcos normativos en el país sobre el tema: el referente a la privacidad, que aparece como una garantía fundamental de la Constitución Federal; la acción de *habeas data*, que reconoce al individuo el derecho de controlar su propia información y la protección de datos de los consumidores, que refiere a los casos relacionados con las iniciativas de procesamiento de la información. En la actualidad, la consolidación de un régimen integrado se encuentra en discusión en el país a través de un proyecto de ley para la protección de datos personales, que pretende proteger al ciudadano también en el espacio virtual⁴⁶. Con ello, se espera regular las prácticas comunes en la red, como el procesamiento de datos para la dirección de anuncios publicitarios y contenidos relevantes, o bien, como la transferencia de esta información entre diferentes empresas; son puntos de especial preocupación en relación con el problema de la protección de datos personales en Brasil.

5.2 Datos personales en Internet en Brasil

5.2.1 Cómo fue realizado el mapeo de Internet en Brasil

El mapeo tuvo por objeto la identificación de actores relevantes en los procesos de vigilancia y control de datos personales en la Internet brasileña. Fueron planteadas seis áreas en el mapeo —

⁴⁶ El proyecto de ley sobre protección de datos personales en Brasil se inspiró en la Directiva 95/46/CE de la Unión Europea y pasó por un período de consulta pública y ahora espera que sea presentada al Congreso Nacional.

legislación, estudios académicos, tecnologías, corporaciones/instituciones, movimientos de la sociedad civil y eventos— aplicándose metodologías específicas a cada una, mismas que se detallan a continuación

i. Legislación

Objetivo General:

Revisar la legislación brasileña a nivel nacional y estatal, que busca identificar leyes, proyectos de ley y marcos de reglamentación relacionados al tratamiento de datos personales en el Internet en Brasil.

Objetivos Específicos:

- a) Identificar leyes vigentes y proyectos de ley a nivel nacional y en tres estados brasileños: Rio de Janeiro, São Paulo y Paraná;
- b) Identificar los legisladores, sus partidos políticos y las regiones del país que representan;
- c) Identificar el año de proposición de la ley o del proyecto de ley;
- d) Identificar los temas más recurrentes relativos a la regulación de los datos personales en el Internet en Brasil;
- e) Identificar los actores responsables de la regulación de datos personales en el Internet en Brasil.

Bases de datos consultadas:

- a) Sistemas de búsqueda en línea del sitio electrónico del Senado Federal (<http://www.senado.gov.br>);
- b) Sistemas de búsqueda en línea del sitio electrónico de la Cámara de los Diputados (<http://www.camara.gov.br>);
- c) Sistemas de búsqueda en línea de los sitios electrónicos de las Asambleas Legislativas de los estados de Rio de Janeiro (<http://www.alerj.rj.gov.br>), de São Paulo (<http://www.al.sp.gov.br>) y de Paraná (<http://www.alep.pr.gov.br>).

Metodología:

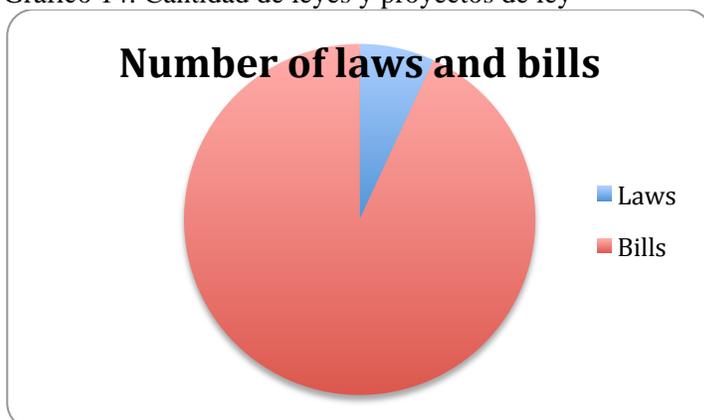
Se analizaron los proyectos de ley y la legislación vigente a nivel nacional y en tres estados brasileños: Rio de Janeiro, São Paulo y Paraná. La selección de los estados consideró aquellos que ya se mostraban con algún avance en la reglamentación del ciberespacio, con el fin de evaluar si, en este contexto, la cuestión de los datos personales también era planteada.

La metodología adoptada se basa en visitar las páginas web en donde se encuentran los proyectos de ley y de la legislación vigente en de la Cámara de los Diputados, del Senado Federal y de las Asambleas Legislativas de los estados escogidos, buscando por el término “internet” en cada uno de ellos⁴⁷. Las páginas de resultados fueron exploradas entre noviembre de 2010 y febrero de 2011, y todos los proyectos o leyes relacionados al tema fueron registrados para un análisis posterior.

En total fueron analizadas 8 leyes y 108 proyectos de ley, lo cual representa un total de 116 registros. El gráfico 14 muestra la cantidad de proyectos pertinentes por instancia analizada.

⁴⁷ Como los buscadores de estos sitios fueron poco útiles, prescindimos de los términos más específicos que componen el diccionario de palabras clave en esta investigación y decidimos buscar sólo por Internet, revisando todos los resultados encontrados. Fueron 832 de los proyectos de ley de la Cámara, 113 de los proyectos de ley del Senado, 116 de la legislación federal en vigor, 493 de los proyectos de ley de la Asamblea Legislativa del Estado de São Paulo, 124 de la legislación vigente en el estado, 493 de los proyectos de la Asamblea Legislativa del Estado de Río de Janeiro, 49 de la legislación vigente en el estado, 30 de los proyectos de ley de la Asamblea Legislativa del Estado de Paraná y 11 de la legislación vigente en el estado.

Gráfico 14: Cantidad de leyes y proyectos de ley



El análisis del material empezó con la creación de un diccionario de temas⁴⁸ y con la clasificación manual de los asuntos más recurrentes. Para cada ley o proyecto, se utilizaron tres tipos de índices: uno principal, que circunscribe la relación del proyecto con la investigación; unos temáticos, para medir la recurrencia de temas, actores y acciones; y los índices de la justificativa, asignados a partir de la lectura de esta sección de los proyectos en la cual los autores argumentan sobre sus objetivos y sobre la importancia del asunto.

Resultados:

a) Descripción General: temas más recurrentes

Identificamos que, de modo general, los tipos de proyectos y leyes vigentes se repitieron con significativa frecuencia, tanto en el nivel federal como en el nivel estadual. Listamos abajo los temas más recurrentes en los resultados encontrados:

responsabilización de cibercafés, solicitando **registro e identificación del usuario** (lo que incluye, a veces, el empleo y uso de cámaras de vigilancia en esos establecimientos), buscando cohibir el crimen y/o proteger a niños y adolescentes;

adopción de medidas para garantizar la seguridad en el internet, que creen una tipificación y designen sanciones para los crímenes practicados a través de la red, como fraudes, falsificaciones, invasiones, interceptación y/o violación de datos, propagación de softwares maliciosos, pornografía y pedofilia etc.;

proyectos de **prohibición del anonimato** y creación de mecanismos de **registro y identificación**, ya sea para el **acceso a la red** (en los proveedores de acceso) o para **oferta y uso de servicios** diversos, como publicación de sitios, blogs, interacción en foros, uso de direcciones electrónicas y registros de dominios; muchos de esos proyectos determinan también **almacenamiento de comunicaciones y logs de acceso de los usuarios**;

disciplinación del acceso y del uso, con adopción de mecanismos de **clasificación indicativa** para el control del acceso a sitios/contenidos adultos; creación de programas educativos en escuelas y propuestas de instalación de **filtros de contenido** en instituciones de enseñanza, reparticiones públicas o aún su ofrecimiento por proveedores de acceso al público en general;

recibimiento de mensajes comerciales no solicitadas (considerado, a veces, como invasión de privacidad, lo que genera el debate con respecto a la obtención de la dirección de correo electrónico del destinatario);

reglamentación de la validez de la firma digital, mediante registro previo y del documento

⁴⁸ Consultar en el Anexo X el diccionario de temas empleado en la clasificación de Leyes y Proyectos de Ley, así como se frecuencia en valores absolutos y porcentajes.

electrónico (frecuentemente como medida de reglamentación del comercio electrónico); **reglamentación de la concesión de datos para investigaciones policiales y de espionaje**, de carácter nacional o internacional, a través de Internet, bien como la institución de delegaciones especializadas en crímenes informáticos.

b) Actores:

Fueron identificados los siguientes actores:

proveedores de acceso a Internet, de hospedaje, de email o de servicios diversos (salas de chat, listas de discusión, foros, sitios web de contenido para adultos y portales);

autores (de sitios y blogs);

interactores/usuarios de esos sitios y servicios;

dueños de cibercafés y establecimientos de juegos electrónicos;

instituciones de enseñanza e investigación (escuelas, universidades etc.);

órganos y entidades de la administración pública.

Los actores más recurrentes fueron los proveedores, que aparecen en 34% de los proyectos/leyes analizados, y entre los interactores/usuarios los niños y adolescentes, que aparecen, cada uno, en 15% de los proyectos/leyes.

c) Niveles de Responsabilización

La mayor parte de los proyectos de ley busca la responsabilización de administradores de la red, proveedores y usuarios por prácticas que involucran identificación y manejo de datos personales. Fueron observados los siguientes niveles de responsabilización de los actores identificados:

corresponsabilidad del proveedor de servicio o dueño del sitio por el contenido publicado para los interactores: el responsable por el sitio debe moderarlo, retirando contenidos impropios e identificando prácticas ilícitas o sus autores;

responsabilización de los autores de correos electrónicos o de comentarios y publicaciones en sitios por los contenidos publicados;

responsabilización de los proveedores, instituciones y dueños de sitios por el disciplinamiento del acceso y del uso, con la formulación de códigos de conducta/seguridad a los cuales estarían sometidos los usuarios;

responsabilización de los proveedores de acceso y servicios, entre ellos los dueños de cibercafés, por la identificación de usuarios a partir del mantenimiento de logs y datos de registro por cierto período de tiempo (determinado o no);

responsabilización de proveedores de acceso y servicios por la seguridad y por el funcionamiento de los sistemas ofrecidos al público;

responsabilización de los proveedores de acceso y servicios por la protección de los datos almacenados (datos de registro, logs o contenido de las comunicaciones de los usuarios).

d) Clasificación de los proyectos/leyes según sus implicaciones para el tratamiento y la regulación de datos personales en Internet

Fue posible clasificar casi la totalidad de los proyectos/leyes en seis grandes rúbricas, según temas/prácticas buscadas y sus consecuencias para el tratamiento y la regulación de datos personales en Internet:

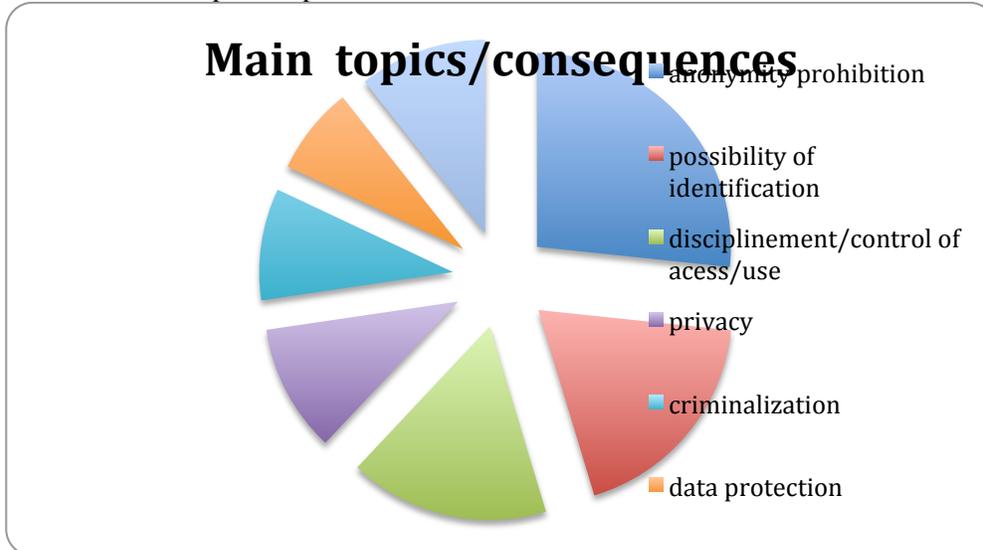
34% institucionalizan rutinas de registro y implican la prohibición del anonimato;

- 24% presuponen la adopción de prácticas que implican la identificación de dueños de sitios, interactores, infracciones y/o infractores;

- 22% involucran el disciplinamiento/control del acceso y/o del uso de la red, y prevén la adopción de filtros de contenido y mecanismos/códigos de conducta que regulen el acceso a sitios considerados inadecuados (especialmente para menores);

- 14% incluyen medidas de defensa de la privacidad;
- 12% se dedican a definir crímenes practicados a través de la red mundial de computadoras;
- 9% encaminan la protección de datos, con adopción de prácticas en favor de la seguridad de las transacciones en la red.

Gráfico 15: Principales tópicos/ consecuencias



e) Tendencias observadas

A partir de la clasificación realizada en el ítem anterior, se presentan las siguientes tendencias:

Privacidad: privilegio de la seguridad que resulta en el esfuerzo de tipificar crímenes y vetar el anonimato

Un conflicto fundamental se manifiesta de forma recurrente en los proyectos y leyes analizados: la intención de proteger la privacidad se confunde con premisas de seguridad y figura casi siempre lado a lado con la intención de vetar el anonimato, de modo que se garantice la seguridad en la red y se combata el crimen. Esta afirmación puede ser corroborada por el significativo porcentaje de proyectos que prevén registro (47% del total) y por el no menos extenso número de proyectos de tipificación criminal o que mencionan en el texto de su justificación la intención de impedir el uso de la red para la práctica de actos ilícitos (67% del total).

Gráfico 16: Red de leyes y proyecto de leyes e indexadores

Entre los proyectos que prevén registro, observamos que el 16% incluye la previsión del almacenamiento de un log de acceso. Otra constante fue la institucionalización de la necesidad de asociar la identidad civil a un terminal o IP, lo que hiere de forma profunda el derecho a las redes abiertas.

Cabe destacar, en este contexto, la adición del Senado al Proyecto de Ley de la Cámara 89/2003, conocida como PL Azeredo. Ya aprobado en el Senado y en trámite en la Cámara de Diputados, se presenta como un proyecto que busca frenar la escalada de los crímenes virtuales, en especial la pedofilia. No obstante, su texto posee inconsistencias que dejan entrever consecuencias que amenazan a las prácticas fundamentales en la cibercultura, criminalizando incluso acciones de uso compartido y acceso a las redes P2P con base en principios de propiedad intelectual. El proyecto instituye la necesidad de mantenimiento de registros de acceso, lo que puede atrasar aún más iniciativas de inclusión digital, y la criminalización de prácticas comunes, como la transferencia de datos o información disponible en una red de computadoras, un dispositivo de comunicación o un sistema informático sin autorización de su legítimo titular.

Cibercafés y prohibición del anonimato

Entre los proyectos/leyes que implican prácticas de prohibición del anonimato en el acceso a Internet, uno de los más recurrentes consiste en la reglamentación del uso de los cibercafés con vistas a prohibir el anonimato en los accesos realizados a través de estos establecimientos: 18% de los proyectos analizados encaminan el tema, y casi la totalidad de esas leyes/proyectos instituye la colecta de datos de registro y de navegación para uso de las computadoras, siendo que algunos prevén, inclusive, la adopción de cámaras de vigilancia en estos ambientes. Parte de estas leyes/proyectos, teniendo en vista el bienestar y la protección del menor, adoptan medidas de disciplinamiento del uso, como la prohibición del acceso de menores de 12 años; reglamentación de condiciones para acceso de los menores de 18 años, prohibición de la venta de cigarrillos y bebidas alcohólicas, y adopción de medidas para garantizar la salud de los usuarios de esos establecimientos (iluminación y volumen adecuados de los equipos de cómputo, así como la determinación de un límite de horas de uso). Los tres estados analizados ya poseen leyes en este sentido⁴⁹.

Protección de niños y adolescentes y los filtros de contenido

La protección de niños y adolescentes apareció como el segundo objetivo/justificativa más recurrente, figurando como la intención de 19% de las leyes/proyectos. Además de la reglamentación de los cibercafés y de la definición de los crímenes informáticos, la obligatoriedad de la oferta de filtros de contenido aparece como tema recurrente, también asociado a este público. Buscando impedir el acceso indebido a sitios en hogares, escuelas y en la administración pública, los filtros fueron citados en 13% de los proyectos/leyes, tanto en el nivel federal como en el nivel estatal, frecuentemente acompañados por la idea de la instauración de mecanismos de clasificación indicativa, presente en 11% de los proyectos analizados.

Correo Basura y *Opt-Out*

El combate contra el spam es el cuarto objetivo/justificativa más frecuente, figurando en 10% de los proyectos. Además del correo basura, el término *opt-out* también fue recurrente, apareciendo cada uno en 9% de los proyectos/leyes analizados. Muchas veces, estos proyectos están relacionados con la intención de impedir la diseminación de virus y programas maliciosos y, por consiguiente, evitar el crimen. En algunos, aparece la preocupación en torno a la privacidad del usuario y de la obtención de su dirección de correo electrónico.

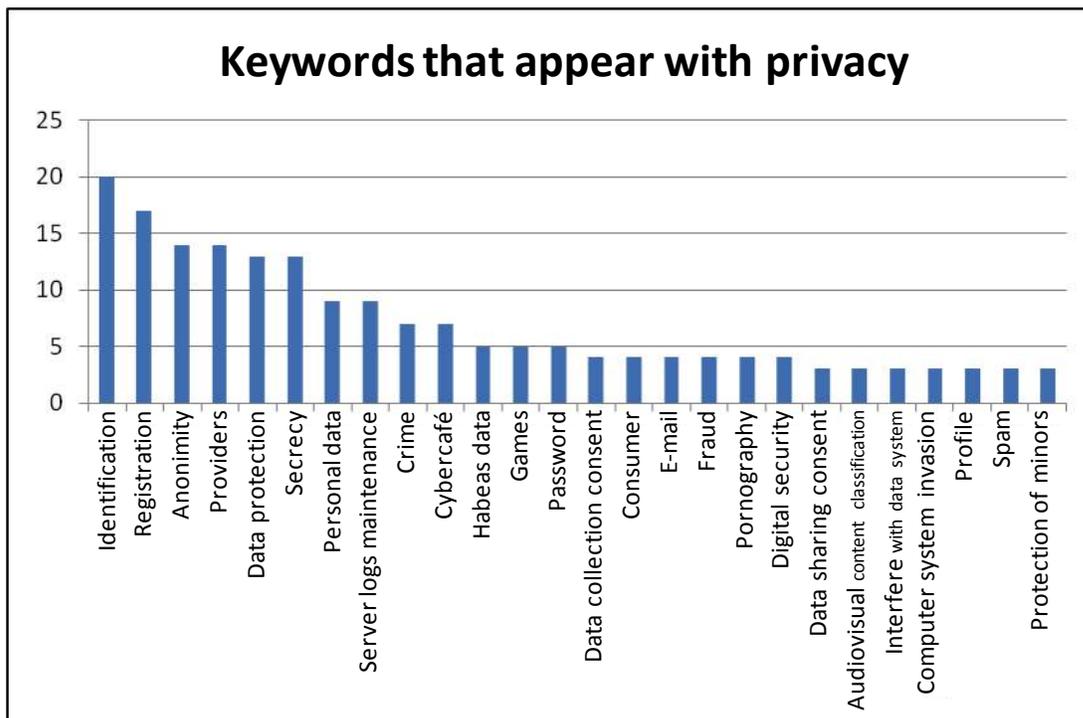
⁴⁹ En Sao Paulo se tiene La ley 12.228/2006, en Rio de Janeiro, la ley 5.132/2007 y en Paraná la ley 16.241/2009.

Protección de datos personales y privacidad: una preocupación ‘menor’

El número de proyectos/leyes cuyo objetivo principal estaba en la garantía de los principios de la protección de datos y de la privacidad fue de 5%. Temas como la anuencia del usuario para colecta/procesamiento/distribución de datos fueron registrados en 6%, 2% y 5% de los proyectos y leyes analizados, respectivamente. La notificación para colecta de datos apareció en 2% y el derecho de acceder a, conocer y/o corregir las informaciones almacenadas en esas bases, en 4%. En general, estos proyectos también incluyeron la defensa de la inviolabilidad de las comunicaciones electrónicas —salvo mediante orden judicial— y la protección de los datos delicados, como orientación sexual, religiosa, política, datos de salud, entre otros.

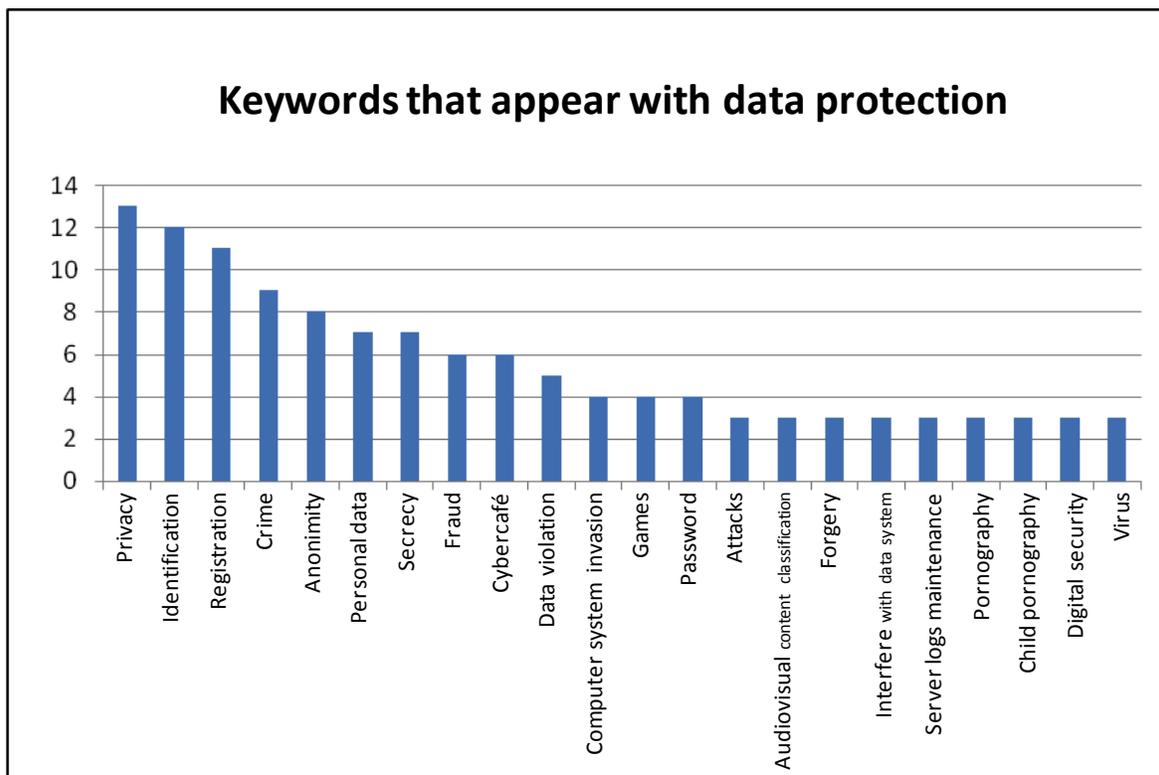
Cuando consideramos los proyectos que abordan el tema de la privacidad, pero que no lo tienen como punto principal, el índice de recurrencia aumenta al 26%. En estos casos, la garantía de la privacidad apareció, muchas veces, en proyectos enfocados en la prohibición del anonimato, vislumbrando la necesidad de un registro y de que se vinculen a la protección de datos. El gráfico 17 presenta la distribución de los aspectos que más aparecieron al lado del término privacidad:

Gráfico 17: indexadores vinculados a privacidad.



El contexto de los proyectos asociados a la protección de datos está relacionado, a su vez, con la privacidad y con la esfera del crimen (y, por ende, con la coacción del anonimato y con las prácticas de registro) y con la seguridad de datos. Se evidencia en el gráfico 18 la frecuencia de conceptos que aparecen asociados al término. Se nota la presencia de términos como fraude, invasión, contraseñas, ataques, interferencia en sistemas de datos y virus:

Gráfico 18: indexadores vinculados a la protección de datos



En muchos casos, la única noción asociada a la protección de datos personales presentada por los proyectos analizados consistía en responsabilizar a la instancia a la que se le exigía el registro, mantenimiento de bitácoras de acceso y/o almacenamiento de mensajes por mantenerlos en la confidencialidad, buscando asegurar así la privacidad de los usuarios. Aunque estos proyectos consideren la necesidad de que se regule la formación de bases de datos mantenidas, en muchos casos, por las empresas proveedoras de servicio, su propósito, en la mayor parte de los casos, está en la prevención de crímenes practicados a través de Internet. Este escenario fue observado en el 22% de los proyectos/leyes analizados. Además de eso, es preciso problematizar la perspectiva de que esta regulación sea suficiente para asegurar la privacidad de los usuarios y el derecho a la libertad de expresión en Internet.

Contexto discordante: marco civil de Internet y ley de protección de datos personales

En el ámbito federal, dos propuestas abiertas a consulta pública por el Ministerio de Justicia se destacan por su relevancia y por discordar de este contexto hegemónico. Una de ellas, la del Marco Civil de Internet en Brasil, consiste en la tentativa de establecer una legislación que determine derechos y responsabilidades en el uso de los medios digitales, orientada hacia la garantía de derechos, y no hacia la restricción de libertades. La propuesta, presentada a la sociedad para su discusión por la Secretaría de Asuntos Legislativos del Ministerio de Justicia, en cooperación con la Escuela de Derecho de Rio de Janeiro de la Fundación Getulio Vargas, recibió más de 2 mil contribuciones durante la consulta pública sobre el asunto. Fue enviada al Congreso Nacional el 24 de agosto de 2011, y ahora será discutida por la Cámara de Diputados y el Senado Federal.

El anteproyecto invierte la curva propuesta por las iniciativas de criminalización, buscando definir primero un conjunto de derechos en lugar de priorizar esfuerzos de tipificación criminal. Dicho anteproyecto define responsabilidades y derechos para usuarios y proveedores de acceso, buscando asegurar la privacidad y la libertad de expresión en la red. Asimismo, prevé que el resguardo de registros de acceso a servicios de Internet dependerá de la autorización del usuario, así como el respeto a normas y directivas relativas a la protección de datos personales. Eso implica que el usuario debe ser claramente informado sobre la finalidad del registro de sus datos. Implica también establecer qué prácticas de tratamiento, distribución y acceso de terceros a sus datos deban depender de su autorización. El anteproyecto garantiza además que los usuarios puedan acceder y corregir sus datos y que su identificación sólo sea asociada a los registros guardados mediante autorización judicial, lo que, sin duda, representa una evolución significativa en relación al PL Azeredo y similares.

Otra iniciativa relevante y central para este informe, también abierta a consulta pública, busca crear una ley de protección de datos personales en el país. El anteproyecto de ley sobre el tema también fue propuesto por el Ministerio de Justicia, esta vez en cooperación con el Observatorio Brasileño de Políticas Digitales del Centro de Tecnología y Sociedad de la Fundación Getulio Vargas de Rio de Janeiro. Buscando anclar el derecho a la privacidad, garantizado constitucionalmente en el país, la propuesta se dirige frontalmente hacia el escenario reciente de proliferación de datos personales en las redes digitales de comunicación, así como de la facilidad de acceso a, distribución y tratamiento de esa información. En este contexto, el anteproyecto defiende que el uso de esa información sea definido con base en las elecciones del titular de las informaciones, y no de acuerdo con la voluntad de aquellos que acceden a/almacenan esos datos. Y para garantizar su operación, prevé la creación de una Autoridad de Garantía responsable, entre otras atribuciones, de la fiscalización de la ley, aplicación de sanciones e interlocución con sectores de la sociedad.

El anteproyecto define “dato personal” como "cualquier información relativa a una persona identificada o identificable, directa o indirectamente, incluyendo toda dirección o número de identificación de una terminal utilizada para conexión a una red de computadoras". Prevé que los individuos sean informados de la colecta de sus datos en el momento en que esta ocurre y que no se disponga de ellos sin previa autorización de su titular. El anteproyecto prevé también que los usuarios sean informados de las posibles consecuencias de su negativa a permitir el uso de datos, y buscar proveer condiciones para que éste ocurra de forma exacta, lícita y con buena fe, dentro de las finalidades previstas. El titular de los datos tiene asegurado su derecho de revisarlos, corregirlos o cancelarlos y, de manera semejante, tiene garantizado el derecho de no ser sometido a decisiones que le afecten, de manera significativa, realizadas por un mero tratamiento automatizado de datos personales destinado a definir su perfil o personalidad. En este punto, el anteproyecto prevé, incluso, que los ciudadanos puedan solicitar explicaciones sobre los parámetros usados en decisiones de esta naturaleza.

ii. Estudios académicos

Objetivo General:

Efectuar un mapeo preliminar de la producción académica relativa a la problemática de los datos personales en el Internet en Brasil.

Objetivos Específicos:

- a) Identificar a investigadores sobre el tema en Brasil, así como las instituciones a las que pertenecen.
- b) Identificar el desarrollo, por año, de la producción académica sobre el tema.

c) Identificar los temas asociados a la problemática del tratamiento y de la regulación de datos personales en Internet en la producción académica brasileña.

Bases de datos consultadas:

- a) Portal de Periódicos Capes
- b) Redalyc

Metodología:

Con el propósito de constituir un panorama de la producción académica y científica relacionada con la protección de datos personales en Internet en Brasil, analizamos 56 periódicos nacionales indexados en el Portal de Periódicos Capes y el índice latinoamericano de Redalyc. En cada uno de ellos, buscamos las siguientes palabras clave, analizando los resultados obtenidos y registrando los artículos pertinentes:

protección de datos + Internet
datos personales + Internet
vigilancia + Internet
monitoreo + Internet
privacidad + Internet
libertad de expresión + Internet
copyright
derechos de autor + Internet
cibercrímenes
crímenes digitales
seguridad digital
seguridad de datos + Internet
regulación + Internet

Las búsquedas fueron realizadas entre los meses de febrero y abril. En el Portal Capes, la búsqueda se restringió a los periódicos enfocados en publicaciones nacionales en las siguientes áreas: Derecho, Comunicación, Ciencia de la Información y Ciencia de la Computación. Ya en el Redalyc, la búsqueda fue efectuada por las palabras clave en portugués y en español, y se consideró, además de los artículos de investigadores nacionales, aquellos de investigadores extranjeros cuyo contexto era Brasil.

En los casos en que el sitio del periódico no contaba con un buscador, el análisis fue hecho manualmente, salvo algunos raros casos en que el volumen de artículos era extremadamente elevado. Antes de realizar la búsqueda, evaluamos el funcionamiento del buscador, optando por usar solamente la palabra Internet en los casos en que el empleo de términos específicos no ofrecía resultados.

Fueron almacenados datos básicos sobre los artículos considerados pertinentes y sus autores. En esta etapa, dichos artículos fueron evaluados también respecto de su vínculo con el tema (A para los más relacionados; B para los menos relacionados). Al final, todo el material registrado pasó por un proceso de clasificación temática, el cual precisó ser automatizado dada la gran cantidad de artículos.

Para evidenciar los temas más abordados, creamos un diccionario de 201 términos con base en el análisis manual de un cuerpo de 50 artículos. Después, fue producido un script que buscó por cada uno de los términos en todos los artículos, registrando el número de apariciones. Finalmente, cada artículo fue clasificado con los aspectos que aparecieron tres veces o más, ordenados por relevancia (del más recurrente al menos recurrente).

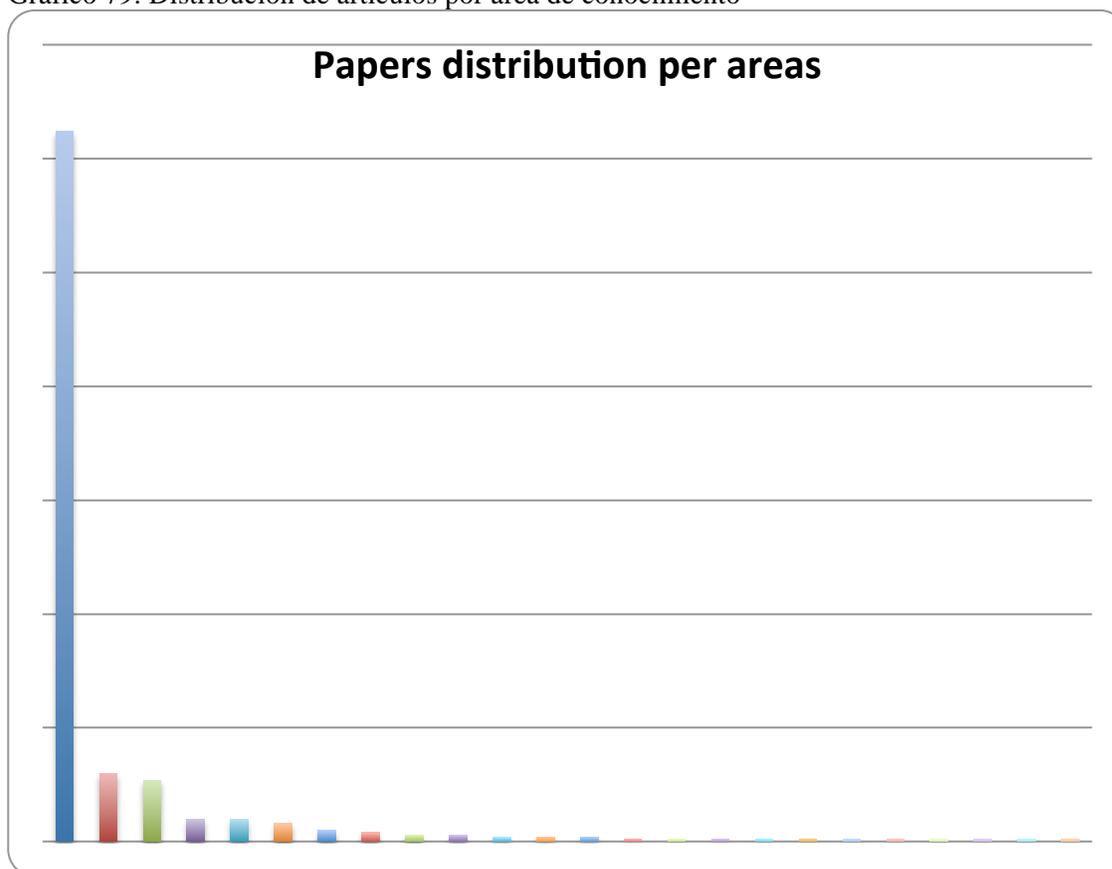
Resultados:

Datos Generales

El conjunto de las búsquedas realizadas dio como resultado 5.358 artículos. De éstos, 429 estaban relacionados con el tema, de los cuales 342 tenían grado de relación A y 87 grado de relación B.

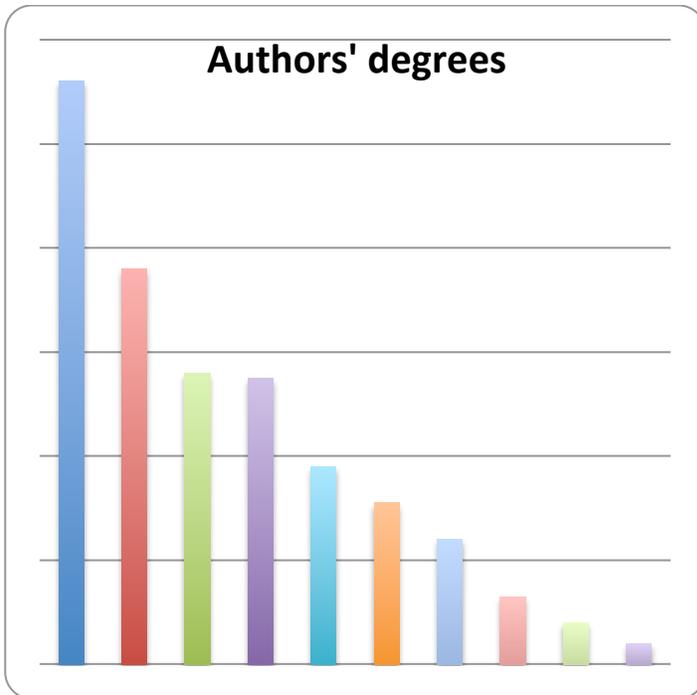
Los datos colectados muestran una prominencia evidente de discusiones provenientes del área de Derecho: 73% de los artículos encontrados pertenecen a esta área del conocimiento. Enseguida, tenemos el área de Comunicación, con 7% y la de Ciencias de la Computación, con 6%. Sociología, Ciencias de la Información y Bioética aparecen luego abajo en el ranking, cada una con 2%. El gráfico 19 muestra la distribución del número de artículos por área del conocimiento.

Gráfico 79: Distribución de artículos por área de conocimiento



En relación con el grado académico de los autores, observamos que la mayoría son Doctores. Enseguida, aparecen los licenciados, con representatividad 32% menor. La cantidad de Maestros y especialistas, a su vez, no presentó gran variación. La gran mayoría de los autores viene del área del Derecho, seguida por investigadores del área de Ciencias de la Información, Ingeniería y Comunicación. El gráfico 20 presenta la distribución de los autores por titulación:

Gráfico 20: Nivel educativo de los autores



El periódico que presentó más resultados relacionados con el tema fue Jus Navegandi, del área de Derecho, en donde encontramos 252 artículos. Vale la pena resaltar que el sitio publica a la vez contenido no tan estrictamente académico, con carácter de opinión, y artículos científicos en el formato estándar, lo que contribuye a la sobresaliente cantidad de resultados observados.

En relación con la distribución de los artículos encontrados en la línea del tiempo, constatamos que los primeros trabajos sobre el tema comienzan a surgir en 1996. El número de artículos se mantiene prácticamente estable hasta 1998, a partir de aquí observamos una tendencia de crecimiento rápido y acentuado que se extiende hasta el 2000. A partir de entonces, el número de artículos relacionados con el tema se estabiliza en un nuevo nivel, que se mantiene durante toda la década de 2000. En los gráficos 21 y 22 se presenta el número de estudios por año. Se observa, en el gráfico 22 que abarca la última década, que la línea de tendencia, ajustada por el método de los mínimos cuadrados, es una recta paralela al eje, lo que representa la estabilización del número de investigaciones anuales.

Gráfico 81: distribución artículos/año (1996-2000)

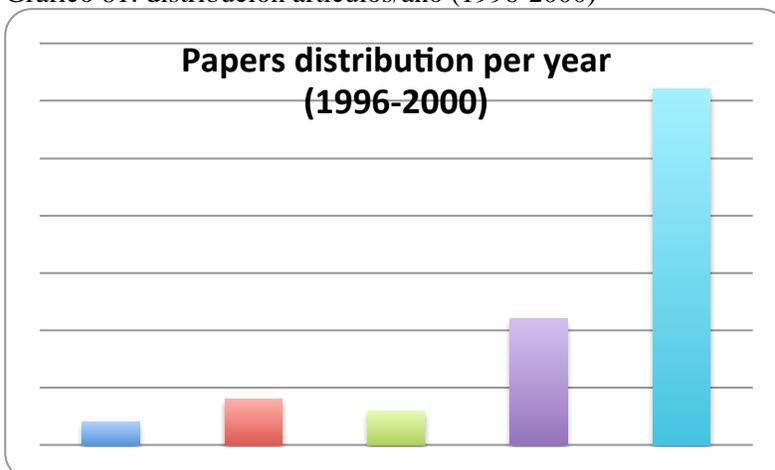
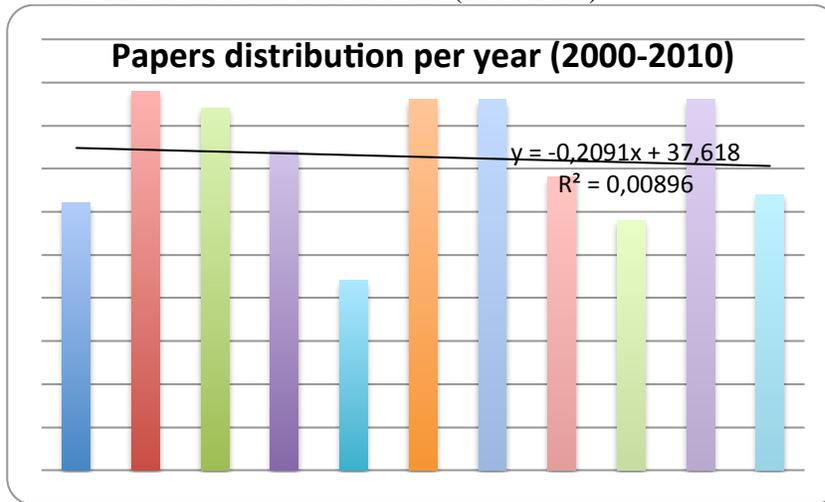


Gráfico 22: distribución artículos/año (2000-2010)



Actores

Fueron identificados los siguientes actores en la producción académica sobre el tema del tratamiento y de la regulación de datos en el Internet en Brasil:

Investigadores (la mayoría Doctores, como puede verse en el gráfico 20). También puede apreciarse en el gráfico los autores cuya producción destaca dentro de las revistas con mayor número de artículos.

Instituciones de investigación y enseñanza;

Vehículos de publicación académica. Una clasificación de los periódicos según el número de publicaciones sobre el tema se puede apreciar en el gráfico 23.

Gráfico 23: Revisas y autores

Journal and authors

This chart shows journals with more articles and identifies the most prominent authors. Areas are sized according to the amount of articles.

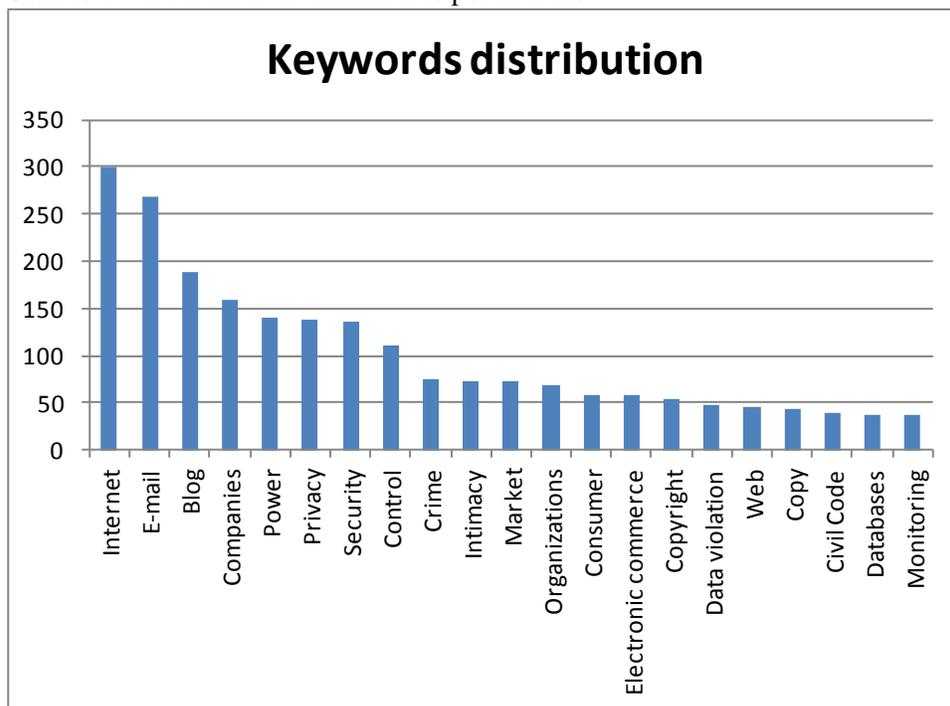


c) Tendencias

Recurrencias y relaciones temáticas

El análisis de los indicadores más frecuentes describe una ley de potencia, lo que indica que algunos cuantos temas aparecieron muchas veces, mientras que un número grande de temas variados presentó recurrencia muy baja: aparecieron pocas veces. Vea enseguida el gráfico con los 21 aspectos más frecuentes. El término Internet apareció 300 veces y lidera la clasificación, seguido de los conceptos e-mail (269), blog (189), empresas (160), poder (141), privacidad (138), seguridad (135), control (110), crimen (74), mercado (72) e intimidad (72). Es preciso resaltar también la recurrencia de los aspectos “derecho de autor” y “copia”, y del par “violación de datos” y “monitoreo”, asociados a la esfera de la seguridad, posicionados entre los 20 primeros de la clasificación. Este análisis considero como indexadores las palabras del diccionario que aparecieron por lo menos cinco veces en un determinado artículo.

Gráfico 24: frecuencia de indicadores por artículo



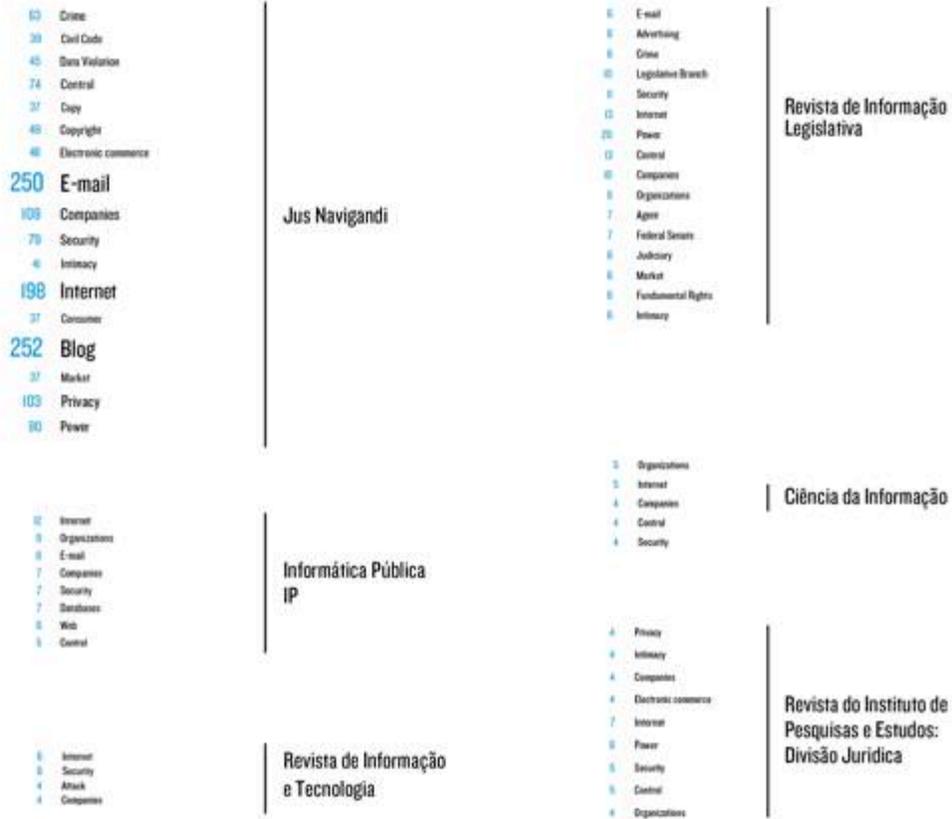
La recurrencia de indicadores por área del conocimiento revela que en Derecho las discusiones en torno a los temas “privacidad” e “intimidad” son más recurrentes que en otras áreas del conocimiento. Ya el término “vigilancia” fue más frecuente en los trabajos de Comunicación y Sociología, mientras que la esfera de la seguridad, que ocupó el quinto lugar de la clasificación en las áreas de Derecho, Informática y Sociología, fue menos recurrente en Ciencias de la Información y en Comunicación. Estas dos últimas áreas presentaron más discusiones sobre los agentes inteligentes y sobre la personalización, mientras que Derecho abordó con más frecuencia el tema del derecho de autor. Ya en la Bioética, los temas salud, violación de datos, biopoder y discriminación fueron más frecuentes que en las demás áreas.

También fue posible identificar, en las revistas con el mayor número de artículos pertinentes, los temas más frecuentes, como muestra el gráfico 25.

Gráfico 25: Indexadores por revista

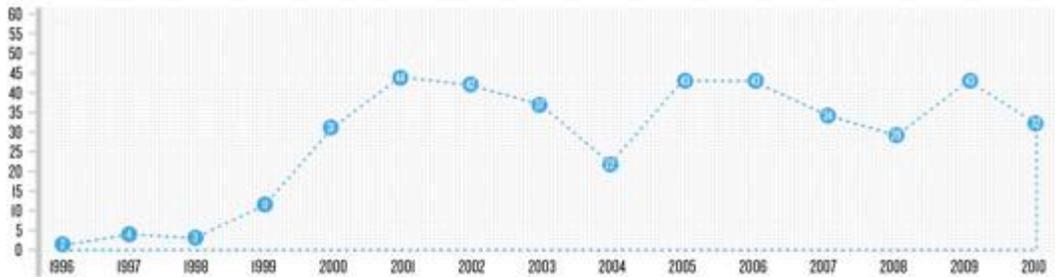
Articles keywords per journals

This chart shows the number of articles with the most frequent keywords in each journal. The keywords selected were mentioned in each paper at least three times.



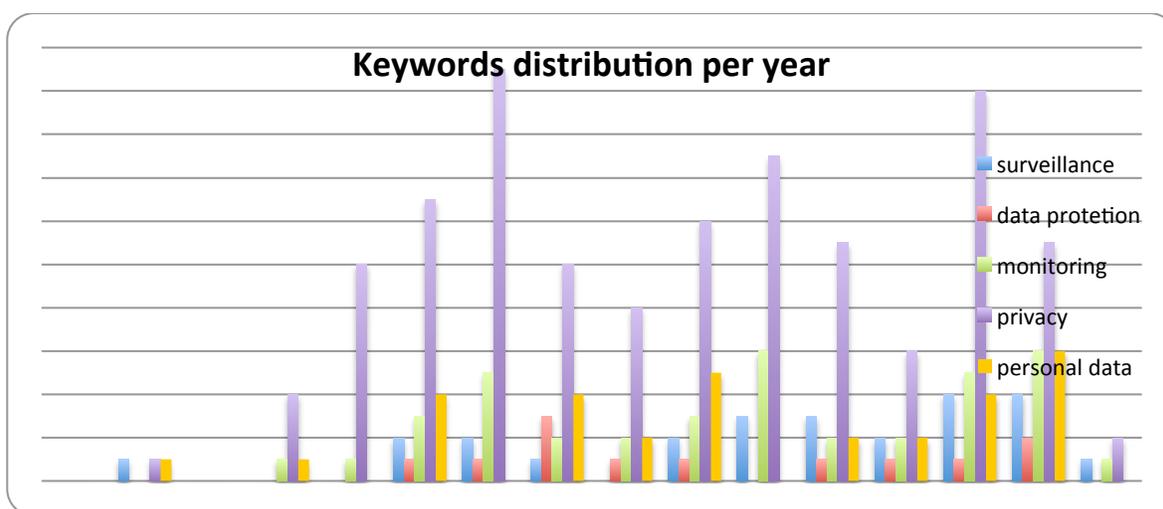
Articles Timeline

Number of papers published per year



Finalmente, observamos que la distribución del número de artículos que contienen los indicadores “vigilancia”, “protección de datos”, “monitoreo”, “privacidad” y “datos personales” no presentó variación significativa a lo largo de los años, y tendió a reproducir la curva de la distribución de artículos en la línea del tiempo. De manera general, la hegemonía del término “privacidad” se mantuvo, así como la frecuencia con que se abordan los temas “vigilancia”, “datos personales” y “protección de datos”, comparativamente bastante menor.

Gráfico26: distribución de los indexadores clave por año



iii. Eventos

Objetivo General:

Investigar eventos relacionados con la regulación/protección de datos personales en el Internet en Brasil.

Objetivos específicos:

- Identificar el tipo y el año de realización del evento.
- Identificar las instituciones promotoras.
- Identificar los principales temas discutidos.

Bases de datos consultadas:

Sitios electrónicos de noticias y de organizaciones

Metodología:

Fueron investigados, en sitios electrónicos de organizaciones y en sitios electrónicos de noticias, eventos relacionados con la regulación y la protección de datos personales en el Internet en Brasil. Los resultados pertinentes fueron registrados en una planilla, que contiene: nombre del evento, fecha de realización, instituciones promotoras, tipo (taller, seminario etc.) y temas discutidos. Las búsquedas fueron realizadas entre los meses de octubre y diciembre de 2010

Resultados:

Datos Generales

Fueron identificados 22 eventos en total, realizados en 2009 y 2010, en formatos de seminarios, debates, conferencias y encuentros (Anexo V). En cuanto a las temáticas más relevantes, cuatro

eventos tuvieron como tema central la protección de datos personales, tres de ellos fueron promovidos por instancias ministeriales (ministerio público y ministerio de justicia), en cooperación con la UERJ, FGV, el Comité Gestor de Internet en Brasil, y uno por la Red Latinoamericana Habeas Data. Se destaca también el tema del establecimiento del marco civil del Internet en Brasil, prioritario en seis eventos, dos de ellos fueron promovidos por el Foro Internacional Software Libre -PUC RS; los otros cuatro eventos acerca del marco civil fueron promovidos por el Instituto CONIP, por la ALERJ, por el Ministerio de Justicia y FGV y por la FEDERASUL. El contexto latinoamericano fue el contexto de cinco eventos, y el contexto específicamente brasileño fue priorizado en 9 eventos.

Actores

Fueron identificados los siguientes actores relevantes entre las instituciones promotoras de los eventos:

Ministerios: Ministerio de Justicia y Ministerio Público Federal

Instituciones de investigación académica: FGV, Escuela Nacional de Defensa del Consumidor, UERJ, Unibrasil, UFSC, PUC RS, FAPEAL, Universidad Blas Pascal, PUC PR

Federaciones: FEBRABAN, FECOMERCIO, FEDERASUL

Asociaciones, Consejos, ONGs, Redes: Carta Mayor, Foro Internacional Software Libre, OAB-SP, Instituto CONIP, ALERJ, Asociación Brasileña de Derecho de Informática y Telecomunicaciones, Red Latinoamericana de Habeas Data, SEBRAE/AL

Empresas: OWASP, Now Digital

Tendencias

Cabe destacar la inversión del gobierno brasileño (vía ministerio público y ministerio de justicia), en los últimos cinco años, en la promoción de eventos en cooperación con la sociedad civil con el objetivo de discutir marcos civiles regulatorios con implicaciones directas sobre el tratamiento de datos personales en el país, tomando en cuenta, especialmente, las redes digitales de comunicación distribuida, como Internet. Esta tendencia es corroborada por la presencia de los referidos ministerios entre las instituciones promotoras más recurrentes de eventos relativos a la protección de datos personales.

iv. Instituciones y Gobierno

Objetivo general: identificar a las instituciones y organizaciones cuyas programaciones y prácticas tengan implicaciones en el tratamiento, la regulación y/o gobierno de datos personales en el Internet en Brasil.

Objetivos específicos:

- a) Mapear las áreas de actuación de las instituciones identificadas.
- b) Identificar, en el ámbito de las instituciones identificadas, las prácticas y acciones recientes de modo que se indiquen sus implicaciones para el tratamiento y la regulación de datos personales en el Internet en Brasil.

Bases de datos consultadas:

Sitios de periodismo, de noticias y de organizaciones.

Metodología:

Fueron investigados, en las bases de datos mencionadas en el ítem anterior, informaciones, documentos y materias que permitiesen la identificación de instituciones y organizaciones nacionales cuyas programaciones y prácticas tengan implicaciones en el tratamiento y la regulación

de datos personales en el Internet en Brasil. Los resultados pertinentes fueron registrados en una planilla para análisis posterior, según las siguientes categorías: nombre de la institución y/u organización, área de actuación, prácticas, acciones recientes y enlace para el sitio electrónico de la institución y/u organización. Las búsquedas fueron realizadas entre los meses de octubre y diciembre de 2010.

Resultados:

Descripción General

Fueron identificadas cuatro instituciones relevantes para el tratamiento, la regulación y/o gobierno de datos personales en el Internet en Brasil: Observatorio del Marco Civil; Programa Cultura Digital; Comité Gestor de Internet; Debate Público Protección de Datos Personales (Anexo VI).

Actores:

Los actores identificados consisten básicamente en las instituciones identificadas:

Observatorio del Marco Civil;

Programa Cultura Digital;

Comité Gestor de Internet;

Debate Público sobre Protección de Datos Personales

Entretanto, vale resaltar que tales instituciones se caracterizan por una composición “híbrida”, involucrando a instancias gubernamentales, corporaciones no gubernamentales, dispositivos tecnológicos y la participación de la sociedad civil. Tal composición puede ser visualizada en las prácticas de estas instituciones, descritas en el anexo VI.

Tendencias:

Conforme a lo apuntado en el ítem anterior, percibimos, entre las instituciones identificadas, una composición de carácter híbrido que busca vincular a diferentes actores —gubernamentales, no gubernamentales, tecnológicos y civiles— en la discusión sobre las redes digitales de comunicación distribuida y sus impactos en la sociedad brasileña. Todas las instituciones identificadas se empeñan fuertemente en la participación de la sociedad civil en este debate, utilizando como una de las herramientas principales el propio Internet. La temática del tratamiento de datos personales en Internet es buscada más directamente por el Debate Público sobre Protección de Datos Personales, que mantiene una posición más clara en cuanto a la promoción de marcos regulatorios de protección de datos personales. La cuestión de los datos personales en Internet también está presente en las otras tres instituciones, en estos casos vinculadas a contextos más amplios de la regulación y gobierno de Internet y de las prácticas que caracterizan a la cultura digital.

v. Movimientos, acciones y organizaciones de la sociedad civil

Objetivo general: identificar los movimientos, acciones y organizaciones cuyas prácticas contribuyan para la promoción del debate público y de la participación de la sociedad en la reflexión sobre el tratamiento y la regulación de datos personales en el internet en Brasil.

Objetivos específicos:

- a) Mapear las áreas de actuación de los movimientos y organizaciones identificados.
- b) Identificar prácticas y acciones recientes con implicaciones para la promoción del debate público y la participación de la sociedad en la reflexión sobre el tratamiento y la regulación de datos personales en el Internet en Brasil.

Bases de datos consultadas:

Sitios de periódicos de circulación nacional, de noticias y de organizaciones.

Metodología:

Fueron investigadas, en las bases de datos mencionadas, información, documentos y materias que permitiesen identificar movimientos y organizaciones nacionales cuyas prácticas tengan implicaciones para la participación de la sociedad civil en el debate público sobre el tratamiento y la regulación de datos personales en el internet en Brasil. Los resultados pertinentes fueron registrados en una planilla para su posterior análisis, según las siguientes categorías: nombre del movimiento y/u organización, área de actuación, prácticas, acciones recientes; enlace para el sitio electrónico del movimiento y/u organización. Las búsquedas fueron realizadas entre los meses de octubre y diciembre de 2010.

Resultados:

a) Descripción general

Han sido identificados 9 movimientos y organizaciones de la sociedad civil cuyas prácticas y acciones favorecen, en mayor o menor medida, la participación de la sociedad brasileña en el debate público sobre regulación y tratamiento de datos personales en Internet. (ANEXO VII). Estos movimientos y organizaciones se distribuyen en diferentes áreas de actuación: derechos humanos, derecho del consumidor, derecho a la comunicación, producción de conocimiento e innovación en tecnologías de la comunicación, activismo político en Internet, defensa de la libertad de expresión en el Internet, protección de datos personales y defensa del derecho a la privacidad en las redes digitales de comunicación

b) Actores:

Han sido identificados los siguientes actores:

Habeasdata

Partido Pirata

Foro del Consumidor

Datos Personales

Instituto NUPEF (Núcleo de Investigaciones, Estudios y Formación)

Intervozes

Instituto CONIP (Conocimiento, Innovación y Prácticas de TI en la Gestión Pública)

Mega Não

Ciberactivismo

Las áreas de actuación, y las prácticas recientes de cada actor pueden ser visualizadas en el anexo VII

c) Tendencias

Aunque el número de actores relevantes de la sociedad civil brasileña sea reducido, notamos su progresivo crecimiento en los últimos años. Se nota también que el tema de la regulación y del tratamiento de datos personales en Internet, cuando no es buscado directamente (como en el caso de la organización Habeas Data, que actúa en favor de una política de protección de estos datos), va a la par con el debate de la militancia en el sentido de la garantía de derechos fundamentales (privacidad, libertad de expresión, entre otros) en el ámbito de las redes digitales de comunicación distribuida.

vi. Tecnologías

Objetivo General:

Identificar a las principales tecnologías utilizadas para capturar, tratar o proteger los datos personales en Internet. Estas tecnologías son generalmente designadas por el término “tracker”

(rastreador).

Objetivos específicos:

- a) Rastrear e identificar los tres principales mecanismos de monitoreo y captura de datos personales (cookies, flash cookies y web beacons) en uso en los cinco sitios que figuran entre los 15 más visualizados en Brasil y en las dos redes sociales más populares del internet en Brasil;
- b) Identificar la función de las cookies y de los beacons utilizados y clasificarlos en tipos, midiendo la variedad de tipos presentes en las redes sociales y sitios analizados;
- c) Identificar a las empresas responsables por los cookies y web beacons utilizados en las redes sociales y en los sitios relacionados, así como sus principales prácticas;
- d) Analizar las políticas de privacidad en las redes sociales y en los sitios relacionados de modo que se verifique el nivel de transparencia en cuanto al uso de los mecanismos de colecta y monitoreo de datos personales identificados.

Bases de datos consultadas:

Cinco sitios que figuran entre los 15 más visualizados por los brasileños: Terra, UOL, Globo.com, Yahoo.com y YouTube⁵⁰.

Dos sitios de red social más populares en Brasil: Orkut y Facebook⁵¹.

Metodología:

En la investigación de los sitios se identificaron y analizaron las cookies HTML, Flash cookies⁵² y beacons⁵³ presentes en cuatro portales (Terra, UOL, Globo.com y Yahoo.com) y un sitio para compartir videos (YouTube). Esta investigación fue complementada por el análisis de las políticas de privacidad de estos sitios, de modo que se observe su conformidad con las prácticas y tecnologías empleadas, así como el nivel de transparencia de la información suministrada al usuario acerca de estas prácticas y tecnologías.

En relación a los sitios de red social, fenómeno extremadamente popular en el país, fueron

⁵⁰ De acuerdo con la clasificación de Alexa, disponible en <http://www.alexa.com/topsites/countries/BR>. Esta medición es realizada con base en la combinación del promedio diario de visitantes y del número de visualizaciones a lo largo del último mes.

⁵¹ El uso de redes sociales en el país consiste en una particularidad brasileña en el escenario latinoamericano. Comienza con la popularización de Orkut, lanzado por Google en 2004. El sitio ganó versión en Portugués en 2005 y acabó teniendo su operación transferida de California a Brasil en 2008, debido a la adhesión en masa en el país. Hoy, los brasileños responden por 50,6% de los usuarios del sitio, según datos del propio Orkut (disponibles en <http://www.orkut.com/MembersAll>). Es visitado por 73% de los internautas activos en el país en marzo de 2010, según datos del IbopeNetRating (Rodrigues: 2010, online).

El crecimiento de Facebook en el país es un fenómeno más reciente, que se aceleró a partir de 2009. Entre agosto de 2009 y agosto de 2010, el sitio pasó de 1,5 millones de visitantes para 9 millones, según datos de comScore. Aún así, Orkut continúa al frente. En el mes de agosto de 2010, por ejemplo, Orkut recibió 29,411 millones de visitantes y Facebook, 8,887 millones de visitas. En el mes analizado, 36,059 millones de usuarios de 15 años o más visitaron un destino de red social en el país.

⁵² Los cookies son pequeños archivos guardados en la computadora del usuario. Pueden ser enviados por el sitio visualizado o por servidores de terceros y permiten atribuirle un identificador a un usuario. Esta información queda guardada en su computadora y a partir de ella es posible monitorear su navegación, además de obtener datos sobre el acceso realizado, como la dirección IP, sistema operativo utilizado etc.

Los cookies flash funcionan como los cookies html, pero sólo pueden ser utilizados con aplicaciones flash. La administración e identificación de estos archivos por parte de los usuarios es menos transparente que la de los cookies html, hecho a partir del propio navegador del usuario y por un protocolo abierto y no propietario.

⁵³ Web beacons permiten el monitoreo de los usuarios sin colocar un archivo en su navegador, como hacen los cookies, lo que disminuye el poder de control del usuario y hace más complejo el rastreo. A pesar de usar también una solicitud a un servidor para enviar un archivo, esta técnica no guarda un identificador en la computadora del usuario. En ella, el monitoreo es hecho a través del acompañamiento de las variables de las sucesivas solicitudes de este archivo. Un ejemplo de esta técnica es el empleo de web bugs, imágenes de un pixel, transparentes – y por lo tanto invisibles – usadas para hacer el rastreo.

identificados y analizados los cookies html y web beacons asociados a las cinco aplicaciones más usadas en Orkut y en Facebook⁵⁴. Esta selección fue basada en las clasificaciones de popularidad ofrecidas por los propios sitios. De este modo, se consideró el uso de las aplicaciones por todos los usuarios, y no sólo por el público brasileño.⁵⁵

La metodología de identificación y análisis de los trackers, inspirada en una medición del uso de trackers en sitios americanos realizada por el The Wall Street Journal (Valentino-Devries: 2010, online), consistió en visitar los sitios analizados excluyendo el registro de cookies del navegador antes y después de cada visita. En cada sitio, fueron visitadas cerca de 30 páginas aleatoriamente, buscando diversificar la navegación y teniendo cuidado para evitar el acceso a enlaces externos⁵⁶.

Los cookies flash fueron analizados de forma semejante, usándose el Website Storage Settings Panel, un mecanismo de la propia Adobe que posibilita la visualización de este tipo de rastreador⁵⁷. Ya para el análisis de los web beacons, contamos con la ayuda del software Ghostery⁵⁸, que ya identificaba a la empresa responsable por el tracker. En el caso de los cookies (html y flash), recurrimos al dominio usado para hospedar al tracker para esta identificación.

Las búsquedas fueron realizadas entre los meses de enero y marzo de 2010. La última etapa de la investigación consistió en analizar, en el sitio de las empresas responsables por los trackers encontrados, las políticas de privacidad, los mecanismos de opt-out y las informaciones prestadas a los usuarios sobre los servicios ofrecidos y las tecnologías de captura de datos personales empleadas. Con base en estos datos, los cookies y beacons fueron clasificados, de modo que sean evidenciadas las tendencias, prácticas y actores predominantes.

Resultados:

a) Datos generales:

Fueron encontrados un total de 334 archivos de cookies html en los cinco sitios analizados, 174 eran provenientes de servidores de terceros. Considerando solamente los cookies no repetidos, tenemos 53. Identificamos solamente 2 cookies flash, colocados por el propio sitio visitado, y 25 web beacons, excluyéndose a los repetidos. El gráfico 27 demuestra la distribución de estos trackers por sitio analizado.

Gráfico 27: cookies y beacons por sitio analizado

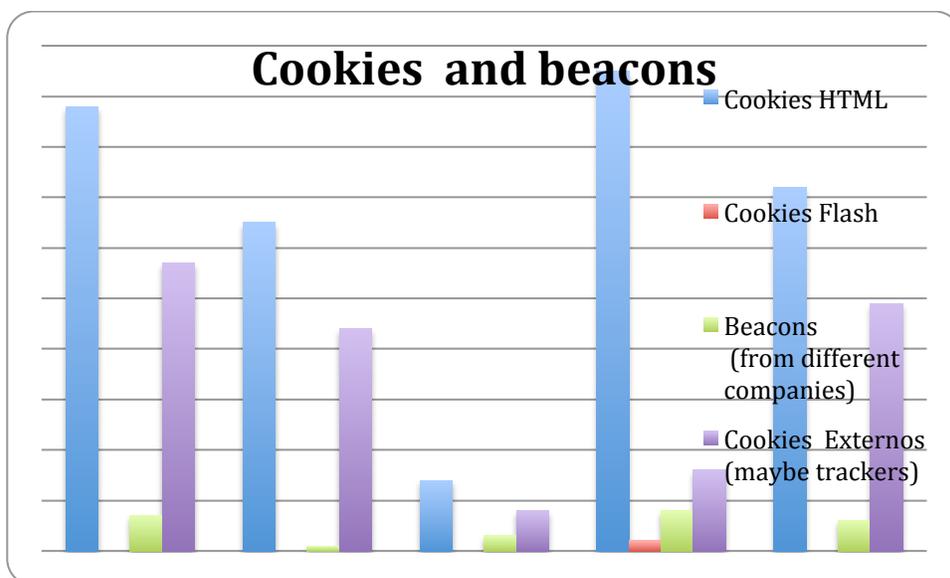
⁵⁴ Como los usuarios de redes sociales se identifican con el sistema de registro de las empresas que ofrecen este servicio no es necesario emplear rastreadores para recoger datos de carácter personal o perfil de usuario. Por lo tanto, nos dedicamos al análisis de las aplicaciones sociales desarrolladas por las empresas asociadas que operan en estas plataformas, cuyo uso no requiere inicio de sesión específico.

⁵⁵ Orkut y Facebook miden la popularidad de sus aplicaciones por tipos o categorías. Para nuestro análisis, consideramos los primeros lugares de las cinco categorías más vistas. Las aplicaciones analizadas fueron: Orkut - Secretos del Mar, Buddy Poke, Feliz cosecha, Baby Adopter y Música, en Facebook - Causas, Texas Hold'em, frases, Badoo, y Quiz Planet.

⁵⁶ Navegamos sin realizar login, una vez que este procedimiento ya identificaría al usuario para la empresa, abriendo la posibilidad de que se empleen otras formas de monitorear al usuario.

⁵⁷ Disponible en http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html.

⁵⁸ El software es una extensión disponible para los principales navegadores del mercado que identifica web beacons y a las empresas que son responsables por ellos. Disponible en <http://www.ghostery.com/>.



Observamos que los sitios Terra, UOL y Yahoo utilizan, en promedio, 3,2 veces más cookies provenientes de servidores externos que el portal Globo.com y YouTube. En relación al número de beacons, UOL y YouTube son los sitios en donde la técnica fue menos empleada (una y tres veces, respectivamente), mientras que Yahoo, Terra y Globo.com aparecen con seis, siete y ocho beacons, respectivamente.

Con excepción de UOL, los cinco sitios analizados citaron la posibilidad de que terceros puedan emplear trackers en su sitio. Esta empresa presentó la política de privacidad más simplificada y fue la única en no hablar de la relación de los cookies con la publicidad o personalización de servicios. También afirmó que sus cookies no son usados para controlar preferencias del internauta, a pesar de admitir su uso para control interno de navegación. UOL y Globo.com fueron las únicas en no citar directamente el empleo de web beacons.

En las dos redes sociales analizadas, encontramos una disparidad significativa entre el número de cookies html encontrados: en Orkut, al analizar las cinco aplicaciones que figuran entre las más populares, encontramos 47 cookies, mientras que en Facebook fueron encontrados 217. Considerando apenas los cookies no repetidos, estos números caen a 13 y 38, respectivamente. La cantidad de web beacons, al contrario, no varió significativamente: fueron 18 trackers de este tipo no repetidos en Orkut, contra 15 de Facebook.

Fueron identificadas 69 empresas, nacionales y extranjeras, responsables por los cookies encontrados en los siete sitios analizados. En el caso de los web beacons, suman 23 empresas. El cookie más recurrente⁵⁹ y el segundo beacon más recurrente son de la empresa DoubleClick, subsidiaria de Google especializada en proveer anuncios y dar soporte a la administración de campañas publicitarias. Otros dos servicios de la empresa figuran en el punto más alto de la lista: el beacon de Google Analytics fue el más recurrente y el de Google AdSense quedó en el tercer lugar de la clasificación.

⁵⁹ La clasificación de recurrencia fue calculada con base en el número de sitios en que el cookie o beacon apareció, entre los siete analizados (Globo.com, YouTube, Terra, Yahoo, Uol, Orkut y Facebook) y no la cantidad total de apariciones del tracker considerado. La lista completa está disponible en el Anexo VIII.

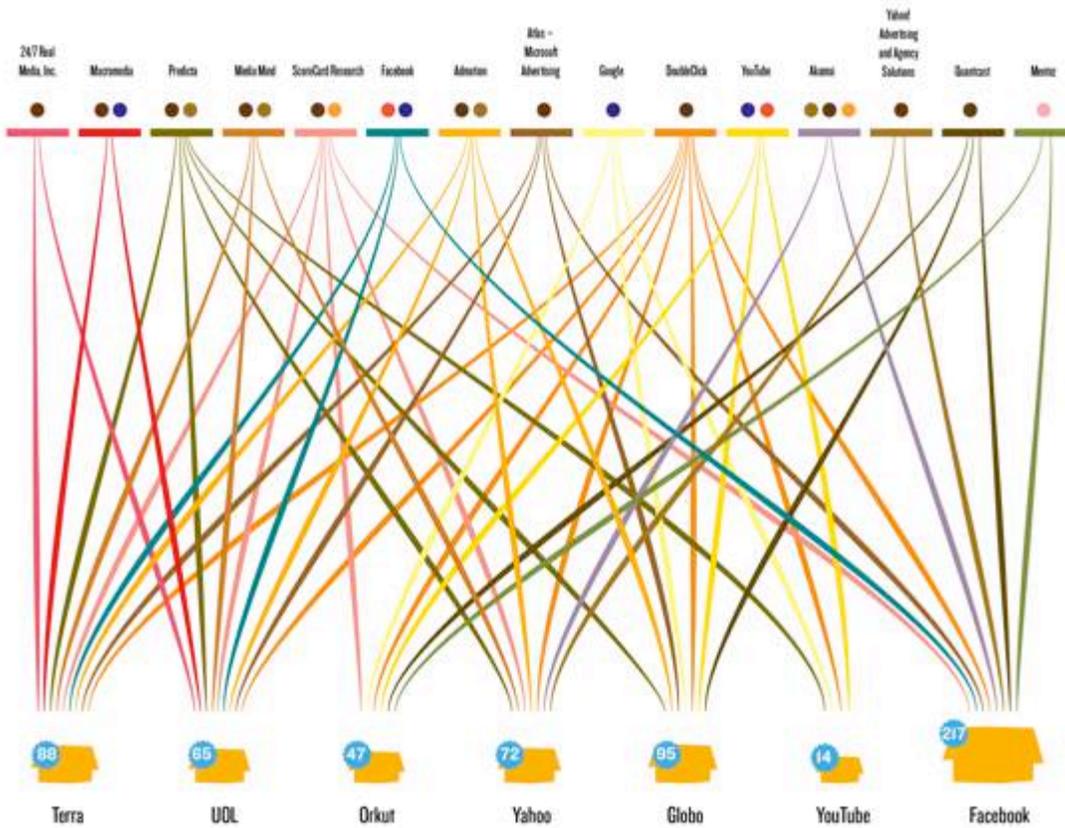
Los gráficos 28 y 29 demuestran el número de cookies y beacons encontrados en la totalidad de los sitios analizados, así como las empresas que los producen.

Gráfico 28: cookies, sitios y empresas

Cookies, websites and companies.

This graph shows the characteristics of most common cookies, the websites where they were found and the companies which use them.

- Cookie #1
- Cookie #2
- Cookie #3
- Cookie #4
- Cookie #5
- Cookie #6
- Cookie #7
- Cookie #8



Cookies and companies distribution among analyzed websites
This graph shows cookies found per website and relates them to the companies.

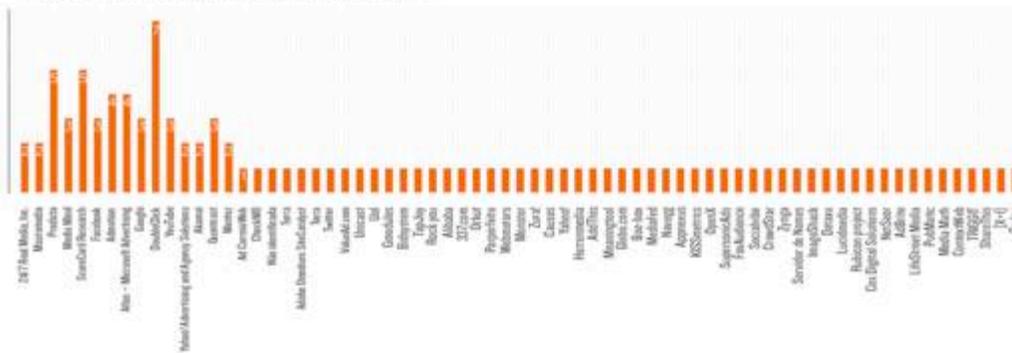
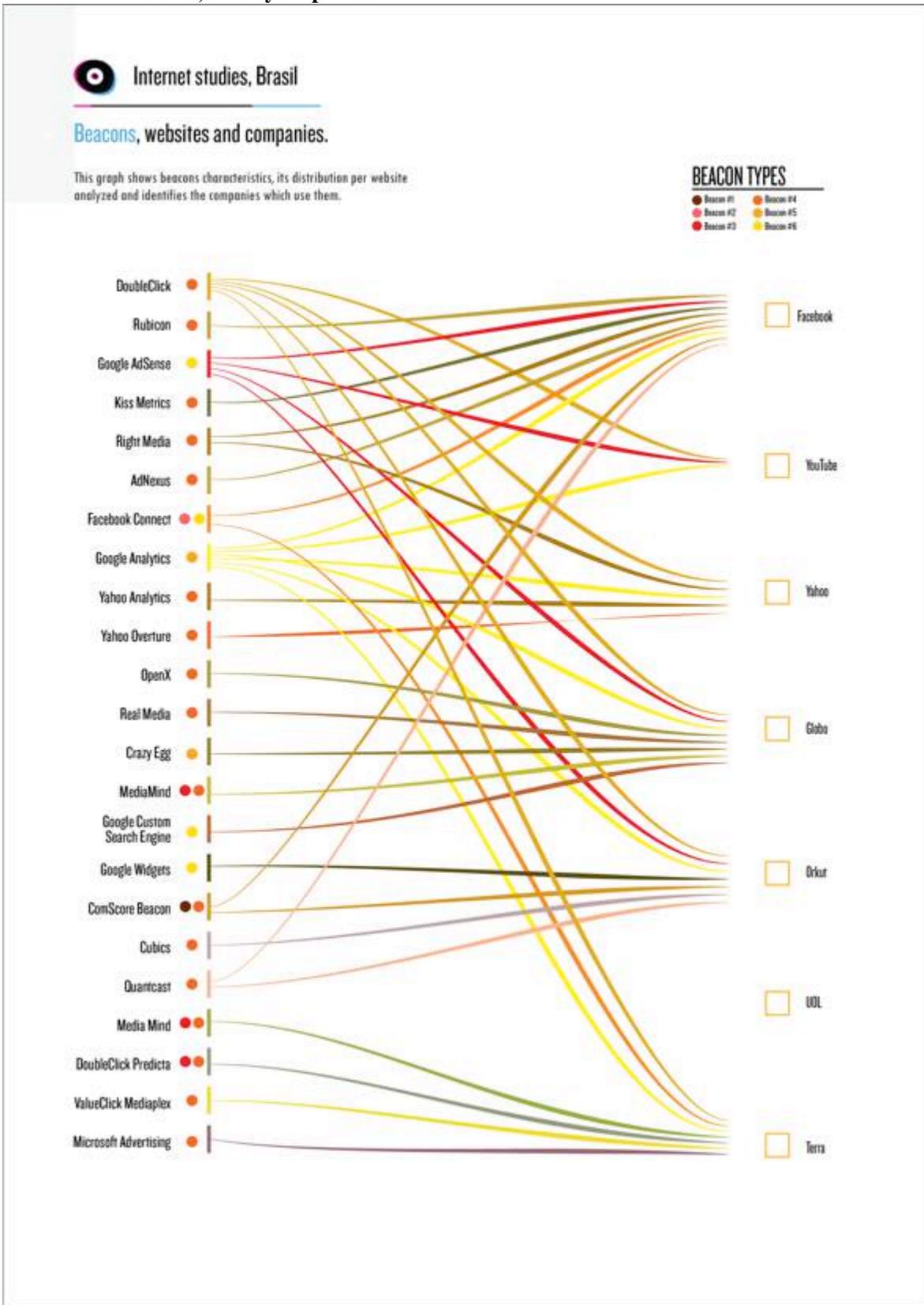


Gráfico 29: beacons, sitios y empresas



b) Actores

empresas responsables por la producción y suministro de los cookies y de los beacons;
sitios que hospedan y utilizan los cookies y beacons;
tipos diferenciados de cookies y beacons, que implican prácticas distintas de empleo y uso de datos personales;
empresas de publicidad contratadas por terceros;
mecanismos de opt-out;
organizaciones, corporaciones y/o acuerdos destinados a conciliar intereses comerciales y respecto a la privacidad del consumidor y/o usuario. Estos actores proveen sellos y/o certificados que indican el respeto a códigos de conducta por parte de las empresas, notablemente en cuanto al tratamiento de datos personales;
navegadores de Internet, los cuales conceden alguna visibilidad en el uso de cookies, así como opciones para desactivarlos;
usuario o internauta⁶⁰.

c) Tendencias observadas

En busca de más clics: la disputa por la atención del internauta

62% de las empresas responsables por los cookies encontrados y 68% de las responsables por los web beacons ofrecen tecnologías para la publicación de anuncios y tienen como negocio promover el monitoreo, análisis y optimización de piezas publicitarias o aplicaciones sociales.

Monitoreo: un mercado repleto de opciones

En apenas siete sitios, identificamos un número significativo de empresas. Entre las 69 que operaron cookies y las 23 que operaron beacons, encontramos, respectivamente, 45 y 19 empresas cuyo negocio está íntimamente asociado a prácticas de monitoreo en Internet. Éstas ofrecen servicios como medición de audiencia, suministran mapas de uso, analizan acceso y flujo de navegación, además de servicios relacionados al marketing, descritos arriba.

Predicta, Navegg, Zura! y Boo-Box: empresas nacionales

Entre las empresas identificadas, encontramos a cuatro nacionales: Predicata, Navegg, Zura! y Boo-Box; la primera es responsable por el segundo cookie más recurrente entre todos los analizados, presente en cinco de los siete sitios analizados.

Transparencia: preocupación lejos de ser universal

Llamó la atención la cantidad de empresas que dificultó su identificación, usando el dominio del cookie html o beacon un nombre diferente al suyo: esta práctica fue observada en 13% de las que operaron cookies y 12% de las responsables por beacons.

Aplicaciones sociales: un punto de vulnerabilidad

El uso de las dos redes sociales analizadas sin instalar o acceder a aplicaciones no se mostró asociado al uso de trackers de terceros, lo que muestra que, en estos sitios, la adición de aplicaciones implica no sólo permitir que sus desarrolladores accedan a información de los perfiles de los usuarios, sino que también los expone a la acción de un elevado número de trackers.

Acción de terceros: repasando responsabilidades

De manera general, constatamos que los sitios analizados permiten que las empresas contratadas por terceros divulguen anuncios en sus sitios. En estos casos, los usuarios quedan sujetos a las prácticas

⁶⁰ Aunque no hayamos analizado las prácticas de los usuarios ante estas tecnologías, ellos están ciertamente presentes entre los actores identificados.

y políticas de privacidad de esas empresas, lo que torna más compleja y dificulta, para los internautas, la administración de su privacidad.

Acuerdos y principios

Entre las empresas que operaron beacons, 32% son miembros de NAI - Network Advertising Initiative⁶¹ y 56% son certificadas por TRUSTe⁶² o se adhieren al acuerdo Safe Harbor⁶³. Entre las que operan cookies, estos números caen a 19% y 23%, respectivamente. Estas corporaciones y acuerdos buscan facilitar el respeto a la privacidad del usuario en el seno de las relaciones comerciales y publicitarias corrientes en Internet.

Políticas de privacidad y opt-out: zona de incertidumbre

Entre las empresas que operaron cookies, 19% no poseían política de privacidad en su sitio. Entre las que operan beacons, el número cae al 4%. La posibilidad de opt-out fue ofrecida por 46% de las empresas que operan cookies. No obstante, salvo raras excepciones, constatamos que el opt-out para beacons no es explicado de forma clara en los sitios de las empresas y políticas de privacidad analizadas, lo que obstaculizó incluso la medición de esta opción para la producción de este informe. Una constatación importante es que, en muchos casos, el mecanismo de opt-out ofrecido por las empresas consiste en instalar un cookie en la computadora del usuario para señalar su opción. Verificamos que este cookie, muchas veces, aparece para el internauta con la misma identificación del cookie de tracking. Esta incertidumbre es acentuada por el hecho de que el opt-out no funciona si el usuario escoge deshabilitar los cookies de su navegador.

Los gráficos 30, 31, 32 y 33 presentan los tipos de cookies y beacons más utilizados, clasificados según su función y propósito, así como las prácticas de las empresas responsables de los mismos en relación a la privacidad de los usuarios de Internet.

⁶¹ NAI es un consejo de empresas que desarrolla normas de autoregulación para la industria de los anuncios online. Ofrece opt-out para cookies de varias de las empresas analizadas a través de su sitio (<http://www.networkadvertising.org/>), pero no cita de forma clara si su opt-out sirve también para los beacons. Este opt-out depende de la colocación de un cookie de la empresa en la computadora del usuario.

⁶² TRUSTe es una empresa con base en California (EE.UU.), que ofrece certificación de prácticas de privacidad para empresas y sus sitios web. Si una empresa es certificada por TRUSTe, eso no significa concordancia con normas como la EU Directive 95/46/EC, sino apenas que la empresa respeta su propia política de privacidad.

⁶³ La adhesión a los Safe Harbor Privacy Principles permite que empresas americanas muestren su respeto y adhesión a las normas de protección de datos de la Unión Europea (EU Directive 95/46/EC).

Gráfico 30: características de las cookies y políticas de las empresas.

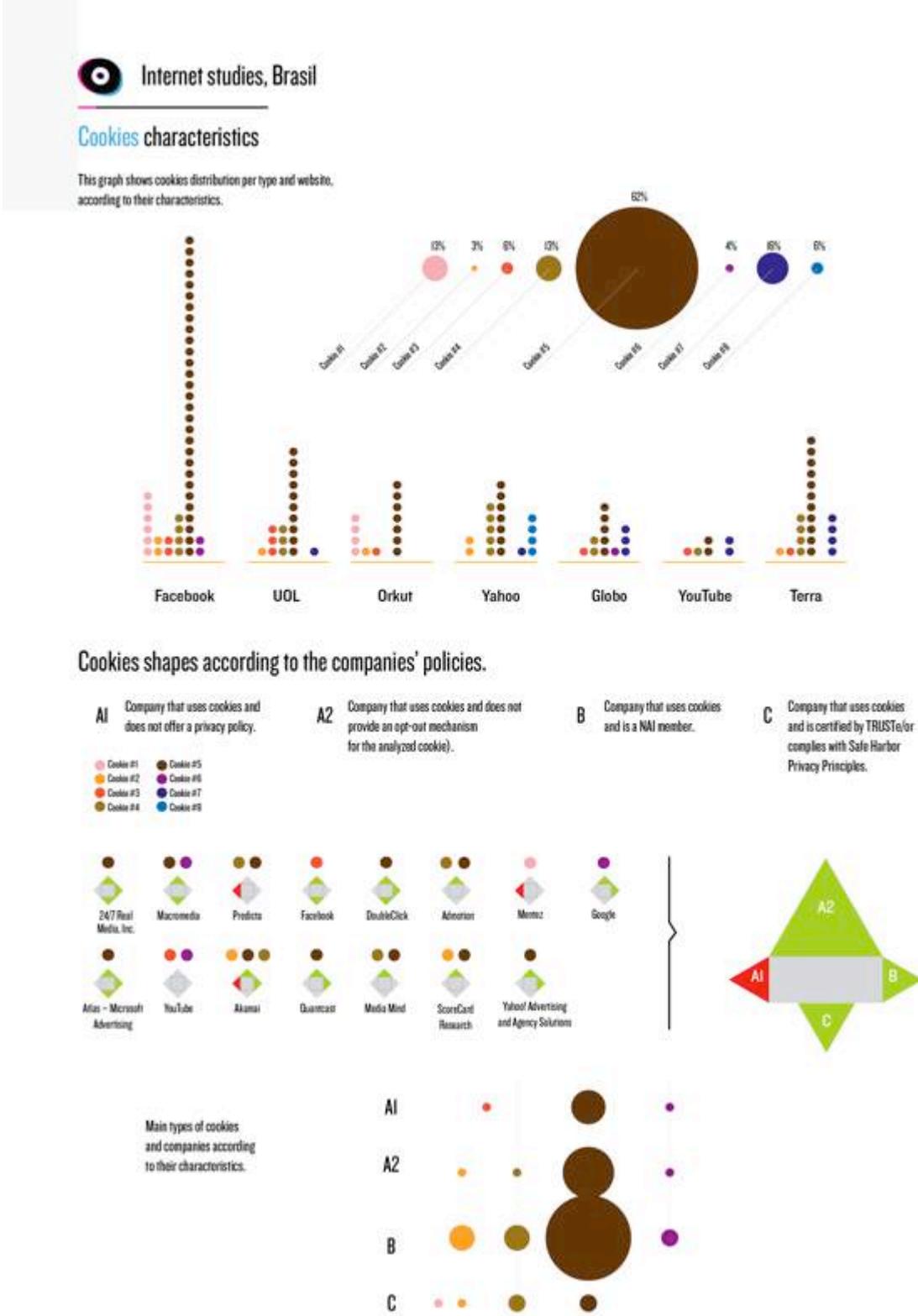


Gráfico 31: Etiqueta (tipología de cookies y empresas).

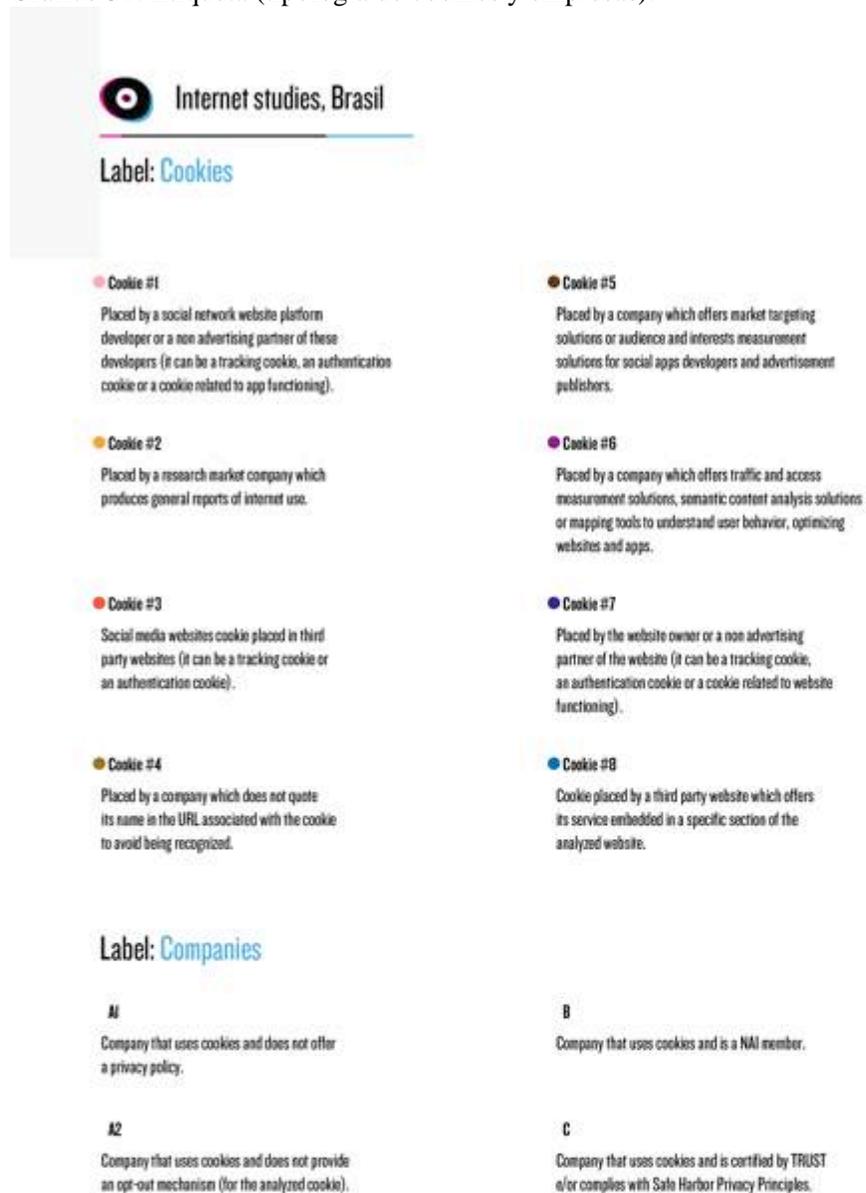


Gráfico 32: Características de los beacons y las políticas de las empresas.

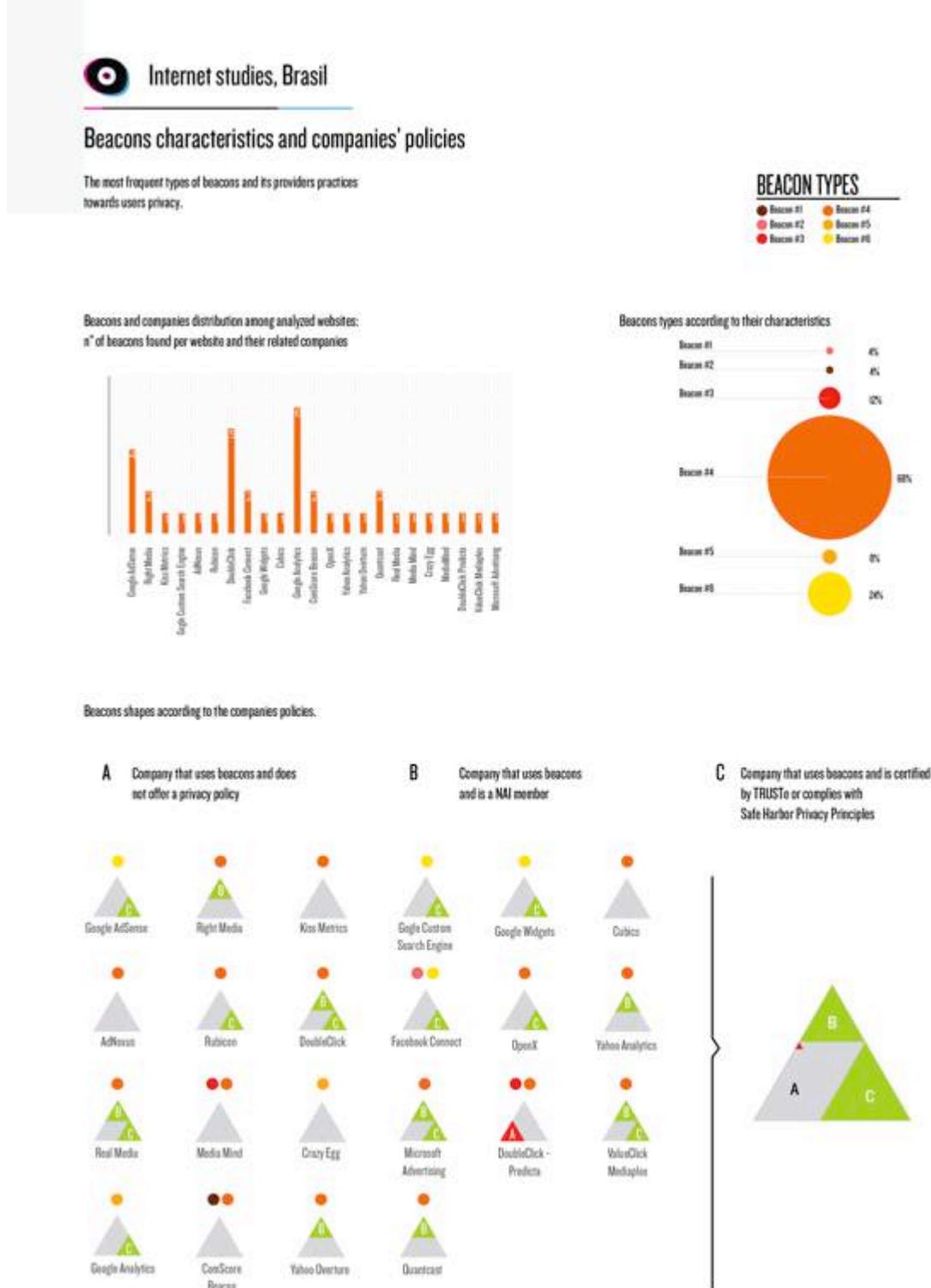
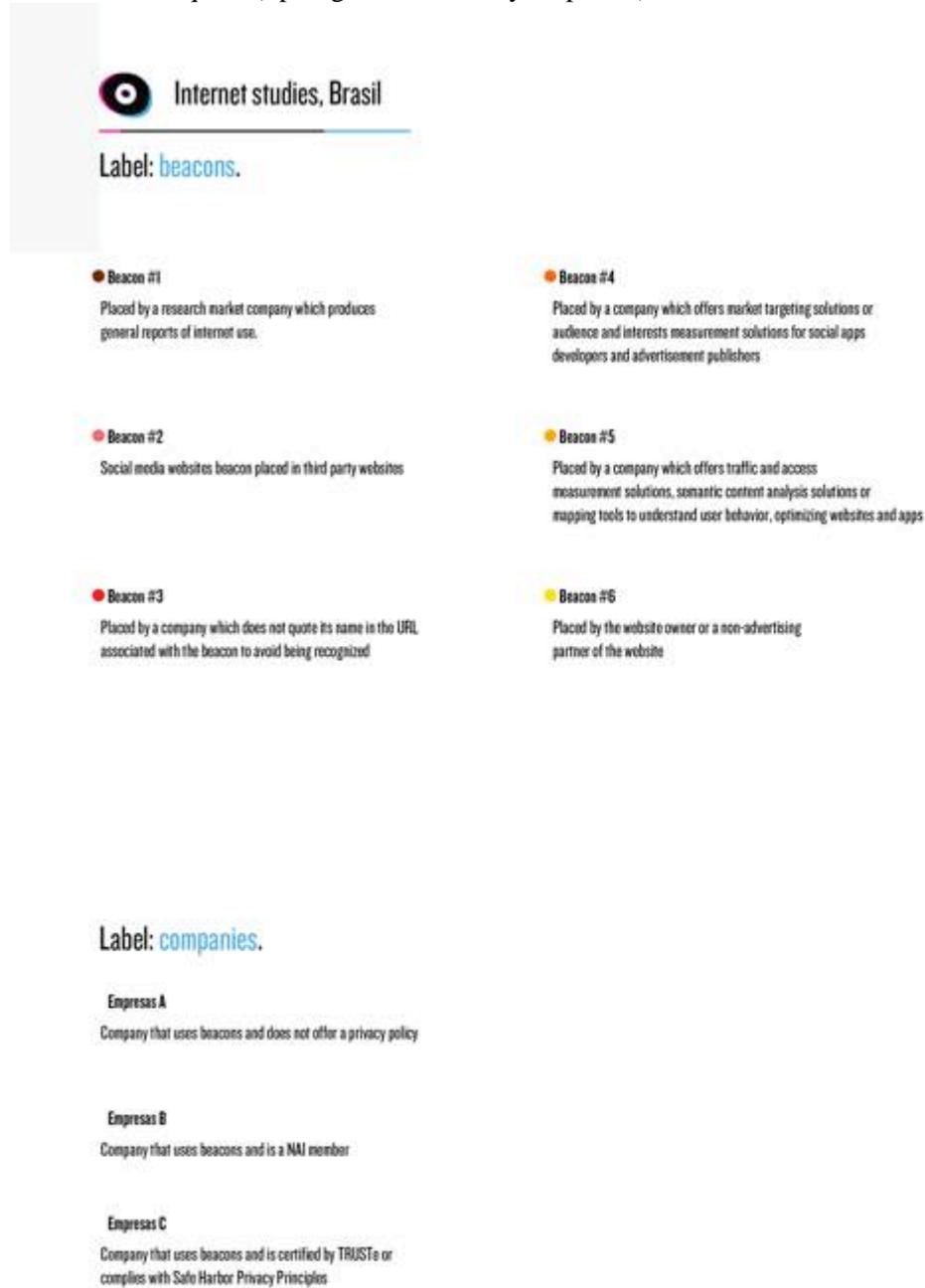


Gráfico 33: Etiqueta (tipología de beacons y empresas).



5.2.2 Encuesta sobre introducción, exposición y uso de datos personales en Internet

De acuerdo con lo propuesto en este proyecto, fue realizada una encuesta de carácter preliminar con cuestiones vinculadas al uso de Internet y la relación de los usuarios con la introducción, exposición y uso de datos personales. El objetivo fue obtener información que indique la percepción del usuario de Internet sobre la eventual exposición y uso de sus datos; probar la claridad y pertinencia de las preguntas para integrarlas en un cuestionario acerca del tema, con la opción de aplicarlo en una escala mayor y más representativa en una fase futura del proyecto.

Las primeras preguntas que compusieron el cuestionario trataron de obtener un perfil socioeconómico de los entrevistados (sexo, ingresos, educación), seguidas de cuestiones sobre hábitos de uso de Internet (locales de uso, frecuencia, horas de uso, actividades desarrolladas). Ese formato de levantamiento se basó en un cuestionario más amplio, aplicado por el Comité Gestor de Internet en Brasil (CGI.br), el cual es realizado periódicamente por dicho comité con la intención de obtener una muestra representativa del perfil socioeconómico brasileño.

Estructurar el levantamiento arriba mencionado a partir del cuestionario del CGI.br abre una futura posibilidad de diálogo interesante, en la medida en que permita comparaciones y cruce de datos entre las encuestas. Publicados desde 2005, los resultados de la encuesta producida por el CGI.br tienen considerable divulgación nacional y aceptación académica. Además de eso, el trabajo ya realizado por ese comité permite agregar otra información que si bien no está relacionada directamente con el tema de esta investigación, es importante para la construcción de un perfil más completo de los entrevistados.

El cuestionario fue respondido voluntariamente a partir del formulario disponible en Internet. El llamado fue hecho a partir de redes sociales (Facebook y Twitter), utilizando contactos ya establecidos por los investigadores. Los encuestados fueron informados de que se trataba de la fase inicial de la encuesta, en la que los datos serían considerados, pero que el propio cuestionario aplicado estaba bajo evaluación.

Como resultado, fueron obtenidas 69 respuestas consideradas válidas, pero con un perfil de muestra bastante específico: usuarios intensivos de Internet, con altos ingresos y escolaridad, tanto para los estándares brasileños como internacionales. Más de la mitad de los entrevistados (58%) poseen algún tipo de posgrado; la mitad está en el tope de la escala de ingresos (más de 5100 reales mensuales, que equivalen a aproximadamente 3100 dólares americanos), y el 89% utiliza Internet diariamente.

Se siguió un modelo de entrevista semiestructurada, o sea, mezclando preguntas cerradas y abiertas. La mayor parte de las cuestiones presentadas ofrecieron respuestas alternativas cerradas. Apenas dos preguntas ofrecieron campos abiertos a respuestas textuales con la intención de que el encuestado discudiese sobre el asunto. La primera pedía una descripción corta sobre eventuales “problemas de privacidad o de uso de sus datos personales en Internet”; la segunda pedía “evaluar y hacer sugerencias para el cuestionario”. Apenas uno de los encuestados criticó el número de preguntas y otro manifestó duda en cuanto a la cuestión “En Brasil, actualmente circulan propuestas de ley buscando combatir el anonimato en Internet. Trate de clasificar su posición con relación a ese asunto, representando el punto 1 de la escala la posición más favorable para los proyectos de ley y la posición 5 la menos favorable”

Con relación al tema de la investigación (percepciones sobre los temas “privacidad” y “uso de datos personales en Internet”), se trató de mantener abierto el sentido tanto de la noción de “privacidad”

como de las ideas de “uso de datos” y “datos personales”. Para eso, fueron presentadas alternativas que permitían a los encuestados inferir sobre el sentido dado a estos conceptos. Por ejemplo, la pregunta nueve, que indaga acerca de algún momento en que el encuestado se sintió víctima de lo que clasificaría como “problemas de privacidad o de uso de datos personales en Internet” (que obtuvo 21% de respuestas afirmativas), fue seguida de una pregunta que pide la descripción de esos problemas. La mayor parte de las respuestas (ocho) apuntó hacia el recibimiento de *spam*, indicando la percepción de que la dirección electrónica fue indebidamente expuesta o comercializada, lo que habría llevado al recibimiento frecuente de correspondencia no solicitada. Otros problemas apuntados fueron invasión de correo electrónico (cuatro respuestas), robo de número de tarjeta de crédito (dos respuestas); robo de identidad (una); *phishing* (una); exposición indebida de contactos personales (una), y exposición no autorizada de dirección física (una).

Se buscó también investigar el comportamiento declarado por los entrevistados en Internet y más específicamente en ambientes de posible exposición de sus datos personales, como las redes sociales. La actividad más mencionada fue la lectura y envío de correos electrónicos (97%), seguida por el uso de sitios de relacionamiento/redes sociales, con 87% (para ese ítem, fueron apuntados como ejemplo los servicios Facebook, Twitter y Orkut). A los que respondieron afirmativamente sobre el uso de sitios de relacionamientos/redes sociales, les fue preguntado sobre cómo perciben el nivel de seguridad de esos servicios, siendo presentada una escala de uno (muy seguro) a cinco (muy inseguro). La mayoría de los entrevistados (38%) escogió el punto intermedio de la escala (tres), el 13% eligió la respuesta “muy inseguro” (punto cinco), el 22% eligió el punto cuatro, el 11% eligió el punto dos y apenas un encuestado se inclinó por el punto uno (muy seguro).

Luego les fueron presentadas a los entrevistados dos preguntas relacionadas al uso de redes sociales y sitios para relacionarse, seguidas de una sobre qué datos considera “personales” y que ofrecen las mismas alternativas de respuestas. Estas preguntas trataron de enlistar diversas clases de datos para los cuales los entrevistados podrían presentar comportamientos estandarizados de uso compartido, siendo estos datos para exposición completa, a cualquier internauta, o para exposición restringida, sólo para personas autorizadas. Las cuestiones y la división presentada parecen funcionar en el sentido de que se puede apreciar que los entrevistados presentan un comportamiento menos restringido cuando se trata de exponer textos, imágenes o indicaciones (de fotos, videos y música de sus artistas favoritos, por ejemplo) de su propiedad. Al mismo tiempo, estos presentan un comportamiento más reservado cuando se trata de exponer materiales multimedia e información que vinculen a amigos y miembros de la familia.

Ese comportamiento reservado también es descrito cuando se trata de la exposición de “datos personales”. Al ser cuestionados acerca de este aspecto, casi la totalidad de los entrevistados — alrededor del 90%— tiende a considerar como información personal su número de teléfono (celular y residencial), dirección, número fiscal y, en grado menor, dirección electrónica. Por otra parte, es alta la mención de materiales multimedia que vinculan a amigos y familiares como datos personales: en torno del 60% cuando los involucrados son amigos y/o el entrevistado; y casi el 80% cuando los involucrados son familiares, incluso niños. Los comentarios hechos por el propio entrevistado y los materiales multimedia de sus artistas favoritos, por él indicados, son las alternativas que reciben menos respuestas (24% y 25%, respectivamente). Lo que ese tipo de respuesta indica es que los entrevistados entendieron la cuestión de modo peculiar, o sea, el “personal” de la expresión “datos personales” no es entendido como algo producido por la persona, sino alguna información delicada sobre ella o su red de contactos.

Fueron aplicadas también cuestiones que trataron de buscar indicios sobre en qué medida temas como privacidad y uso de datos personales en Internet despiertan preocupaciones para los entrevistados. Dos preguntas bastante parecidas indagaban acerca del nivel de preocupación, el

menor punto de la escala correspondía a “nada preocupado” y el quinto punto de la escala, el más alto, a “muy preocupado”. Una de las interrogantes se refirió a la “exposición de sus datos personales en la red” y otra al “uso comercial de sus datos personales en la red”. Para las dos cuestiones el mayor número de respuestas coincidió con los puntos altos de la escala, cuatro y cinco. No obstante, la cuestión que involucraba el uso comercial apuntó al nivel más alto de la escala, con 36% y 32% para el nivel cuatro; mientras que para la cuestión que implicaba la pura exposición de datos personales en la red, el penúltimo nivel de la escala recibió el mayor número de resultados, 34% (22% para el nivel cinco). Cuestionados sobre qué agentes estarían más interesados en usar/tener acceso a los datos personales de los entrevistados, éstos escogieron en primer lugar a las empresas (84%), seguidas por los criminales (63%), después por los gobiernos/Estado (41%) y al final por la policía (18%). La respuesta con relación a los interesados ayuda a dejar más claras las respuestas anteriores, dada la elección alta para la alternativa “empresas”. Posiblemente muchos parecen escoger esa alternativa teniendo en mente el envío de *spam*.

Dado el trámite en el legislativo brasileño del proyecto que busca aplicar leyes más rígidas con relación a las actividades anónimas en Internet, fueron introducidas cuestiones sobre el asunto, tanto desde el punto de vista de la práctica (el uso de pseudónimos para comentarios en blogs y redes sociales, por ejemplo), como de la percepción sobre cuánto permite el anonimato la infraestructura tecnológica actual de Internet. La gran mayoría de los entrevistados (42%) afirmó que nunca utiliza pseudónimos, número que cae abruptamente al nivel dos de la escala (16%) hasta que gradualmente alcanza el 5% para el último punto, es decir, “siempre”. Con relación a la percepción acerca del nivel de anonimato en Internet, la mayoría de los encuestados escogió el punto intermedio (37%) de una escala entre “totalmente anónimo” (0%) y “nada anónimo” (17%). La tendencia de los entrevistados, entretanto, fue de percibir Internet como poco anónimo, ya que el ítem dos de la escala recibió 11% de las respuestas y el ítem cuatro 26%.

Aunque los datos aquí presentados no posean representatividad estadística, en función del número de cuestionarios respondidos y del perfil de la muestra que no responde a la estructuración socioeconómica, estos ofrecen índices interesantes. Se nota, por ejemplo, que los entrevistados dicen comportarse de manera menos cautelosa cuando expresan opiniones y gustos personales. Esa actitud cambia y se torna más cautelosa cuando se trata de datos y materiales multimedia que involucran a familiares y amigos, y es bastante más restrictiva cuando se trata de exponer teléfonos personales, dirección domiciliaria y número de documentos de identificación. Ese cambio parece estar relacionado principalmente con preocupaciones en relación a la seguridad.

Se debe tomar en cuenta el alto nivel de escolaridad de los entrevistados; no obstante, la calidad de las respuestas permite afirmar que las cuestiones fueron bastante bien comprendidas y que permiten la aplicación más amplia de la muestra, de manera que con una estructura estadística alcance a todos los segmentos sociales brasileños y, finalmente, a América Latina.

Cabe resaltar que la investigación y las cuestiones presentadas, además de tener como función ofrecer indicadores sobre la percepción con relación al uso y la exposición de datos personales en Internet, acaban por llamar la atención pública sobre el asunto, contribuyendo para un debate más amplio del problema.

Creemos, además, que este informe constituye una primera e importante etapa en la consolidación de la Red latinoamericana de estudios.

5.3 Datos personales en Internet en México

5.3.1 Cómo se realizó el mapeo del caso de Internet y datos personales en México

La forma de identificar las temáticas que han tenido relevancia a propósito de la protección y control de los datos personales en la parte de Internet en México, se ha dividido en tres grandes rubros:

Investigadores, líneas de investigación
Agentes públicos y privados
Tecnologías

A cada uno de estos rubros se le aplicó una metodología específica para así llegar a los resultados más apropiados a los objetivos de la investigación, como se muestra a continuación.

i. Investigadores y líneas de investigación

Objetivos: a) explorar la producción académica de investigadores mexicanos que escriban sobre el tema en México, investigadores mexicanos que manejen el tema en otros países, investigadores extranjeros que traten el tema en México y extranjeros refiriéndose a un nivel global acerca del tema.

b) Identificar líneas de investigación relacionadas con el tema del proyecto, identificar fuentes de información, además de seleccionar los artículos o documentos por el año de su publicación y país de elaboración.

Metodología

El método que se diseñó para elaborar este primer rubro fue, ubicar dentro de la Internet fuentes de información válida y segura donde se pudieran consultar autores, analizar su línea de investigación comprándola con los objetivos del proyecto y analizar los artículos teniendo siempre en cuenta el criterio antes señalado de selección de autores.

Observaciones: Para fines de la investigación, de los 28 investigadores consultados hay:

22 investigadores de nacionalidad mexicana.
5 investigadores de nacionalidad española.
1 un investigador de nacionalidad argentina.

Entre los diferentes autores que han escrito acerca de este tema, se han encontrado líneas de investigación que han ayudado a tener un parámetro de lo que se ha escrito acerca de este tema:

La privacidad y la protección de datos personales en el ámbito de la ciberdelincuencia y la seguridad informática.

La era de la información y legislación

Derecho de seguridad y de protección de datos.

Transparencia y seguridad

Sociedad de la vigilancia

Medios y educación

Además, 19 investigaciones tienen relación directa con los temas que se tratan en esta investigación, y los 9 investigadores restantes tienen una relación indirecta con ésta. Refiriéndonos a los investigadores mexicanos, todos abordan directamente la protección de datos personales, tecnologías, leyes, Internet, regulación, derechos e identidad en México, y finalmente los 5 investigadores españoles, al igual que el investigador argentino, refieren el tema de forma global. Las líneas de investigación de cada uno de los consultados están dirigidas a la protección de datos

personales, tecnologías, vigilancia y legislación. Dichas investigaciones tienen como año de elaboración el 2010.

Los artículos de los investigadores pertenecen a varias instituciones como son:

Biblioteca Jurídica.com

Protección de Datos personales y privacidad.org

UNAM (UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO) “Boletín Mexicano de Derecho comparado”

El Universal. Diario de circulación nacional en México

Biblioteca Jurídica Virtual UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO (UNAM)

Comisión para el Acceso a la información pública

Instituto de Transparencia de Sonora

La Jornada. Diario de circulación nacional en México

Gobierno del Estado de México

Debate.com.mx

INEGI (INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA)

Página de la Presidencia de la República. México

Isegoria revistas

Universidad de Sevilla

Red Iberoamericana de el derecho informático

UAM (UNIVERSIDAD AUTÓNOMA DE MÉXICO) en la revista “El cotidiano”

Universidad de Guadalajara en la revista “Comunicación y sociedad”

Universidad de Sevilla en “Pixel-Bit. Revista de medios y comunicación”

Instituto Tecnológico y de Estudios superiores de Monterrey en “Global media Journal”

Universidad Oberta de Catalunya en “RU&SC Revista de universidad y sociedad del conocimiento”

Universidad de Murcia en “RED Revista de Educación”

Facultad latinoamericana de C.S en “Perfiles latinoamericanos”

ii Agentes públicos y privados:

En lo que respecta a los agentes públicos y privados, en especial de las dependencias de gobierno que tienen bases de datos de protección de datos personales: el IFAI no contiene una base de datos personales a diferencia del INEGI, que si contiene una base de datos al igual que el IFE con el padrón electoral.

La metodología que se utilizó para este segundo rubro fue identificar en la Internet movimientos u organizaciones públicas o privadas que estuvieran o estén haciendo acciones a favor de la protección y control de los datos personales, ya sea de forma nacional, estatal o hasta internacional.

Objetivos:

a) Determinar que movimientos u organizaciones tienen prácticas que ayudan a la propagación y reflexión sobre el tema de protección de datos personales en el uso de la Internet en México.

b) Señalar las acciones realizadas por organizaciones a favor del control y protección de datos personales, identificar acciones más recientes y describir las formas en que se han realizado dichas acciones.

Observaciones: Existen diferentes instituciones públicas y privadas que tienen un interés por la salvaguarda de los datos personales al entrar a la red, dentro de estas instituciones hay 3 que son privadas y 18 que son públicas, el año de todas estas acciones fueron en el 2010, se tomó este año ya que es donde unas iniciaron con el tema y otras por que la acción más importante se llevo a a

cabo en ese año.

De las instituciones consultadas 3 son españolas, 1 estadounidense, 1 chilena y 16 son mexicanas, dentro de las acciones realizadas por dichas instituciones se encuentran: a) Introducir el tema de la protección de datos, dar a conocer artículos especializados en la legislación federal de protección de datos, b) Publicar en páginas de Internet, c) Dar a conocer la problemática vinculada con la exclusión por medio del Internet y d) Publicar artículos en los cuales se expone la preocupación que hay por la falta de organización y legislación de datos personales.

De las 21 instituciones, 7 están orientadas de forma internacional y 14 de ellas nacional.

Para ilustrar lo antes mencionado, se muestra una tabla con el nombre del agente, si es público o privado y la acción desarrollada:

Tabla 3. Carácter público o privado de los agentes		
Agente	Público o privado	Acción que se desarrollo
IEAIP(Instituto Estatal de Acceso a la Información Pública)	Público	Invitación a deliberar acerca de la protección de datos
IFAI (Instituto Federal de Acceso a la Información)	Público	Pronunciamiento del IFAI sobre el presupuesto de egresos
Blog, Gurú político	Público	Introducir el tema de la protección de datos
Revista Transparencia de Nuevo León	Público	Evento: “Archivos y Rendición de Cuentas”, organizado conjuntamente con el National Security Archive de la George Washington University
Benemérita Universidad Autónoma de Puebla	Público	Artículo especializado en la legislación federal de protección de datos, dentro de su página de Internet
Universidad Autónoma de Nuevo León	Público	Se realizó un panel de protección de datos, llamado "Perfectible el sistema de protección de datos"
Alianza Cívica	Público	Realizó en Sonora una capacitación en lo que respecta a la protección de datos personales

iii Tecnologías: Para la elaboración de este tercer rubro se han identificado las tecnologías que se relacionan con el objetivo de la investigación.

Objetivos: a) Identificar las tecnologías que por sus características pueden ser medios para controlar y proteger los datos personales de los usuarios.
b) Identificar empresas o sistemas que para su operación controla o maneja datos personales.

Observaciones: En el aspecto de “Tecnologías” se encuentran Google-maps, las llamadas “cookies”, facebook, redes wi-fi y street view, las cuales se encargan de dar a conocer la ubicación de la población, de llevar un registro de páginas visitadas y de facilitar la comunicación. Todas las anteriores tecnologías facilitan la obtención de datos personales.

i Investigadores y líneas de investigación

Autor: **Avilés Karina**

Título: *Se dispara el delito de robo de identidad.*

Tema: En México se ha agravado el delito de robo de identidad, el robo de identidad es el delito con más rápido crecimiento en el mundo por la facilidad que existe de suplantar con otra fotografía y otros datos la identidad de otras personas y realizar delitos, este tipo de fraudes se pueden llevar a cabo mediante correos falsos, procesos que se realizan en la banca en línea, venta de bases de datos o a través de ataques de personas especializadas en esa actividad. Pese a ello, no existe una legislación específica en materia y es muy importante tener conciencia al respecto, porque es muy fácil compartir datos en redes sociales y desconocer el uso que otros pueden dar a nuestra información.

Tipo de documento: Noticia de periódico.

Año de Publicación: 2010

Publicación:

<http://www.jornada.unam.mx/2011/02/21/index.php?section=politica&article=016n2pol>

Palabras clave: seguridad.

Autor: **Carrillo Edgardo**

Título: La protección de datos personales en los tiempos de Facebook.

Tema: Esto es de un texto de la conferencia "La protección de datos personales en los tiempos de Facebook", donde nos explica la importancia y también el peligro o lo que repercute cuando subes a tu perfil de facebook fotografías provocativas o tomando alcohol, por ello da unas recomendaciones para proteger nuestros datos personales en Internet: primero que nada crear una cultura de la autoprotección empezando por conocer las condiciones de uso de las redes sociales, en que se suscriben y luego aplicando por lo menos los controles de seguridad, por lo tanto comprender las semejanzas entre la vida real e Internet, tener contacto solo con personas conocidas, no reenviar cadenas, no competir para tener más amigos, proteger la computadora, configurar adecuadamente las opciones de seguridad.

Tipo de documento: Artículo de blog.

Año de Publicación: 2010

Publicación: <http://transparenciasonora.org/colateral/index.php?artids=19&cat=1&categoria=1>

Palabras clave: privacidad y delincuencia.

Autor: **Castells Manuel**

Título: Internet, libertad y sociedad, una perspectiva analítica

Tema: Nos habla de cómo la creación del Internet ha sido un arma para el control de información.

Tipo de documento: Artículo de revista.

Año de publicación: 2003

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=3050041>

Palabras clave: Control, tecnología, Internet, seguridad.

Autor: **Cunjamá López Emilio Daniel**

Título: Sociedad de la vigilancia y estado policial: análisis de las tecnologías y aparatos de control.

Tema: Las tecnologías de la vigilancia requieren de objetos a vigilar, el individuo se sujeta a ser vigilado en tanto permita ser objetivado por el ojo del vigilante, de esta forma puede ser captado por la mirada del otro, por lo tanto, la tecnología de la vigilancia representa la relación entre sujeto (vigilante) y objeto (vigilado). El gran supuesto en México es que la policía te vigila, Hacienda te vigila, estamos vigilando tu salud, en si, el estado te vigila, por lo tanto, el Estado es el sujeto vigilante y la sociedad es el objeto vigilado. De hecho el Estado promueve que la sociedad como institución vigile a la sociedad misma: "si ves un acto ilícito denúncialo", pero ¿qué sucede cuando la sociedad deja de ser ese objeto, sujeto, dócil y decide des objetivarse, salirse de cuadro, moverse en la foto y además ser ella misma quien tome las fotos? ¿Cuando los vigilantes empiezan a ser

vigilados, cuando se convierten en objetos a observar y ya no son los únicos que vigilan?

Tipo de documento: Artículo de Revista

Año de publicación: 2001

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=32513865002>

Palabras clave: Vigilancia, control, tecnologías.

Autor: **Crespo José Antonio**

Título: Datotráfico e inseguridad.

Tema: La mancuerna que prevalece en el país, corrupción e impunidad, propicia que los datos confidenciales sean fácilmente filtrados y que circulen en Tepito o en redes de Internet, lo cual genera incentivos a no proporcionar esa información, a eludir ese requerimiento en lo posible. Mientras tanto, se discute precisamente la ley para la protección de datos personales que busca evitar la divulgación de la información confidencial que los ciudadanos proporcionamos al gobierno y empresas privadas.

Tipo de documento: Artículo de blog.

Año de publicación: 2010

Publicación:

<http://www.debate.com.mx/eldebate/Articulos/ArticuloOpinion.asp?idArt=9823390&IdCat=6115&Page=2>

Palabras clave: protección, corrupción.

Autor: **Flores Vargas Rosalba**

Título: Evitar el tráfico y uso de datos personales sobre todo por empresas

Tema: Evitar el tráfico y uso de datos personales sobre todo por empresas, así como la suplantación de identidad y hasta secuestros, serán tareas de la recién creada comisión Especial de Protección de Datos Personales, cuyo presidente, el diputado panista Gustavo Parra, destacó que convocará a foros y debates académicos para que no sólo se incluya la visión de un legislador sino del conjunto de la sociedad, ahora lo que le toca hacer en la entidad es primero, darle difusión que la ciudadanía sepa que tiene protección de sus datos.

Tipo de documento: Artículo página web.

Año de publicación: 2010

Publicación: <http://poderedomex.com/notas.asp?id=61000>

Palabras clave: Protección y identidad, datos personales

Autor: **García Barrera Myrna Elia**

Título: La protección de datos personales en México.

Tema: Nos habla que en estos tiempos de la globalización y el impulso de las nuevas TICs específicamente el desarrollo del Internet y de las tecnologías de la información, en conjunción con otros factores, han dado lugar a la incorporación de nuestras leyes un par de derechos de muy reciente cuño e nuestro sistema sobre los cuales todavía hace falta definir muchos elementos, los cuales son: los derechos de acceso a la información y la protección de los datos personales.

Tipo de documento: Presentación.

Año de publicación: 2010

Publicación: <http://www.scribd.com/doc/39205110/La-Proteccion-de-Datos-Personales-en-Mexico>

Palabras clave: Datos personales, transparencia.

Autor: **García González Aristeo**

Título: La protección de datos personales, derecho fundamental del siglo XXI. Estudio comparado.

Tema: Este estudio gira en torno a la importancia que cada día va cobrando el desarrollo tecnológico puesto que se ha convertido en una revolución para aquellos métodos tradicionales de organización. Aunado a ello, el tratamiento de la información representa un riesgo, sobre todo si se

trata de datos concernientes a la persona. Por tal motivo, el uso y control sobre los datos personales a cada persona, debe serle reconocido ya no sólo como una garantía, sino además como un derecho fundamentalmente protegido. De ahí la importancia de reconocer un derecho fundamental a la protección de datos a nivel constitucional y más aún, garantizando su protección.

Tipo de documento: Artículo de revista.

Año de publicación: 2010

Publicación: <http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=42712003>

Palabras clave: Derechos humanos, individuales y de intimidad.

Autor: Gómez-Robledo Alonso

Título: Protección de datos personales: el caso del poder ejecutivo federal.

Tema: Es un estudio que tiene como finalidad describir el marco jurídico preexistente a la Ley Federal de Acceso a la Información pública Gubernamental, la cual establece la confidencialidad y tratamiento de cierta información relativa a personas físicas. Se identifican los principios de protección de datos personales contenidos en los tratados internacionales que México ha suscrito y cómo éstos han sido asimilados por la LAI en el capítulo VI "protección de datos personales". Se abordan de la misma manera las acciones que ha llevado a cabo el poder ejecutivo federal, para el adecuado tratamiento de datos personales alojados en sus archivos, que van desde la adopción de legislación secundaria hasta el uso de herramientas informáticas para el registro de sistemas de datos personales.

Tipo de documento: Libro.

Año de publicación: 2010

Publicación: <http://www.bibliojuridica.org/libros/5/2299/3.pdf>

Palabras clave: Acceso a la información, ley, protección.

Autor: González María de Luz

Título: Información privada, sin control en Internet

Tema: Es un artículo donde expone la facilidad con la que se puede obtener las listas de clientes, números de las compañías telefónicas, tarjetas de crédito, es una búsqueda que EL UNIVERSAL encontró varias páginas que ofrecen bases de datos desde 10 mil pesos, y pone en evidencia la complicidad que existe con la policía, ya que si quisieran pudieran rastrear a los que consultan tales páginas para comprar datos personales.

Tipo de documento: Noticia de periódico.

Año de publicación: 2010

Publicación: <http://www.eluniversal.com.mx/nacion/177168.html>

Palabras clave: Seguridad, Internet y regulación.

Autor: González Solís Arturo

Título: Un retraso a la democracia.

Tema: Este artículo habla de que en el senado se discute la participación de México en un acuerdo multinacional que autorizaría al proveedor de Internet revisar la información que los usuarios hacen circular por la red. Expertos en tecnología consideran que se avecina un atentado contra la libertad, la privacidad y el libre uso del Internet. En EUA desde el 2007 se promueve este convenio pretende que un proveedor de Internet revise y analice los paquetes de cargas y descargas de los usuarios, con el fin, señalan, de disminuir los índices de piratería en el sector Internet.

Tipo de documento: Artículo de revista.

Año de publicación: 2010

Publicación:

http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=498:un-retrazo-a-la-democracia&catid=104:elderechoinformatico-mexico&Itemid=119.

Palabras clave: Tecnología e Internet.

Autor: **González Hugo**

Título: Propone SEGOB regular Internet como estrategia de inclusión social en el imaginario de los pobres.

Tema: Habla de la discusión sobre la regulación de Internet, se plantea la posibilidad de aplicar una regulación de los contenidos en Internet, Leopoldo Brito (director de contenidos), manifestó la preocupación en el sentido de una legislación en materia de contenidos en Internet y sugirió una autorregulación con legislación, para que así los padres de familia tengan claro conocimiento de los contenidos que están permitidos, todo esto por el grave problema de pornografía infantil, la violencia y el abuso sexual, el único problema que esta en debate es, quién va a ser la persona que regule el contenido de Internet.

Tipo de documento: Artículo página web.

Año de publicación: 2010

Publicación: <http://www.presidencia.gob.mx/prensa/ultimasnoticias/?contenido=30874>

Palabras clave: Regulación, Internet, libertad.

Autor: **Herrera Ramos Mario**

Título: La segmentación digital en México.

Tema: En este estudio se propone el concepto de "segmentación digital" para describir el acceso diferencial de individuos, hogares y regiones a los bienes y servicios proporcionados mediante el uso de la tecnología de la información y de comunicaciones. Se presenta evidencia de que en México hay segmentación digital en diversos niveles: con los países de la OCDE entre empresas grandes y pequeñas, así como entre las productoras y las que se dedican al comercio entre los hogares que cuentan con posibilidades de tener computadora.

Tipo de documento: Artículo de revista.

Año de publicación: 2005

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=11501802>

Palabras clave: Tecnologías, Internet, brecha digital.

Autor: **Ibarra Cadena Blanca Lilia**

Título: Transparencia en las Américas a la mitad del camino.

El derecho a la información y los beneficios sociales.

Temas: Nos cuenta de las actividades que pasaron en la VI semana internacional de transparencia, nos cuenta que se tocaron temas como la transparencia en América latina, protección de datos por los gobiernos, protección de datos de identidad personal, los límites de la seguridad nacional, ¿cuál es la información que se debe reservar por motivos de seguridad nacional?

Habla acerca de la importancia de la transparencia de la información y la información pública, y los beneficios que trae esto, para ello puso algunos ejemplos de los diferentes sectores de la sociedad, en los cuales la utilidad de este tema es muy diferente uno con otro, pero no menos importante: por ejemplo en una empresa, tener un gobierno que rinda cuentas transparentes crea confianza, conocer el procedimiento de licitaciones construye credibilidad, conocer programas gubernamentales y sus reglas permite a los empresarios obtener incentivos. Como ama de casa: conocer los servicios de salud consigue beneficios, obtener información sobre trámites para la asistencia de la familia, saber si las obras se están realizando, conocer los programas de capacitación para la obtención de empleos. Estudiantes: realizar trabajos de investigación, conocer sobre requisitos, preguntar sobre el funcionamiento de los gobiernos.

Tipo de documentos: Artículo página web.

Año de publicación: 2010

Publicación: www.caip.org.mx/articulos/2010/0107_blic.htm

Palabras clave: Derecho, protección de datos, libertad de comunicar, seguridad, Transparencia,

derecho a la información, rendición de cuentas.

Autor: **Jiménez Horacio**

Título: OCDE Urge ley de protección de datos personales.

Tema: Noticia sobre la preocupación de la OCDE para que MÉXICO a través del Instituto Federal de Acceso a la Información Pública, saque una ley sobre la protección de datos personales, argumentó que de las 30 naciones miembros de la OCDE, 28 cuentan con una legislación especializada en la materia de protección de datos y solo Turquía y México carecen de ella. En representación del IFAI la comisionada Singrid Arzt Colunga, presentó a los integrantes del foro una serie de planteamientos y consultas que buscan enriquecer el proyecto de iniciativa de ley sobre protección de datos personales que actualmente (marzo 2010) se elabora en comisiones de la cámara de diputados.

Tipo de documento: Noticia de periódico.

Año de publicación: 2010

Publicación: www.eluniversal.com.mx/notas/664335.html

Palabras clave: Ley de protección de datos y marco de privacidad.

Autor: **Luna Pla Issa**

Título: La protección de los datos personales en el DF.

Tema: Habla acerca de la legislación que en el 2008 sacó el DF sobre la materia de la protección de los datos personales, la ley de protección de datos personales para el DF representa cambios sustanciales en el tratamiento y conformación de los sistemas en posesión del gobierno, así como un reto administrativo para dar garantía a los derechos que esta ley otorga. Entonces las leyes de datos personales, como la del DF cumplen dos funciones: 1) diseñar un entramado de normas vinculadas para proteger los datos personales, esto implica normas y procedimientos para su creación, uso y sustracción, así como para el tratamiento que de ellas dan los entes públicos, 2) garantizar el ejercicio de los llamados derechos ARCO: de acceso, rectificación, cancelación y oposición, todas ellas libertades fundamentales que al titular de los datos puede ejercer ante el ente público.

Tipo de documento: Artículo de Revista.

Año de publicación: 2010

Publicación: <http://www.juridicas.unam.mx/publica/rev/decoinc/cont/15/cmt/cmt5.htm>

Palabras clave: Ley de protección de datos personales.

Autor: **Martínez Nurit**

Título: ONG: RENAUT vulnera seguridad personal.

Tema: Se habla acerca del registro de los celulares en el RENAUT, nos explica que mucha gente se ampara, ya que organizaciones en la defensa del consumidor alertaron que el registro de celulares con datos personales resultará un mayor riesgo y la seguridad de las personas serán más vulnerables, sobre todo niños y jóvenes, frente a esa situación. Al Consumidor dijo que para quien lo solicite proporcionarán apoyo y se ha puesto a disposición el paquete-defiendas, que es la demanda de amparo para solicitar este recurso legal.

Tipo de documento: Noticia de periódico.

Año de publicación: 2010

Publicación: <http://www.eluniversal.com.mx/nacion/176914.html>

Palabras clave: Seguridad, vulnerabilidad, riesgo, corrupción y datos personales.

Autor: **Munuera Giner Francisca**

Título: Nuevas tecnologías y exclusión, hay vida más allá de Internet.

Tema: Nuevas formas de pobreza y exclusión social constituyen la cara negativa de una sociedad que defiende valores como la libertad, convivencia, tolerancia e igualdad de oportunidades. Las nuevas tecnologías de la información y la comunicación abren nuevas posibilidades en la

consecución de los mismos, pero a su vez pueden generar nuevas situaciones de exclusión derivadas del actual modelo de crecimiento económico que exige una gran flexibilidad de adaptación a una sociedad en permanente y vertiginoso cambio. Las personas y colectivos socialmente más desfavorecidos o aquellos otros que no dispongan de la formación adecuada para ir integrando el uso de las nuevas tecnologías quedarán excluidas de los procesos de participación social. De todos dependerá, en parte, que los asumamos como productos negativos de la modernidad o que emprendamos actuaciones educativas que no se rijan solamente por parámetros económicos sino por parámetros de justicia social.

Tipo de documento: Artículo de revista.

Año de publicación: 2004

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=36802606>

Palabra clave: Tecnologías, pobreza, exclusión social, educación e igualdad.

Autor: Ortiz Henderson Gladys

Título: Acceso y usos de las tecnologías de la información y comunicación entre las niñas y niños mexicanos: caso de la ciudad de Monterrey.

Tema: El siguiente texto muestra algunos de los resultados de una investigación realizada sobre el acceso y los usos de las tecnologías de la información y comunicación Tics, entre las niñas y los niños de quinto y sexto de primaria de la ciudad de Monterrey. Las temáticas que se abordan son las características del entorno mediático en el que las niñas y los niños se desenvuelven poniendo especial atención en el acceso hacia la red Internet, en el cómo aprenden a usar la red Internet y cómo navegan en ésta.

Tipo de documento: Artículo de revista.

Año de publicación: 2003

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=68712864005>

Palabra clave: Tecnologías, pobreza, exclusión social, educación y acceso.

Autor: Pérez Luó Antonio Enrique

Título: La tutela de la libertad informática en la sociedad globalizada.

Tema: Este trabajo cifra su propósito en un triple y convergente objeto: 1) en primer término analiza algunos de los episodios más relevantes que reflejan el riesgo informativo para los derechos y libertades, 2) se ofrece un cuadro sumario de la respuesta jurídica a los atentados contra las libertades, dicha respuesta se ha materializado en tres generaciones de leyes de protección de datos personas, cuyos respectivos rasgos informadores se apuntan, 3) se aboga por una respuesta jurídica global.

Tipo de documento: Artículo de página web.

Año de publicación: 2010

Publicación: <http://isegoria.revistas.csic.es/index.php/isegoria/article/view/521/521>

Palabra clave: derechos y libertades.

Autor: Rangel Rodríguez Samuel

Título: Redes sociales y transparencia: entre lo público y lo privado.

Tema: Inicia comentando qué son los datos personales, son aquéllos tales como el domicilio, el número telefónico, el registro federal de contribuyentes, la religión, la orientación sexual, las cuentas bancarias, la vida afectiva y familiar de una persona, sus expedientes clínicos, sus datos biométricos, tales como su huella digital y el iris, entre otros, en sí daros que afecten a la intimidad de cada persona, ahora pongámonos a pensar si estos datos caen en manos de delincuentes. Mientras que en otros países sobre todo en Europa, existen autoridades federales y locales que se encargan de velar por la protección de los datos personales de todos y cada una de las personas, verificando que la autoridad no haga mal uso de ellas, incluso sancionando, lo malo es que en nuestro país los avances son pocos.

Tipo de documento: Artículo de página web.
Año de publicación: 2010
Publicación: www.caip.org.mx/articulos/2009/0728srr.html
Palabra clave: Internet, redes sociales, vulnerabilidad.

Autor: **Romero Pavía**

Título: El uso de las TIC s en la educación básica de jóvenes y adultos de comunidades rurales y urbanas del sureste de México.

Tema: El uso de las tecnologías de la información y la comunicación en los diferentes niveles y sistemas educativos tienen un impacto significativo en el desarrollo del aprendizaje de los estudiantes y en el fortalecimiento de sus competencias para la vida y el trabajo que favorecerán su inserción en la sociedad del conocimiento. En este trabajo se investiga el uso de las Tics en la educación básica de jóvenes y adultos a través del Modelo de Educación para la Vida y el Trabajo, en sus modalidades virtuales y en línea en comunidades rurales y urbanas del Estado de Yucatán. Los resultados de este estudio documentan la opinión de las personas jóvenes y adultas con respecto a sus habilidades para el uso de las Tics, su opinión acerca de las dos modalidades y las dificultades que enfrentan como usuarios. Los resultados se discuten bajo el Programa Sectorial de Educación 2007-2012 de México.

Tipo de documento: Artículo de revista.
Año de publicación: 2001
Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=54715149004>
Palabra clave: Tecnologías, exclusión, brecha digital.

Autor: **Saavedra Ponce Viridiana**

Título: Comaip: la ley debe contemplar la protección de datos personales.

Tema: Presidentes de los organismos de transparencia del occidente del país, de visita por Jalisco, aseguraron que debe legislarse en materia de protección a los datos personales. De acuerdo con César Octavio López, presidente de la Conferencia Mexicana para el Acceso a la Información Pública, "el ITEI es una institución consolidada y eso garantiza la continuidad de los trabajos".

Tipo de documento: Noticia de periódico.
Año de publicación: 2010
Publicación: <http://www.lajornadajalisco.com.mx/2009/08/06/index.php?section=politica&article=007n2pol>
Palabras clave: Datos personales y transparencia.

Autor: **Sánchez Martínez José Alberto**

Título: Internet y la vigilancia de sí: morphing y post-image en el siglo de las cámaras y pantallas.

Tema: Es posible sospechar que el siglo XXI será el siglo de las cámaras y las pantallas, el de una realidad que será grabada y retransmitida. A diferencia del otro siglo, el XX, las cámaras y las pantallas cobrarán una relevancia sin igual, sobre todo en el diálogo que ejercen lo digital e Internet. Algunos sospechan algo más, que en nuestro siglo crecerá el uso de cámaras y pantallas hacia la video vigilancia. Lo que este trabajo busca no es asumir la video vigilancia desde una perspectiva del control del estado, sino tratar de entender qué pasa con la cámara y la pantalla en la relación que establece con Internet, cómo se relacionan con los cibernautas, con uno mismo, qué rol asume uno. El texto explora la identidad como estatuto de la video vigilancia, la crisis de la imagen de sí mismo, hasta la criollización visual que desemboca en el morphing y la post image

Tipo de documento: Artículo de revista.
Año de publicación: 2000
Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=32513865004#>
Palabras clave: Internet, tecnologías, vigilancia del software.

Autor: **San Martín Velasco Cristos**

Título: Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México.

Tema: La privacidad y la protección de datos personales son elementos, importantes en las distintas modalidades del comercio electrónico, pero particularmente han tomado mayor relevancia en el área de Bussines, al momento en que los consumidores llevan a cabo transacciones comerciales por medios electrónicos, compras en Internet o simplemente al intercambiar datos e información con otros usuarios, empresas y gobierno en la red. El tema de protección de datos personales está tomando cada vez mayor importancia en otro tipo de portales de comercio electrónico como son el Government to bussines , sobre todo a medida que el gobierno mexicano implementa gradualmente el sistema E-Gobierno, por medio del cual pretende garantizar a los ciudadanos el libre acceso a una gama de servicios públicos.

Tipo de documento: Artículo de página web.

Año de publicación: 2010

Publicación:

<http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf>

Palabras clave: datos personales, transparencia.

Autor: **Siles González Ignacio**

Título: A la conquista del mundo en línea: Internet como objeto de Estudio (1990-2007) en comunicación y sociedad.

Tema: Este artículo explora el desarrollo de la investigación sobre Internet entre 1990 y 2007. Para esto, se analizan los principales ejes temáticos de los estudios sobre tal medio a lo largo de casi dos décadas y se presentan diversos debates que han definido su evolución como objeto de estudio. Se sugiere a final de cuentas, que los estudios sobre Internet constituyen un campo de conocimientos en proceso de construcción, con creciente legitimidad académica.

Tipo de documento: Artículo de revista.

Año de publicación: 2001

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=34601003>

Palabras clave: Internet, identidad.

Autor: **Tello Leal Edgar**

Título: Las tecnologías de la información y comunicación y la brecha digital: su impacto en la sociedad de México.

Tema: Es deseable alcanzar una sociedad del conocimiento donde la inclusión de los individuos en la generación del conocimiento sea total, que las sociedades del conocimiento sean fuentes de desarrollo para todos y sobre todo para los países menos adelantados. El presente artículo tiene como propósito analizar el papel de la brecha digital y la brecha cognitiva en las sociedades del conocimiento como causales de la exclusión de las empresas e individuos en el uso de las tecnologías de la información y comunicación en México. En consecuencia, hoy encontramos una nueva forma de exclusión, denominada brecha digital, capaz de ampliar el abismo que separa a las regiones y a los países y a los grupos de ciudadanos de una sociedad. La brecha cognitiva pone de manifiesto el potencial de exclusión que pueden conllevar las sociedades del conocimiento, cuando su desarrollo se limita a promover una economía del conocimiento. Así mismo el trabajo aporta cifras de la brecha digital en México, tanto en los hogares como en las empresas, a fin de poner de manifiesto que existe un acceso desigual entre las zonas geográficas, del país, que no sólo depende de la infraestructura disponible, sino de las habilidades de la población para utilizar las tecnologías de la información y comunicación.

Tipo de documento: Artículo de revista.

Año de publicación: 2001

Publicación: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=78011231006>

Palabras clave: Tecnologías, exclusión.

Autor: **Winocur Iparraguirre Rosalía**

Título: La computadora e Internet como estrategia de inclusión social en el imaginario de los pobres.

Tema: Las nuevas tecnologías forman parte del imaginario popular, aunque la mayoría de las personas no tenga acceso a ellas, estos imaginarios construyen deseos, expectativas y aspiraciones, pero también temores y ansiedades de que la computadora se convierta en un factor de exclusión social, esta investigación se centra en San Lorenzo Chimalpa en Chalco.

Tipo de documento: Artículo de blog.

Año de publicación: 2010

Publicación: http://campus.usal.es/~teoriaeducacion/rev_numero_06/n6_res_winocur_rosalia.htm

Palabras clave: Tecnologías y exclusión social.

Autor: **Zabia de la Mata Juan**

Título: Protección de datos: comentarios al reglamento.

Tema: En noviembre de 2005, la RED Iberoamericana de Protección de Datos, creó mediante la declaración de México el grupo de "instrumentos de autorregulación" con el fin de analizar la validez y eficacia de los códigos de conducta o instrumentos análogos, teniendo en cuenta la importancia de las iniciativas de los propios responsables de ficheros o tratamientos para que la protección de datos se lleve a cabo a través de instrumentos de autorregulación. Se elaboró un documento "Autorregulación y protección de datos personales" en que se habla de: incorporar en los textos legales sobre protección de datos disposiciones explícitas referentes a utilizar mecanismos de autorregulación e invitar a los estados y a los responsables del tratamiento de datos personales a promover la adopción y aplicación de mecanismos de autorregulación.

Tipo de documento: Libro

Año de publicación: 2010

Publicación:

www.books.google.com/books?id=R4GWPWwW8JcC&pg=PA644&dq=proteccion+de+datos+per+sonales+mexico

Palabras clave: Seguridad jurídica, derechos fundamentales y protección de datos.

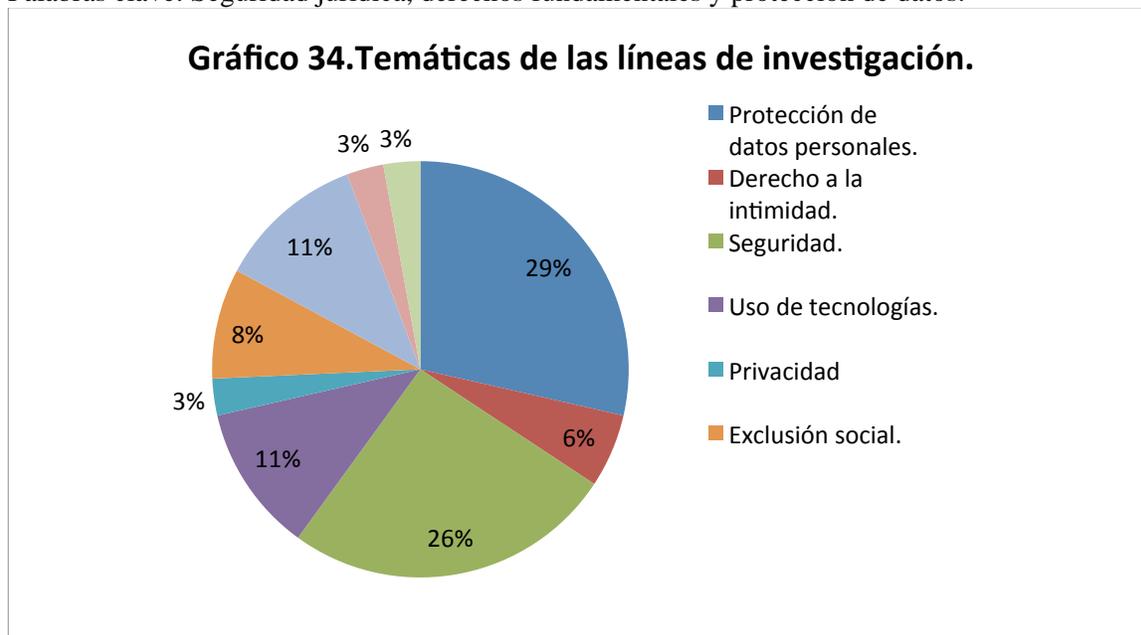
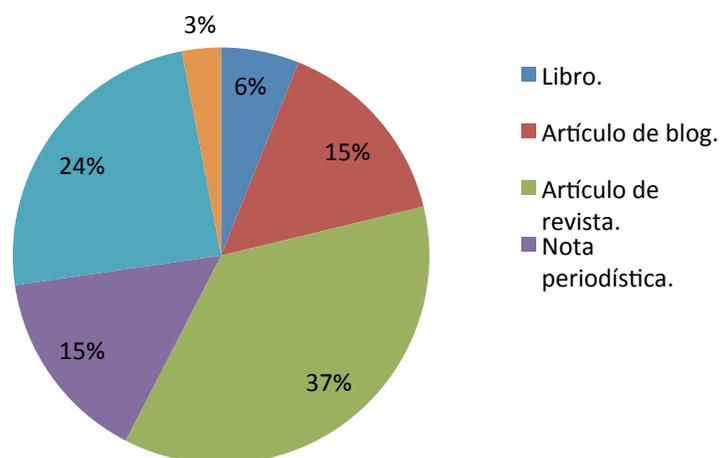


Gráfico 35. Modalidades de los documentos.



La protección de datos personales en México, constituye una problemática que ha generado diversas vertientes en su estudio; la naturaleza misma del fenómeno ha incidido en la construcción de algunas categorías de análisis para la comprensión del tema. Sin embargo, la producción de documentos y de información al respecto pareciera no ser tan sólida en su construcción científica. Mayoritariamente, las aportaciones al tema provienen de modalidades de publicación como son el artículo en blog, notas periodísticas de opinión, etc. Luego, pareciera que el estudio de la protección de datos personales en México se encuentra aislado de la producción del conocimiento científico que debiera darse en universidades y centros de investigación y docencia. Los resultados del mapeo realizado indican que el 76% de las fuentes de información provienen de blogs, grupos editoriales o de portales electrónicos; mientras que el 24% de algún proyecto de investigación albergado en algún centro de investigación y tutelado por un investigador. Asimismo, el tema de la protección de datos personales en México, es una problemática que no logra consolidarse como debate en la construcción de la agenda pública gubernamental.

ii Agentes relevantes

Agente: **Gurú político.**

Tipo/Modalidad: Público, blog.

Propuesta: Posicionar el tema de la protección de datos personales en la definición de la agenda pública gubernamental.

Año: 2010

Descripción: De los creadores del Centro de Inteligencia Política (CEINPOL) que funcionó del 1 de Febrero de 2009 a Junio de 2010, llega ahora Gurú Político (fundado el 1 de Julio de 2010). Un sitio de Internet mexicano especializado en contenidos editoriales exclusivos de carácter político y con un análisis diario del acontecer nacional e internacional. Hecho desde Acapulco, Guerrero, México. Gurú Político no es prensa, no es un medio noticioso: es un medio de opinión y análisis exclusivamente.

Ámbito de incidencia: Uso de las tecnologías y seguridad.

Agente: **Transparencia de Nuevo León**

Tipo/Modalidad: Público, Revista.

Propuesta: Evento: "Archivos y Rendición de Cuentas", organizado conjuntamente con el National Security Archive de la George Washington University.

Año: 2010

Descripción: Es una revista cibernética en donde se busca la transparencia de los datos, además de publicar documentos relacionados con la protección de datos personales, esta es patrocinada por la Comisión de Acceso a la Información Pública de Nuevo León.

Ámbito de incidencia: Uso de las tecnologías y protección de datos personales.

Agente: **Benemérita Universidad Autónoma de Puebla**

Tipo/Modalidad: Público, Universidad.

Propuesta: Publicación de un artículo especializado en la legislación federal de protección de datos, dentro de su página de Internet

Año: 2010

Descripción: Es una página de la Benemérita Universidad Autónoma de Puebla, que corresponde a la Dirección de Comunicación Institucional, la cual se encarga de publicar todas las actividades e inquietudes de los universitarios.

Ámbito de incidencia: protección de datos personales y difusión de la ciencia.

Agente: **Instituto Federal de Acceso a la Información (IFAI)**

Tipo/Modalidad: Público, Instituto.

Propuesta: VIII Encuentro Iberoamericano de Protección de datos en la Ciudad de México del 29 de Septiembre de 2010.

Año: 2010

Descripción: Se organizaron una serie de conferencias. Entre las mejores es la de Chantal Bernier sobre la protección de datos personales en la era digital.

Ámbito de incidencia: Internet, uso de tecnologías y vulnerabilidad.

Agente: **Universidad Autónoma de Nuevo León**

Tipo/Modalidad: Público; Universidad.

Propuesta: Se realizó un panel de protección de datos denominado "Perfectible el sistema de protección de datos"

Año: 2010

Descripción: El tema principal en el panel fue la reforma de Ley Federal de Protección de Datos Personales, no ha recibido difusión ni importancia.

Ámbito de incidencia: difusión del tema protección de datos personales.

Agente: **Alianza cívica, A.C. Construyendo ciudadanía activa.**

Tipo/Modalidad: Público; Asociación civil.

Propuesta: Definición de los datos personales que están protegidos por la ley.

Año: 2010

Descripción: Realizó en Sonora una capacitación respecto a la protección de datos personales.

Ámbito de incidencia: Protección de datos personales, opinión y participación.

Agente: **Mercedes Benz**

Tipo/Modalidad: Empresarial.

Propuesta: Realizó un apartado en su página web, en donde aclara que se va a hacer o a dónde van a ir sus datos personales al ingresar

Año: 2010

Descripción: Dejan en claro que el manejo de los datos personales están apegados a la ley al realizar cualquier transacción

Ámbito de incidencia: protección de datos personales; seguridad.

Agente: **PC World**

Tipo/Modalidad: Privado; Portal.

Propuesta: Dio a conocer por medio de su página un artículo donde se conocen 10 formas de cómo navegar seguro por la Internet.

Año: 2010

Descripción: Es un portal en línea que permite tomar decisiones acertadas y oportunas. Además de ofrecer acceso rápido al contenido de la revista, reúne una serie de servicios que ayudan a encontrar las respuestas a los problemas que surgen más frecuentemente al trabajar con una computadora. A raíz de la preocupación de poder navegar seguro, ESET informa 10 pasos sencillos para poder navegar seguro en Internet. Unos de los pasos más importantes son: evitar los enlaces sospechosos, no acceder a sitios web de dudosa reputación, evitar el ingreso de información personal en formularios dudosos y aceptar solo contactos conocidos.

Ámbito de incidencia: uso de las tecnologías; seguridad.

Agente: **Universidad Nacional Autónoma de México (UNAM)- CERT**

Tipo/Modalidad: Público.

Propuesta: El UNAM-CERT es un equipo de profesionales en seguridad en cómputo, además de que se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún ataque, así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.

Año: 2010

Descripción: Es un equipo que se encarga de la seguridad de sitios que han recibido ataques.

Ámbito de incidencia: protección de datos personales, seguridad, y ataques en la red.

Agente: **Subdirección de seguridad de la información. UNAM.**

Tipo/Modalidad: Público.

Propuesta: Da a conocer esquemas de protección computacionales.

Año: 2010

Descripción: Las acciones que realiza son dar respuesta a incidencias, elaboración de boletines de seguridad en cómputo, así como el diseño de esquemas de seguridad.

Ámbito de incidencia: seguridad.

Agente: **Habeas Data**

Tipo/Modalidad: Público;

Propuesta: Informa que México será por primera vez sede de la conferencia de comisionados de protección de datos.

Año: 2010

Descripción: Habeas Data es la organización de profesionales de la privacidad más importante de América Latina, se dedica a fomentar a impulsar la conciencia sobre la protección de Datos Personales en Argentina y América Latina, además contiene cerca de 600 documentos entre leyes, normas reglamentarias, proyectos, jurisprudencia, artículos, noticias, seminarios y conferencias, entre los artículos encontrados es el que habla de: Informa acerca del próximo gran evento que está a favor de la protección de datos personales.

Ámbito de incidencia: protección de datos personales.

Agente: **E-nnovative**

Tipo/Modalidad: Empresarial.

Propuesta: Dar a conocer la problemática vinculada con la exclusión por medio del Internet.

Año: 2010

Descripción: Es una empresa mexicana dedicada al desarrollo y diseño de páginas web, pone a su disposición las herramientas necesarias para mantener a la vanguardia su computadora, dentro de esta página web contiene un BLOG en el cual varios escriben artículos relacionados con la tecnología como el siguiente: Analiza como el Internet además de ser un instrumento que vincula, también excluye y pone el ejemplo de la declaración tributaria.

Ámbito de incidencia: violencia, Internet, exclusión, tecnologías.

Agente: **Ciudad cívica.**

Tipo/Modalidad: Público; Blog.

Propuesta: Analiza las tecnologías de la información y como ha llegado la exclusión social a raíz de ellas.

Año: 2010

Descripción: Ciudad Viva es una iniciativa de la CONSEJERIA DE OBRAS PÚBLICAS Y VIVIENDA, que se inscribe dentro de un proyecto político de mejora de la habitabilidad urbana y territorial, se trata acerca de la revalorización de los barrios, el cual es el elemento clave de conexión con las personas que viven en la ciudad.

Ámbito de incidencia: exclusión social; tecnologías.

Agente: **Diario crítico de México.**

Tipo/Modalidad: Público; Grupo editorial.

Propuesta: Da a conocer noticias acerca de la tecnología y la exclusión social.

Año: 2010

Descripción: Es un grupo editorial el cual publica artículos de toda índole, además de estar en diferentes países, desde España y toda América Latina.

Ámbito de incidencia: exclusión social, uso de la tecnología.

Agente: **Cultura para todos.**

Tipo/Modalidad: Público; Blog.

Propuesta: Da el seguimiento acerca de la tecnología y como ayuda a la cultura y con ello a lograr una sociedad más justa y equitativa.

Año: 2010

Descripción: Es un blog donde se quiere la igualdad en el acceso a la cultura, sin exclusión. El objetivo de este proyecto de inclusión es lograr la accesibilidad a personas con alguna discapacidad y así garantizar una cultura para todos.

Ámbito de incidencia: Inclusión y acceso a la información.

Agente: **Protección de datos personales.**

Tipo/Modalidad: Público; Fundación y perfil.

Propuesta: Es una fundación a favor de la protección de datos personales, el cual ha fundado un grupo en Facebook con el fin de informar, educar y posicionar en el debate ciudadano el tema de la protección de datos personales en Chile y en el extranjero.

Año: 2010

Descripción: Es una página de una fundación con el mismo nombre, la cual se encarga de informar y educar acerca de la importancia que se le debe de tener a este asunto de los datos personales, al estar en Facebook lo que intenta es informar a los jóvenes o a la gente en general acerca de la importancia de este asunto.

Ámbito de incidencia: protección de datos personales.

Agente: **Privacy international**

Tipo/Modalidad: Público;

Propuesta: Es una organización que hace campañas a nivel internacional sobre cuestiones de privacidad, desde 1987.

Año: 2010

Descripción: Privacy International es una organización no gubernamental con la función primordial de promoción y apoyo, los objetivos son: dar a conocer y proporcionar educación acerca de las amenazas a la privacidad personal, para controlar la naturaleza, la eficacia y el alcance de las medidas para proteger la privacidad y los datos personales, para llevar a cabo la investigación sobre las amenazas a la privacidad personal, para controlar e informar sobre las actividades de vigilancia de las fuerzas de seguridad y de inteligencia. Este año sus campañas, la actividad de los medios de comunicación y proyectos que abarca continuar con la labor de promoción de las garantías de privacidad en los países en desarrollo.

Ámbito de incidencia: protección de datos personales; privacidad.

Agente: **CSO, España.**

Tipo/Modalidad: Público; Blog.

Propuesta: Es un blog que contiene noticias para la seguridad dentro del ciberespacio, como es el de "Redes sociales: beneficios y riesgos para la privacidad de los datos".

Año: 2010

Descripción: Da a conocer diferentes temas relacionados con la protección de datos personales y la privacidad en Internet.

Ámbito de incidencia: Protección de datos personales.

Agente: **Salomón**

Tipo/Modalidad: Público; Grupo editorial.

Propuesta: Publicación de artículos en los cuales se expone la preocupación que hay por la falta de organización y legislación de datos personales.

Año: 2010

Descripción: Es un artículo que habla de las deficiencias en los temas de seguridad de datos en Estados Unidos, y la relación que puede existir con España, para este 2011, donde la nueva ley española de protección de datos presume que puede ser potencialmente caro para las empresas que no cumplan con esta ley de protección. Algunos temas de seguridad de datos más importantes que proyectan para 2011 en E.U.A son: los robos de información "low tech" aumentarán, la pérdida de información como resultado de pérdida de dispositivos electrónicos aumentará, la minimización de la información recolectada será más común para minimizar las pérdidas de información.

Ámbito de incidencia: protección de datos personales.

Agente: **Política Digital**

Tipo/Modalidad: Público

Propuesta: Promueve el buen uso de tecnologías de información y comunicación para la calidad de las instituciones públicas en los tres poderes, en ámbito federal, estatal y municipal.

Año: 2010

Descripción: Es un artículo que toca el tema de los servicios públicos estatales de salud donde en Sinaloa, por ejemplo, el sistema propietario de expedientes médicos ha ayudado a tener una mayor información de pacientes y enfermedades, este piloto de proyecto, podrá beneficiar en el sentido de que podemos comunicarnos entre instituciones hospitalarias y clínicas, lo cual puede desarrollar una estrategia común en servicios de salud electrónicos.

Ámbito de incidencia: uso de tecnologías.

Gráfico 36. Tipos de agentes

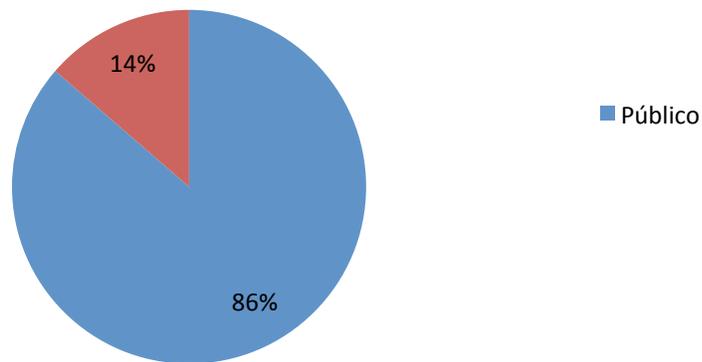
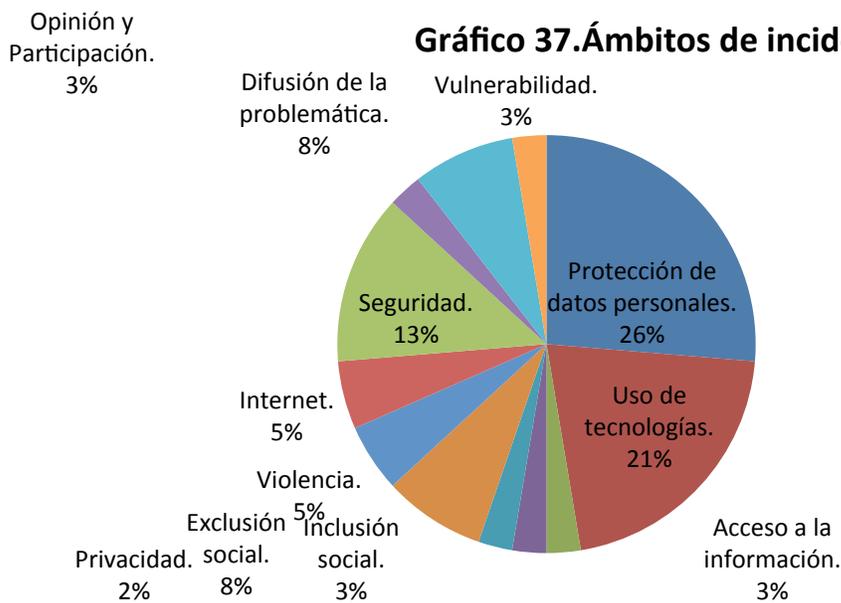


Gráfico 37. Ámbitos de incidencia.



La producción de información respecto del tema pareciera provenir de agentes considerados como públicos. El carácter público de estos agentes resulta de su propia modalidad. Es decir, la construcción y actualización de los diferentes blog, páginas web, portales de asociaciones civiles, grupos editoriales, etc. se llevan a cabo a partir de las aportaciones de los individuos interesados en el tema. No obstante, el debate de la protección de datos personales en México continúa volátil. Los datos indican que el debate es intensamente heterogéneo en la definición y atención del problema.

iii Tecnologías y Normatividad. La protección de datos personales en México

Siguiendo el modelo teórico propuesto para la identificación de la tipología de los sistemas constitucionales en materia de libertades informativas,⁶⁴ el reconocimiento constitucional de la

⁶⁴ El modelo se basa en la observación de las reglas del reconocimiento de las libertades y derechos. De ahí que existan, en esa tipología: 1. constituciones que no poseen previsiones respecto de esas libertades y derechos; 2. constituciones que no protegen y que no reconocen esas libertades y derechos, o que sin hacerlo delegan su reglamentación en una ley de carácter particular; 3. constituciones de corte decimonónico, llamadas así por el reconocimiento de esas libertades y derechos, pero con carácter genérico, es decir, partiendo de percepciones teóricas clásicas; 4. constituciones minimalistas,

protección de datos personales puede conocerse atendiendo a dos grupos de constituciones. En el primero de ellos, se encuentran aquellas constituciones paradigmáticas, pues han incorporado una cláusula constitucional relativa al reconocimiento de la protección de datos personales, derecho a la autodeterminación informativa o libertad informática; excluyéndose por lo tanto su proclamación y reconocimiento como un derecho derivado de la intimidad y la vida privada. En el segundo grupo de leyes fundamentales, se aglutinan aquellas de corte decimonónico y minimalista, pues la protección de datos no es reconocida como un derecho autónomo, sino más bien, considerado por el orden jurídico como un derecho que deriva de la intimidad personal y a consecuencia de ello, se desarrolla su protección a través de una o varias leyes reglamentarias particulares.

Para lo que aquí nos interesa, es importante apuntar que el carácter paradigmático de las constituciones que reconocen a la protección de datos personales como un derecho autónomo y al *Habeas Data* como su mecanismo jurídico *ad hoc* de tutela, se debe a que se identifican con Estados constitucionales y democráticamente consolidados o bien, con Estados nacionales producto de una ruptura político-institucional.

En consecuencia, el reconocimiento de la protección de datos personales con esa denominación u otras diferentes a las de intimidad y vida privada, como un derecho fundamental se localiza en los textos constitucionales de: Albania, Argentina, Armenia, Azerbaijan, Bolivia, Brasil, Cabo Verde, Colombia, Confederación Suiza, Croacia, Ecuador, Eslovaquia, Eslovenia, España, Estonia, Federación Rusia, Finlandia, Gabón, Georgia, Guatemala, Hungría, Kazakhsan, Macedonia, Moldavia, Nicaragua, Países Bajos, Paraguay, Perú, Polonia, Portugal, República Checa, Rumania, Serbia y Montenegro, Sudáfrica, Suecia, Ucrania y Venezuela.

De forma paralela a su reconocimiento, en las cartas fundamentales de Bolivia, Brasil y Cabo Verde se ha instituido para su salvaguarda y promoción efectiva un mecanismo constitucional denominado *Habeas Data*.

Antes de dar cuenta de la evolución del derecho a la autodeterminación informativa en el ámbito internacional, vale la pena señalar que hay una diversidad de datos personales. En este sentido, el término *datos personales* se refiere a todo tipo de información relacionada con una persona identificada o identificable, como la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad; ya sean de carácter público o privado y que sean o hayan sido procesados de forma manual o automática.⁶⁵ Como puede verse, el riesgo a que está expuesta la dignidad humana, frente a las diversas técnicas de procesamiento de datos, hace que estos sean sensibles, es decir, que se les considere como “...información cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación.”⁶⁶

que además de reconocer libertades y derechos en materia informativa, otorgan al individuo un mínimo de posibilidades para su participación en los asuntos públicos; 5. constituciones cuasi-paradigmáticas, que permiten además del ejercicio de las libertades y derechos, incorporar instituciones que concedan el ejercicio de la democracia, y 6. constituciones paradigmáticas, llamadas así por presentar además de la constitucionalización de las libertades y derechos, instituciones para su fortalecimiento, como por ejemplo la introducción de garantías jurídicas *ad hoc*. Cfr. Villanueva, Ernesto. *Derecho comparado de la información*, Universidad Iberoamericana-Fundación Konrad Adenauer, México, 2002, pp. 31-33.

⁶⁵ Cabría agregar a la concepción de los datos personales, la implicación de su cesión o comunicación a terceros. Al respecto *vid.* Messía de la Cerda Ballesteros, Jesús Alberto. *La cesión o comunicación de datos de carácter personal*, Thomson-Civitas, Madrid, 2003.

⁶⁶ Pierini, Alicia. *op. cit. supra*, p. 25.

Por tanto, se coincide con la tesis que sostiene que un dato personal aislado, no posee valor alguno, sino que lo adquiere al ser relacionado con otros que permitan identificar a un individuo.⁶⁷ Esto, pone ampliamente de manifiesto el riesgo a que está expuesta la privacidad y la intimidad del individuo, ante la amenaza latente que representa la informatización de actividades. La vigilancia silenciosa que se hace de sus pasos, es ante los enemigos de la vida democrática, el argumento que permite fundamentar el interés del Estado por elaborar una política y normas de protección de la seguridad nacional e internacional, pero también para vulnerar y socavar los valores de libertad y dignidad de la persona.⁶⁸

Por otra parte, el origen de la prerrogativa para acceder a la información en México, se remonta a la reforma constitucional de 1977. Con en ella, se adicionaron 10 palabras a la parte final del artículo 6º constitucional, para establecer: *El derecho a la información será garantizado por el Estado.*

En el marco de la también llamada *reforma política*, impulsada por el entonces Presidente de la República José López Portillo, se pretendió mediante la misma, permitir el acceso de los partidos políticos a los medios de comunicación masiva, es decir, a los tiempos de la radio y la televisión.⁶⁹

⁶⁷ Cfr. Riande Juárez, Noé Adolfo. *¿Por qué debe legislarse en México en materia de Protección de Datos Personales Automatizados?* Ponencia presentada en el marco del VIII Congreso Iberoamericano de Derecho e Informática, celebrado del 21 al 25 de noviembre de 2000 en el Campus Estado de México del Tecnológico de Monterrey. Dice este autor que: *Cuando se pretende el respeto al dato vinculado a un inventario, a una nómina o a una estadística, desinteresándose de su relación con las personas, lo que se protege es el servicio o buen desempeño de un mecanismo administrativo o productivo pero no a las personas en su intimidad, en su dignidad, su integridad o su libertad.* Así también vid. la Sentencia del Tribunal Supremo de España bajo el rubro *Protección de datos de carácter personal. Alcance de la expresión «dato personal». Datos de carácter personal: Clases. Solicitud de información a la Dirección General de Tráfico sobre la titularidad y cargas de los vehículos registrados a nombre de personas determinadas. Datos de carácter personal no accesibles al público. Correcta denegación.* En ella el Supremo estableció que: *La expresión «dato personal» no es sinónima de «dato de carácter personal» porque no siempre un dato es un dato de carácter personal y por qué, además, hay datos de carácter personal que no son datos personales.* Cfr. Amadeo Gadea, Sergio Luis. *Informática y nuevas tecnologías*, LA LEY, Madrid, 2001, pp. 9-10.

⁶⁸ Esta tendencia a la vejación y menosprecio por la libertad y dignidad de la persona, ha cobrado mayor auge tras el atentado terrorista a las Torres Gemelas del *World Trade Center (WTC)* de Nueva York el 11 de septiembre; a consecuencia de ello, se implementaron medidas de reforzamiento de la seguridad en los aeropuertos internacionales de diversas ciudades del Mundo, con el fin de que agentes de la *Transportation Security Agency (TSA)*, registraran el equipaje, documentos e identidad los pasajeros que ingresen por vía aérea al territorio de los Estados Unidos de Norteamérica.

⁶⁹ En la Exposición de Motivos que acompañó a la Iniciativa de reformas y adiciones a la Constitución Política de los Estados Unidos Mexicanos, y que fuera presentada por el Ejecutivo Federal, se consideró que: El carácter de interés público que en la iniciativa se reconoce a los partidos políticos, hace necesario conferir al Estado la obligación de asegurar las condiciones para su desarrollo, y de propiciar y suministrar el mínimo de elementos que estos requieran en su acción destinada a recabar la adhesión ciudadana. También se hace necesario garantizar en forma equitativa a los partidos políticos nacionales, la disposición de los medios que les permitan difundir con amplitud sus principios, tesis y programas, así como los análisis y opiniones que formulen respecto de los problemas de la sociedad. Para este fin, se estima conveniente establecer como prerrogativa de los partidos políticos, su acceso permanente a la radio y la televisión, sin restringirlo a los períodos electorales. Esta prerrogativa de los partidos políticos tiene el propósito de dar vigencia en forma más efectiva al derecho a la información, que mediante esta iniciativa se incorpora al artículo sexto constitucional, que será básico para el mejoramiento de una conciencia ciudadana y contribuirá a que ésta sea más enterada, vigorosa y analítica, lo cual es esencial para el progreso de nuestra sociedad. Siendo los partidos políticos entidades fundamentales en la acción ideológica y política, el ejercicio de su derecho a difundir sus ideas en los medios de comunicación social se traducirá en el mayor respeto al pluralismo ideológico y cobrará plenitud la libertad de expresión y su correlativo derecho a la información. Por otra parte, la diversidad de opiniones expresadas de manera regular por los partidos políticos en medios tan importantes como son la radio y la televisión, sumadas a las de otras fuentes generadoras de información, contribuirán a que ésta sea más objetiva y a que la opinión pública, al contar con una mayor variedad de criterios y puntos de vista, esté mejor integrada. Cfr. Comisión Federal Electoral. *Reforma Política*; Gaceta informativa de la Comisión Federal Electoral, Tomo III, México, 1978, p. 12. Así había sido entendido inicialmente el Derecho a la Información por el Pleno de la SCJN, al haber emitido la tesis aislada de jurisprudencia P. LXXXIX/96, bajo el Rubro: Garantías individuales (Derecho a la Información). Violación grave prevista en el segundo párrafo del artículo 97 constitucional. La configura el intento de lograr la impunidad de las autoridades que actúan dentro de una cultura del engaño, de la

En las ponencias presentadas en la Cámara de Diputados, “...se puso de relieve la relación del derecho a la información con el juego democrático y electoral, ya que sólo puede optar conscientemente quien está informado y no quien está influido o desorientado; por tanto, el derecho a la información se exige a través del Estado para hacer posible la democracia.”⁷⁰

En principio, la Constitución Política de los Estados Unidos Mexicanos reconocía el derecho a la intimidad y a la privacidad concretándolos en los ámbitos personal, familiar, así como de las propiedades y posesiones (domicilio y papeles)⁷¹ y de las comunicaciones privadas.⁷² Del primero de ellos puede decirse que se encontraba concebido conforme a los planteamientos y conceptos que han informado a los textos constitucionales de carácter liberal, pues se le reconocía como un Derecho Humano de primera generación; respecto al segundo cabe señalar que se trata de un derecho que deriva del anterior, pero su fin es proteger la privacidad de las comunicaciones, correspondiendo su configuración a los Derechos Humanos de tercera generación.

Cronológicamente puede identificarse a México como un país que en materia de protección de datos personales se cataloga hasta antes del año 2002 como decimonónico, pues la protección de la libertad informática se consideró como una extensión del derecho a la intimidad y a la vida privada y su protección se ejercía a través de una serie de normas jurídicas particulares.

Con el propósito de homologar a nivel nacional los criterios en materia de transparencia y acceso a la información pública, el 13 de diciembre de 2006, los gobernadores Luis Armando Reynoso Femat del Estado de Aguascalientes; José Reyes Baeza Terrazas de Chihuahua; Fidel Herrera Beltrán de Veracruz; Amalia García Medina de Zacatecas, así como Alejandro Encinas Rodríguez, Jefe de Gobierno del Distrito Federal, presentaron ante la Cámara de Diputados del Congreso de la Unión una iniciativa de reformas y adiciones a la Constitución Política de los Estados Unidos Mexicanos; la cual hicieron suya los coordinadores de todas las fuerzas políticas representadas en la cámara baja y consecuentemente la presentaron al Pleno el 19 de diciembre de 2006.

La *Iniciativa Chihuahua*⁷³ –como coloquialmente se le llamo– propuso reformar el artículo 6°

maquinación y del ocultamiento, por infringir el artículo 6o. también constitucional, misma que fuera ampliada por la diversa tesis aislada P. XLV/2000, bajo el rubro: Derecho a la Información. La Suprema Corte interpretó originalmente el artículo 6o. constitucional como garantía de partidos políticos, ampliando posteriormente ese concepto a garantía individual y a obligación del estado a informar verazmente.

⁷⁰ Carpizo, Jorge. *Nuevos Estudios Constitucionales*, Porrúa-UNAM, México, 2000, p. 401.

⁷¹ Así, el artículo 16° constitucional, en su párrafo primero, establece que: Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

⁷² En el párrafo décimo segundo del mismo artículo 16° (antes noveno párrafo), se establece que: Las comunicaciones privadas son inviolables. La Ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente, por escrito, deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

⁷³ La génesis de esta iniciativa se encuentra en la denominada *Declaración de Guadalajara* firmada el 22 de noviembre de 2005.

Complementariamente, la *Declaración México*, emanada de los trabajos del *IV Encuentro Iberoamericano de protección de datos personales* (2005), concluyó: 1. Asumir que la protección de datos personales es un derecho fundamental autónomo. 2. Asumir y tomar en cuenta las implicaciones de datos personales en telecomunicaciones y en la implementación del gobierno electrónico. 3. Es necesario estudiar el desarrollo normativo y la globalización en el ámbito del marketing, el sector financiero y transferencias internacionales de datos. 4. Asumir a los datos de salud como especialmente protegidos. 5. Es necesario contar con una ley de protección de datos, que considere los principios internacionalmente reconocidos en entidades públicas y privadas.

constitucional “...para ampliar los alcances del derecho a la información en todos los niveles de gobierno y los partidos políticos.”

Respecto de la protección de datos personales propuso: *La información que se refiera a la vida privada y los datos personales se considerará como confidencial y será de acceso restringido en los términos que fije la ley.*

La propuesta que hicieran los gobernadores de “cambio constitucional”, consideraba que los datos personales, además de ser confidenciales, deberían ser de acceso restringido. Tal planteamiento supone en primer lugar, que todos los datos personales son confidenciales por antonomasia, lo cual inhibe la posibilidad de expedir una ley particular que regule diversas categorías de datos personales y; en segundo lugar, al establecer que el acceso a los datos personales sea restringido provocaría el debilitamiento de instituciones públicas importantísimas como los registros públicos de la propiedad, comercio, civil, etcétera.⁷⁴

Tras la ardua labor que representa la reforma constitucional, el 20 de julio de 2007 se publicó en el *Diario Oficial de la Federación* el Decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos.

Particularmente, en las fracciones II y II se estableció que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes; y que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Sin embargo, el proceso legislativo de reforma constitucional ha propiciado la incorporación y extensión del derecho a la protección de datos personales al ámbito del proceso penal y cuando su posesión se encuentra en poder de particulares.

En este tenor de ideas, la reformulación del proceso penal en el año 2008, trajo consigo que la Constitución Política de los Estados Unidos Mexicanos le estableciera una orientación acusatoria y oral; y al regirse bajo los principios de publicidad, contradicción, concentración, continuidad e inmediación, reconoce a toda víctima u ofendido, el derecho para que se resguarde su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de

⁷⁴ Sobre este particular, las Comisiones Unidas de Puntos Constitucionales y de la Función Pública de la Cámara de Diputados del Congreso de la Unión, en el dictamen por el que perfeccionaron y aprobaron la *Iniciativa Chihuahua*, establecieron:

“...se establece una segunda limitación al derecho de acceso a la información, misma que se refiere a la protección de la vida privada y de los datos personales. Esta información no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental, que es el de la intimidad y la vida privada.

Es fundamental esclarecer que aunque íntimamente vinculados, no debe confundirse la vida privada con los datos personales. La primera se refiere al ámbito de privacidad de las personas respecto de la intervención tanto del estado como de otros particulares. Los datos personales, en cambio, son una expresión de la privacidad.

La fracción segunda establece también una reserva de ley en el sentido que corresponderá a ésta, determinar los términos de la protección y las excepciones a este derecho. Así es perfectamente posible considerar que cierta información privada o datos personales, que adquieran un valor público, podrán ser divulgados a través de los mecanismos que al efecto determine la ley. Este es el caso, por ejemplo, de los registros públicos de la propiedad, de los salarios de los funcionarios públicos o bien de la regulación del ejercicio del consentimiento del titular de la información para que esta pueda ser divulgada. En otras palabras, existen circunstancias en que, por ministerio la ley, los datos personales podrán ser divulgados sin el consentimiento del titular.

En otros casos, la ley deberá prever la posibilidad de que, algunos datos personales, puedan ser divulgados cuando un órgano jurisdiccional o administrativo determine que existen razones particulares que justifiquen su divulgación, previa garantía de audiencia del implicado. De cualquier forma, las autoridades deberán realizar una cuidadosa ponderación que justifique el hecho de que una información que pertenece al ámbito privado, puede ser divulgada por así convenir al interés público.”

delitos de violación, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa.

No obstante lo anterior, el Congreso de la Unión observó que desde el punto de vista constitucional no bastaba con el ámbito de cobertura de los datos personales conforme a lo previsto en el artículo 6°, pues era necesario proteger los datos personales que poseen los particulares; así como extender el derecho que toda persona tiene para la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

En tal sentido, se adiciono la fracción XXIX-O al artículo 73 constitucional y un segundo párrafo al artículo 16.

Desde un ángulo prospectivo, se observa que el trabajo legislativo desarrollado por el Congreso de la Unión, no sólo aquilato la experiencia internacional en la materia; debe considerarse que estimulo la discusión, aprobación y expedición de una Ley Federal de protección de datos personales en posesión de los particulares,⁷⁵ además de ampliar la denominación del Instituto Federal de Acceso a

⁷⁵ Debe señalarse en el ámbito federal la existencia de siete iniciativas para la expedición de normas reguladoras de los datos personales, de las cuales cinco buscan la expedición de una Ley Federal de Protección de Datos Personales.

El Diputado Luis Miguel Barbosa Huerta, presentó la Iniciativa con proyecto de Ley Federal de Firma y Comercio Electrónicos, Mensajes de Datos y Servicios de la Sociedad de Información, misma que fuera dictaminada y aprobada en la Cámara de Diputados con 422 votos en pro y una abstención, el martes 26 de noviembre de 2002; dictaminada y aprobada en la Cámara de Senadores con 84 votos en pro, el martes 8 de abril de 2003 y por tanto, turnada al Ejecutivo federal para los efectos constitucionales correspondientes (Gaceta Parlamentaria, número 999, martes 14 de mayo de 2002; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/58/2002/may/20020514.html#Ini20020514Barbosa>).

El diputado Jesús Aguilar Bueno, del grupo parlamentario del Partido Revolucionario Institucional (PRI), presentó el jueves 7 de octubre de 2004, la Iniciativa que reforma el Código Penal Federal en materia de pornografía infantil, corrupción de menores, comunicación y correspondencia, revelación de secretos y acceso ilícito a sistemas y equipos de informática, falsificación de documentos en general, amenazas y revelación de datos personales, delitos en contra de las personas en su patrimonio; al Código Federal de Procedimientos Penales en materia de aseguramiento del inculcado y careos, así como la Ley Federal Contra la Delincuencia Organizada, en materia de la naturaleza, objeto y aplicación de la ley (Gaceta Parlamentaria, número 1600-I, jueves 7 de octubre de 2004; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html>).

1. El Senador Antonio García Torres, del grupo parlamentario del PRI, en la sesión de la Comisión Permanente del miércoles 14 de febrero de 2001 (Gaceta Parlamentaria, número 688, jueves 15 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010215.html>).

2. El Diputado Miguel Barbosa Huerta, del grupo parlamentario del Partido de la Revolución Democrática (PRD), en la sesión del jueves 6 de septiembre de 2001 (Gaceta Parlamentaria, número 832, viernes 7 de septiembre de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/sep/20010907.html>).

En razón a esto, fue turnada a la Cámara de Diputados, previa aprobación por parte de la Cámara de Senadores, la Minuta con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales, misma que hasta la fecha se encuentra en estudio ante la Comisión de Gobernación y Seguridad Pública de la Cámara de Diputados (Gaceta Parlamentaria, número 1082, jueves 5 de septiembre de 2002; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/58/2002/sep/20020905.html#Minuta20020905DatosPersonales>).

En concordancia con ello, el Senador García Torres, presentó ante la Cámara de Senadores una iniciativa de reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos con el objeto de garantizar el derecho de toda persona a la protección y al acceso de sus datos personales (Gaceta Parlamentaria, número 692, miércoles 21 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio>).

A lo largo del año 2005, se tuvo la expectativa de que fuese aprobada la Minuta con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales; sin embargo, las diferencias políticas al interior de la Cámara de Diputados, pero sobre todo por las consideraciones que esgrimieran las Comisiones unidas de Gobernación y Economía en el *Anteproyecto de dictamen con modificaciones de las Comisiones unidas de Gobernación y Economía sobre la minuta con proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales*.

3. No obstante lo anterior, el Diputado Jesús Martínez Álvarez, del grupo parlamentario de Convergencia, sometió a la consideración del Pleno de la Cámara de Diputados, Iniciativa de Ley Federal de Protección de Datos Personales (Gaceta

la Información Pública, amplió sus facultades para que además de tener a su cargo la promoción y difusión del ejercicio del derecho a la información y resolver sobre la negativa a las solicitudes de acceso a la información y la protección de los datos personales en poder de las dependencias y entidades, difunda el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promueva su ejercicio y vigile la debida observancia de las disposiciones relativas a la protección de datos personales en posesión de las sociedades de información crediticia y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sean para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Desde otro ángulo, debe considerarse que coloco a la protección de datos personales en el sitio constitucional que le corresponde.⁷⁶

No obstante el reconocimiento constitucional a la información relativa a la vida privada y la incorporación del derecho a la protección de los datos personales como derechos fundamentales autónomos, de manera previa se configuro un sistema normativo integrado por un catálogo de leyes y disposiciones reglamentarias a través de las cuales se protegen los datos personales. Hoy en día se cuenta con una Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y 30 leyes de transparencia de carácter estatal, una diversidad de reglamentos municipales y otros más correspondientes a órganos constituidos y constitucionales autónomos del Estado.

Por todo ello, es posible dar cuenta de la existencia de disposiciones jurídicas que regulan los datos personales en materias como: ejercicio y protección de los derechos político-electorales de los ciudadanos, comercio electrónico, fiscal y crediticia, información estadística y geográfica, laboral, control vehicular, identificación de la población, salud, derechos de autor, telecomunicaciones,

Parlamentaria, número 1895-I, jueves 1 de diciembre de 2005; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html#Iniciativas>.

Senado

4. Por su parte, el Diputado David Hernández Pérez, del grupo parlamentario del Partido Revolucionario Institucional (PRI), presento otra Iniciativa de Ley Federal de Protección de Datos Personales (Gaceta Parlamentaria, número 1953-I, jueves 23 de febrero de 2006; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas>).

5. La diputada Sheyla Fabiola Aragón Cortés, del grupo parlamentario del Partido Acción Nacional (PAN), presento también una Iniciativa de Ley Federal de Protección de Datos Personales, (Gaceta Parlamentaria, número 1972-I, miércoles 22 de marzo de 2006, disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas>).

Finalmente, debe dejarse constancia de la iniciativa por el que se adiciona el inciso N) a la fracción XXIX del artículo 73 de la Constitución General, a efecto de dotar de atribuciones al Congreso de la Unión, para legislar en materia de protección de datos personales en posesión de particulares, presentada por los diputados Luis Gustavo Parra Noriega, María del Pilar Ortega Martínez, Rogelio Carbajal Tejada, Dora Alicia Martínez Valero, Esmeralda Cárdenas Sánchez y Jesús de León Tello, integrantes del Grupo Parlamentario del PAN.

⁷⁶ De forma previa a la reforma constitucional de julio de 2007, las Entidades Federativas de Morelos y México, constitucionalizaron el derecho a la protección de datos personales.

Mediante Decreto número 1069, publicado en el Periódico Oficial del 11 de agosto de 2003, se adiciono el artículo 23-A a la Constitución Política del Estado Libre y Soberano de Morelos; en dicho precepto se establece que el Congreso del Estado establecerá un organismo autónomo para tutelar el derecho de acceso a la información pública de todas las personas, proteger los datos personales y realizar estadísticas, sondeos y encuestas imparciales que coadyuven al cumplimiento de las funciones de los poderes públicos y al desarrollo democrático del Estado, denominado Instituto Morelense de Información Pública y Estadísticas.

Por otra parte, mediante Decreto número 44, publicado en la Gaceta del Gobierno del 30 de abril de 2004, se adicionaron dos párrafos al artículo 5 de la Constitución Política del Estado Libre y Soberano de México, en los que primeramente se establece la garantía protección, respeto y difusión del derecho a la información, y en segundo término, se obliga a los poderes públicos y órganos autónomos a transparentar sus acciones, garantizar el acceso a la información pública y proteger los datos personales en los términos que señale la ley reglamentaria.

control empresarial, entre otras.⁷⁷

Además de ese elenco normativo, existen otras disposiciones contenidas en Tratados Internacionales, leyes secundarias o reglamentarias de preceptos constitucionales, códigos, reglamentos, convenios, acuerdos, lineamientos, etcétera, las cuales ejercen una enorme influencia en la conformación del marco jurídico de la protección de datos personales, el cual, va acompañado de una agresiva política de transparencia, rendición de cuentas y acceso a la información.

Singular relevancia adquieren las obligaciones internacionales contraídas en la materia por México, entre ellas, las derivadas del *Acuerdo de Asociación Económica, Concertación Política y Cooperación entre los Estados Unidos Mexicanos y la Comunidad Europea y sus Estados Miembros, la Decisión del Consejo Conjunto de dicho Acuerdo; y la Decisión del Consejo Conjunto del Acuerdo Interino sobre Comercio y Cuestiones Relacionadas con el Comercio entre los Estados Unidos Mexicanos y la Comunidad Europea*, de 8 de diciembre de 1997; el que podría considerarse como Tratado de Libre Comercio entre México y los Estados Miembros de la Unión Europea.⁷⁸

En dicho Acuerdo, se reconoce a las TIC como uno de los sectores clave en el desarrollo de la SI, así como del desarrollo económico y social. Por ello, el gobierno de México y los de los Estados miembros de la Unión Europea, se comprometen a la realización de diversas acciones, como el establecimiento del diálogo sobre la cooperación, en relación a la reglamentación tocante a los servicios internacionales en línea, incluidos los aspectos relacionados con la protección de la privacidad y de los datos personales; así como fomentar el acceso recíproco a bases de datos, según las modalidades que serán convenidas.

Por tanto, en los artículos 41 y 51 del Acuerdo, se convino en primer lugar, la cooperación para lograr y mejorar el nivel de protección y prevenir los obstáculos a los intercambios que requieran transferencia de datos de carácter personal. En segundo término, garantizar un grado elevado de protección respecto al tratamiento de los datos de carácter personal y de otra índole, de conformidad con las normas adoptadas por los organismos internacionales competentes en la materia y por la Comunidad. Dichas normas se encuentran enunciadas en el Anexo del Acuerdo y son: las Directrices para la reglamentación de los archivos de datos personales informatizados, modificadas por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1990; la Recomendación del Consejo de la OCDE sobre las directrices por las que se rige la protección de la privacidad y los flujos transfronterizos de datos personales, de 23 de septiembre de 1980; el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981; y, la Directiva CE/95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Como puede observarse, México debe no solamente cumplir con las obligaciones contraídas en las materias descritas en el texto del Acuerdo, sino también con el contenido de otras disposiciones de carácter internacional emanadas de los foros en los que tiene la calidad de miembro; amén de ello, cumplir con las disposiciones de la Unión Europea en materia de protección de datos personales.

⁷⁷ Sobre el particular Cfr. Piña Libien, Hiram Raúl. *El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano*, Instituto de Transparencia y Acceso a la Información Pública del Estado de México, México, 2008.

En una orientación similar Gómez-Robledo, Alonso y Ornelas Núñez, Lina. *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, UNAM, México, 2006.

⁷⁸ Cfr. *Decreto Promulgatorio del Acuerdo*, publicado en el Diario Oficial de la Federación de 26 de junio de 2000; así como el Diario Oficial de las Comunidades Europeas del 28 de octubre de 2000 L 276/45.

Esto es, con los requerimientos y exigencias de la Directiva 95/46/CE, en cuanto a la observancia de los principios rectores de la libertad informativa.

Nada o poco de trascendente tendrían, si lo anterior se coloca en términos simples de cumplimiento de las obligaciones internacionales contraídas; sin embargo, la trascendencia que reviste la aplicación de la Directiva 95/46/CE, no depende del mero cumplimiento de obligaciones, sino de la incorporación del Derecho Comunitario en el ámbito del Derecho interno de un tercer país. En otras palabras, de la incorporación al Derecho Mexicano del Derecho de la Unión Europea, de la supranacionalidad con que se conduce el segundo para lograr su vigencia, aplicación y armonización

6. CONCLUSIONES

El objetivo inicial de este proyecto fue llevar a cabo una primera etapa en la promoción de un debate público e influencia en políticas públicas, relativos a la protección de datos personales en América Latina. En esta primera etapa el proyecto se ha centrado en dos países: Brasil y México, y se pretendió identificar los principales actores institucionales, legales, académicos, sociales y tecnológicos en torno a tres temas: a) Documentos nacionales de identificación, b) video-vigilancia en espacios públicos, y c) Internet.

Después de una detallada presentación y organización de los datos que sustentan la investigación llevada a cabo en ambos países, misma que fue descrita en los apartados anteriores de este informe, se ensayan a continuación algunas conclusiones importantes de esta investigación. Estas conclusiones fueron organizadas de dos maneras. En primer lugar, analizándose los resultados de los estudios separados por tema y por país (temas "a" a "f"). Y, finalmente, se destacan algunas consideraciones generales para cada país, descritas desde la perspectiva de un análisis comparativo que puede servir como punto de partida para futuros estudios transnacionales, en particular con la participación de otros contextos socioeconómicos y culturales de países de América Latina.

a) Sobre la proliferación de CCTV en Brasil

Algunos aspectos deben ser recordados y destacados después de los levantamientos realizados para este primer mapeo de la situación de la proliferación del CCTV en Brasil. Primero se debe tener en cuenta, como ya se afirmó, que el presente estudio es preliminar: tiene la intención de marcar la primera aproximación sistematizada del tema en Brasil, con amplia colecta de datos y restringida profundización cualitativa en las implicaciones y repercusiones de las principales tendencias levantadas. Aun así, es válido recordar las dimensiones continentales de los dos países, principalmente de Brasil, que fue lo que dirigió el enfoque territorial de los estudios en tres estados y el Distrito Federal, más sus capitales.

En el caso de los sistemas de CCTV, se puede percibir claramente un creciente interés en la temática y, principalmente, en la aplicación cada vez más difundida de cámaras de vigilancia y sistemas integrados, con un mercado pujante y estructurado en diversos niveles (de empresas multinacionales a pequeñas y medianas empresas locales de monitoreo y seguridad), y de un interés creciente del mercado inmobiliario en las cuestiones relacionadas con la seguridad patrimonial, funcionando como palanca para el crecimiento y comercialización de equipos de vigilancia electrónica por imagen, especialmente en la popularización de esos sistemas y en el comercio minorista.

Las grandes y pequeñas empresas coexisten en lo que los informes de empresas de mercado internacional llaman un ecosistema de proveedores, estimulando el mercado y presentando a Brasil como: a) desafío para empresas internacionales aún no establecidas en el país, pues tendrían que adaptarse a una competencia más disputada debido a la estructura de mercado ya instituida; b) y como reflejo y ejemplo del gran potencial mercantil de América Latina, en especial de los demás países, para equipos y tecnologías de CCTV y monitoreo por imagen. Por lo tanto, es notable la importancia que tiene Brasil en el interés internacional de empresas de CCTV, con relación a las tecnologías y el mercado, tornándolo propicio para futuras y masivas inversiones, principalmente si se toman en cuenta los dos megaeventos deportivos que el país albergará en el espacio de apenas dos años, la Copa del Mundo de Fútbol en 2014 (con impacto en varias capitales nacionales) y los Juegos Olímpicos de 2016 (con impacto concentrado en la región metropolitana de Rio de Janeiro). En este caso específico, hay un inmenso debate en el escenario político, en la academia y en la prensa, sobre las reales implicaciones de esos megaeventos deportivos para Brasil y las regiones

involucradas. Existen innumerables críticas sobre posibles desdoblamientos negativos relacionados con varias cuestiones, entre ellas, el uso de recursos públicos en obras para los eventos, el impacto de políticas públicas en áreas como la infraestructura urbana y la vivienda social, las relaciones entre los órganos de política locales y las instituciones supranacionales responsables de los eventos (como la FIFA y el Comité Olímpico Internacional), y finalmente con relación a las estructuras de monitoreo y seguridad instaladas por demanda de los eventos.

Se nota, además, que hay un importante crecimiento del interés científico en el asunto, demostrando el potencial para el debate de la temática CCTV en el ambiente académico brasileño. En ese aspecto, se resalta el predominio de trabajos académicos de formación (tesis, disertaciones o trabajos de conclusión de curso) sobre artículos en periódicos y trabajos en eventos, como demostración, por un lado, de un momento inicial de ampliación en la educación superior de estudios sobre vigilancia y, por otro lado, un significativo proceso de formación y entrenamiento de profesionales, maestros y doctores con investigaciones en las áreas correlacionadas con la vigilancia electrónica por imágenes, CCTV, videovigilancia, etc.

Queda claro también el momento contradictoriamente opuesto presentado por el escenario jurídico brasileño en los estados y capitales estudiadas, en el que poca o ninguna atención es dedicada a las discusiones sobre las acciones e implicaciones que tiene la actividad de videovigilancia, así como a las particularidades de las situaciones en que esta actividad se da. Es latente, en las leyes y proyectos de ley encontrados, una preocupación meramente instrumental con la aplicación de cámaras de vigilancia en el monitoreo de individuos o grupos en espacios públicos y privados. Tal escenario no se diferencia en la legislación específica de las otras dos grandes temáticas del presente estudio, como se verá más adelante.

Finalmente, es necesario demarcar el pronóstico preocupante que se tiene delante de este mapeo. A pesar del estimulante crecimiento en el número de estudios/investigadores relacionados con el tema CCTV en Brasil en los últimos años y de la importante evolución del interés en esa temática en el ambiente académico en el país, se percibe una cierta irregularidad entre la organización del mercado y el bajo nivel de participación de la sociedad civil en el debate sobre el tema reflejado en la construcción de la legislación. Se tiene, por un lado, una alta valoración de la seguridad y, por consiguiente, de todo el aparato tecnológico destinado a cuestiones de seguridad patrimonial e individual privada con un mercado preparado para atender tal demanda y, por otro lado, un ambiente jurídico despreocupado en comprender la lógica de la creciente implantación de sistemas de CCTV y sus posibles implicaciones con relación a la privacidad, libertades individuales y configuración de los espacios en las ciudades.

b) Sobre el documento nacional de identificación en Brasil

Con respecto al tema del Registro de Identidad Civil (TIC) en Brasil, existen 24 legisladores, vinculados a 53 documentos (proyectos de ley, leyes, debates etc). De esos documentos, solo 2 discuten la implementación del documento, o sea, tratan de reflexionar de manera crítica. La gran mayoría (41 documentos) solo abordan la implementación como algo técnico. Es importante subrayar que diputados de partidos que en general proponen el debate o la participación pública, en ese caso solo se limitan a solicitar que la posibilidad de uso del documento sea ampliada para los discapacitados. Además, existen 3 documentos que no solo tratan de la implementación de nuevas formas de identificación, también proponen la creación de bancos de ADN para ayudar a identificar a la población. Teniendo en cuenta los actores privados, públicos e investigadores, aproximadamente 85% está de acuerdo con el documento, o sea no discute, cuestiona o reflexiona acerca del tema. Como ha sido mencionado por Doneda y Kanashiro (Bruno, Firmino y Kanashiro, 2009), la implementación de un documento único en Brasil tiene en primer lugar un aspecto

tecnocrático o una supremacía técnica que borra sus características políticas. A menudo conduce al reconocimiento de una verdadera incapacidad de la oposición para cuestionar los procedimientos. Así, en general, lo que se destaca (incluso en la prensa) es un sistema de identificación prácticamente desprovisto de manchas oscuras o negativas. Este hecho por sí solo ya indica la importancia de un análisis más preciso de un sistema cuyas consecuencias se harán sentir directamente entre todos los brasileños.

De hecho, el proceso de aplicación del documento único de identidad en el país no pasa adecuadamente por el ámbito jurídico. La lentitud para la reglamentación de la ley que instituyó el documento y su implementación sin esta regulación, pone de manifiesto este escenario.

Tampoco existen en Brasil mecanismos legales que pueden estar vinculados específicamente a ese proceso y que estipulen las formas de control y supervisión del propio documento. Del mismo modo, no existe ninguna disposición legislativa clara sobre el acceso y uso de datos personales que serán parte del documento y su base de datos relacionados. Es importante subrayar de nuevo que los sistemas informáticos para colección de datos personales son muchas veces de empresas privadas del sector de seguridad electrónica.

Además de la ausencia de leyes, el nuevo documento único en Brasil no ha estado ligado a debates públicos, políticos o académicos que puedan aclarar a los ciudadanos los procesos que ahora ocurren en el país. La población del país tampoco cuestiona el nuevo documento, ni la recolección de datos personales (incluso biométricos), ya que existe una cultura de proporcionar tales datos en su vida diaria, incluyendo las huellas digitales ya presentes en el antiguo documento de identificación (RG). En otras palabras, Brasil presenta un cuadro poco común de ausencia de leyes, altos niveles de aceptación de parte de la población para proporcionar datos, ausencia de información y debate de los proyectos existentes en el país (incluso informaciones técnicas para los legisladores), y ausencia de investigaciones que puedan contribuir para informar la población.

La gran mayoría de investigaciones que tratan de biometría e identificación, son de áreas exactas, más preocupadas en proponer sistemas técnicos más eficientes. Entre los estudios de las humanidades, hay una presencia mayor de investigaciones sobre gestión de la información, y muy poco de estudios críticos o que reflexionen sobre el tema.

Así, el país se caracteriza por ser un mercado muy atractivo para la industria de seguridad electrónica y para lo que hoy se ha llamado la industria de la identificación. Uno de los actores importantes identificados en ese caso es Abrid (Asociación de Empresas de Tecnología de Identificación Digital). Es importante mencionar que otros eventos como el Congreso de Ciudadanía Digital y también Certforum plantean cuestiones relacionadas con la aplicación de RIC. En estos eventos, es recurrente entre los promotores, organizadores, patrocinadores o simpatizantes, la presencia de algunas empresas vinculadas a Abrid, tales como Akyiama Corporation, Gemalto, GD Burti, M.I. Montreal Informática, Oberthur Technologies, NEC, etc

Es posible indicar que en el país existe una distribución desigual del poder entre el Estado, las empresas y los ciudadanos, debilitando a los últimos que se encuentran sin medios para ejercer un control sobre sus propios datos personales. La lentitud de regulación de la ley 9.454/97 desplazó, por ejemplo, una posible revisión judicial previa y participación popular. Se constituyó así un desequilibrio de la distribución del poder entre el individuo y el Estado (así como las empresas privadas que participan de ese proceso). No existen posibilidades legales de control efectivo o protección de los ciudadanos sobre sus datos personales, causando un desequilibrio que no es compensado por las posibles soluciones - por ejemplo, la opción de tecnologías menos invasivas.

Hay crecientes posibilidades de control y vigilancia de los ciudadanos en Brasil, mientras que los ciudadanos de otros países pueden tener debates públicos u políticos, investigaciones académicas, así como normas y sistemas de identificación que les permiten una protección contra los riesgos específicos de un sistema de identificación única. En este sentido, la "brecha digital" amenaza con aumentar entre los ciudadanos de diferentes países, no exactamente en la forma en que el tema es mencionado comúnmente (es decir, en torno al acceso a la información y servicios de la Sociedad de la Información), sino en la forma de acceso a la información y control posterior ejercido con mayor intensidad sobre los ciudadanos de ciertos países. En Brasil, existe un riesgo real de ubicar al país en este último grupo caracterizado por un mayor control.

c) Sobre datos personales en Internet en Brasil

Cabe destacar y retomar algunos elementos mencionados en este tema sobre el problema del tratamiento y la regulación de datos en el internet en Brasil, tomando en cuenta las consideraciones finales de esta parte del informe.

En el ámbito de la legislación, consideramos que el actual cuadro de leyes y proyectos de ley en Brasil revela que la protección de datos personales es una preocupación minoritaria, si consideramos la cantidad de proyectos y leyes que la defienden. La mayoría de los proyectos sobre el tema en el ámbito de la legislación brasileña escoge como centro de sus preocupaciones la posibilidad de que el internauta común cometa un crimen. Es decir, en la gran mayoría de los casos, se privilegia la seguridad y el combate contra el 'ciberdelito', en detrimento de la protección de datos personales, de la garantía de anonimato y de la defensa de la privacidad. En otros términos, el internauta común es menos visto como un ciudadano cuyos derechos (relativos a la privacidad, al anonimato en las comunicaciones y a los datos personales) precisan ser defendidos, que como un potencial criminal que debe ser frenado. Actores como los consumidores, las personas jurídicas, empresas e instituciones públicas (los cuales están más directamente implicados en la colecta, tratamiento y uso de datos personales en Internet) están entre los menos citados, apareciendo, respectivamente, en 5%, 3%, 2% y 2% de los proyectos/leyes analizados. Pocos proyectos/leyes se enfocan en la regulación del uso de datos personales con fines comerciales, buscando fenómenos como la elaboración de los perfiles computacionales —conjuntos de datos sobre gustos, preferencias e intereses de los internautas, colectados muchas veces sin su autorización, y que son usados para prever su comportamiento y dirigir ofertas publicitarias en supuesto acuerdo con su personalidad—. Esta observación es corroborada por el bajo índice de presencia de los términos "perfiles" y "publicidad", los cuales aparecen, respectivamente, en 3% y 2% de los proyectos analizados. Se puede deducir, además, que Internet es menos buscado como un medio de comunicación y de producción de contenidos que debe ser democratizado y asegurado, que como un medio potencial de acciones criminales que debe ser controlado. Esta concepción de Internet está especialmente presente en los proyectos/leyes que escogen a los cibercafés como foco de control y responsabilización, exigiendo que estos establecimientos identifiquen a sus usuarios y archiven sus datos de registro. Tales establecimientos han cumplido un papel importante en la inclusión digital en Brasil, dado que la gran mayoría de la población de bajos recursos no tiene acceso a Internet desde sus casas (conforme fue apuntado en la introducción de este tema; Cf. Ítem 5.1. de este informe). Este papel es menospreciado por la gran mayoría de los proyectos/leyes brasileñas que determinan tales establecimientos como uno de los principales focos de potenciales ciberdelitos. Un síntoma evidente de este sentido atribuido a los cibercafés consiste en la prohibición, prevista en algunos proyectos de ley, de que estos sean construidos en la proximidad de escuelas.

Uno de los proyectos más representativos de la mayoritaria tendencia de criminalización es la agenda del Senado al Proyecto de Ley de la Cámara 89/2003, conocido como PL Azeredo (Cf. Ítem 5.2.1 de este informe). Este proyecto muestra cómo el imperativo de la seguridad y la intención de

atender los intereses de las industrias del copyright pueden restringir la libertad, la posibilidad de colaboración, creación y desarrollo del conocimiento en el ámbito de las redes digitales de comunicación, especialmente Internet⁷⁹.

Entretanto, a pesar de que la gran mayoría de los proyectos de ley privilegian el combate al cibercrimen, en detrimento de la protección de datos personales, la actual coyuntura política brasileña acabó por favorecer la propuesta de un anteproyecto de ley de protección de datos personales (Cf. Ítem 5.2.1 de este informe). Este anteproyecto, que fue propuesto por el Ministerio de Justicia, tiene más posibilidades de ser enviado a la Cámara de Diputados para votación, que muchos otros proyectos de ley que actúan en contra de la protección de datos personales en Internet. Así, aunque el número de proyectos de ley que amenazan la privacidad de los usuarios de Internet, oponiéndose al establecimiento de marcos legales que aseguren la protección de datos personales, sea mayor, el contexto gubernamental brasileño favorece que el anteproyecto de ley de protección de datos personales se dirija a la Cámara de Diputados. De este modo, es urgente y oportuna la sensibilización de la sociedad brasileña respecto de las implicaciones del tratamiento y de la regulación de los datos personales en Brasil.

El panorama encontrado en la legislación brasileña, notoriamente inclinada hacia privilegiar una programación dirigida al combate contra el cibercrimen en detrimento de una programación dirigida a políticas de protección de datos personales, no se repite integralmente en la producción académica sobre el tema. El mapeo de los estudios existentes mostró que el tema “privacidad” es el séptimo más frecuente, mientras que “crimen” ocupa la novena posición entre los temas más recurrentes. No obstante, es importante considerar, de acuerdo con lo que se vio en la clasificación de indicadores por artículo (Cf. Gráfico 24) y en la clasificación de indicadores por artículo y por periódico (Cf. Gráfico 25), junto con el análisis preliminar de los resúmenes de los artículos, que la producción académica refleja dos grandes vías en que se aborda la problemática de los datos personales en Internet. La primera asocia esta problemática con las áreas de la privacidad y del control, mientras que la segunda la asocia con las esferas de la seguridad y del crimen. Cabe notar, además, que en este escenario las empresas/organizaciones y el mercado despuntan como actores importantes, seguidos de los consumidores y comercio electrónico.

Aún en el mapeo de los estudios existentes destacamos la hegemonía del Derecho como el área de conocimiento en donde más se produce y más se publican artículos relativos a la privacidad y a la regulación de los datos personales en Internet. Este dato indica, al menos en términos cuantitativos, la superioridad de una perspectiva jurídica sobre la problemática de los datos personales en las redes digitales de comunicación. En el área de comunicación, la segunda en la escala de producciones académicas, la temática de la vigilancia es más frecuente al compararla con las áreas del conocimiento más recurrentes. Se destaca además el salto cuantitativo de la producción general sobre el tema a partir del año 2000, estabilizándose en la última década, lo que se justifica por la propia difusión de las tecnologías digitales de comunicación, especialmente Internet, en el ámbito mundial y brasileño. En el análisis de recurrencia de los cinco términos clave más pertinentes a nuestra investigación (“datos personales”, “vigilancia”, “protección de datos”, “monitoreo” y “privacidad”), resaltamos la preponderancia del concepto “privacidad” en todos los años presentes en el alcance de la investigación (1999-2011). El término “datos personales” aparece con una frecuencia significativamente inferior, comparada con la del término “privacidad”, aunque se mantenga recurrente a lo largo de los años mencionados. Este escenario puede indicar que el

⁷⁹ Es importante destacar que el proyecto ha recibido duras críticas que condujeron a un activismo social organizado en contra de su aprobación, la cual continúa discutiéndose en el país. Entre estos movimientos cabe mencionar *Mega No* (<http://meganao.wordpress.com/>), que tenía el objetivo manifiesto, apoyado por distintos blogs, de pretender ser un núcleo contra la marcada tendencia de vigilancia en la red, así como una petición en línea disponible en <http://www.petitiononline.com/veto2008/petition.html>, firmada por más de 150 000 personas.

tratamiento de la cuestión de los datos personales en Internet se enfoca en problemas relativos a la privacidad, lo que no agota las muchas implicaciones de esta cuestión para la vida social, política, económica e individual. Entretanto, tal hipótesis sólo puede ser verificada con una investigación específica sobre el tema, lo que no está previsto en los límites de este informe.

Si en el ámbito de las publicaciones académicas el tema “datos personales” pierde importancia comparado con “privacidad”, no sucede lo mismo en el sector de eventos, porque se realizaron, en los últimos dos años, cuatro eventos (entre un total de 22) enfocados en el tratamiento y regulación de datos personales en el Internet en Brasil. El tema “privacidad” también está presente entre los eventos, pero no de forma comparativamente preponderante. Se destaca también la presencia de agentes gubernamentales (específicamente el Ministerio Público y el Ministerio de Justicia) entre las instituciones promotoras más frecuentes de estos eventos.

Esta presencia se articula con la proposición del anteproyecto de ley de protección de datos personales, mencionado en el tema relativo a la legislación, y reaparece en las instituciones cuyas acciones tienen implicaciones en la regulación del tratamiento de datos personales en el internet en Brasil. Tres de las cuatro instituciones identificadas son iniciativas promovidas por la cooperación de ministerios con instituciones de enseñanza e investigación y con la sociedad civil. Identificamos así, esfuerzos del gobierno brasileño en el sentido de fomentar, en los últimos años, el debate público acerca de la regulación y del tratamiento de datos personales en Internet.

La respuesta de la sociedad a este fomento pudo ser identificada en el mapeo de los movimientos y organizaciones de la sociedad civil. Aunque numéricamente aún poco relevante (nueve en total), destacamos el progresivo crecimiento de estos movimientos en los últimos años, así como su intersección con diferentes áreas de actuación (derechos humanos, derecho del consumidor, derecho a la comunicación, producción de conocimiento e innovación en tecnologías de la comunicación, activismo político, defensa de la libertad de expresión y cultura digital), lo que favorece la pluralidad del debate público sobre el tema. Resaltamos también, tanto en las instituciones como en los movimientos y organizaciones de la sociedad civil, el uso de Internet como un actor decisivo en la promoción de la participación de la sociedad en el debate público sobre datos personales en Internet. Las plataformas y los foros de discusión online ocupan un lugar importante entre las acciones recientes que fueron identificadas.

El último campo mapeado, concerniente al papel de las tecnologías de colecta, monitoreo y tratamiento de datos personales en Internet, tal vez sea el que tenga menor visibilidad en el conjunto de los otros campos, con algunas excepciones. A pesar de la presencia masiva de estas tecnologías en los sitios, plataformas y servicios más populares del internet en Brasil, se le da relativamente poca relevancia a este actor tanto en el ámbito de la legislación (con la excepción de los anteproyectos del Marco Civil del Internet en Brasil y de la Protección de datos personales), como en la producción académica y en los movimientos y organizaciones. Hay indicios de que las instituciones implicadas en el gobierno y regulación del Internet en Brasil, identificadas en esta investigación, son las más relacionadas con esta temática. De este modo, podemos indicar un contraste entre la poca visibilidad de este actor y su fuerte presencia en el ámbito del Internet en Brasil. Contribuyen para esta poca visibilidad dos tendencias identificadas en este contexto: la dificultad de detectar la presencia de este tipo de tecnología en los sitios, aplicaciones y servicios que usamos cotidianamente; y el margen aún significativo de vaguedad por parte de estos sitios en lo que concierne a la explicitación en cuanto a sus políticas de privacidad, sus prácticas de colecta, monitoreo y tratamiento de datos personales (como se detalló en el tema pertinente, 19% de las empresas que operan cookies no poseen políticas de privacidad en sus sitios. Cabe señalar además, el poco margen de elección dado al usuario, lo que dificulta el control de éste sobre sus datos personales. Este aspecto puede ser constatado en al menos cuatro tendencias identificadas: a) el

hecho de que más de la mitad de las empresas que operan cookies no ofrecen el mecanismo opt-out (el cual le permite al usuario desactivar tales mecanismos, en caso que no quiera que sus datos sean recolectados o monitoreados); b) el hecho de que este mecanismo, cuando se ofrece, sea de difícil acceso y/o uso (como en el caso de las empresas que operan beacons); c) la transferencia de responsabilidad, por parte de los sitios analizados, a empresas contratadas por terceros, haciendo que sus usuarios queden sujetos a las políticas de privacidad de éstas; d) la vulnerabilidad del usuario de aplicaciones de redes sociales, puesto que sus acciones se ven sujetas a un gran número de trackers y la información de su perfil se vuelve accesible para los desarrolladores de estas aplicaciones.

Tomando en cuenta la presencia masiva de estos dispositivos de colecta, monitoreo y tratamiento de datos personales en sitios populares del Internet en Brasil, en contraste con el pequeño margen de conocimiento y control, por parte del usuario, de estos dispositivos y de sus implicaciones, consideramos de gran relevancia la difusión de la información producida en esta investigación para la promoción del debate y para la influencia de políticas públicas sobre el tema en Brasil. El carácter estratégico de estos dispositivos en la planificación de servicios, publicidad, audiencia y uso en los sitios de Internet, también destacado entre las tendencias identificadas en este informe, indica que tales dispositivos y prácticas tienden a aumentar y a tornarse más complejos. Se evidencia así la importancia de la participación de la sociedad civil en el debate público sobre las implicaciones de estos dispositivos en la privacidad, la libertad y el control sobre los datos personales del internauta brasileño. Este informe pretende ser una vía de promoción de esta participación.

d) Sobre la proliferación de CCTV en México

Con base en el análisis de los CCTV realizado aquí, se pueden advertir las formas como estos sistemas oscilan entre el cuidado y el control de la población. Si bien a escala municipal, los CCTV aparecen como un apoyo a la operación de los sistemas de semáforos, su espacio de actuación se ha expandido a otras áreas, particularmente a la seguridad pública, y, aunque en algunos casos tienden a acoplarse con otros dispositivos de vigilancia —como en el caso de Tlalnepantla— o adquirir una mayor independencia —como sucede con Toluca—, en ambos su uso se orienta, por lo general, a localizar comportamientos considerados como anormales o atípicos —todos ellos, por supuesto, fundados en prejuicios—, evolucionando en herramientas para el control y la contención de movimientos sociales y políticos. Esto pone en la mesa de discusión la utilización de los CCTV como medios para la inclusión de ciertos sectores sociales y la exclusión de otros, lo que constituye distintas ciudadanías.

Con respecto al consumo, también es posible observar el comportamiento de las personas en los centros comerciales. El consumo se transforma en el elemento que define la ciudadanía urbana, el espacio arquitectónico y la experiencia de consumo en los centros comerciales contribuyen a su definición. Los centros comerciales son espacios donde los individuos dan sentido a su subjetividad y confirman, al mismo tiempo, el sentido de pertenencia a una comunidad. Sin embargo, estos espacios tienen dos caras: son espacios públicos a los que cualquier persona puede ingresar, pero en los que no todos pueden acceder al consumo ahí ofertado, siendo espacios de exclusión social, lo que se refuerza, como se ha mostrado, con la puesta en marcha de distintos dispositivos de vigilancia, tanto electrónicos como “cara a cara”. Asimismo, la utilización de los CCTV sirve para regular la vida en el espacio laboral, convirtiendo a aquellos en mecanismos de control y disciplina.

De ahí que sea necesario introducir al debate en las ciencias sociales, la forma en que esta vigilancia se realiza en tales espacios, en la medida que su presencia es un tema político que apunta a la propia definición de la ciudadanía, en el sentido de los procesos de exclusión y desigualdad social que ella

produce. El recurso a los CCTV y a otros tipos de dispositivos de vigilancia, en los espacios públicos y privados de las ciudades, se está transformando en una vía para incrementar los procesos de desigualdad en el acceso a ciertos aspectos de la ciudadanía. Estas tecnologías no son, como se ha estudiado, instrumentos neutros; su instalación no sólo responde a las necesidades de una mayor seguridad y protección social. Aunado a ello, aquellos devienen en mecanismos que permiten magnificar los procesos de tipificación, a través de los cuales se define a las personas que son, o no, legítimos usuarios de ciertos espacios. Por eso, se constituyen en procesos que adicionan a otros, ya establecidos por las dinámicas de la esfera económica y política, nuevas formas de diferenciación social. Su impacto, por lo tanto, no resulta menor. En la actualidad los sujetos se encuentran sometidos cada vez a la mirada de aquellos en el contexto del espacio urbano: en las oficinas públicas y privadas, la calle, los centros comerciales, por mencionar algunos ejemplos. Los individuos se encuentran, de esa manera, frente a un contexto de vigilancia permanente, en el que, a cada momento, se pone en juego su estatus como ciudadanos.

Sin duda, no es lo mismo utilizar un CCTV para controlar y contener un movimiento social y político, que para detectar un posible “no-consumidor” que pudiese generar una distorsión en el comportamiento esperado en un centro comercial, o a un empleado que utiliza los pasillos de su espacio laboral para la socialización; el impacto en sus derechos ciudadanos y políticos no es el mismo. Pero, si consideramos que las instituciones sociales —como lo son aquí la ciudad y los centros comerciales— funcionan como soportes que permiten la constitución de la individualidad del sujeto moderno, es decir, la construcción de su interioridad, al igual que su ciudadanía, queda claro que la vigilancia tiene un peso específico en su conformación: puede ser un soporte e, igualmente, transformarse en máquinas de negación de la individualidad y, por ende, de ciertos derechos.

A partir de la justificación de que la instalación del CCTV responde a la necesidad de garantizar la seguridad, se impone un miedo a la variedad de comportamientos, formas de ser, que se considera escapan a un comportamiento tipificado como “normal”. Esto es lo Bauman denomina como mixofobia: una reacción que busca generar una comunidad de semejantes que garantice la exclusión de la alteridad, aunque, por lo general, únicamente se logre su gestión y administración. El desarrollo de este tipo de comportamiento entre quienes operan los CCTV en diferentes espacios, conduce a la reducción, cada vez más acentuada, de la capacidad para negociar sentidos de actuación, así como de una capacidad de convivencia con lo otro. Como apunta el propio Bauman (2008), los extraños tienden a parecer más aterradores cuanto llegan a ser más lejanos, desconocidos e incomprensibles, con lo cual se va desvaneciendo el diálogo con ellos. El problema radica, entonces, en que la mixofobia es alimentada por la práctica de segregación territorial que la genera y la recrea. De acuerdo con lo anterior, resulta pertinente considerar en qué medida contribuye a ello la instalación de los CCTV en un país en el que, de por sí, los problemas de desigualdad son enormes y avanzan constantemente.

e) Sobre sistemas de identificación en México

En México, la vigilancia y sus tecnologías están estrechamente ligadas al tema de la seguridad, puesto que las entidades públicas y privadas se sirven de sus herramientas para enfrentar la inseguridad generada ante el alza de los delitos. Por lo anterior, aun cuando en México se cuenta con diversos antecedentes en cuanto al registro y la identificación de la población, el proyecto de cédula única de identificación única y la cédula de identidad personal para menores, constituyen casos especiales de esta tradición de registro e identificación.

Estas particularidades son las que han llamado nuestra atención para identificar líneas problemáticas que es importante retomar en un futuro para poder realizar investigaciones más profundas. En

primer lugar se encuentra el nexo entre la intención de los gobiernos de recolectar datos personales concentrándolos en sistemas de identificación única y los efectos de esta recolección en la eficiencia real de los aparatos burocráticos existentes. La premisa que puede argumentarse es que sistemas de este tipo solo pueden contribuir a la construcción de sociedades más democráticas en la medida que los problemas en cuanto a un uso y tratamiento los datos sea regulado con claridad y precisión.

Se ha señalado que en México existe una normatividad más específica en torno a los datos de la población que el Gobierno Federal puede recabar, a diferencia de la falta de regulación federal que se presenta para el caso de CCTV y de Internet. Sin embargo, las controversias suscitadas por el proyecto de cédula de identidad ciudadana, revelan que es necesario ahondar en el estudio y propuesta de acciones concretas para articular los intereses y perspectivas de los diferentes agentes interpelados por dispositivos de este tipo. La pregunta que surge en este momento es por el carácter de estas propuestas, ya que es necesario reflexionar si se han de ocupar de impactar en las leyes, en los reglamentos o en la lógica de organización de los agentes e instituciones involucrados en la planeación, puesta en marcha y administración

Así, para el caso de México, un nuevo proyecto de identidad personal ha sido altamente cuestionado en la esfera de lo público. Las ventajas de este cuestionamiento han consistido en revelar un campo fértil para el debate, las desventajas son que este debate ha estado, en gran medida, guiado por inclinaciones partidistas y políticas, lo que llama a incentivar una discusión desde otros ámbitos como el de las organizaciones no gubernamentales y la academia para involucrar en la argumentación perspectivas distintas y fortalecer algunas de las ya existentes.

En un nivel más concreto, las controversias que se suscitaron alrededor del proyecto de cédula de identidad ciudadana, se concentran en tres puntos críticos: a) la necesidad real de un nuevo documento de identificación ciudadana frente a la ya existencia de formas de identificación; se advirtió acerca de la duplicidad de documentos, así como del gasto innecesario de recursos, b) las instancias de carácter público y privado que serían las indicadas para realizar el manejo y control de la gestión de la cédula, sobre todo en un contexto de cuestionamiento al manejo de datos que se ha realizado en el país, por parte de organismos públicos y privados y c) lo adecuado o inadecuado de las modificaciones a la normatividad existente, para permitir la recolección de una cantidad de datos biométricos que diferentes actores han señalado como excesiva, innecesaria, e incluso, violatoria de los derechos de privacidad.

Cruza de manera transversal a cada uno de estos tres puntos, el cuestionamiento acerca de la fortaleza institucional que tiene el Estado. Este cuestionamiento se expresa en la desconfianza que diversos agentes han manifestado acerca de la capacidad existente para administrar racionalmente el proceso de identificación ciudadana sin mezclarlo con intereses políticos coyunturales. Otra expresión del cuestionamiento al estado y los gobiernos ha girado en torno a la capacidad para aplicar la normatividad existente que protege los datos personales, toda vez que existe la percepción, entre la población, de que no se ha dado respuesta clara y contundente acerca de si ha habido casos de venta y fuga de bases de datos personales. Este punto es especialmente crítico en el contexto de violencia delictiva que vive el país, en el cual la desconfianza de la población está latente, redundando en una reticencia a la participación pública y a colaborar con los gobiernos para otorgar información que, se percibe- no está realmente protegida y por lo tanto puede colocar a los individuos en situaciones de mayor vulnerabilidad ante la delincuencia, sea ésta violenta o no. Por último, el cuestionamiento a la fortaleza institucional del Estado se ha expresado en la pugna entre fuerzas políticas en el país que no logran conciliar del todo el rumbo de la normatividad para llevar a cabo procesos como el de la cédula de identidad, así, observamos en la presente investigación que las reformas al Reglamento de la Ley General de Población, han originado acciones de inconformidad entre diversos agentes.

Frente a este panorama es que la investigación realizada se presenta como pertinente para incentivar el debate en el ámbito académico, sobre todo si consideramos que aun cuando el registro y acreditación de la identidad de los mexicanos ha sido un proceso que ha acompañado la consolidación del Estado en México, la discusión en torno a la protección de datos es relativamente reciente, destacando el área del Derecho como pionera en esta discusión. Los aportes de esta área son invaluableles en la medida que explicitan la lógica jurídica de la puesta en marcha de proyectos como el abordado, sin embargo, aún se percibe como necesario realizar aproximaciones transdisciplinarias toda vez que, como se ha visto, los problemas que se tejen alrededor de la cédula no son de carácter exclusivamente jurídicos.

f) Sobre datos personales en Internet en Mexico

Consideraciones finales

Como se puede ver, las investigaciones realizadas en Brasil indican que el papel de las empresas e industria privadas es muy fuerte en los espacios de Internet y video vigilancia, siendo ambos agentes importantes en la expansión de la videovigilancia en espacios públicos y privados, y del seguimiento de datos a través de Internet.

Obsérvese también que la brecha en la legislación destinada a proteger los datos personales se refleja tanto en el contexto de la vigilancia por vídeo, como en el nuevo documento de identificación nacional. Este escenario no se reproduce íntegramente en Internet, donde hay un contexto de conflicto entre, por una parte, una mayoría de los proyectos de ley que desafían el anonimato de navegación en Internet y exigen mecanismos de identificación y monitoreo de los usuarios, y por otra, una minoría de iniciativas de ley que buscan garantizar la privacidad y protección de datos personales en Internet. Éstos últimos, aunque son menos, tienen una efectividad relativamente fuerte, pues fueron propuestas del gobierno brasileño que pudieron llevarse a cabo frente a la mayoría de los proyectos de ley mencionados.

La producción académica ha mostrado, tanto en el tema de la video vigilancia como en el de Internet, un crecimiento significativo de artículos publicados sobre el tema en los últimos 10 años, destacando una fuerte presencia de las humanidades y las ciencias sociales, así como de las ciencias jurídicas (en el caso de Internet). Se destaca también, en estos dos temas, el carácter crítico de esta producción académica, lo que no se observa en los estudios académicos sobre el nuevo documento de identificación nacional en Brasil, en su mayoría provenientes del área de las ciencias exactas y con una producción crítica poco significativa.

En general, el debate jurídico sobre protección de datos en Brasil, se centra casi exclusivamente en las cuestiones relativas a Internet, por lo que no es común en temas relacionados con cámaras de seguridad o con el nuevo documento de identificación. Los tres ámbitos indican, con ligeras diferencias de grado, un debate público mínimo sobre el tema central de la investigación. Aunque en el ámbito de Internet se nota un incremento de grupos de interés -relativamente organizados- que se movilizan en torno al debate legal, esto es aún limitado y localizado, y es aún más escaso en los casos de identificación nacional y cámaras de vigilancia. Tal panorama apunta a la necesidad de difundir los datos presentados en este informe, con el objetivo de contribuir al crecimiento de este debate en Brasil y América Latina.

7. BIBLIOGRAFÍA

- Amadeo, S. (2001). “*Informática y nuevas tecnologías*”. Madrid: La Ley.
- Arizaga, M. C. (2000), “Las murallas y barrios cerrados. La morfología espacial del ajuste en Buenos Aires” Caracas: *Nueva Sociedad*, Núm. 166, pp. 26-37.
- Arteaga, N. (2011). “Urban Surveillance in Mexico”. En Rodrigo Firmino, Fabio Duarte and Clovis Ultramar (Coordinadores). *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (págs. 324-340). IGI Books
- Arteaga, N. (2011). “Security Metamorphosis in Latin America”. En Vida Bajc & Willen de Lint (Coordinadores). *Security and Everyday Life* London: Routledge. (págs. 236-257).
- Arteaga, N. (2010a). “Privacy and Surveillance in Mexico and Brazil”: A Cross-National Analysis. En Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon (Coordinadores). *Surveillance, privacy and the Globalization of Personal Information: International Comparisons*. Mc-Gill-Queen's University (págs. 212-229).
- Arteaga, N. (2010b). “Video-Vigilancia Del Espacio Urbano: Tránsito, Seguridad y Control Social”. México: *Andamios*, 7 (14), 263-286
- Arteaga, N. (2010c). “Consolidación De Los Archipiélagos De Seguridad en América Latina”. México: *Espiral*, 17 (49), 163-195
- Arteaga, N. (2010d). Orquestracao de Vigilancia Eletronica: Uma Experiencia Em CFTV No. México. En Bruno F, Rodrigo Firmino Marta M. Kanashiro (Coordinadores). *Tecnologia, visibilidade e vigilancia* (págs. 17-35). Sulina
- Arteaga, N. (2009a). “*Sociedad y Vigilancia en el Sur-Global. Mirando América Latina*”. México: Miguel Angel Porrúa-UAEM. ISBN 9786074011715
- Arteaga, N. (2009b). “The Merida Initiative: Security-Surveillance Harmonization in Latin America”. *European: Review of Latin American and Caribbean Studies*, 87, Octubre 2009, 103-110
- Arteaga, N. (2007a). “An Orchestriaton Of Electronic Surveillance: A CCTV Experience in Mexico”. *International Crimal Justice Review*, 17 (4), 325-335
- Arteaga, N. (2007b). “Seguridad Pública en el Estado de México: Perspectiva Gerencial y Micro-Gestión De Riesgos”. *Revista Criminalia*, LXXII (2), 75-94
- Bauman, Z. (2008a), “*Confianza y temor en la ciudad. Vivir con extranjeros*, Arcadia”, Barcelona:Tusquets
- Bauman, Z. (2008b), “*Tiempos líquidos. Vivir en una época de incertidumbre*”, México: CONACULTA, Tusquets.
- Bruno, F. (2006). “Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas”. Brasil: *Revista Fronteira* (UNISINOS), VIII, p.152 - 159, 2006.

- Bruno, F. (2008). “Monitoramento, classificação e controle nos dispositivos de vigilância digital”. Porto Alegre: *Revista FAMECOS*, 36, p.1–7.
- Bruno, F. (2009). “Distributed Surveillance: Video, Monitoring and Mobility in Brazil”. *Wi Journal of mobile media*, Summer, p.1 – 10.
- Bruno, F.; Firmini, R.; Kanashiro, M. (orgs). (2010). “*Vigilância e visibilidade: espaço, tecnologia e identificação*”. Porto Alegre: Sulina.
- Caldeira, T. (2000). *Cidades e muros, crime, segregação e cidadania em São Paulo*. São Paulo: Editora 34/Edusp.
- Carpizo, J. (2000) “*Nuevos Estudios Constitucionales*”, México Porrúa-UNAM
- Castel, R. (2003b) “*Propiedad privada, propiedad social, propiedad de sí mismo: conversaciones sobre la construcción del individuo moderno*”. Argentina: Politeia
- Castells, M. (2003). “*Internet, libertad y sociedad, una perspectiva analítica*”, Disponible en: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=3050041>
- Chabat, J. (2010). “La Iniciativa Mérida y la relación Mexico-Estados Unidos en Busca de la Confianza Pérdida” Méxio:CIDE.
- Christopherson, S. (1994), “The Fortress City: Privatized Spaces, Consumer Citizenship, *Post-Fordism*”: A Reader, A. Amin. Oxford: Blackwell, pp. 409-427.
- Cunjamá, E. D., Loría H. (2010). “Sociedad de la vigilancia y Estado policial: Análisis de las tecnologías y aparatos de control”. *El Cotidiano*, núm. 161, mayo-junio. México: Universidad Autónoma Metropolitana Azcapotzalco. pp 5-11
- D’Ottaviano, M. C. L. (2006). Condomínios Fechados na Região Metropolitana de São Paulo: fim do modelo centro rico versus periferia pobre? *Anais*, In: XV Encontro Nacional de Estudos Populacionais, ABEP, Caxambú/MG.
- Dubie, P. (2003) “*La protección de datos en Latinoamérica y el interés de España por un nivel de protección adecuado*”. Entrevista realizada por Ruipérez García Pablo Revista de Informática, Universidad Nacional de Educación a Distancia (UNED).
- Ellin, N. (1977), “Shelter from the Storm, or Form Follows Fear and Vice Versa”, en Ellin, N.; Blakely, E.J .Nueva York: *Architecture of Fear*; Princeton Architectural Press.
- Figueroa B. (2003), “Reflexiones sobre la pertinencia y concreción de un registro de población”, México: *Estudios Demográficos y Urbanos*, 52; 5-31.
- Flint, J. (2006), “Surveillance and Exclusion Practices in the Governance of Access to Shopping Centers on Periphery Estates”, *Surveillance and Society*, 4(1), pp. 52-68.
- García, P. J. y Villa M. (2001), “De la sociedad vigilante a la urbanidad preventiva”, México: *Perfiles Latinoamericanos*, núm. 19.
- Gaytán, P. (2010). “Vigilar y negociar. Imaginario sociomediático de la seguridad pública y campo

- vacío ciudadano”. *El Cotidiano*, núm. 161, mayo-junio, México: Universidad Autónoma Metropolitana – Azcapotzalco pp 13-22
- Giddens, A. (1987), “*The nation-state and violence*, Berkeley”. California: University of California Press.
- Giglia, A. (2001), “Los espacios residenciales cerrados: el caso de Villa Olímpica”, en María Ana Portal (coord.). *Vivir la diversidad. Identidades y culturas en dos contextos urbanos*, México: CONACYT.
- Gill, M. y Spriggs A. (2005). “*Assessing the impact of CCTV*. London”: Home Office Research, Development and Statistics Directorate, 43. Disponible en: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7998&rep=rep1&type=pdf>>, Último acceso: 20 feb. 2009.
- Gómez, S. (1986), “Democracia y poder en México: el significado de los fraudes electorales en 1979, 1982, 1986”, México: *Nueva Antropología*, 31; 127-157.
- Gómez-Robledo, A. y Ornelas, L. (2006). “*Protección de datos personales en México: el caso del Poder Ejecutivo Federal*”, México: UNAM.
- González L. (1981). “La República Restaurada y Vida Social” México: El Colegio de México.
- González L. (1988), “El liberalismo triunfante”, en José Velazquez (ed.), *Historia General de México*, México: El Colegio de México.
- Hernández, H. (2008), “*Democracia y federalismo: la credencial electoral con fotografía como instrumento formal de la transición democrática*”. México: Universidad Autónoma de Baja California.
- Hilbert, M. (2001). “*Latin America on its path into the digital age: where are we?* Santiago. United Nations: Publication.
- Kanashiro, M.M. (2006a). “A inserção das câmeras de monitoramento para segurança no Brasil”. Caxambu: *XXX Encontro Anual da ANPOCS, Anais*.
- Kanshiro, M.M. (2006b). “Sorria, você está sendo filmado: a inserção das câmeras de monitoramento para segurança em São Paulo”. Sao Paulo: En *Dissertação de Mestrado*, Unicamp.
- Kanashiro, M.M. (2008) “Surveillance cameras in Brazil: exclusion, mobility regulation, and the new meanings of security”. Brazil: En *Surveillance & Society* (Online), v. 5, p. 270-289.
- Katz, J. y Hilbert, M (2003). “*Building an Information Society: a Latin American and Caribbean Perspective*”. Santiago: United Nations Publication.
- Lajud L. y Quiroz, M. 2007 “La Necesidad de Legislar para Regular el Uso de la video Vigilancia en México”. México: Universidad Autónoma de Puebla.
- López, L. (1999), “*Centros Comerciales: espacios que navegan entre la realidad y la ficción*”, México: Nuestro Tiempo.

- Lyon, D. (2009) *“Identifying citizens”*. Cambridge: Polity Press.
- Marioto, M. y Firmino, R. J. (2010). “Medo e segurança na cidade contemporânea: estratégias de marketing para condomínios horizontais em Curitiba”. Brazil: En *Relatório de pesquisa*. Curitiba: PUCPR.
- Messía de la Cerda Ballesteros, J. A. (2003). *“La cesión o comunicación de datos de carácter personal”*, Madrid: Thomson-Civitas.
- Nieto, H. (2007) “Registro Nacional de Población”. México: En Revista de los Tribunales Agrarios no. 43 Septiembre-Diciembre.
- Nougrères, A. B. y Doneda, D. et al. (2008). *“Proteção de dados pessoais na América Latina”*. Brazil: En *Habeasdata.org.br*, 20 abril 2008.
- Pérez, A. (1989). “Los derechos humanos en la sociedad tecnológica”. En G. Losano, Mario, et. al. *Libertad informática y leyes de protección de datos personales*. Madrid: Centro de Estudios Constitucionales. pp. 145 y ss.
- Pierini, A. et al. (1999). *“Habeas Data”*, Universidad, Buenos Aires.
- Piña, H. R. (2008). *“El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano”*. México: Instituto de Transparencia y Acceso a la Información Pública del Estado de México.
- Riande, N. (2000). “¿Por qué debe legislarse en México en materia de Protección de Datos Personales Automatizados?”. Ponencia presentada en el marco del *VIII Congreso Iberoamericano de Derecho e Informática*, celebrado del 21 al 25 de noviembre de 2000 en el Campus Estado de México del Tecnológico de Monterrey.
- Rotker, S. (2000), “Ciudades escritas por la violencia (a modo de introducción)”, en Susana Rotker (ed.), *Ciudadánías del miedo*. Caracas, Venezuela: Nueva Sociedad-The State University of New Jersey.
- Shields, R. (1992), *“Lifestyle Shopping. The subject of consumption”*, London: Routledge.
- Villanueva, E. (2002). *“Derecho comparado de la información”*. México: Universidad Iberoamericana-Fundación Konrad Adenauer.
- Villegas M. (1973), *Historia moderna de México: El Porfiriato y vida social*, México: Hermes.
- Wood, D. M. y Firmino, R. (2009). “Inclusion or Repression? Opening up questions of identification and exclusion in Brazil through a case of 'identity fraud'.” Londres: En *Second Multidisciplinary Workshop on Identity in the Information Society. Proceedings of II IDIS*.
- Wood, D. M y Graham, S. “Digitalizing surveillance: categorization, space, inequality”.Londres: En *Critical social policy*, vol. 23, n. 2: 227-248.
- Zukin, S. (1995), *“The cultures of cities”*. Blackwell, Cambridge, Massachusetts, US.

Documentos Oficiais

Agencia de notícias do Tribunal Superior Eleitoral (TSE). *Justica Eleitoral inicia recadastramento biométrico dos eleitores de Goiânia*. 2011. Disponível em:

<<http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1368545>>, Último acesso: 19 abr 2011.

CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa TIC de Domicílios 2010*. São Paulo, 2011.

Diario Oficial de la Federación (2008), 25 de agosto de 2008; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5057719&fecha=25/08/2008

Diario Oficial de la Federación (2011), 19 de enero de 2011; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5174983&fecha=19/01/2011

Gaceta informativa de la Comisión Federal Electoral (1978), Tomo III, México, 1978.

Gaceta Parlamentaria (2001). Núm. 688, jueves 15 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010215.html>

Gaceta Parlamentaria (2001). Núm. 692, miércoles 21 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio>

Gaceta Parlamentaria (2001). Núm. 832, viernes 7 de septiembre de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/sep/20010907.html>

Gaceta Parlamentaria (2002). Núm. 1082. 5 de septiembre de 2002; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/58/2002/sep/20020905.html#Minuta20020905DatosPersonales>

Gaceta Parlamentaria (2002). Núm. 999, martes 14 de mayo de 2002; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/58/2002/may/20020514.html#Ini20020514Barbosa>

Gaceta Parlamentaria (2004). Núm. 1600-I, jueves 7 de octubre de 2004; disponible en: <http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html>

Gaceta Parlamentaria (2005). Núm. 1895-I, jueves 1 de diciembre de 2005; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html#Iniciativas>

Gaceta Parlamentaria (2006). Núm. 1953-I, jueves 23 de febrero de 2006; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas>

Gaceta Parlamentaria (2006). Núm. 1972-I, miércoles 22 de marzo de 2006, disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas>

International Telecommunication Union (ITU) (2010). *Measuring the Information Society*. Geneva.

Jacinto, S. *Frequência digital nas escolas constituirá identidade cidadã*. Serviço de comunicação do Serviço Federal de Processamento de Dados (Serpro), Notícias 2004. Disponível em:

<http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040823_01>, Último acceso: 29 mar. 2009.

Secretaría de Gobernación (1982b), *Diagnóstico del registro civil en México, 1980*, México: Secretaría de Gobernación

United Nations Conference on Trade and Development (UNCTAD) (2002). *Electronic Commerce Strategies for Development: The Basic Elements of an Enabling Environment for E-Commerce*. Geneva. Disponible en <<http://www.unctad.org/en/docs/c3em15d2.en.pdf>>. Último acceso: 30 de junio de 2011.

Recursos electrónicos

ComSCORE. Orkut Continua Liderando o Mercado de Redes Sociais no Brasil, e a Audiência do Facebook Quintuplica. *ComScore*, 7 out. 2010. Disponível em: <http://www.comscore.com/por/Press_Events/Press_Releases/2010/10/Orkut_Continues_to_Lead_Brazil_s_Social_Networking_Market_Facebook_Audience_Grows_Fivefold>. Último acceso: 12 maio 2010.

El Informador. (2011). *Conectarán cámaras públicas y privadas para ampliar vigilancia*. Disponible desde el 15 de mayo de 2011 en <http://www.informador.com.mx/jalisco/2011/277745/6/conectaran-camaras-publicas-y-privadas-para-ampliar-vigilancia.htm>

Espinosa de los Monteros Hernández, Roberto [Online], “El Registro Civil: una historia sesquicentenario”, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Secretaria de Gobernación Available at: <<http://www.inehm.gob.mx/Portal/PtMain.php?pagina=exp-registro-civil-articulo>> [Viewed 04-05-2010]

Fernández, Emilio. (2010). Camiones tendrán videocámaras. En *El Universal*. Obtenido el 10 de mayo de 2011 desde <http://www.eluniversaledomex.mx/ecatepec/nota2519.html>

<http://www.al.sp.gov.br>

<http://www.alep.pr.gov.br>

<http://www.alerj.rj.gov.br>

<http://www.alexa.com/topsites/countries/BR>

<http://www.camara.gov.br>;

<http://www.causaencomun.org.mx>.Causa en Común

http://www.cedla.uva.nl/10_about/institute.html

http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.pdf , Consultado el 16 de julio de 2011

<http://www.eluniversal.com.,mx/notas/739734.html>

<http://www.eluniversal.com.mx/nacion/176153.html>

<http://www.eluniversal.com.mx/nacion/184095.html>

<http://www.eluniversal.com.mx/notas/740779.html>

<http://www.ghostery.com/> <http://www.networkadvertising.org/>

http://www.gobernacion.gob.mx/es/SEGOB/Sintesis_Informativa?uri=http%3A%2Fwww.SEGOB.swb%23swbpress_Content%3A1549&cat=http%3A%2F%2Fwww.SEGOB.swb%23swbpress_Category%3A1

<http://www.imldb.iom.int/viewDocument.do?id=%7B4E02258C-8466-4A4F-AD72-DFADC0E4F602%7D> Consultado el 16 de julio de 2011

<http://www.informador.com.mx/mexico/2011/320634/6/corte-desecha-juicio-contracedula-de-identidad.htm>

<http://www.jornada.unam.mx/2009/10/31/index.php?section=politica&article=011n1pol>,

<http://www.jornada.unam.mx/2009/11/25/index.php?section=politica&article=009n1pol>

<http://www.jornada.unam.mx/2009/12/15/index.php?section=politica&article=003n1pol>

<http://www.jornada.unam.mx/2010/01/20/index.php?section=politica&article=008n2pol>

<http://www.jornada.unam.mx/2010/02/17/index.php?section=politica&article=007n2pol>,

<http://www.law.duke.edu/about/mission>

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

<http://www.milenio.com/node/621419>

<http://www.orkut.com/MembersAll>

<http://www.publicaciones.cucsh.udg.mx/ppperiod/esprial/index.htm>

<http://www.renapo.gob.mx/swb/swb/RENAPO/Beneficioscedi>

<http://www.renapo.gob.mx/swb/swb/RENAPO/cedi>

<http://www.renapo.gob.mx/swb/swb/RENAPO/MedidasCEDI>

<http://www.renapo.gob.mx/swb/swb/RENAPO/renapo>

<http://www.senado.gov.br>

<http://www.surveillance-and-society.org/ojs/index.php/journal/about/editorialPolicies#focusAndScope>

- IMS Research (2011). *Brazil is Not The Only Nut to Crack in Latin American CCTV Market*. Disponible en: <http://bit.ly/ims_cctv>, acceso en 10/02/2011.
- Jiménez, R. (2011). Invertirán 96 mdp en videovigilancia de Edomex. *El Universal*. Disponible desde el 24 de marzo de 2011 en <http://www.eluniversal.com.mx/notas/754273.html>. Obtenido el 16 de junio de 2011.
- Rodriguez, J. C. (2010). O Orkut será superado pelo Facebook no Brasil?. En *Webinsider*, 3 de mayo de 2010. Disponible en : <<http://webinsider.uol.com.br/2010/05/03/o-orkut-sera-superado-pelo-facebook-no-brasil/>>. Último acceso: 12 de mayo de 2010.
- Rodríguez, Y. (2011). Vigilarán 11 mil cámaras principales calles del DF. *W Radio*. Disponible desde el 13 de junio, en <http://www.wradio.com.mx/nota.aspx?id=1488591>. Consultado el 16 de junio de 2011.
- Surveillance Studies (2006) A Report on the Surveillance Society. En *Full report for the Information Commissioner of the UK*. Disponible en: <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>, Último acceso: 30 de febrero de 2009.
- Torpey, J. (2000), *The invention of the passport. Surveillance, citizenship and the State*, Cambridge: Cambridge University Press.
- Valentino-Devries, J. (2010). What the know about you. En *The Wall Street Journal*, 31 jul. 2010. Disponible en: <<http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html>>. Último acceso: 20/01/2010. 7. BIBLIOGRAPHY
- Amadeo, S. (2001). “*Informática y nuevas tecnologías*”. Madrid: La Ley.
- Arizaga, M. C. (2000), “Las murallas y barrios cerrados. La morfología espacial del ajuste en Buenos Aires” Caracas: *Nueva Sociedad*, Núm. 166, pp. 26-37.
- Arteaga, N. (2011). “Urban Surveillance in Mexico”. En Rodrigo Firmino, Fabio Duarte and Clovis Ultramar (Coordinadores). *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (págs. 324-340). IGI Books
- Arteaga, N. (2011). “SecurYTE Metamorphosis in Latin America”. En Vida Bajc & Willen de Lint (Coordinadores). *Security and Everyday Life* London: Routledge. (págs. 236-257).
- Arteaga, N. (2010a). “Privay and Surveillance in Mexico and Brazil”: A Cross-National Analysis. En Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon (Coordinadores). *Surveillance, privacy and the Globalization of Personal Information: International Comparisons*. Mc-Gill-Queen's University (págs. 212-229).
- Arteaga, N. (2010b). “Video-Vigilancia Del Espacio Urbano: Tránsito, Seguridad y Control Social”.México: *Andamios*, 7 (14), 263-286
- Arteaga, N. (2010c). “Consolidación De Los Archipiélagos De Seguridad en América Latina”.México: *Espiral*, 17 (49), 163-195
- Arteaga, N. (2010d). Orquestracao de Vigilancia Eletronica: Uma Experiencia Em CFTV No.

- México. En Bruno F, Rodrigo Firmino Marta M. Kanashiro (Coordinadores). *Tecnología, visibilidad e vigilancia* (págs. 17-35). Sulina
- Arteaga, N. (2009a). “*Sociedad y Vigilancia en el Sur-Global. Mirando América Latina*”. México: Miguel Angel Porrúa-UAEM. ISBN 9786074011715
- Arteaga, N. (2009b). “The Merida Initiative: Security-Surveillance Harmonization in Latin America”. *European: Review of Latin American and Caribbean Studies*, 87, Octubre 2009, 103-110
- Arteaga, N. (2007a). “An Orchestration Of Electronic Surveillance: A CCTV Experience in Mexico”. *International Criminal Justice Review*, 17 (4), 325-335
- Arteaga, N. (2007b). “Seguridad Pública en el Estado de México: Perspectiva Gerencial y Micro-Gestión De Riesgos”. *Revista Criminalia*, LXXII (2), 75-94
- Bauman, Z. (2008a), “*Confianza y temor en la ciudad. Vivir con extranjeros*, Arcadia”, Barcelona:Tusquets
- Bauman, Z. (2008b), “*Tiempos líquidos. Vivir en una época de incertidumbre*”, México: CONACULTA, Tusquets.
- Bruno, F. (2006). “Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas”.Brasil: *Revista Fronteira* (UNISINOS), VIII, p.152 - 159, 2006.
- Bruno, F. (2008). “Monitoramento, classificação e controle nos dispositivos de vigilância digital”. Porto Alegre: *Revista FAMECOS*, 36, p.1–7.
- Bruno, F. (2009). “Distributed Surveillance: Video, Monitoring and Mobility in Brazil”. *Wi Journal of mobile media*, Summer, p.1 – 10.
- Bruno, F.; Firmini, R.; Kanashiro, M. (orgs). (2010). “*Vigilância e visibilidade: espaço, tecnologia e identificação*”. Porto Alegre: Sulina.
- Caldeira, T. (2000). *Cidades e muros, crime, segregação e cidadania em São Paulo*. São Paulo: Editora 34/Edusp.
- Carpizo, J. (2000) “*Nuevos Estudios Constitucionales*”, México Porrúa-UNAM
- Castel, R. (2003b) “*Propiedad privada, propiedad social, propiedad de sí mismo: conversaciones sobre la construcción del individuo moderno*”. Argentina: Politeia
- Castells, M. (2003). “*Internet, libertad y sociedad, una perspectiva analítica*”, Disponible en: <http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=3050041>
- Chabat, J. (2010). “La Iniciativa Mérida y la relación Mexico-Estados Unidos en Busca de la Confianza Pérdida” México:CIDE.
- Christopherson, S. (1994), “The Fortress City: Privatized Spaces, Consumer Citizenship, *Post-Fordism*”: A Reader, A. Amin. Oxford: Blackwell, pp. 409-427.

- Cunjamá, E. D., Loría H. (2010). “Sociedad de la vigilancia y Estado policial: Análisis de las tecnologías y aparatos de control”. *El Cotidiano*, núm. 161, mayo-junio. México: Universidad Autónoma Metropolitana Azcapotzalco. pp 5-11
- D’Ottaviano, M. C. L. (2006). Condomínios Fechados na Região Metropolitana de São Paulo: fim do modelo centro rico versus periferia pobre? *Anais*, In: XV Encontro Nacional de Estudos Populacionais, ABEP, Caxambú/MG.
- Dubie, P. (2003) “*La protección de datos en Latinoamérica y el interés de España por un nivel de protección adecuado*”. Entrevista realizada por Ruipérez García Pablo Revista de Informática, Universidad Nacional de Educación a Distancia (UNED).
- Ellin, N. (1977), “Shelter from the Storm, or Form Follows Fear and Vice Versa”, en Ellin, N.; Blakely, E.J .Nueva York: *Architecture of Fear*; Princeton Architectural Press.
- Figueroa B. (2003), “Reflexiones sobre la pertinencia y concreción de un registro de población”, México: *Estudios Demográficos y Urbanos*, 52; 5-31.
- Flint, J. (2006), “Surveillance and Exclusion Practices in the Governance of Access to Shopping Centers on Periphery Estates”, *Surveillance and Society*, 4(1), pp. 52-68.
- García, P. J. y Villa M. (2001), “De la sociedad vigilante a la urbanidad preventiva”, México: *Perfiles Latinoamericanos*, núm. 19.
- Gaytán, P. (2010). “Vigilar y negociar. Imaginario sociomediático de la seguridad pública y campo vacío ciudadano”. *El Cotidiano*, núm. 161, mayo-junio, México: Universidad Autónoma Metropolitana – Azcapotzalco pp 13-22
- Giddens, A. (1987), “*The nation-state and violence*, Berkeley”.California: University of California Press.
- Giglia, A. (2001), “Los espacios residenciales cerrados: el caso de Villa Olímpica”, en María Ana Portal (coord.). *Vivir la diversidad. Identidades y culturas en dos contextos urbanos*, México: CONACYT.
- Gill, M. y Spriggs A. (2005). “*Assessing the impact of CCTV*. London”: Home Office Research, Development and Statistics Directorate, 43. Disponible en: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7998&rep=rep1&type=pdf>>, Último acceso: 20 feb. 2009.
- Gómez, S. (1986), “Democracia y poder en México: el significado de los fraudes electorales en 1979, 1982, 1986”, México: *Nueva Antropología*, 31; 127-157.
- Gómez-Robledo, A. y Ornelas, L. (2006). “*Protección de datos personales en México: el caso del Poder Ejecutivo Federal*”, México: UNAM.
- González L. (1981). “La República Restaurada y Vida Social” México: El Colegio de México.
- González L. (1988), “El liberalismo triunfante”, en José Velazquez (ed.), *Historia General de México*, México: El Colegio de México.

- Hernández, H. (2008), *“Democracia y federalismo: la credencial electoral con fotografía como instrumento formal de la transición democrática”*. México: Universidad Autónoma de Baja California.
- Hilbert, M. (2001). *“Latin America on its path into the digital age: where are we?”* Santiago. United Nations: Publication.
- Kanashiro, M.M. (2006a). “A inserção das câmeras de monitoramento para segurança no Brasil”. Caxambu: *XXX Encontro Anual da ANPOCS, Anais*.
- Kanshiro, M.M. (2006b). “Sorria, você está sendo filmado: a inserção das câmeras de monitoramento para segurança em São Paulo”. Sao Paulo: En *Dissertação de Mestrado*, Unicamp.
- Kanashiro, M.M. (2008) “Surveillance cameras in Brazil: exclusion, mobility regulation, and the new meanings of security”. Brazil: En *Surveillance & Society* (Online), v. 5, p. 270-289.
- Katz, J. y Hilbert, M (2003). *“Building an Information Society: a Latin American and Caribbean Perspective”*. Santiago: United Nations Publication.
- Lajud L. y Quiroz, M. 2007 “La Necesidad de Legislar para Regular el Uso de la video Vigilancia en México”.México: Universidad Autónoma de Puebla.
- López, L. (1999), *“Centros Comerciales: espacios que navegan entre la realidad y la ficción”*, México: Nuestro Tiempo.
- Lyon, D. (2009) *“Identifying citizens”*. Cambridge: Polity Press.
- Marioto, M. y Firmino, R. J. (2010). “Medo e segurança na cidade contemporânea: estratégias de marketing para condomínios horizontais em Curitiba”.Brazil: En *Relatório de pesquisa*. Curitiba: PUCPR.
- Messía de la Cerda Ballesteros, J. A. (2003). *“La cesión o comunicación de datos de carácter personal”*, Madrid: Thomson-Civitas.
- Nieto, H. (2007) “Registro Nacional de Población”. México: En Revista de los Tribunales Agrarios no. 43 Septiembre-Diciembre.
- Nougrères, A. B. y Doneda, D. et al. (2008). *“Proteção de dados pessoais na América Latina”*. Brazil: En *Habeasdata.org.br*, 20 abril 2008.
- Pérez, A. (1989). “Los derechos humanos en la sociedad tecnológica”. En G. Losano, Mario, et. al. *Libertad informática y leyes de protección de datos personales*. Madrid: Centro de Estudios Constitucionales. pp. 145 y ss.
- Pierini, A. et al. (1999). *“Habeas Data”*, Universidad, Buenos Aires.
- Piña, H. R. (2008). *“El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano”*. México: Instituto de Transparencia y Acceso a la Información Pública del Estado de México.

Riande, N. (2000). “¿Por qué debe legislarse en México en materia de Protección de Datos Personales Automatizados?”. Ponencia presentada en el marco del *VIII Congreso Iberoamericano de Derecho e Informática*, celebrado del 21 al 25 de noviembre de 2000 en el Campus Estado de México del Tecnológico de Monterrey.

Rotker, S. (2000), “Ciudades escritas por la violencia (a modo de introducción)”, en Susana Rotker (ed.), *Ciudadanía del miedo*. Caracas, Venezuela: Nueva Sociedad-The State University of New Jersey.

Shields, R. (1992), “*Lifestyle Shopping. The subject of consumption*”, London: Routledge.

Villanueva, E. (2002). “*Derecho comparado de la información*”. México: Universidad Iberoamericana-Fundación Konrad Adenauer.

Villegas M. (1973), *Historia moderna de México: El Porfiriato y vida social*”, México: Hermes.

Wood, D. M. y Firmino, R. (2009). “Inclusion or Repression? Opening up questions of identification and exclusion in Brazil through a case of 'identity fraud'.” Londres: En *Second Multidisciplinary Workshop on Identity in the Information Society. Proceedings of II IDIS*.

Wood, D. M y Graham, S. “Digitalizing surveillance: categorization, space, inequality”.Londres: En *Critical social policy*, vol. 23, n. 2: 227-248.

Zukin, S. (1995), “*The cultures of cities*”. Blackwell, Cambridge, Massachusetts, US.
Documentos Oficiales

Agencia de notícias do Tribunal Superior Eleitoral (TSE). *Justica Eleitoral inicia recadastramento biométrico dos eleitores de Goiânia*. 2011. Disponível em:
<<http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1368545>>, Último acesso: 19 abr 2011.

CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa TIC de Domicílios 2010*. São Paulo, 2011.

Diario Oficial de la Federación (2008), 25 de agosto de 2008; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5057719&fecha=25/08/2008

Diario Oficial de la Federación (2011), 19 de enero de 2011; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5174983&fecha=19/01/2011

Gaceta informativa de la Comisión Federal Electoral (1978), Tomo III, México, 1978.

Gaceta Parlamentaria (2001). Núm. 688, jueves 15 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010215.html>

Gaceta Parlamentaria (2001). Núm. 692, miércoles 21 de febrero de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio>

Gaceta Parlamentaria (2001). Núm. 832, viernes 7 de septiembre de 2001; disponible en: <http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/sep/20010907.html>

Gaceta Parlamentaria (2002). Núm. 1082. 5 de septiembre de 2002; disponible en:
<http://gaceta.diputados.gob.mx/Gaceta/58/2002/sep/20020905.html#Minuta20020905DatosPersonales>

Gaceta Parlamentaria (2002). Núm. 999, martes 14 de mayo de 2002; disponible en:
<http://gaceta.diputados.gob.mx/Gaceta/58/2002/may/20020514.html#Ini20020514Barbosa>

Gaceta Parlamentaria (2004). Núm. 1600-I, jueves 7 de octubre de 2004; disponible en:
<http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html>

Gaceta Parlamentaria (2005). Núm. 1895-I, jueves 1 de diciembre de 2005; disponible en:
<http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html#Iniciativas>

Gaceta Parlamentaria (2006). Núm. 1953-I, jueves 23 de febrero de 2006; disponible en:
<http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas>

Gaceta Parlamentaria (2006). Núm. 1972-I, miércoles 22 de marzo de 2006, disponible en:
<http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas>

International Telecommunication Union (ITU) (2010). *Measuring the Information Society*. Geneva.

Jacinto, S. *Frequência digital nas escolas constituirá identidade cidadã*. Serviço de comunicação do Serviço Federal de Processamento de Dados (Serpro), Notícias 2004. Disponível em:
<http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040823_01>, Último acesso: 29 mar. 2009.

Secretaría de Gobernación (1982b), *Diagnóstico del registro civil en México, 1980*, México: Secretaría de Gobernación

United Nations Conference on Trade and Development (UNCTAD) (2002). *Electronic Commerce Strategies for Development: The Basic Elements of an Enabling Environment for E-Commerce*. Geneva. Disponible en <<http://www.unctad.org/en/docs/c3em15d2.en.pdf>>. Último acceso: 30 de junio de 2011.

Recursos electrónicos

ComSCORE. Orkut Continua Liderando o Mercado de Redes Sociais no Brasil, e a Audiência do Facebook Quintuplica. *ComScore*, 7 out. 2010. Disponível em:
<http://www.comscore.com/por/Press_Events/Press_Releases/2010/10/Orkut_Continues_to_Lead_Brazil_s_Social_Networking_Market_Facebook_Audience_Grows_Fivefold>. Último acesso: 12 maio 2010.

El Informador. (2011). *Conectarán cámaras públicas y privadas para ampliar vigilancia*. Disponible desde el 15 de mayo de 2011 en
<http://www.informador.com.mx/jalisco/2011/277745/6/conectaran-camaras-publicas-y-privadas-para-ampliar-vigilancia.htm>

Espinosa de los Monteros Hernández, Roberto [Online], “El Registro Civil: una historia sesquicentenario”, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Secretaría de Gobernación Available at:

<<http://www.inehrm.gob.mx/Portal/PtMain.php?pagina=exp-registro-civil-articulo>> [Viewed 04-05-2010]

Fernández, Emilio. (2010). Camiones tendrán videocámaras. En *El Universal*. Obtenido el 10 de mayo de 2011 desde <http://www.eluniversaledomex.mx/ecatepec/nota2519.html>

<http://www.al.sp.gov.br>

<http://www.alep.pr.gov.br>

<http://www.alerj.rj.gov.br>

<http://www.alexa.com/topsites/countries/BR>

<http://www.camara.gov.br>;

<http://www.causaencomun.org.mx>.Causa en Común

http://www.cedla.uva.nl/10_about/institute.html

http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.pdf , Consultado el 16 de julio de 2011

<http://www.eluniversal.com.mx/notas/739734.html>

<http://www.eluniversal.com.mx/nacion/176153.html>

<http://www.eluniversal.com.mx/nacion/184095.html>

<http://www.eluniversal.com.mx/notas/740779.html>

<http://www.ghostery.com/> <http://www.networkadvertising.org/>

http://www.gobernacion.gob.mx/es/SEGOB/Sintesis_Informativa?uri=http%3A%2Fwww.SEGOB.swb%23swbpress_Content%3A1549&cat=http%3A%2Fwww.SEGOB.swb%23swbpress_Category%3A1

<http://www.imldb.iom.int/viewDocument.do?id=%7B4E02258C-8466-4A4F-AD72-DFADC0E4F602%7D> Consultado el 16 de julio de 2011

<http://www.informador.com.mx/mexico/2011/320634/6/corte-desecha-juicio-contracedula-de-identidad.htm>

<http://www.jornada.unam.mx/2009/10/31/index.php?section=politica&article=011n1pol>,

<http://www.jornada.unam.mx/2009/11/25/index.php?section=politica&article=009n1pol>

<http://www.jornada.unam.mx/2009/12/15/index.php?section=politica&article=003n1pol>

<http://www.jornada.unam.mx/2010/01/20/index.php?section=politica&article=008n2pol>

<http://www.jornada.unam.mx/2010/02/17/index.php?section=politica&article=007n2pol>,

<http://www.law.duke.edu/about/mission>

http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html

<http://www.milenio.com/node/621419>

<http://www.orkut.com/MembersAll>

<http://www.publicaciones.cucsh.udg.mx/ppperiod/esprial/index.htm>

<http://www.renapo.gob.mx/swb/swb/RENAPO/Beneficioscedi>

<http://www.renapo.gob.mx/swb/swb/RENAPO/cedi>

<http://www.renapo.gob.mx/swb/swb/RENAPO/MedidasCEDI>

<http://www.renapo.gob.mx/swb/swb/RENAPO/renapo>

<http://www.senado.gov.br>

<http://www.surveillance-and>

[society.org/ojs/index.php/journal/about/editorialPolicies#focusAndScope](http://www.society.org/ojs/index.php/journal/about/editorialPolicies#focusAndScope)

IMS Research (2011). *Brazil is Not The Only Nut to Crack in Latin American CCTV Market*.

Disponible en: <http://bit.ly/ims_cctv>, acceso en 10/02/2011.

Jiménez, R. (2011). Invertirán 96 mdp en videovigilancia de Edomex. *El Universal*. Disponible desde el 24 de marzo de 2011 en <http://www.eluniversal.com.mx/notas/754273.html>. Obtenido el 16 de junio de 2011.

Rodríguez, J. C. (2010). O Orkut será superado pelo Facebook no Brasil?. En *Webinsider*, 3 de mayo de 2010. Disponible en : <<http://webinsider.uol.com.br/2010/05/03/o-orkut-sera-superado-pelo-facebook-no-brasil/>>. Último acceso: 12 de mayo de 2010.

Rodríguez, Y. (2011). Vigilarán 11 mil cámaras principales calles del DF. *W Radio*. Disponible desde el 13 de junio, en <http://www.wradio.com.mx/nota.aspx?id=1488591>. Consultado el 16 de junio de 2011.

Surveillance Studies (2006) A Report on the Surveillance Society. En *Full report for the Information Commissioner of the UK*. Disponible en: <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>, Último acceso: 30 de febrero de 2009.

Torpey, J. (2000), *The invention of the passport. Surveillance, citizenship and the State*, Cambridge: Cambridge University Press.

Valentino-Devries, J. (2010). What the know about you. En *The Wall Street Journal*, 31 jul. 2010. Disponible en: <<http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html>>. Último acceso: 20/01/2010.