La política de Internet desde una perspectiva internacional

Seis informes nacionales

TOBIAS WANGERMANN Y HELMUT REIFELD
EDITORES

La política de Internet desde una perspectiva internacional

Seis informes nacionales

Konrad Adenauer Stiftung

La política de Internet desde una perspectiva internacional : Seis informes nacionales / Wangermann, Tobías y Reifeld, Helmut (eds.) - 1a. ed. - Buenos Aires : Konrad Adenauer Stiftung, 2011.
112 p. ; 23 x 16 cm.

ISBN: 978-987-1285-26-6

1. Internet. I. Título
CDD 070.4

Título original en alemán:
Netzpolitik aus internationaler Perspektive - Sechs Länderberichte

Traducción del original: Renate Gabriela Hoffman
Corrección: Jorge Galeano
Diseño de interior y tapa: Ana Uranga

Programa Regional Medios de Comunicación y Democracia en Latinoamérica
Suipacha 1175, 2° piso
C1008AAW Buenos Aires
Argentina
Tel.: +54-11-43 93 28 60
www.kasmedios.org

ISBN: 978-987-1285-26-6

Impreso en Argentina

Hecho el déposito que establece la Ley 11.723

Diciembre 2011

ÍNDICE

PREFACIO

La presencia de Internet en casi todos los órdenes de la vida, privados y públicos, impulsó la discusión política en torno a las condiciones políticas generales, aplicables al uso de estos medios. El área denominada política de Internet no sólo abarca las condiciones jurídicas para la operación y el uso de este medio de comunicación, sino que refleja también las correspondientes posiciones culturales y políticas. Se trata tanto de cuestiones atinentes al derecho de autor, la seguridad de los derechos personales, el acceso a la información, como también la lucha contra el crimen o las condiciones de competencia.

La institución de una comisión técnica del Parlamento Alemán "Internet y sociedad digital", una intensa discusión en los medios, así como un creciente número de debates y plataformas muestran que ya no se trata de un tema reservado a unos pocos expertos en la materia, sino que ha llegado hasta la médula misma de la sociedad. A través del concepto "derechos cívicos digitales" se establece también una relación entre libertad y regulación que es ilustrativa de la relación entre Estado y ciudadano.

El debate alemán en torno a la política de Internet se ve caracterizado por una serie de aspectos. Algunos puntos cruciales son el reclamo de seguridad de datos, en especial en lo que se refiere a los datos personales, la libertad de Internet sin injerencia del Estado, la discusión en torno a los derechos de autor y su aplicación, y los riesgos que encierra el medio, aunque con una velada crítica al afán regulador del Estado. Actualmente, el debate en torno a algunos de estos aspectos como conservación de datos, normas más restrictivas para el acceso a Internet y protección de los derechos de autor se encuentra estancado.

El mero hecho de que Internet sea un medio de comunicación global obliga a introducir condiciones generales e instrumentos de validez internacional. Pero también focaliza la mirada en un mercado internacional de conceptos y modelos políticos que deben dar respuesta a una serie de preguntas pendientes de solución. Un intercambio sobre estos conceptos puede enriquecer el debate en Alemania.

La presente publicación echa una mirada a las decisiones y debates sobre la política de Internet práctica en otros países con el fin de ofrecer un marco de referencia para el debate alemán en esta cuestión. Los informes de seis Estados democráticos de diferentes continentes describen el tratamiento que se da a los temas centrales en cada uno de ellos. En función de su labor internacional, la Fundación Konrad Adenauer se interpreta como una instancia mediadora en este proceso. Por último deseo expresar mi agradecimiento a todos los autores y traductores por el aporte realizado.

Michael Thielen
Berlín, enero de 2011

Secretario General de la
Fundación Konrad Adenauer

INTRODUCCIÓN

TOBIAS WANGERMANN

El vertiginoso desarrollo tecnológico y la difusión explosiva de los medios digitales como Internet, y la telefonía móvil han determinado su irrupción en todos los órdenes de la vida, sea laboral, público o privado. Su interconexión global en tiempo real, las escasas barreras de acceso y las posiciones interactivas permiten una comunicación tanto cuantitativa como cualitativa diferente a la que estábamos habituados en el pasado.

No sorprende, pues, que el debate acerca de las condiciones generales para el uso de los medios digitales ocupe un espacio importante en la actual discusión política y social al lado de otros temas políticos tradicionales. De hecho, el tema de los medios digitales está presente tanto en las secciones culturales de los medios gráficos como en el debate parlamentario y también nos acompaña en las cuestiones diarias que hacen al uso de estos medios, al margen de que lo que se esté discutiendo sea la protección de los derechos de la personalidad, como lo muestran los debates en torno a Streetview de Google, Facebook, la conservación de datos en Internet, el peligro que corre la neutralidad de la red o las opciones que existen para una mejor protección de los niños.

En Alemania existe gran sensibilidad por estos temas y las decisiones políticas son sometidas a una exhaustiva y crítica discusión. Se espera que la dirigencia política impulse una política que garantice un adecuado equilibrio entre libertad y regulación. Para agotar las posibilidades que ofrecen las redes se considera necesario que la política de Internet garantice por un lado la seguridad debida a través del ejercicio de su función reguladora con el fin de salvaguardar el Estado de derecho y, por el otro, asegure la libertad necesaria para hacer un uso creativo de estos medios en el plano económico, científico, cultural, político

y social. Además, las exigencias que los usuarios plantean en relación con este equilibrio son divergentes entre sí e incluso fluctuantes, según el uso que cada uno de ellos haga de los medios.

Planteada esta realidad, la política enfrenta un dilema. En efecto: difícilmente puede abarcar con los instrumentos propios de una legislación nacional un medio interconectado globalmente que sobrepasa el límite territorial o el ámbito de vigencia del derecho nacional. Aun cuando en el momento del uso pueda establecerse una relación directa entre la localización correspondiente y el ámbito de vigencia jurídica, permitiendo la intervención de la justicia, el problema sigue vigente y reclama un marco de entendimiento internacional, habida cuenta de que los proveedores y usuarios frecuentemente se enfrentan a condiciones por cierto diversas.

En cualquier caso, la política queda convocada a definir las condiciones marco, tanto en el plano nacional como internacional. Y en muchos campos de acción efectivamente ha aceptado ese desafío.

Basta con mirar a nuestros vecinos y al escenario de la política europea para comprender que pueden existir soluciones totalmente diversas y que también allí el debate es conducido en términos controvertidos. La llamada Ley promotora de la difusión y la protección de la creación en Internet o Ley Hadopi (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*) de un modelo de tres avisos ("3-strikes-out") en Francia, o los esfuerzos de regulación "Censilia" en alusión a la Comisaria Europea de Asuntos del Interior, Cecilia Malmström, ponen de manifiesto el grado de conflictividad que pueden alcanzar éstas como otras intervenciones en campos jurídicos vecinos como el de la libertad de la información, la protección de datos personales, el derecho de propiedad o los derechos de personalidad.

Una mirada a cada una de estas problemáticas revela que los objetos que originalmente estaban regulados por una legislación específica a menudo presentan propiedades totalmente diferentes en su manifestación digital, amén de desarrollarse también en un entorno diferente. La movilidad casi ilimitada en espacio y tiempo, la transformabilidad y conectividad de los datos en Internet y la rápida innovación de sus posibilidades de procesamiento le otorgan una dinámica propia, difícil de abarcar por las instituciones sociales.

En el contexto digital se constituye siempre una nueva relación entre el marco jurídico, la aplicación de la ley en sentido estricto y los intereses de los usuarios y ciudadanos respecto de la responsabilidad del Estado en el sentido más amplio, no importa si se trata de derechos de autor, protección y seguridad

de datos, neutralidad de la red, difusión de la red o acceso a la información. Libertad, democracia y Estado de derecho deben demostrar en este contexto que son valores fundamentales de nuestro orden constitucional siempre vigentes.

Es evidente que una infraestructura globalmente interconectada como es Internet, plantea desafíos políticos y sociales iguales o similares en otros países. Resulta, entonces, natural preguntar qué tratamiento merecen temas como marco jurídico, instituciones y estructuras o repercusiones del debate político sobre Internet en la opinión pública en estos otros países.

Los diferentes informes nacionales intentan ofrecer un panorama general de la situación en Estados Unidos, Gran Bretaña, España, Polonia, India y Corea. La selección estuvo a cargo de la red de Oficinas de la Fundación Konrad Adenauer en el exterior, y es también el fruto de reflexiones acerca de la limitación y dispersión de las fuentes. Los países seleccionados presentan estructuras jurídicas y democráticas en gran parte asimilables, habiéndose incluido países europeos y no europeos.

Para una mejor comparación de los datos y de las informaciones brindadas en cada uno de los informes, se envió a las autoras y a los autores previamente el siguiente catálogo orientativo de preguntas:

- ¿Qué lugar ocupa la discusión sobre una política de Internet en el debate político de su país?
- ¿Se exige la conservación de datos, p. ej., para combatir el crimen, y cómo se fundamenta y discute políticamente esta medida?
- ¿Cómo se maneja el tema de la protección y seguridad de datos y qué instituciones existen para garantizarla?
- ¿Qué normas existen acerca del libre acceso a datos públicos (p. ej., datos de la administración pública, así llamados datos abiertos) y qué modelos existen para hacer uso de este derecho?
- ¿Se bloquea en la práctica el acceso a Internet, cómo se regula esta facultad y qué tratamiento se le otorga?
- ¿Qué conflictos se plantean con el derecho de autor vigente, y cómo se solucionan o discuten estos conflictos?
- ¿Existen programas políticos para asegurar la difusión de banda ancha en todo el territorio nacional?
- ¿Intervienen en el debate asociaciones de la sociedad civil?

No fue nuestro interés primario hacer un listado comparable de datos sino ante todo facilitar una impresión sobre la aplicación y discusión política de temas

concernientes a Internet en otros países. Las contribuciones describen qué instituciones, programas y estructuras intervienen en la implementación de objetivos relacionados con una política de Internet, y qué instrumentos son de aplicación con el fin de regular eventuales conflictos jurídicos. La discusión es ilustrada en función de ejemplos que simultáneamente permiten presentar a diversos actores de la política de redes.

Se advierte claramente que en casi todos los casos se asigna una elevada prioridad política y sobre todo económica a la difusión de una red de banda ancha. También quedan al descubierto los esfuerzos que es necesario hacer, por ejemplo en India, para lograr conectividad en todo el país y la importante brecha que existe entre el medio urbano y rural. Fuertes diferencias se aprecian a la hora de comparar la institucionalización en forma de organismos o comisiones encargados de vigilar la aplicación de los programas aprobados, así como su regulación y control. En el caso de Corea existe un organismo dependiente directamente del Primer Ministro, en tanto que en Polonia la institucionalización se hace a través de registros de datos sectoriales. El éxito de una plataforma de venta *online* de pasajes de tren en India que libera a los clientes de las redes de intermediarios corruptos, ilustra la estrecha relación que existe entre la innovación tecnológica y las transformaciones sociales.

La perspectiva de una llamada sociedad digital y la consiguiente dinámica que se genera a partir de la participación en las diferentes opciones de una sociedad del conocimiento, dependen de numerosas condiciones económicas y también políticas, lo que reafirma la función clave de una activa política de cara a las redes de comunicación digitales. Una condición fundamental es una conexión de banda ancha. Igual importancia le cabe a una mayor competencia entre diferentes medios de comunicación. Una condición para el uso proactivo de este medio es la elaboración de estrategias sobre cómo obtener y evaluar informaciones para el intercambio de opiniones, las reglas jurídicas y éticas en la red y las opciones creativas que ofrece este medio.

El acceso a la red y la capacidad de manejo de las ofertas digitales de Internet son categorías fundamentales para la viabilidad futura de un país. Se trata tanto de una dimensión económica como cultural y política e incluso social. Nuestra sociedad sólo podrá beneficiarse con las oportunidades económicas, científicas, culturales y políticas que brinda Internet, si en esta creación de valor participa la mayor cantidad de personas posible. En tal sentido, Alemania y Europa compiten con otros países por ideas y conceptos innovadores en el campo de las tecnologías de la información.

INFORMES NACIONALES

ESTADOS UNIDOS

ROMAN SEHLING

LA POLÍTICA DE INTERNET EN ESTADOS UNIDOS

El triunfo de Barack Obama despertó en muchas empresas la esperanza de que el presidente *Internet* tomara medidas a favor de la neutralidad de la red, dando así cumplimiento a sus promesas electorales. En un principio todo parecía indicar que efectivamente habría un cambio de política respecto de la red. Una serie de asesores de primera línea de Obama venía directamente de Google o de Facebook y Julius Genachowski, conocido defensor de una red neutral, fue designado para presidir la importante Comisión Federal de Comunicaciones (*Federal Communications Commission* - FCC). Además, el paquete de medidas económicas aprobado en 2010 contemplaba 7.200 millones de dólares para la difusión de Internet y banda ancha en todo el país. La intención no era sólo fortalecer la neutralidad de la red sino, sobre todo, generar un entorno de mayor competencia entre los diferentes proveedores, fortaleciendo su capacidad innovadora y, de este modo, contribuir, en el más largo plazo, a la expansión de la economía norteamericana en su conjunto.

Sin embargo, la realidad actual es otra. Las compañías telefónicas y de televisión por cable siguen resistiendo la estricta aplicación de la neutralidad de la red y abogan por el derecho de un tratamiento diferenciado de los paquetes de datos. De no ser así, sus perspectivas de ganancias se verían considerablemente menguadas. Argumentan, además, que una baja en sus ganancias les impediría realizar importantes inversiones en la ampliación y renovación tecnológica de las redes con un resultado contrario al que el propio presidente Obama había fijado como objetivo. Los proveedores de Internet se vieron confirmados en sus convicciones por una sentencia dictada el 2011

por la justicia estadounidense en la que se señala que la Comisión Federal de Comunicaciones carece de autoridad para aplicar el principio de neutralidad de la red.

Entre tanto Google parece haber llegado a un acuerdo con la empresa de telecomunicaciones Verizon que podría servir de modelo para el resto del sector. El acuerdo establece la neutralidad de la red para la transmisión de datos vía red fija. Quedan exceptuadas de la regulación las redes móviles. De llegar otras empresas a un acuerdo similar, podrían evitarse nuevos y tediosos juicios. También el Congreso norteamericano parece preferir esta solución de compromiso. No debe olvidarse que en particular los diputados republicanos están preocupados por una excesiva participación del Estado en la economía. En vista de que cada vez se impone más la trasmisión de datos, voz y video en un solo cable y se acentúa la tendencia de pasar de la red fija a la telefonía móvil, parece aconsejable adaptar la Ley de Telecomunicaciones de 1996 (*Telecommunications Act)* a las innovaciones más recientes, si no se desea poner en peligro el futuro desarrollo de Internet.

Otros temas como derecho de autor, conservación de datos y protección de la privacidad también son materia de debate, aunque estos aspectos se ven opacados por la discusión en torno a la neutralidad de la red que plantea el mayor antagonismo con los intereses corporativos. Por otro lado aumenta el interés por los aspectos internacionales de la política de Internet como la importancia de la red y de las nuevas tecnologías en la lucha por la libertad de los pueblos oprimidos y la colaboración de empresas tecnológicas norteamericanas en la censura política practicada en regímenes represivos. Además de estas decisiones en materia de política interior de otros países, se asigna gran importancia al peligro del terrorismo o de una guerra cibernética, luego de las "exitosas" demostraciones en los últimos años en Estonia y Georgia.

DIFUSIÓN DE LA RED

Ante la gran cantidad de problemas serios en la política interior y exterior que enfrenta Estados Unidos, la política de Internet ocupa en el debate público norteamericano más bien un lugar marginal. No obstante, en 2008, *bloggers* y organizaciones de consumidores muy bien interconectados lograron que la pregunta acerca de la posición de los candidatos demócratas frente a la

neutralidad de la red fuera elegida como pregunta más votada por la audiencia durante un debate promovido por las redes sociales MySpace/MTV.[1]

Aun cuando la opinión pública le asigna al tema una importancia limitada, los políticos son obviamente conscientes de la relevancia que tiene lo que ha dado en llamarse gobierno de Internet (*Internet Governance)*. En Estados Unidos existen más de 700 millones de computadoras y el 65% de los hogares posee acceso a Internet vía banda ancha. Por otra parte, su número se ha duplicado en los últimos cuatro años.[2] Entre diciembre de 1999 y diciembre de 2007, la cantidad de conexiones con una velocidad de transmisión de al menos 200 kbps pasó de 2.800.000 a 121.200.000.[3] Según la Fundación Información, Tecnología & Innovación (*Information, Technology & Innovation Foundation*), la economía norteamericana creció en los últimos diez años debido a Internet en dos billones de dólares. La Consultora TechNet considera factible un crecimiento anual de 300.000 millones de dólares, en la medida en que todo el territorio norteamericano cuente con conexión a Internet.[4]

Pese a estos datos alentadores, Estados Unidos enfrenta la realidad de un creciente atraso frente a numerosos países europeos y asiáticos. Este retraso se refleja en las tasas de transmisión de datos y en el hecho de que ciertos sectores de la población y regiones rurales siguen sin estar conectados, o lo están sólo en forma parcial. Según la FCC, entre un 92% y un 95% de los hogares tiene acceso a un operador de red, el 78% puede elegir entre dos proveedores, pero sólo un 4% puede optar entre tres o más operadores. La FCC considera que este estado de cosas es insuficiente para promover una sana competencia.[5]

Durante la última década, Internet ha cobrado creciente importancia para el desarrollo económico de la sociedad norteamericana de la información, además de influir en prácticamente todos los órdenes de la vida. En este contexto, el debate gira en torno a cómo debe impulsarse el crecimiento y la innovación para hacer factible un nuevo Google, según dichos del propio presidente. Durante

---

1 Glaser, Mark, "TechPresident, 10 Questions Put Spotlight on 'Voter-Generated Content'," PBS, 28. November 2007, http://www.pbs.org/mediashift/2007/11/techpresident-10questions-put-spotlight-on-voter-generated-content332.html.

2 Hatch, David, "The FCC Keeps It Broad," *National Journal*, 20 de marzo de 2010.

3 Figliola, Patricia Moloney und Gilroy, Angele A., und Kruger, Lennard G., *The Evolving Broadband Infrastructure: Expansion, Applications, and Regulation* (Washington, DC: Congressional Research Service, 2009)

4 Wasserman, Elizabeth, "Charging Up for the Next New Things", *CQ Weekly*, 9 de Julio de 2007, pp. 2017-2022.

5 Perine, Keith, "The Medium, Or the Message?" *CQ Weekly*, 10. Mai 2010, pp. 1140-1144.

su campaña electoral, Obama había abogado por la neutralidad de la red y prometido facilitar más fondos estatales para la expansión de la red de banda ancha.

¿SERVICIOS DE INFORMACIÓN O DE COMUNICACIÓN?

En los últimos años ingresaron al Congreso una serie de iniciativas legislativas sobre la neutralidad de Internet, aunque ninguna de ellas llegó a ser aprobada por ambas Cámaras.[6] Por tal razón, las Directivas de la Comisión Federal de Comunicaciones siguen basándose en la Ley de Telecomunicaciones de 1996 que, en principio, no es más que una reforma de la Ley de Comunicaciones de 1934, aunque sin duda esencial en vista de los años trascurridos. La ley de 1996 creó la FCC, cuya función y facultad es garantizar que los proveedores de telefonía fija y móvil, así como de televisión por cable o por satélite, actúen como *common carriers,* es decir como empresas de servicios públicos. La intención era asegurar que todos los usuarios recibieran servicios de igual calidad y que los proveedores no discriminaran entre diferentes grupos de usuarios.

Sin embargo, lo que estaba en juego en la ley era más que garantizar la competencia entre los siete proveedores regionales de telefonía fija. Con anterioridad a la ley, los mercados de las compañías telefónicas habían estado geográficamente delimitados, una limitación que quedó derogada en 1996. A partir de entonces, las siete compañías podían usar recíprocamente sus redes. El precio por el uso estaba regulado por el Estado. Al mismo tiempo se facilitó a nuevos competidores el acceso a las redes de estos proveedores, lo que permitió ofrecer los primeros servicios de Internet. Por razones obvias, en 1996 el concepto banda ancha aparece apenas una vez en el texto de la ley, en tanto que el término *Internet* al menos aparece once veces.[7]

En 1996, los diputados aún diferenciaban entre servicios de telecomunicaciones y servicios de información en relación con la adjudicación del mandato de *common carrier*, una distinción que al cabo de pocos años derivó en problemas dado que los proveedores de redes que usaban su red telefónica para ofrecer

---

6 Tessler, Joelle, "House Vote 239: Telecommunications Overhaul." *CQ Weekly*, 1. Januar 2007, pp. 62-62 y Tessler, Joelle, "2006 Legislative Summary: Telecommunications Overhaul." *CQ Weekly*, 18 de diciembre de 2006, pp. 3370-3370 y Wasserman, Elizabeth, "Charging Up for the Next New Things," *CQ Weekly*, 9 de Julio de 2007, pp. 2017-2022.

7 Wasserman, Elizabeth, "The New Telecom Wars: Looking to Update A Landmark Law," *CQ Weekly*, 14 de noviembre de 2005, pp. 3049-3056.

acceso a Internet (p. ej., DSL) quedaban sometidos a un control más estricto y debían tributar más al Estado que los operadores de red que ofrecían el mismo servicio a través de su red de televisión por cable. En términos de la ley, los primeros eran operadores de servicios de telecomunicaciones y los segundos proveedores de servicios de información.

Estas reglas fueron flexibilizadas en 2005 y los proveedores de Internet DSL declarados proveedores de servicios de información. Paralelamente, en aquellos años surgieron los primeros planteos jurídicos. Una serie de operadores de red (entre ellos la Cox Communications y AT&T) habían comenzado a imponer a sus clientes limitaciones en el uso de las redes y a negar a otros proveedores de servicios (VoIP) directamente el derecho a usar sus redes.[8]

Como consecuencia de esta situación, en 2005 se aprobó un *Internet Policy Statement* que introdujo cuatro principios que debían sustituir las reglas de "*common carrier*", vigentes hasta ese momento. Sin embargo, estos principios no constituían reglas jurídicamente obligatorias y, por ende, no admitían acciones legales para forzar su aplicación.[9]

Según estos cuatro principios, los usuarios de Internet debían tener la posibilidad de:

1. acceder a todos los datos legales demandados,
2. ejecutar todo tipo de aplicaciones,
3. conectar todo tipo de equipos que no dañaran la red del proveedor y
4. elegir entre diferentes operadores.

Estos cuatro puntos fueron criticados como muy poco precisos para constituir una directiva, pese a lo cual el Congreso no procedió a dictar una ley más específica.[10]

NEUTRALIDAD DE LA RED BAJO OBAMA

En vista de la demora en aprobar una reforma de la Ley de Comunicaciones de 1996, el gobierno del presidente Obama intentó tomar otro camino y alcanzar el objetivo de la neutralidad de la red a través de la FCC. La Comisión Federal de

---

8 "Controlling the Internet," *CQ Researcher*, 12 de mayo de 2006.
9 Kroepsch, Adrianne, "Obama Win Yields Shift in High-Tech Priorities," *CQ Weekly*, 1 de diciembre de 2008, pp. 3187-3189.
10 Ruane, Kathleen Ann, *The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC* (Washington, DC: Congressional Research Service, 2010)

Comunicaciones fue creada en el marco de la Ley de Comunicaciones de 1934 y su función es regular las diferentes vías de comunicación (transmisión por radio, televisión, cable, satélite y línea), garantizando que todos los ciudadanos tengan acceso a los servicios de comunicación en condiciones de igualdad y a un precio razonable. La Comisión está integrada por cinco miembros que son nombrados por el Presidente con acuerdo del Senado y su mandato dura cinco años. En ningún momento pueden integrar la Comisión más de tres miembros de un mismo partido.[11]

El nuevo presidente de la Comisión, Julius Genachowski, intentó transformar los principios mencionados más arriba en disposiciones federales y complementarlos con dos normas más: 1) los proveedores de la red debían dar un tratamiento neutral a los paquetes de datos, aplicaciones y servicios, y 2) debían informar acerca de cómo administraban los volúmenes de datos transmitidos en sus redes.[12]

EL PLAN NACIONAL DE BANDA ANCHA

Hasta la fecha, el presidente Obama cumplió al menos parcialmente su promesa electoral de imponer la neutralidad de la red y facilitar más fondos públicos para la difusión de la banda ancha. El paquete de medidas económicas de 2010 contemplaba 7.200 millones de dólares para estudios y créditos que fomentaran la difusión de la banda ancha en todo el territorio nacional.[13] Simultáneamente, el Congreso instó a la FCC, como organismo competente, a elaborar un Plan Nacional de Banda Ancha. Siguiendo el principio de "gobierno abierto", la FCC presidida por Julius Genachowski dió el buen ejemplo y comenzó a recibir un año atrás propuestas de ciudadanos, organizaciones de consumidores y operadores de red. Finalmente, y al cabo de 454 eventos públicos y 74.000 páginas con comentarios, publicó su plan.

El plan contempla cuatro puntos programáticos:

---

11 Figliola, Patricia Moloney, *The Federal Communications Commission: Current Structure and Its Role in the Changing Telecommunications Landscape* (Washington, DC: Congressional Research Service, 2010).

12 Anderson, Nate, "FCC Chairman wants network neutrality, wired and wireless," página web de ars technica, 21 de septiembre de 2009, http://arstechnica.com/tech-policy/news/2009/09/fcc-chairman-wants-network-neutrality-wired-and-wireless.ars.

13 Kruger, Lennard G., *Broadband Infrastructure Programs in the American Recovery and Reinvestment Act* (Washington, DC: Congressional Research Service, 2010)

1. Se establece la ampliación de la infraestructura de redes de banda ancha, con especial énfasis en su difusión en las regiones rurales a un precio accesible para todos en un plazo de diez años.
2. Se deberán destinar a la cobertura con banda ancha al menos 15.500 millones de dólares de los fondos del *Universal Service Fund* que en la actualidad están destinados a promover la difusión de la telefonía fija.
3. Se estimulará la competencia entre los proveedores de red con el consiguiente beneficio para los consumidores.
4. Se promoverán medidas sobre seguridad cibernética, tanto en lo referido a la prevención de un uso abusivo de datos, como también en lo atinente al espionaje económico interior y exterior.

No obstante, estos puntos sólo prevén un fomento indirecto de la neutralidad de la red. Sería importante que proveedores que deseen obtener recursos del Estado también se comprometan a respetar el principio de neutralidad.[14]

Por otro lado, una sentencia reciente de una Corte de Apelaciones de Estados Unidos estableció que la FCC carece de autoridad para obligar a los proveedores de banda ancha a observar el principio de neutralidad.[15] Con su fallo, el tribunal hizo lugar a una acción del proveedor de red Comcast que en 2007 decidió bloquear el tráfico P2P, en especial el tráfico de la aplicación BitTorrent. Ante los estrados judiciales, Comcast argumentó que la medida era necesaria para permitir que todos los usuarios siguieran teniendo acceso libre. Un uso excesivo de conexiones *Peer-to-Peer*, sostuvo, hubiera sobrecargo la red. Según BitTorrent, Comcast violó con esa medida las declaraciones emitidas en 2005 por la FFC conocidas como "Internet Policy Statement". La FCC recogió la queja de BitTorrent e instó a Comcast a no discriminar en lo sucesivo a proveedores de servicios específicos.[16]

Comcast decidió apelar la medida, por lo que la FCC se vio obligada a defender su facultad: en esta causa, la FCC invocó su poder secundario (*ancillary authority*), ya que los proveedores de Internet habían dejado de ser clasificados como proveedores de servicios de telecomunicaciones y se remitió a las disposiciones recientemente sancionadas con el propósito de asegurar el

---

14 Munro, Neil, "Obama's Tech Plans Put Telecoms On The Defensive," *National Journal*, 14 de marzo de 2009 y Muno, Neil, "Tech Giants Anything But Neutral In Access Fight," *National Journal*, 20 de marzo de 2010.
15 Pike, George, "What the Future Holds for Net Neutrality," *Information Today*, junio 2010, año 27, Nr. 6, pp. 1,45.
16 Perine, Keith, "The Medium, Or the Message?" *CQ Weekly*, 10 de mayo de 2010, pp. 1140-1144.

desarrollo de Internet y servicios de comunicación eficientes en todo el territorio federal. Desde la perspectiva del tribunal, sin embargo, estas disposiciones eran meras "declaraciones políticas" y como tales carecían de fuerza de ley. Según este fallo, la FCC parece carecer por el momento de autoridad suficiente para exigir que los diferentes proveedores de banda ancha observen el principio de neutralidad.[17]

Claro que con esto el problema está lejos de haber sido solucionado en forma definitiva. En teoría, Genachowski tiene la posibilidad de recategorizar a todos los proveedores de banda ancha como proveedores de servicios de telecomunicaciones y a partir de ahí regularlos como *common carriers,* es decir como empresas de servicios públicos. Se trata de una posición que en las presentes circunstancias parece viable, al menos desde el punto de vista legal. En 2002, tres de los nueve magistrados de la Corte Suprema de Justicia (entre ellos el juez conservador Antonin Scalia) privilegiaron esta clasificación en el caso *NCTA vs. Brand X*.[18] Claro que aun así no quedaría del todo claro si la FCC tiene autoridad suficiente para introducir esta clasificación y lo más probable es que semejante decisión desencadene una avalancha de acciones legales. En su lugar, Genachowski busca llegar a un compromiso según el cual los proveedores de Internet volverían a ser declarados empresas de servicios públicos, pero quedarían eximidos de la mayoría de las estrictas condiciones que conlleva esta clasificación. En cambio, deberían comprometerse a no aplicar prácticas discriminatorias en la oferta de sus servicios y en el cálculo de la tarifa, lo que se acercaría mucho a una definición de neutralidad de la red.

Es posible que la implementación de este plan hubiera demandado el resto del año y que los consiguientes litigios judiciales hubieran tardado años en resolverse, por lo que finalmente habría tenido que intervenir el Congreso. El último proceso de reforma demandó casi veinte años y apenas concluyó catorce años atrás. En tal sentido no sorprende que una serie de congresistas prefieran no verse involucrados en este proceso. El diputado demócrata y presidente de la Comisión de Energía y Comercio de la Cámara de Representantes, Henry Waxmann, y su colega del Senado y Presidente del Comité de Comercio, Ciencia y Transporte de esa Cámara, Jay Rockefeller, verían con buenos ojos que la

---

17 Brauer-Rieke, Aaron K., The FCC Tackles Net Neutrality: Agency Jurisdiction and the Comcast Order," *Berkeley Technology Law Journal*, año 24, pp. 593-615 y Perine, Keith, "The Medium, Or the Message?" *CQ Weekly*, 10 de mayo de 2010, pp. 1140-1144 y Ruane, Kathleen Ann, *The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC* (Washington, DC: Congressional Research Service, 2010)

18 Ruane, Kathleen Ann, *The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC* (Washington, DC: Congressional Research Service, 2010).

FCC desarrolle su estrategia en cooperación con los operadores de la red y sólo desean involucrarse en forma directa en el más largo plazo. Una opinión similar sustenta el Consejo Tecnológico de Industrias Informáticas (*Information Technology Industry Council – ITIC*) que advierte sobre los riesgos de una regulación excesivamente estricta, dado que ésta podría afectar el crecimiento económico. Sin embargo, es de suponer que sus colegas republicanos en la Cámara de Representantes y en el Senado tengan una visión totalmente diferente de las actividades de la FCC. Desconocen un mandato político general de la FCC: las leyes siguen siendo escritas en el Congreso, señaló al respecto la senadora Kay Bailey Hutchison.[19]

¿CHOQUE DE TITANES?

Entre tanto, la mayoría de los operadores de red ha dejado entrever que seguirán respetando la neutralidad de la red sin necesidad de ser obligados explícitamente a hacerlo. No obstante, se reservarían el derecho de cobrar tarifas más altas por ciertos paquetes de datos y páginas web o limitar el acceso a las mismas en caso de ocupar demasiada capacidad. La argumentación transcurrió aquí por carriles similares a los de otros países. Sin la perspectiva de elevados márgenes de ganancias, los proveedores de Internet como Verizon, AT&T y Comcast no pueden obtener fondos en Wall Street para ampliar sus redes y concretar nuevas inversiones y proyectos innovadores. Argumentan que sus redes ya están parcialmente sobrecargadas por el creciente flujo de datos que deben canalizar. Junto con sus lobistas y asociaciones secotriales como la CTIA Wireless Association luchan sencillamente por preservar el derecho a retener el poder de decisión sobre sus redes.[20]

Walter McCormick, CEO de la U.S. Telecom Association, opina que el gobierno comprende muy bien el problema de la inversión privada y, por ende, los legisladores (por ahora) no definirían la neutralidad de la red en términos más precisos o estrictos que los que actualmente estarían practicando los proveedores de Internet.[21] Por su parte, los oferentes de la red se muestran dispuestos a desarrollar nuevas tecnologías para mejorar sus servicios, pero advierten que estas inversiones deben ser financiadas y también apoyadas.

---

19 Perine, Keith, "The Medium, Or the Message?" *CQ Weekly*, 10 de mayo de 2010, pp. 1140-1144.
20 Wasserman, Elizabeth,"Charging Up for the Next New Things," *CQ Weekly*, 9 de Julio de 2007, pp. 2017-2022.
21 Munro, Neil, "Obama's Tech Plans Put Telecoms On The Defensive," *National Journal*, 14 de marzo de 2009.

A título de ejemplo, McCormick menciona las medidas de protección contra ciberataques y se remite a la prioridad normal que les asiste a clientes más importantes. ¿Acaso la transmisión de datos médicos como radiografías debe recibir el mismo tratamiento que el video de un hámster en YouTube?, pregunta.

AT&T sostiene, además, que Google también debería obligar a sus servicios de buscadores a observar neutralidad, ya que de lo contrario la empresa podría privilegiar las páginas web de sus socios. Al margen de todo esto, los proveedores de Internet se muestran preocupados por una legislación que consagre la neutralidad de la red y no les permita seguir el modelo comercial de la industria del entretenimiento, combinando sus redes con ofertas exclusivas de sus socios entre los que figuran estudios cinematográficos, desarrolladores de juegos, fabricantes de celulares y canales de televisión.[22] Consideran que una ampliación de la banda ancha es más importante que la neutralidad de la red.

Claro que a largo plazo esto podría derivar en un número declinante de compañías que, además, estarían integradas verticalmente y no necesariamente tendrían un interés en la innovación tecnológica. En opinión de los críticos, este desarrollo también explicaría por qué Estados Unidos ha venido perdiendo posiciones en los últimos años frente a otros Estados de la OCDE en lo que hace a la calidad de los servicios de Internet. Entre los principales críticos están Google, Amazon, Ebay y Facebook con activo apoyo de numerosas organizaciones de consumidores como Public Knowledge y Free Press, además de *think tanks* como la Sunlight Foundation, el Centro para la Democracia y la Tecnología o también la Electronic Frontier Foundation. No obstante, estas compañías sólo establecen alianzas circunstanciales con los numerosos lobistas de las empresas de Internet que, además, varían en función de los temas. Sin embargo, según David Sohn del Centro para la Democracia y la Tecnología, todas las partes coinciden en la necesidad de que empresas pequeñas o nuevas puedan ofrecer sus servicios en igualdad de condiciones, para que nada pueda impedir el surgimiento de un próximo Google ni se obstruya la libertad de desarrollo, y las innovaciones puedan realizarse sin necesidad de obtener un permiso especial de los proveedores.

---

22 Munro, Neil, "Obama's Tech Plans Put Telecoms On The Defensive," *National Journal*, 14 de marzo de 2009 und Muno, Neil, "Tech Giants Anything But Neutral In Access Fight," *National Journal*, 20 de marzo de 2010.

¿SE HA PODIDO EVITAR LA BATALLA?

Con millonarios pagos anuales a sus lobistas, los dos contrincantes Google y Verizon parecían no limitarse ya a recíprocas denuncias ante la justicia sino a hostigarse también más activamente en el marco del debate político. A comienzos de agosto de 2010, sin embargo, ambas empresas sorprendieron con una propuesta de compromiso que los defensores de la neutralidad de la red calificaron de puñalada a la propuesta elaborada por Genachowski.

El acuerdo alcanzado establece la neutralidad de la red para la transmisión de datos por la red fija, pero no extiende esa neutralidad a las redes móviles. En los términos planteados en el acuerdo, Verizon recibiría más recursos económicos por ciertos servicios como la transmisión de datos médicos de alta calidad y programas de entretenimiento especiales. Esta decisión se dio a conocer poco después de finalizadas las negociaciones entre la FCC y los proveedores de Internet.[23] En caso de que otras empresas adhieran a este acuerdo, se volverían redundantes nuevos y tediosos juicios, y el resto del sector y la FCC podrían finalmente sumarse al acuerdo. El Congreso norteamericano también parece privilegiar este tipo de solución. No hay que olvidar que en particular los diputados republicanos se muestran preocupados por una excesiva intervención del Estado en la economía.

23 Shilds, Todd und Stone, Brad, "The FCC's Crusade to Keep the Internet Free," Bloomberg Bussinesweek, 11 de agosto de 2010.

GRAN BRETAÑA

LA POLÍTICA DE INTERNET EN GRAN BRETAÑA*

LAURA JOHNSON

1. INTERNET EN EL DEBATE POLÍTICO

En los últimos años, las cuestiones atinentes a Internet han pasado más bien a un segundo plano en el debate político de Gran Bretaña. Por un lado, la crisis económica y financiera ocupa la primera plana del debate y, por el otro, el Reino Unido cuenta hoy con un marco legal de cierta madurez dentro del cual se desenvuelven las actividades en la red. Sin embargo, existen algunos temas que han captado la atención de miembros del Parlamento y de la prensa. Entre estos temas figura la iniciativa del gobierno británico destinada a la conservación a gran escala de datos personales en el marco del Programa de Modernización de la Interceptación (*Interception Modernisation Programme* – IMP) y el proyecto de crear un gran banco de datos de pacientes del Sistema Nacional de Salud de Gran Bretaña (*National Health Service - NHS*).[24] También desató considerables discusiones políticas la propuesta del gobierno de aplicar una dura política contra el intercambio ilegal de datos.[25] Otro tanto ocurrió con cuestiones referidas a la seguridad y protección de datos personales a partir de un reciente escándalo por escuchas telefónicas y una gigantesca pérdida de datos sufrida

---

* Traducción al alemán: Sandra H. Lustig

24 David Leppard, "There's no hiding place as spy HQ plans to see all", *The Sunday Times*, 5 de octubre de 2008. http://www.timesonline.co.uk/tol/news/uk/article4882622.ece (último acceso: 22/9/2010); James Sturke und Denis Campbell, „NHS database raises privacy fears, says doctors", *guardian.co.uk*, 7 de marzo de 2010 18.40 GMT. http://www.guardian.co.uk/society/2010/mar/07/nhs-database-doctors-warning (último acceso: 25/09/2010).

25 Kevin Anderson, "Government details proposed filesharing crackdown", *guardian.co.uk*, 25 de agosto de 2009 12.16 GMT. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (último acceso: 14/09/2010).

por el gobierno en 2007. Pese a que estos temas no guardan relación con Internet y están relacionados con pérdidas de datos en soporte papel o con escuchas telefónicas ilegales, muestran que un caso similar en relación con la seguridad de los datos electrónicos podría alcanzar una amplia cobertura mediática y provocar un importante debate público. En estos momentos, sin embargo, el debate sobre la mayoría de los temas referidos a Internet está más bien reservado a los programas dedicados a temas tecnológicos y a las secciones técnicas de los diarios y la prensa especializada.

2. EL DEBATE EN TORNO A LA CONSERVACIÓN DE DATOS

La primera invitación formulada por el Ministerio del Interior británico a los prestadores de servicios de telecomunicaciones a conservar datos estuvo acompañada del proyecto de implementar un Código de Conducta Voluntario sobre Retención de Datos *(Voluntary Code of Practice on Data Retention*) basado en la Segunda Parte de la Ley sobre Antiterrorismo, Crimen y Seguridad (*Anti-Terrorism, Crime and Security Act*) de 2001. El Código de Conducta exigía la conservación de la base de datos de clientes y datos de telefonía por espacio de doce meses; mensajes cortos, correos electrónicos y datos de proveedores de servicios de Internet debían ser guardados por espacio de seis meses; y protocolos de actividades en la red (incluidas las URLs visitadas) durante cuatro días. Los datos a conservarse incluían los datos de usuario y de tráfico. No se exigía, y tampoco estaba permitida, la conservación de contenidos, es decir lo que efectivamente se decía en una llamada telefónica o en un correo electrónico, por ejemplo. Los datos específicos referidos al tráfico de correos electrónicos eran: nombre de usuario, fecha y hora en la que se iniciaba y terminaba una sesión, dirección IP, desde la cual se hacía el "logueo", así como el nombre de usuario, las direcciones de correo electrónico en los campos "de" y "CC", "fecha" y "hora" de los correos electrónicos enviados y recibidos.[26]

En suma, el Código de Conducta permitía la conservación de datos por parte de los proveedores de servicios de telecomunicaciones para fines comerciales como la facturación a los clientes más allá del período necesario para ello, y hasta los plazos establecidos en el Código. No obstante, cuando los datos almacenados por una empresa superaban el período estipulado para fines comerciales, debían ser identificados como tales, y la empresa no podía recurrir a ellos para

---

26 Home Office Retention of Communications Data under Part II: Anti-Terrorism, Crime & Security Act 2001: Voluntary Code of Practice, Appendix A. http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (último acceso 13/09/2010).

fines propios. La conservación de datos en el marco de estas directivas se ajustaba a las disposiciones de la Ley de Protección de Datos (*Data Protection Act*) de 1998 que en el inc. 5 del Anexo 2 establece que "es necesario que el proveedor de servicios de telecomunicaciones retenga datos para permitir al Ministro de Interior cumplir con su función de proteger la seguridad nacional". Las autoridades de seguridad, inteligencia y ejecución podían obtener acceso a datos de comunicaciones conservados en virtud del Código de Conducta voluntario en función de la Ley de Regulación de Facultades de Investigación *(Regulation of Investigatory Powers Act* - RIPA) de 2000, supervisada por el Comisionado de la Información (*Information Commissioner*).[27] (Ver párrafo 3)

En marzo de 2009, y siguiendo la política de la Unión Europea, el Reino Unido aprobó la parte final de la Directiva de la UE sobre la conservación de datos 2006/24/CE respecto del acceso a Internet, correo electrónico y telefonía vía Internet. La Directiva establecía que los proveedores de los servicios de Internet en los Estados miembros debían conservar datos sobre las comunicaciones mantenidas, es decir datos acerca de quién se había comunicado con quién y cuándo por un período entre seis meses y dos años. Con la decisión de conservar los datos por el período de doce meses, el Reino Unido fácticamente transformó el Código de Conducta en una norma legal obligatoria. Previo a la adopción de las disposiciones legales de la UE se trataron varios temas referidos a la efectiva capacidad de los afectados de dar cumplimiento a la ley. Se trató de establecer si los proveedores de servicios de Internet más pequeños disponían de recursos económicos y de la tecnología necesaria para cumplir con las nuevas disposiciones sobre conservación y consulta de datos.[28] Se trataba de un aspecto especialmente importante para el gobierno, ya que debía compensar a los proveedores de Internet por los costos adicionales que implicaba cumplir con las nuevas normas legales, tal como lo viene haciendo ya en cumplimiento del Código con varios de los grandes proveedores de Internet. [29] El gobierno consideró este aspecto al determinar que los oferentes más importantes, por ejemplo BT, que ya almacenan datos en gran escala, también eran responsables por la retención de los datos transportados por usuarios más pequeños. En consecuencia, el gobierno sólo debería compensar a estos proveedores más importantes por la consulta de datos y no por su almacenamiento. Por lo

---

27 Home Office Retention of Communications Data under Part II: Anti-Terrorism, Crime & Security Act 2001: Voluntary Code of Practice http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (último acceso: 13/09/2010).

28 Chris Williams, "Home Office preps fudgetastic ISP data rules: Cash-strapped Whitehall gives small ISPs free pass", *The Register*, 13. Oktober 2008 14:10 GMT. http://www.theregister.co.uk/2008/10/13/home_office_eudrd/ (último acceso: 14/09/2010).

29 Ibídem

tanto sólo quedarían obligados a almacenar datos sobre las comunicaciones mantenidas en cumplimiento de las normas de la UE los proveedores formalmente notificados por el Ministro del área. El Ministro está obligado a emitir la notificación, a menos que otro proveedor ya esté almacenando los datos en cuestión.[30] Al igual que en el caso del Código voluntario, el acceso a las informaciones almacenadas sobre el uso de Internet y del correo electrónico está sujeto a la Ley de Regulación de Facultades de Investigación RIPA.

A fin de cumplir con el plazo fijado por la UE, en marzo de 2009 la Directiva fue traspuesta en derecho británico a través de un decreto del ejecutivo y, por lo tanto, no requería la aprobación del Parlamento. No obstante, estaba previsto que la Directiva quedara incorporada a un Proyecto de Ley sobre Datos de Comunicaciones *(Communications Data Bill*) más integral. El proyecto, que hasta la fecha no ingresó al Parlamento, estaba diseñado de modo tal de cumplir con la Directiva de la UE a través de la sanción de una ley para la posterior implementación del Programa de Modernización de las Interceptaciones.

El Programa de Modernización de las Interceptaciones había sido establecido para analizar nuevas tecnologías y posibilidades de implementar las medidas necesarias con el fin de asegurar la recopilación, conservación y consulta de datos de Internet. En el marco del programa debían elaborarse planes para la apertura de paquetes de datos y el acceso y registro de datos, por ejemplo acerca de quién tenía contacto con quién y cuándo a través de redes sociales como Facebook, Webmail, Instant Messenger así como juegos *online*. Estos planes exceden en mucho las medidas previstas en la Directiva de la UE para la conservación de datos. En enero de 2010 se anunció la creación de la Dirección de Capacidades en Comunicaciones (*Communications Capabilities Directorate* - CCD) situada en órbita del Ministerio del Interior británico. La nueva Dirección está integrada por dos equipos autárquicos: uno es responsable de las interceptaciones tradicionales, por ejemplo las escuchas telefónicas, en tanto que el segundo trabaja sobre el IMP.[31]

Otro aspecto del IMP, materia de debate varios años atrás, fue la creación de un banco de datos centralizado para datos del tráfico de comunicaciones. El

---

30 Chris Williams, "UK.gov to tap BT as data harvester", *The Register*, 16 de febrero de 2009 09:52 GMT. http://www.theregister.co.uk/2009/02/16/eu_data_retention_transposition/ (último acceso: 15/09/2010).

31 "Entanet raises concern over government's communications interception plans", *infosecurity.com*, 16 de febrero de 2010 http://www.infosecurity-magazine.com/view/7341/entanet-raises-concern-over-governments-communications-interception-plans/ (último acceso: 15/09/2010).

objetivo era concentrar datos de usuarios de todos los proveedores de servicios de comunicaciones en un sistema central único. Supuestamente estos planes fueron impulsados por los servicios secretos, en particular el Cuartel General de Comunicaciones de Gobierno de la Gran Bretaña *(Government Communications Headquarters* - GCHQ*,*), unidad especial de ciber guerra, que en un programa llamado "Dominio de Internet" ("*Mastering the Internet*") trabaja en el desarrollo de tecnologías y métodos con el fin de extraer conocimientos de grandes cantidades de datos supervisados. Es de suponer que el proyecto de crear un gigantesco banco de datos centralizado fue abandonado a raíz de las durísimas críticas recibidas años atrás. La principal crítica fue que un banco de datos de este tipo permitiría a las autoridades obviar la solicitud de datos individuales según lo estipulado en la RIPA y que, por ende, también podría acceder a los datos sin incurrir en costos mayores (que son los que actualmente se producen por el procesamiento de las diferentes consultas) ni control por parte del Comisionado para la Interceptación de Comunicaciones. Por otra parte, los expertos en tecnología afirmaron que el banco de datos no sería un instrumento eficaz en la lucha contra el terrorismo, la principal razón, expresamente mencionada, para su creación. Otra de las principales críticas fue que existía la posibilidad de generar resultados equivocados con la consiguiente acusación de usuarios inocentes.[32]

El futuro de todos los planes sobre conservación de datos electrónicos es más que dudoso desde la asunción de la nueva coalición de gobierno. Actualmente se continúa trabajando en el IMP, aunque el acuerdo de coalición suscrito por los conservadores y los liberales al momento de asumir el gobierno habla de poner "fin a una conservación de datos de Internet y correos electrónicos que no obedezca a una buena razón", sin que, por el momento, esté claro lo que esto finalmente implicará. Gran Bretaña ya traspuso la Directiva de la UE sobre Conservación de Datos en una ley nacional y es poco probable que esta decisión sea revisada, dado que el país es uno de los principales defensores de este programa en Europa. Cabe esperar que los organismos de seguridad ejerzan una fuerte presión para seguir avanzando en el marco del IMP con los planes de una Inspección Profunda de Paquetes (*Deep Packet Inspection*) e incluso de un gran banco de datos centralizado, proyectos en los que ya fueron invertidos considerables fondos.[33]

---

32 Chris Williams, "UK.gov £12bn comms überdatabase 'wouldn't spot terrorists'", *The Register*, 8. Oktober 2008 12:19 GMT. http://www.theregister.co.uk/2008/10/08/us_gov_data_mining_report/ (Letzter Zugriff 15.09.2010); Chris Williams, "Confusion reigns ahead of comms überdatabase debate", *The Register*, 9. Januar 2010 13:57 GMT. http://www.theregister.co.uk/2009/01/09/imp_eudrd/ (último acceso: 14/09/2010).

33 Chris Williams, "ConLibs leave open question over net surveillance", *The Register,* 14. Mai 2010 10.02 GMT, http://www.theregister.co.uk/2010/05/14/conlib_imp/ (último acceso: 13/09/2010).

3. PROTECCIÓN Y SEGURIDAD DE DATOS EN GRAN BRETAÑA

Las tres principales leyes que regulan la protección y seguridad de datos en el Reino Unido son la Ley sobre el uso indebido de las computadoras *(Computer Misuse Act*) de 1990, la Ley sobre protección de datos (*Data Protection Act)* de 1998 y la Ley de regulación de los poderes de investigación (*Regulation of Investigatory Powers Act)* del año 2000.

La Ley sobre el uso indebido de las computadoras definió qué actos debían considerarse un delito en relación con el acceso a las computadoras y cuáles otros no, y especificaba tres tipos de delitos: el intento consciente de obtener acceso a un programa o a datos almacenados en una computadora sin estar facultado para ello; el intento de obtener acceso no autorizado a una computadora con la intención de cometer o promover otros delitos como la obtención de datos financieros y administrativos; y las acciones no autorizadas con la intención de afectar el funcionamiento de una computadora, un programa de computación o de datos almacenados en una computadora o impedir u obstaculizar el acceso a programas o datos almacenados en una computadora. La ley castiga estos delitos en Inglaterra y Gales con una pena privativa de libertad no superior a los 12 meses y en Escocia con seis meses de prisión, o con una multa pecuniaria que no supere el monto máximo establecido por ley.[34]

La Ley sobre protección de datos que dio cumplimiento a una Directiva de la UE estableció los principios y las exigencias que debía observar la conservación de datos privados. La ley obliga a organizaciones que procesan datos personales a respetar una serie de principios: procesamiento justo y legal de los datos; procesamiento de datos para fines limitados; procesamiento adecuado, relevante y proporcional; procesamiento correcto y actualizado; conservación de los datos únicamente por el plazo necesario; procesamiento conforme con los derechos individuales; procesamiento seguro de los datos y no transmisión a países sin adecuada protección. La ley concede al individuo el derecho de saber qué informaciones se almacenan sobre su persona y de corregir informaciones incorrectas.[35] Compete a la Oficina del Comisionado para la Información, un ente británico autárquico, entre otras funciones, velar por el cumplimiento de los principios consagrados en la Ley sobre protección de datos. Asesora a

---

34 Government Legislation Website: Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents (último acceso: 21/09/2010).

35 Government Legislation Website: Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/schedule/1 (último acceso: 21/09/2010); Information Commissioner's Office Website: Data Protection Act http://www.ico.gov.uk/for_the_public/the_acts.aspx (último acceso: 22/09/2010).

organizaciones acerca del cumplimiento de la ley y a los ciudadanos acerca de los derechos que le asisten. Tiene también una oficina que recibe las quejas de los ciudadanos que consideran que una organización viola las disposiciones de la ley. La Oficina del Comisionado no abona compensaciones directas en caso de infracciones a la ley, pero puede obligar a organizaciones a modificar sus procedimientos para dar cumplimiento a la ley.[36]

La Ley de regulación de los poderes de investigación, aprobada en el año 2000, es el primer instrumento legal que regula las facultades de las autoridades públicas para vigilar e interceptar comunicaciones. La ley define qué instancias están facultadas para solicitar acceso a datos de comunicación almacenados como correos electrónicos enviados, tal como se describiera más arriba, y qué instancias pueden interceptar comunicaciones, por ejemplo para leer el contenido de un correo electrónico. Los permisos para interceptar una comunicación deben ser otorgados por el Ministro, pero los entes autorizados pueden solicitar directamente a los prestadores de servicios de comunicación acceso a informaciones almacenadas. Entre los entes que según la ley RIPA están autorizados a obtener acceso a informaciones cabe destacar a la policía, los servicios de inteligencia, el Servicio Nacional de Inteligencia Criminal *(National Criminal Intelligence Service*) y la Agencia para el Crimen Seriamente Organizado *(Serious Organised Crime Agency*), la Agencia de Recaudación Tributaria y Aduanera (*HM Revenue and Customs*), el Servicio de Salud Pública (NHS) y los Concejos Deliberantes, posiblemente la instancia más controvertida. Algunos pocos casos de escuchas que involucraron a ediles en asuntos de poca importancia tuvieron amplia repercusión en los medios.[37] Los organismos autorizados para acceder a los datos conservados deben demostrar que el acceso es en interés de la seguridad nacional, la prevención o detección de delitos o interferencias, el bienestar económico de Reino Unido, la seguridad pública, la protección de la salud pública; la fijación y recaudación de todo tipo de impuestos, aranceles o contribuciones a ser pagados a un ente público; prevención de muerte o lesión; prevención y atenuación de la lesión o daño de la salud física o síquica de una persona.[38] El Código de conducta para la interceptación de comunicaciones *(Interception of Communications Coda of Practice*) complementa lo dispuesto en la RIPA y establece medidas

---

36 Information Commissioner's Office http://www.ico.gov.uk/complaints/data_protection.aspx (último acceso: 22/09/2010).

37 "Spy law 'used in dog fouling war'", *BBC News*, 27 de abril de 2008 11.35 GMT. http://news.bbc.co.uk/1/hi/uk/7369543.stm (último acceso: 26/09/2010).

38 Government Legislation Website: Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents (último acceso: 21/09/2010).

de protección que deben observarse cuando se accede a los datos. El tribunal competente en los procesos relativos a los poderes de investigación *(Investigatory Powers Tribunal* - IPT) es un ente independiente, no partidario, cuya función también es controlar el cumplimiento de la ley. Todo aquel que considere que las autoridades han trasgredido las disposiciones establecidas en la RIPA respecto de su persona, puede interponer ante el Tribunal una queja o un reclamo según lo establecido en la Ley de Derechos Humanos para que el asunto sea investigado por tribunal.[39]

El Reino Unido brinda, además, a los entes públicos y las áreas críticas de la infraestructura nacional con apoyo técnico para protección de sus sistemas y datos. El Centro para la Protección de la Infraestructura Nacional (*Centre for the Protection of National Infrastructure* - CPNI) ofrece asesoramiento integral sobre seguridad a las organizaciones y empresas que conforman la infraestructura nacional para reducir su vulnerabilidad. El asesoramiento abarca la seguridad de las instalaciones, del personal y de la tecnología informática. Los entes gubernamentales deben garantizar que se tomen los recaudos necesarios dentro de sus ámbitos de trabajo para mejorar la seguridad e identificar la infraestructura a ser protegida. En particular se trata de las áreas de comunicaciones, servicios de emergencia, energía, finanzas, alimentos, gobierno, salud, transporte y agua. Entre los asesoramientos que brinda para organizaciones y empresas cuyas infraestructuras son de relevancia nacional figuran medidas de capacitación y asesoramiento personal a cargo de equipos integrados por asesores y expertos especializados, así como asesoramiento *online* y entrega de material de apoyo. El CPNI también puede intercambiar conocimientos acerca de peligros y vulnerabilidades con oficinas claves de la infraestructura nacional y proponer posibilidades sobre cómo prevenir estos peligros. Además, existe una estrecha cooperación entre el CPNI, la Oficina Nacional Antiterrorista *(National Counter Terrorism Security Office*) de la policía y una red nacional de asesores especializados en seguridad antiterrorista de esa fuerza de seguridad que brindan apoyo al CPNI en lo referido al asesoramiento a organizaciones críticas. En dependencias del GCHQ funciona la Autoridad

---

39 Ibídem; recientemente el juez que entiende en una causa ante el Tribunal Europeo de Derechos Humanos dictó sentencia contra un ciudadano del Reino Unido. El ciudadano había alegado que se había violado su derecho a que se respete "su vida privada y familia, su domicilio y su correspondencia" (Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales) por escuchas supuestamente autorizadas sobre la base de la RIPA. El juez elogió las disposiciones de la RIPA y la jurisprudencia del IPT en la materia. ("UK's secret surveillance regime 'does not breach human rights'", *The Register*, 20 de mayo de 2010 08:02 GMT http://www.theregister.co.uk/2010/05/20/surveillance_human_rights_ruling/ (último acceso: 17/09/2010).

Nacional Técnica para aseguramiento de la información (CESG) que también brinda apoyo al CPNI. La CESG tiene a su cargo la seguridad informática (IA) dentro del GCHQ y cumple esta función asesorando y brindado apoyo para garantizar la seguridad de datos electrónicos y de comunicaciones. La CESG ofrece un espectro de asesoramiento técnico que abarca el asesoramiento de temas específicos en aseguramiento informático e instrucción sobre el uso de productos criptográficos y otros productos certificados en seguridad informática. Además, la CESG elabora documentación sobre seguridad sistémica y brinda asesoramiento para la elaboración de documentación técnica. La CESG brinda apoyo a oficinas y autoridades gubernamentales, las Fuerzas Armadas y las diferentes organizaciones y empresas que controlan una infraestructura considerada de importancia nacional.[40]

Para ayudar a empresas y organizaciones que no forman parte de la infraestructura nacional clave, se desarrollaron normas industriales que elaboran directivas para empresas respecto de las estrategias de protección de datos que deben implementar. *Stay Safe Online* (Mantente seguro *online*), una iniciativa privada, también apoya a ciudadanos, instituciones educativas y pequeñas empresas, asesorándolas *online* acerca de la protección de datos.[41]

4. *OPEN DATA*: EL LIBRE ACCESO A LOS DATOS PÚBLICOS

La Ley de Libertad de Información (*Freedom of Information Act*) establece que los procedimientos internos de los actos del gobierno y de la administración pública deben ser informados a la opinión pública. La ley es de aplicación a casi todos los organismos públicos así como a empresas que están totalmente en poder de entes públicos. Esto significa que de acuerdo con lo establecido en la ley, los organismos públicos deben brindar información cuando así sea requerida, siempre que dicha información no esté referida a una de 23 excepciones específicamente enumeradas.[42] La ley también establece que los organismos públicos deben tener un plan autorizado sobre la forma en la que proporcionen activamente informaciones a la sociedad. La Oficina del

---

40 The National Technical Authority for Information Assurance website http://www.cesg.gov.uk/ (último acceso: 26/09/2010).

41 Stay Safe Online Website http://www.staysafeonline.org/ (último acceso: 26/09/2010).

42 Government Legislation Website: Freedom of Information Act 2000 (http://www.legislation.gov.uk/ukpga/2000/36/schedule/1?view=plain); Respecto de directrices sobre excepciones ver página web The Information Commissioner's Office http://www.ico.gov.uk/for_organisations/freedom_of_information/information_request/reasons_to_refuse.aspx (último acceso: 27/09/2010).

Comisionado para la Información que supervisa el cumplimiento de la Ley de Libertad de Información y la legislación RIPA desarrolló un modelo para un plan de publicación que cubre todos los aspectos necesarios para obtener la aprobación, y es de acatamiento obligatorio para todos los organismos públicos. El modelo toma en consideración el tipo de información a ser facilitado, incluidas directivas separadas para determinados tipos de entes públicos como escuelas y concejos deliberantes. Además, cada entidad debe tener y publicar una instrucción para los diferentes tipos de documentación disponibles. Por otra parte, la norma establece que las organizaciones que están en condiciones de administrar una página en Internet, deben facilitar informaciones *online* y deberán publicar en la página también la instrucción correspondiente en un lugar fácil de encontrar.[43] Por lo demás es asunto de los diferentes entes y organismos gubernamentales determinar cuántas de sus informaciones se facilitarán *online*. El Banco de Inglaterra y la Oficina Nacional de Estadísticas administran series temporales de datos económicos y el Registro de la Propiedad incluso vende el acceso *online* a los precios de los inmuebles efectivamente obtenidos en el mercado.[44]

5. BLOQUEO A PÁGINAS DE INTERNET

La Fundación de Vigilancia de Internet (*Internet Watch Foundation* - IWF), una entidad independiente creada en 1996, posee una *hotline* a la que usuarios de Internet pueden denunciar *online* páginas de Internet que potencialmente muestren "contenidos de abuso sexual infantil, obscenidades criminales con adultos e incitación al racismo".[45] Para páginas de Internet en servidores ubicados en el Reino Unido, la Fundación cuenta con un servicio que informa a proveedores de Internet y empresas de *hosting* sobre páginas ilegales para que puedan quitarlas de sus redes. Para páginas que muestran imágenes de abuso infantil y que están ubicadas en servidores en el exterior, la Fundación coordina una iniciativa liderada por el sector que busca bloquear el acceso a las páginas respectivas, facilitando a los proveedores de Internet, operadores de telefonía

---

43 The ICO Model Publication Scheme http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/generic_scheme_v1.0.pdf (último acceso: 27/09/2010).

44 Bank of England website http://www.bankofengland.co.uk/statistics/gdpdatabase/ (último acceso: 26/09/2010); Office for National Statistics website http://www.statistics.gov.uk/cci/nugget.asp?id=192 (último acceso: 26/09/2010); The Land Registry Website http://www.landsearch.net/landregistry/?gclid=CIf6stWrraQCFYGX2AodRmCQcg (último acceso: 26/09/2010).

45 Internet Watch Foundation Website http://www.iwf.org.uk/ (último acceso: 26/09/2010).

celular, buscadores y proveedores de contenidos una lista con las URL de páginas que muestran el abuso a niños.[46] Estas páginas son clasificadas según el derecho británico y cada imagen es categorizada siguiendo los criterios del Consejo de Emisor de las Directrices para la Imposición de Penas (*Sentencing Guidelines Council)* británico. La lista contiene entre 500 y 800 páginas web y es actualizada dos veces por día. Los sistemas y procesos de la Fundación son analizados y auditados periódicamente por expertos independientes. Toda persona puede interponer una acción legal contra la calificación de una ULR por parte de la IWF, si cree que esta calificación le niega acceso a contenidos legales.[47]

Según datos publicados en la prensa, el 98,5% de los proveedores de Internet utiliza actualmente los servicios de la IWF para borrar o bloquear páginas ilegales, aunque el gobierno comienza a adoptar un rol más activo en este asunto.[48] En marzo de este año se prohibió a las oficinas públicas usar proveedores de Internet que no bloquearan activamente las páginas web clasificadas por la IWF como proveedoras de imágenes de abuso sexual infantil. La orden impartida a todos los departamentos de gobierno, organismos y *quangos* (quasi organizaciones no gubernamentales) establecía que esta nueva política debía ser aplicada a compañías proveedoras de internet, compañías de telefonía móvil, buscadores y empresas que proveen programas de filtrado del acceso a Internet.[49]

Según el párrafo 3 de la Ley Antiterrorista de 2006, el gobierno tiene el derecho de obligar a las compañías que proveen servicios de *hosting* en el Reino Unido a borrar material extremista. No obstante, el ex Ministro de Seguridad, Lord West, admitió que hasta el momento la disposición demostró ser innecesaria, ya que la policía había persuadido a las empresas de *hosting* a retirar ese tipo de material en forma voluntaria. En la actualidad, el gobierno no cuenta con las facultades legales para bloquear páginas cuyo servidor se encuentra ubicado en el exterior. No obstante, puede recomendar que las empresas proveedoras de *software* para el filtrado del acceso a Internet incorporen estas páginas al bloqueo de páginas

---

46 Ibídem http://www.iwf.org.uk/public/page.103.htm (último acceso: 26/09/2010).
47 Ibídem http://www.iwf.org.uk/public/page.148.htm (último acceso: 26/09/2010).
48 Jane Merrick, "Internet providers face child porn crackdown", *The Independent*, 6 de septiembre de 2009 http://www.independent.co.uk/news/uk/crime/internet-providers-face-child-porn-crackdown-1782530.html (último acceso: 18.09.2010).
49 Sean O'Neill, "Government ban on internet firms that do not block child sex sites", *The Times*, 10 de marzo de 2010. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece (último acceso: 18/09/2010).

no aptas para menores, lo que significa que quedarían bloqueadas para ciertos usuarios, por ejemplo escuelas primarias y preparatorias.[50]

En lo que se refiere a los usuarios individuales, la Ley de Economía digital, aprobada sobre el fin del último período legislativo, faculta al Ministro a instruir a proveedores de Internet a bloquear temporalmente cuentas de usuarios cuando se considera que éstos han vulnerado regularmente las normas sobre propiedad intelectual.[51] Un agregado introducido a último momento en la cláusula 8 del proyecto de ley concede al Ministro de Economía la facultad de instruir a los proveedores de servicios de Internet a "[bloquear] un sitio en Internet del que el tribunal se ha cerciorado de que fue, es o probablemente será usado para o en relación con una actividad que viola el derecho de autor".[52]

6. EL CONFLICTO EN TORNO A LOS DERECHOS DE AUTOR

En relación con el fortalecimiento de los derechos de autor en la lucha contra el intercambio de archivos se presentó recientemente un conflicto de orden legislativo. La Ley de Economía Digital, aprobada en abril de 2010, prevé un procedimiento en el trato de las violaciones al derecho de autor *online* que abarca a libros, películas y música. Según la ley, los titulares de los derechos de autor que se consideran vulnerados en sus derechos pueden enviar un informe acerca de la infracción cometida al respectivo proveedor de Internet, cuya responsabilidad es llevar un registro de este tipo sobre las infracciones cometidas por los usuarios. Si los clientes alcanzan una cantidad determinada de violaciones, sus direcciones IP son incorporadas a un listado anónimo de infracciones al derecho de autor. Los titulares de los derechos pueden obtener acceso a la lista con ayuda de una decisión judicial y, en tal caso, iniciar acciones legales contra los usuarios que cometen estas infracciones. La ley aumenta la pena máxima para quienes infringen el derecho de autor *online*. Un punto controvertido es la facultad que la ley le confiere al Ministro para instruir a los proveedores de Internet a adoptar medidas técnicas contra usuarios que han cometido un cierta cantidad de transgresiones. Entre las medidas se

---

50 Chris Williams, "UK Gov moves to block Hamas kids site", *The Register*, 14 de enero de 2010. http://www.theregister.co.uk/2010/01/14/ellman_hamas/ (último acceso: 18/09/2010).

51 Richard Taylor, "The Digital Economy Act 2010 and online copyright infringement", *The Law Gazette*, 9 de septiembre de 2010. http://www.lawgazette.co.uk/in-practice/the-digital-economy-act-2010-and-online-copyright-infringement (último acceso: 17/09/2010).

52 Charles Arthur, "Digital economy bill rushed through wash-up in late night session", *guardian.co.uk*, 8. April 00.05 BST. http://www.guardian.co.uk/technology/2010/apr/08/digital-economy-bill-passes-third-reading (último acceso: 17/09/2010).

cuenta la acotación del ancho de banda o el bloqueo temporal de una cuenta.[53] En junio de 2009 quedó descartado un plan anterior que contemplaba la posibilidad de bloquear el acceso a Internet en forma permanente.[54] *Ofcom*, organismo regulador del sector de las comunicaciones, sobre todo en cuestiones de competencia, tiene a su cargo la reglamentación de la ley. El organismo autárquico es responsable de las áreas de televisión, radio, comunicación por redes fijas y telefonía móvil así como de las ondas radiales de los equipos inalámbricos. La Ley de Comunicaciones de 2003 establece que el organismo debe promover los intereses de ciudadanos y consumidores asegurando una programación ampliamente diversa y de elevada calidad, proteger a los consumidores de contenidos ofensivos y, lo que es fundamental, garantizar una amplia selección de servicios de comunicación electrónicos, entre ellos la banda ancha.[55]

Las disposiciones de la propia Ley de Economía Digital de 2010 y el borrador de un código reglamentario elaborado por el *Ofcom* han desencadenado considerables controversias entre las diferentes partes afectadas. Se han formulado objeciones a las normas a ser utilizadas para demostrar las infracciones, ya que el proyecto del *Ofcom* no establece qué medios podrán usarse para obtener pruebas ni cuánta prueba es necesaria.[56] Se teme que todos los usuarios de una dirección IP se vean castigados por las acciones de una sola persona, por ejemplo que se responsabilicen a los padres por las descargas ilegales de sus hijos. Además, los proyectos de bloquear el acceso a Internet se consideran un ataque a los derechos cívicos.[57] Otras controversias surgieron más recientemente respecto de la financiación de la nueva política a implementar. La ley prevé que el costo derivado de la persecución de personas que descargan datos en forma ilegal se repartan entre los titulares de los derechos de autor y los proveedores de los servicios de comunicación

---

53 Richard Taylor, "The Digital Economy Act 2010 and online copyright infringement", The Law Gazette, 9 de septiembre de 2010. http://www.lawgazette.co.uk/in-practice/the-digital-economy-act-2010-and-online-copyright-infringement (último acceso: 24/09/2010).
54 Kevin Anderson, "Government details proposed filesharing crackdown", guardian.co.uk, 25 de agosto de 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (último acceso: 23/09/2010).
55 Ofcom website. http://www.ofcom.org.uk/about/what-is-ofcom/ (último acceso: 7/10/2010).
56 "Draft filesharing code flawed, says Open Rights Group", Charles Arthur, *guardian.co.uk*, 22 de Julio de 2010 15.40 BST. http://www.guardian.co.uk/technology/2010/jul/22/filesharing-ofcom-open-rights-group (último acceso: 23/09/2010).
57 Kevin Anderson, "Government details proposed filesharing crackdown", guardian.co.uk, 25 de agosto de 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (último acceso: 23/09/2010).

en una relación de 75:25. Los titulares de los derechos han protestado contra el hecho de que se vean obligados a hacer frente a la mayor parte del costo económico. El gobierno justificó el borrador de la ley señalando que las medidas beneficiarían al sector creativo en unos 200.000 millones de libras esterlinas por año y que, por lo tanto, sería adecuado que los titulares asuman la mayor parte de los costos. Un grupo de defensores del consumidor, por su parte, centra su crítica en el peligro de que los proveedores de Internet trasladen los costos adicionales a los precios. Producto de ese aumento, señala la agrupación, miles de consumidores "podrían no poder hacer frente al costo que demandaría acceder a una banda ancha".[58] Esto, argumentan, contradice de manera directa la política del gobierno empeñado en promover una mayor difusión de la banda ancha.[59]

7. PROGRAMAS PARA LA DIFUSIÓN NACIONAL DE BANDA ANCHA

Hacia fines de enero de 2009, el Ministro de Comunicaciones laborista dio a conocer un "compromiso de acceso universal a banda ancha". Según este compromiso contraído por el gobierno, para 2012 todos los hogares en Gran Bretaña deben tener la posibilidad de acceder a los servicios de banda ancha con una velocidad mínima de 2Mbps. Esta promesa fue una de varias publicadas en el informe "*Digital Britain*" del mismo mes.[60] El plan prevería la cooperación entre el gobierno y los proveedores de Internet privados en los esfuerzos por universalizar el acceso a Internet. El proyecto oficial contemplaba crear un impuesto de 0,50 libras esterlinas sobre todas las conexiones de telefonía fija para financiar la implementación de esta medida.[61] Sin embargo, la idea de crear un impuesto fue abandonado antes de las elecciones de mayo y en el nuevo proyecto de presupuesto presentado por el Ministro de Finanzas en el mes de junio quedó eliminado por completo.[62] Dado que no existía respaldo

---

58 Mark Sweney, "0Illegal downloads: music industry to carry cost of catching pirates", *guardian.co.uk*, 14 de septiembre de 2010 15.37 BST. http://www.guardian.co.uk/technology/2010/sep/14/illegal-downloads-music-industry (último acceso: 24/09/2010).
59 Kevin Anderson, "Government details proposed filesharing crackdown", guardian.co.uk, 25 de agosto de 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (último acceso: 23/09/2010).
60 Digital Britain: The Final Report http://interactive.bis.gov.uk/digitalbritain/report/executive-summary/universal-service-committment/ (último acceso: 17/09/2010).
61 Jane Wakefield, "Broadband tax 'to be made law'", *BBC News*, 23 de septiembre de 2009 12:56 GMT http://news.bbc.co.uk/1/hi/8270772.stm (último acceso: 15/09/2010).
62 Chris Williams, "Broadband tax scrapped in 'wash-up'", *The Register*, 7. April 2010 12:14 GMT. http://www.theregister.co.uk/2010/04/07/broadband_cider/ (Letzter Zugriff 15.09.2010).

jurídico para obligar a los proveedores de Internet a implementar la medida ni se contaba con subsidios para fomentar la ampliación de la oferta, se cuestionó la factibilidad de alcanzar el objetivo formulado por el gobierno. Una estimación más reciente sugiere que sigue habiendo unos 160.000 hogares que no tienen posibilidad alguna de acceder a un servicio de banda ancha y que unos dos millones de hogares sólo tienen conexiones inferiores a 2 Mbps.[63]

El 15 de julio próximo pasado, el nuevo Ministro de Cultura, Jeremy Hunt, alargó el plazo para una cobertura total con Internet banda ancha para 2015. BT ya se comprometió a invertir unos 2.500 millones de libras esterlinas para ampliar su red de banda ancha fibra óptica, aunque advirtió que sin la ayuda del gobierno no podía aumentar sus inversiones más allá de esa cifra.[64] El gobierno proyecta facilitar fondos para apoyar la ampliación de Internet redireccionando recursos presupuestados, pero no desembolsados, de un plan de reconversión a la televisión digital.[65] La Oficina para la Difusión de Banda Ancha en el Reino Unido dependiente del Departamento de Innovaciones y Capacidades Empresarias (BIS por sus siglas en inglés) está a cargo del desarrollo de planes para la implementación de la nueva promesa del gobierno y la inversión efectiva de fondos públicos. La primera medida de esta Oficina será lanzar tres proyectos piloto en áreas rurales. Se trata de analizar cuál es la mejor forma de invertir fondos estatales en regiones en las que conectar accesos de alta velocidad a Internet, resulta económicamente poco interesante.[66]

8. SOCIEDAD CIVIL Y POLITICA DE INTERNET

Diversas organizaciones sectoriales participan en el debate acerca de cuestiones referidas a Internet. El debate incluye consultas formales del gobierno a las grandes asociaciones industriales, por ejemplo la asociación bancaria APACS, hasta la presión informal que ejercen ciertos sectores de electorado sobre los miembros del Parlamento para obtener mejor acceso a banda ancha en distritos electorales rurales, por ejemplo. Algunas asociaciones se crean especialmente con el fin de interactuar con el gobierno en estos temas. El Consejo Asesor para la Seguridad de la Información *(Information Assurance*

---

63 Graeme Wearden, "Broadband target put back to 2015" *guardian.co.uk*, 15. Juli 2010 17:54 BST. http://www.guardian.co.uk/technology/2010/jul/15/fast-broadband-target-put-back (último acceso: 15/09/2010).
64 Ibídem.
65 Department for Business Innovation & Skills website: Broadband Delivery UK http://www.bis.gov.uk/BDUK (último acceso: 15/09/2010).
66 Ibídem.

Advisory Council - IAAC), cuyo objetivo es "trabajar en pos de una sociedad de la información segura" reúne a decisores de la economía, la política, la policía y los investigadores científicos con el propósito de elaborar ideas. Los miembros del Panel de Enlace del IAAC con el Gobierno representan un amplio espectro de organismos gubernamentales y de seguridad, entre los que figuran la Oficina para la Seguridad Cibernética del Reino Unido, el Centro para la Protección de la Infraestructura Nacional, el Ministerio de Defensa y la Agencia para el Crimen Seriamente Organizado.[67] Existen numerosos otros grupos de la más diversa extracción cuyo propósito es presionar al gobierno, entre ellos cabe destacar a la ONG *Privacy International* y la organización *Open Rights Group*.[68] El gobierno puede interactuar con estos grupos mediante consultas sobre proyectos de ley, iniciativas formales y participación en audiencias parlamentarias. Pero también puede usar canales menos formales como eventos organizados por The Royal Institute of International Affairs (Chatham House), una entidad sin fines de lucro.

67 The Information Assurance Advisory Council website http://www.iaac.org.uk/ (último acceso: 24/09/2010).

68 Privacy International website http://www.privacyinternational.org/ (último acceso: 27/09/2010); Open Rights Group website http://www.openrightsgroup.org/ (último acceso: 27/09/2010).

ESPAÑA

LAS PERSPECTIVAS ESPAÑOLAS EN RELACIÓN AL CONTROL Y LA LIBERTAD DE OPINIÓN EN INTERNET

HANS GÜNTER KELLNER

Aproximadamente la mitad de los hogares españoles tiene acceso a Internet, de los cuales casi todos cuentan con una conexión de banda ancha, ya sea por ADSL o cable. Según un estudio de la "Fundación Orange" de la compañía de telecomunicaciones francesa France Telekom (eEspaña 2010[69]), las conexiones de banda ancha están especialmente difundidas en las regiones metropolitanas de Madrid y Cataluña, lo que los autores no sólo adjudican a la popularidad de estas conexiones, sino también a su disponibilidad. En regiones de mayor extensión geográfica como Castilla-La Mancha, Castilla y León o Extremadura, en muchos lugares no se ofrece DSL o conexión por cable debido a los altos costos de las inversiones que deberían efectuarse. No existe, por otra parte, un derecho legal a reclamar la conexión a Internet.

La lectura de los correos electrónicos es el uso más asiduo que los españoles le dan a Internet. En la comparación europea, España se destaca sobre todo por el consumo de medios de información. En efecto, el 64% de los españoles que poseen Internet lee allí los diarios (UE: 43%), el 42% escucha radio o mira televisión (UE: 37%). El 32% de los españoles también visita redes sociales como Facebook y Tuenti, una suerte de versión española del StudiVZ alemán. El organismo de protección de datos comparte las quejas acerca de los malos estándares de protección de las redes sociales estadounidenses y, en cambio, elogia la cooperación con la red española "Tuenti". De considerarlo necesario, Tuenti incluso solicita a sus clientes enviar copia de su documento de identidad para verificar la edad del usuario. Los menores de 14 años requieren el consentimiento de los padres para participar en una red social virtual.

---

69 http://www.informeeespana.es/docs/eE2010.pdf.

Por el contrario, Internet se usa por debajo de la media europea en lo que se refiere a compras y operaciones bancarias. Menos del 40% de los usuarios españoles de Internet realiza transferencias por Internet, en tanto que en la UE ya suman la mitad. Según datos de la industria discográfica, el uso de redes P2P para intercambio de obras protegidas por los derechos de autor está ampliamente difundido en España, aunque por el momento no se cuentan con datos confiables. Según el estudio eEspaña 2010, en 2009 el 11% de los usuarios españoles de Internet intercambió archivos de películas, en tanto que un 7,5% intercambió música. Estas cifras son declinantes respecto del año anterior.

MARCO JURÍDICO

La legislación española respecto de Internet es relativamente reciente. El 1 de julio de 2002 el Parlamento aprobó la "Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico" (LSSI). La ley hace especial énfasis en la seguridad jurídica para el comercio electrónico e implicó la puesta en práctica de la Directiva 2000/31/EU adoptada dos años antes por el Parlamento Europeo y el Consejo, además de otras disposiciones europeas anteriores en materia de defensa del consumidor.

El instrumento legal trata, asimismo, cuestiones atinentes a la libertad de los proveedores de contenidos y derechos de los usuarios. Al momento de su sanción fue reconocido, sobre todo, por ser el primer marco jurídico para el control de los usuarios de la red. Durante las deliberaciones parlamentarias mismas se agregaron disposiciones de la Unión Europea sobre protección de la privacidad y almacenamiento de datos de conexión, páginas de Internet visitadas y comunicaciones electrónicas. La ley ilustra los problemas que se plantean a la hora de implementar normas nacionales en la red global. En España está oficialmente prohibida la publicidad no deseada ("*spam*"), algo que en la práctica no garantiza, sin embargo, una protección efectiva ante ofertas de todo tipo, juegos de azar u ofertas engañosas.

Mientras que la mayor parte del articulado de la ley apenas concitó interés al momento de su deliberación parlamentaria, hubo un fuerte debate en torno a cuestiones referidas al control o incluso bloqueo de ciertas páginas web. Se habló de una "Ley Orwell" e incluso de la recreación de un organismo de

censura. En los años subsiguientes, la ley fue actualizada sin que los temores de una posible censura se confirmaran.

LUCHA CONTRA CONTENIDOS DE RELEVANCIA PENAL

La democracia parlamentaria española, instalada tan sólo en 1978, ha tenido tradicionalmente dificultades para aceptar un control de contenidos, no sólo en Internet sino en todo tipo de publicaciones. Como ejemplo valga citar el tratamiento dado a escritos de la extrema derecha, o anticonstitucionales que en España se imprimían y comercializaban libremente hasta entrada la década de 1990. El país se convirtió así en uno de los mercados más importantes de este tipo de literatura, sin que ello obedeciera a una efectiva influencia social de estos sectores, sino más bien a la idea de que una sociedad democrática no debe reprimir ni siquiera tendencias antidemocráticas y, por el contrario, entablar un discurso abierto con estas manifestaciones para demostrar así su especial fortaleza y capacidad defensiva.

Sólo cuando la lucha contra el terrorismo de ETA se hizo extensiva a los escritos de organizaciones que en opinión de la justicia estaban controladas por la red terrorista, comenzó a prevalecer la opinión de que la libertad de opinión debe respetar ciertos límites, aun en una democracia. A partir de una profunda reforma del Código Penal en 1995, los escritos "que nieguen o justifiquen los delitos de genocidio o pretendan la rehabilitación de regímenes o instituciones que amparen prácticas generadoras de los mismos" finalmente se equipararon a los escritos que hacían apología del terrorismo. En ese momento ya estaban prohibidas las publicaciones referidas a delitos evidentes como la pornografía infantil.[70]

EL CASO BATASUNA

En 2002, una nueva Ley Orgánica de Partidos Políticos permitió prohibir el partido Batasuna, brazo político de ETA, así como sus organizaciones sucesoras. El Tribunal Europeo ratificó dicha prohibición. Como consecuencia de esta medida también debían cesar las actividades del partido en Internet. Este caso ilustra cómo funciona la ley y cuáles son los problemas en su aplicación.

---

70 Para más detalle sobre la legislación española sobre Internet: "Aplicación Práctica de La LSSI-CE", Paloma Llaneza González, Barcelona 2003.

En España, igual que en otros países, la justicia tiene un rápido acceso a servidores nacionales. Si bien los proveedores de los servicios no están obligados a supervisar los contenidos guardados en sus servidores, sí, en cambio, deben retirarlos de la red cuando un juez de instrucción así lo dictamine. La ley aprobada en 2002 también permite limitar el acceso a páginas en la red, es decir no sólo ejercer control sobre la oferta sino también sobre la demanda, cuando se ha emitido la orden judicial correspondiente.

En aquel momento, el conocido juez español de Primera Instancia e Instrucción, Baltasar Garzón, dispuso bloquear varias páginas web de Batasuna en España. La LSSI, que había sido aprobada poco antes, preveía la posibilidad de bloquear el acceso a determinadas páginas. En principio, la medida parecía razonable: si bien la justicia no tenía acceso a los servidores en el exterior donde estaban almacenadas estas páginas, buscaba evitar al menos el acceso desde el territorio al que estaban dirigidos los contenidos. No se pretendía prevenir el delito, ya que esto resultaba imposible, sino las consecuencias en el interior del país.

En el caso de batasuna.org y varias páginas similares, el magistrado había instado a la Organización Internacional de Registro ICANN (*Internet Corporation for Assigned Names and Numbers*) a borrar estas URLs y a no permitir registros de nuevas páginas con los nombres Batasuna, Euskal Herritarrok o Herri Batasuna. Asimismo se solicitó a varios servidores en Australia y Estados Unidos borrar el dominio batasuna.org y páginas similares. No obstante, ninguno de estos destinatarios quiso reconocer la jurisdicción de la justicia española, habida cuenta de que las páginas en parte habían sido registradas desde Francia. Otros dominios fueron registrados bajo identidades falsas. Incluso se llegó a decir que el ex dirigente socialista Ernest Lluch había registrado una página para el brazo político de ETA, lo que no dejaba de ser especialmente cínico, considerando que Lluch había sido asesinado por ETA con anterioridad al registro. Como dirección del supuesto dueño del dominio se indicó la casa en la que los terroristas habían ejecutado a Lluch. Recién años después de que se suprimiera el acceso desde España, las páginas desaparecieron de Internet.

El caso Batasuna ilustra las dificultades a las que se enfrentan las autoridades para llevar adelante una persecución penal en Internet, algo que también se aplica a otros delitos como el tema de la pornografía infantil, tan discutido en Alemania.

ALMACENAMIENTO DE DATOS

La posibilidad de bloquear páginas desencadenó fuertes protestas en España, en tanto que se articularon pocas objeciones a la obligación de los proveedores de conservar los datos de conexión de sus clientes. La norma establece que deben conservarse durante un año los números IP para la identificación de los usuarios y toda actividad relacionada en la red. Es así que la policía, por orden judicial, puede hacer un seguimiento de hasta un año para verificar quién visita qué páginas y, en particular, qué contenidos ha almacenado en servidores en la red. Mucho más fuerte, en cambio, fue la protesta de los defensores de los consumidores contra disposiciones similares destinadas a identificar una posición determinada en la red de telefonía móvil. Estas disposiciones facultan a la policía a determinar el lugar de un teléfono móvil activo por espacio de un año, incluso con efecto retroactivo. Los proveedores de servicios no necesitan, en cambio, conservar los contenidos de los correos electrónicos.

DERECHO DE AUTOR: ¿TODO ESTÁ PERMITIDO?

La industria discográfica española ha dado la voz de alerta. En cinco años se habrá terminado la producción musical española si el gobierno no mejora la protección de los derechos de autor, advierte el cantautor Luis Eduardo Aute. Grupos musicales consolidados como Ketama han terminado por separarse porque mientras circulan innumerables copias ilegales de sus discos, las ventas en las casas de música están estancadas. Las cifras hablan a las claras: para 2009, Productores de Música de España, asociación que nuclea a la mayor parte de la industria discográfica española, dio a conocer una caída en las ventas de €126.500.000 de euros a €77.000.000. Una situación similar plantea la industria cinematográfica: Filmax, una de las productoras más conocidas, se ha declarado en quiebra. Como consecuencia de la situación creada, los grandes sellos musicales y productoras cinematográficas han despedido al 90% de sus empleados en tan solo seis años.[71]

La industria cultural le echa la culpa al escaso respeto por los derechos de autor y en eso es secundada hasta por el gobierno de Estados Unidos que incluyó a España en sus informes anuales sobre contravenciones a los derechos de autor.[72] Según noticias publicadas en diarios españoles, el presidente de Estados

---

71 http://www.elpais.com/articulo/opinion/Descargas/ilegales/gratuitas/elpepuopi/20100804elpepiopi_9/Tes.
72 http://www.elpais.com/articulo/cultura/EE/UU/abronca/Espana/pirata/elpepicul/20090506elpepicul_1/Tes.

Unidos Obama incluso habría llamado al jefe de gobierno español Zapatero para instarlo a apurar una reforma legislativa.[73]

El gobierno de Estados Unidos critica en particular una instrucción de la procuraduría general española impartida a las fiscalías en las provincias de no evaluar las violaciones a los derechos de autor como delitos cuando no se puede demostrar afán de lucro. Claro que la procuraduría general no hace más que aplicar la legislación vigente.

Gran revuelo causó entre la industria discográfica como entre sectores de Internet el sobreseimiento de un operador de una página de Internet en un caso de supuestas violaciones a los derechos de autor en mayo de 2010.[74] En la página siguen indicándose hasta la fecha los títulos de las películas que se pueden ver en "*streaming*" por Internet o que pueden ser bajadas de la red. Incluso hay un ranking de los títulos más vistos. El sobreseimiento se fundó en el hecho de que la bajada no se había efectuado directamente desde la página en cuestión, sino que un clic sobre el título de la película conducía a *links* a servidores como "megaupload" desde donde se podían bajar estas películas.

El operador de la página, accesible hasta la fecha, fue sobreseído pese a que la masiva publicidad era una prueba evidente de afán de lucro. La razón por la cual el operador fue sobreseído estriba en que la ley penal española establece que la obra protegida por el derecho de autor tiene que ser ofrecida por el inculpado, es decir que la mera inclusión de un "*link*" no basta.

En España, el fallo fue interpretado de tal modo que el derecho de autor no tiene vigencia fáctica en Internet. Esa misma impresión generan los abogados que se ocupan de estos casos a través de los mensajes que transmiten en sus múltiples conferencias. Por otra parte, la industria discográfica, como parte actora, incurrió en un error fundamental, afirma Paloma Llaneza González, una de las expertas más renombradas en derecho de Internet en España. La industria discográfica, señala la abogada, habría querido ganar a toda costa un juicio penal mediático que desembocara en una pena privativa de libertad para el operador de la página. De haber presentado una demanda por daños y perjuicios, las perspectivas de éxito hubieran sido mejores y probablemente la página se habría bajado. Sin embargo, el planteo equivocado del sector hizo que la página del comerciante imputado siga publicando hasta la fecha los *links* para

---

73 http://www.elpais.com/articulo/tecnologia/Estados/Unidos/coloca/Espana/paises/pirateria/elpeputec/20100520elpeputec_1/Tes.
74 http://www.filmica.com/david_bravo/.

bajar toda la producción cinematográfica internacional y que en España cunda la falsa creencia de que infringir el derecho de autor es absolutamente normal.

LA "LEY SINDE"

El Ministerio de Cultura español ha elaborado ahora un proyecto de ley con el que intenta limitar las violaciones al derecho de autor en Internet. Una de las disposiciones del proyecto prevé sancionar también la publicación de *links* según lo señalado más arriba. Sin embargo, la ley no enfoca el tema desde el derecho penal. Por el contrario, está previsto crear una Comisión para Protección del Derecho de Autor en el área del Ministerio de Cultura que a solicitud de los titulares de los derechos (autores, editoriales, industria discográfica, etc.) tendrá la facultad de proceder al cierre de páginas en Internet si constata allí una violación de estos derechos. Previamente se oirá a los operadores de las páginas que tendrán la posibilidad de interponer un recurso ante el Tribunal Nacional contra el cierre de la página. El tribunal debe decidir en el término de cuatro días.

El Tribunal Nacional no emite un fallo sobre el fondo de la cuestión, es decir no decide si efectivamente existe una violación a los derechos de autor, sino sólo si el cierre de la página limita un derecho fundamental como es la libertad de opinión. El operador puede recurrir el cierre de la página ante los tribunales locales.

La única persona conforme con esta regulación, que aún espera ser debatida en el parlamento, es la ministra de Cultura González-Sinde, apellido que la prensa utiliza para denominar la ley. La ministra recalca que de este modo se persigue a "quien se enriquezca de modo ilegal a expensas del trabajo de otro", es decir viole el derecho de autor. El proyecto no penaliza las bajadas ilegales como sí ocurre en Francia, por ejemplo.

Las asociaciones de usuarios de Internet sostienen que si el gobierno quisiera aplicar esta ley debería incluso cerrar las páginas de buscadores como Google, ya que allí se encuentran numerosos *links* a páginas en las que se cometen infracciones al derecho de autor. [75][76] Constitucionalistas consideran que se ha violado un principio importante. Una disputa en torno a una violación de un derecho de autor se desarrolla siempre entre dos partes, a saber el titular del derecho que ve lesionado ese derecho, y una segunda parte que es imputada de

---

75 http://www.noalcierredewebs.com/.
76 http://www.internautas.org/html/3588.html.

violarlo. Este proyecto de ley convierte a un organismo del gobierno en parte, dice Paloma Llaneza.

Casi nadie en España entiende por qué el gobierno no presenta sencillamente un proyecto de reforma a la ley penal con la que se transformaría en delito también la publicación de "*links*" a páginas desde las que se pueden bajar obras protegidas por el derecho de autor. Presumiblemente, el gobierno de Zapatero teme que la gran cantidad de juicios por posibles violaciones a los derechos de autor se prolongarían demasiado en el tiempo, habida cuenta de que la justicia española está totalmente desbordada. De ser así, las medidas a tomarse no tendrían un efecto disuasivo, sospecha el gobierno.

El constitucionalista Lucrecio Rebollo de la Universidad Uned se lamenta de que surja la impresión de que temas como el derecho de autor le resultan al gobierno sencillamente incómodos y quiera sacárselos de encima. En España, los derechos de autor, las asociaciones de titulares de derechos y las medidas destinadas a garantizar sus intereses, así como un impuesto a los soportes de la información o un arancel por la reproducción en el espacio público, son extremadamente impopulares y las asociaciones de usuarios de Internet intervienen en forma permanente en el debate acerca de los derechos de autor en la red.

Se espera que el Parlamento trate todavía este año el proyecto de ley enviado por el Ministerio de Cultura. Debido a que no existen mayorías claras en ambas Cámaras no se puede predecir en qué términos finalmente se aprobará la norma. El Partido Popular incluso quiere devolverlo al gobierno y pedir su total reelaboración.

POLONIA

LAS DISCUSIONES EN TORNO A INTERNET Y SU INFLUENCIA SOBRE EL DEBATE POLÍTICO*

ANETA ZWOLIŃSKA | DR. BOHDAN WYŻNIKIEWICZ

Internet fue desde sus comienzos un medio de fuerte presencia y creciente importancia en la vida pública de Polonia.

Las encuestas realizadas por la Oficina Principal de Estadísticas de Polonia (GUS, por sus siglas en polaco) revelan que el 95% de las empresas en el año 2008 tenían computadoras y que casi el 59% de los hogares contaban con al menos una computadora comparada con el promedio del 68% de la UE. Según Eurostat, el 51% de los hogares en Polonia tenía en 2009 una conexión de banda ancha (en 2008 fue el 38%). El promedio de la UE fue del 56% en 2009 y del 49% en 2008. Estas cifran indican que existe la clara necesidad de impulsar fuertemente el desarrollo de Internet si Polonia desea ponerse a la par de otros Estados miembros de la UE.

Al igual que en otras sociedades democráticas, el desarrollo de Internet y su creciente importancia se generan en forma espontánea. Frecuentemente, las medidas oficiales son la reacción ante hechos consumados y las regulaciones que se establecen suelen ser posteriores a los acontecimientos. A modo de ejemplo valga citar el impuesto a las transacciones financieras hechas por Internet (Transfer), o también el interés de las autoridades tributarias por la facturación obtenidos a través del *shopping online*, entre otras actividades comerciales. Otro ejemplo es la introducción de normas legales que califican de delito la seducción de menores en Internet.

La irrupción de Internet generó también una serie de debates como consecuencia de los nuevos fenómenos en la red. Las regulaciones legales referidas a Internet y a su influencia sobre el derecho, se ven rápidamente superadas por los permanentes cambios en la red. Lentamente el Estado toma

---

***** Traducción al alemán: Iwona Łatwińska

nota de que ciertas cuestiones relevantes en Internet no son susceptibles de ser reguladas legalmente y que es necesario aceptar ese hecho.

Hasta ahora, los políticos vienen manteniendo cierta distancia respecto de Internet, a pesar de que se visualizan dos formas básicas de comunicación por vía de este medio. La primera se refiere a los debates de destacados dirigentes políticos en chats de Internet, sobre todo durante las campañas electorales. En segundo lugar cabe mencionar los *blogs* de los políticos utilizados fundamentalmente para formular tesis y comentarios controvertidos que rápidamente son recogidos y difundidos por otros medios.

Los mensajes de los políticos de la oposición suelen tener más llegada a la opinión pública que aquellos del partido oficialista. Muy popular se ha vuelto la participación regular en los *blogs* administrados por miembros de la Sejm, el parlamento polaco. Además, muchos observadores consideran que este tipo de acciones contribuye a ganar adeptos políticos. La mayor popularidad goza por lejos el *blog* de un político ultraliberal que hace tiempo viene haciendo política por fuera del parlamento.

El funcionamiento mismo de Internet genera discusiones cada vez que se teme que los cambios o soluciones jurídicas propuestas podrían poner en peligro los intereses de los usuarios en sentido más amplio.

En diciembre de 2008 el gobierno anunció la "Estrategia del desarrollo hacia una Sociedad de la Información en Polonia hasta 2013", conocida como "Estrategia de la Informatización". Dicha estrategia tiene por finalidad "posibilitar a la sociedad un uso general y efectivo del conocimiento y de las informaciones para un desarrollo social, económico y personal en armonía". Según esta estrategia se proyecta la implementación de medidas orientadas a la persona (desarrollo de los recursos intelectuales y sociales), la empresa (mayor efectividad, innovación y competitividad) y la administración pública (incremento de la eficacia y del acceso online a servicios de la administración pública).

Previo a la elaboración de esta estrategia se celebraron múltiples consultas con diferentes sectores sociales, instituciones públicas y privadas, institutos de investigación académica y científica así como organizaciones no gubernamentales. La estrategia busca cumplir también con las prioridades fijadas por la política europea que enuncia el Comunicado de la Comisión Europea "i2010 - Una sociedad de la información europea para el crecimiento y el empleo".

ALMACENAMIENTO DE DATOS

Por ahora, el almacenamiento de datos no es materia de debate público en Polonia. Las cuestiones relacionadas con el almacenamiento se consideran parte del ámbito jurídico de la protección de los datos personales y la opinión pública no muestra mayor interés por este tópico. Sólo ocasionalmente se discute en el parlamento cuánto tiempo pueden conservar la justicia y los servicios secretos datos personales sensibles y cuáles son las informaciones que pueden almacenarse. En general se establece un plazo de cinco años para la conservación de los datos.

PROTECCIÓN DE DATOS PERSONALES, SEGURIDAD DE DATOS E INSTITUCIONES COMPETENTES

El progreso económico y el desarrollo de nuevas tecnologías –sobre todo en el sector de las IT– constituyen una creciente amenaza para la privacidad de las personas y la protección de sus datos personales. La enorme cantidad de datos almacenados por diferentes instituciones públicas y privadas hizo prácticamente imposible cualquier control por parte de un individuo sobre la circulación y el contenido de informaciones que lo afectan personalmente. Se comprendió, entonces, la necesidad de que el Estado intervenga para garantizar esta parte de la privacidad.

La Constitución de la República de Polonia del año 1997 incorporó al derecho polaco el principio de la protección de datos personales. El Art. 51 de la Constitución dice: "Sólo existe la obligación de brindar informaciones acerca de la propia persona sobre la base de una ley. Toda persona tiene el derecho a acceder a los documentos oficiales y recopilaciones de datos que lo afecten. Sólo la ley puede limitar este derecho". Y agrega la Constitución: "Toda persona tiene derecho a corregir o eliminar informaciones falsas, incompletas u obtenidas de manera ilegal."

También de 1997 data la Ley de Protección de Datos Personales. La ley precisa el derecho garantizado por la Constitución que tienen todos los ciudadanos polacos de decidir a quién, en qué medida y con qué fin le entregarán datos referidos a su persona. Además, la ley regula el procesamiento de datos así como los derechos que se refieren exclusivamente a personas físicas. Sin embargo, las disposiciones de la ley no son de aplicación al procesamiento de informaciones por parte de otros entes como personas jurídicas, organizaciones sin carácter jurídico y personas físicas que desarrollan una actividad económica

sobre la base de las disposiciones de la Ley sobre la Libertad de la Actividad Económica, sancionada en 2004.

En virtud de la ley que establece la protección de datos se creó la figura del Inspector General para la protección de datos referidos a la persona (GIODO, por sus siglas en polaco). Su función es velar por el cumplimiento del derecho que asiste a los ciudadanos de ver protegidos sus datos personales. El Inspector General lleva un registro nacional abierto sobre las recopilaciones de datos personales. Estos datos pueden ser conservados de diferente modo, ya sea en forma de recopilación de datos o de datos individuales cuando son almacenados en sistemas de tecnología informática (por ejemplo, en la red de computación en la oficina). Por recopilación de datos personales se entiende todo conjunto estructurado de datos de carácter personal, accesible según determinados criterios. Un ejemplo de este tipo de recopilación es el legajo con datos personales de los trabajadores, el registro de pacientes de un consultorio médico o el registro de contribuyentes.

La recopilación de datos debe ser comunicada previamente por el administrador al Registro de Recopilación de Datos que funciona en la órbita del Inspector General para la Protección de Datos Personales.

Quedan eximidos de la obligación de registrarse los siguientes casos:

- Administradores de datos que en razón de diferentes normas están alcanzados por el secreto de Estado,
- Datos recopilados como producto de tareas de investigación operativa por parte de representantes de los órganos facultados a tal fin,
- Datos procesados en el marco de procesos judiciales,
- Datos de personas que utilizan servicios médicos y servicios de escribanos y abogados,
- Datos elaborados para la realización de elecciones así como plebiscitos locales y generales.

En Internet se puede acceder al índice de las categorías de información indicadas en el registro a través del sistema e-giodo. Este sistema permite la búsqueda de conjuntos de datos en virtud de numerosos criterios como el nombre del conjunto, del administrador o de su sede. El registro contiene informaciones que son comunicadas por los administradores de datos durante el trámite de registro. No brinda informaciones sobre personas concretas.

El temor de convertirse en víctimas de la delincuencia cibernética es uno de los impedimentos para un mayor uso de las tecnologías de la información y las

comunicaciones (TIC), según surge del informe del GIODO. Estos temores están plenamente justificados. El caso ocurrido en 2004 de un analista de sistemas de 23 años que robó de la empresa de su empleador los datos personales de un millón de polacos e intentó vender estos datos por medio millón de euros a agencias de publicidad, es apenas uno de muchos ejemplos.

Un estudio realizado por la empresa Symantec sobre delitos como *phishing* o *pharming* revela que en el último tiempo han aumentado en Polonia las operaciones bancarias y el uso de servicios *online*. El mayor riesgo que enfrentan estas operaciones son los ataques de *hackers*.

En Polonia existen organizaciones comerciales que buscan luchar contra las infracciones a la seguridad en Internet. La más importante es CERT Polska (Computer Emergency Response Team). Actúa en las estructuras del principal operador de Internet de Polonia e incluso es financiada por éste. CERT Polska desarrolla sus actividades desde 1996 y desde 1997 es miembro de FIRST (*Forum of Incidents Response and Security Teams*). En el marco de este foro trabaja con otras organizaciones asimilables en todo el mundo. Entre las principales tareas de CERT cabe destacar:

- Registro y procesamiento de casos que afectan la seguridad en Internet,
- Advertencia a usuarios de Internet sobre la aparición de amenazas inminentes,
- Ejecución de medidas que lleven a una mayor concientización pública acerca de la seguridad de las TIC,
- Desarrollo de estudios y elaboración de informes sobre la seguridad de los recursos de Internet polacos,
- Realización de tests independientes de productos y soluciones del área de la seguridad de las TIC.

Las actividades de CERT Polska demuestran que una entidad comercial que desarrolla sus actividades en el mercado digital puede impulsar al mismo tiempo medidas que benefician tanto a la compañía como a la sociedad.

ACCESO A INFORMACIONES PÚBLICAS

Son informaciones públicas aquéllas que han sido elaboradas por una administración pública o que se refieren a ésta o a otro ente público, siempre que éstos cumplan funciones públicas y sirvan al patrimonio comunal o nacional.

El Art. 61 de la Constitución polaca garantiza el derecho a obtener información sobre las medidas adoptadas por órganos públicos. El acceso a esta información está regulado por la Ley sobre Acceso a Informaciones Públicas de 2001.

Según esta ley, el derecho a acceder a la información pública abarca:

- La obtención de informaciones públicas, entre ellas las informaciones procesadas de modo tal que sean de especial importancia para el interés público,
- Vista de documentos oficiales,
- Acceso a las sesiones de los órganos colegiados de la administración pública surgidos de elecciones generales.

La disposición precedente implica una limitación sustancial a la implementación del derecho a información, ya que el Art. 61 de la Constitución polaca habla de acceso a documentos. El derecho de acceder a un documento incluye el derecho a obtener una copia de este documento con lo que se tiene acceso permanente al documento y la posibilidad de procesar y publicar las informaciones obtenidas (Art. 54 de la Constitución). Por el contrario, el acceso a la información pública no comprende el derecho a acceder por esta vía a las fuentes de la información.

Todo ciudadano polaco tiene el derecho constitucionalmente garantizado de acceder a la información pública. La ley correspondiente amplía este derecho a los extranjeros. En general, para dar cumplimiento a la ley, las informaciones se publican en documentos oficiales como el Boletín de la Información Pública (BIP por sus siglas en polaco). El BIP es un sistema único de páginas de Internet creado para facilitar informaciones públicas de manera general y gratuita. Están obligados a informar a través de las páginas del BIP los órganos de la administración pública, la gestión territorial y la gestión económica, así como sindicatos, partidos políticos y otras instituciones y entes estatales que cumplen funciones públicas.

El acceso a las informaciones públicas comprende también el derecho a acceder a las sesiones de la administración pública y a los materiales que documentan estas sesiones (material audiovisual, TIC, etc.). Sin embargo, tener acceso a las sesiones de los órganos públicos no implica el derecho a participar en las mismas. Los ciudadanos pueden observar el desarrollo de las sesiones y sus participantes, pero no tienen derecho a voz o voto.

En general, el acceso a la información pública es gratuito y un ciudadano interesado en las informaciones no necesita demostrar que posee un interés legal en obtenerlas.

Una información pública no publicada en el Boletín de la Información Pública debe ser facilitada a pedido de un interesado. Los empleados de los organismos públicos que tienen la obligación de facilitar información pública pueden ser sancionados con multas pecuniarias, limitación de la libertad o privación de libertad de hasta máximo un año, en caso de negarse a brindar esta información.

BLOQUEO DE PÁGINAS EN INTERNET

En la legislación actual no existen disposiciones que permitan bloquear determinadas páginas de Internet. En noviembre de 2009, el Ministerio de Finanzas anunció la creación de un "registro de páginas web y servicios ilegales". La base legal para este registro debía ser la incorporación de un artículo a la ley sobre el derecho de las telecomunicaciones con la finalidad de dificultar el acceso vía Internet a páginas web con las siguientes características:

- Páginas con contenidos que difunden la ideología fascista u otra de carácter totalitario, o bien un régimen fascista u otro de carácter totalitario,
- Páginas con imágenes pornográficas de menores de quince años, pornografía con actos de violencia o presencia de animales, pornografía con fotos hechas o procesadas que representen a menores,
- Contenidos descritos de modo tal que impliquen un engaño cometido con alevosía con la finalidad de obtener ventajas patrimoniales, por ejemplo mediante información obtenida por la fuerza, que pueda servir para la ejecución de operaciones financieras sin consentimiento del titular de los activos,
- Contenidos que constituyan una forma de publicidad prohibida o brinden informaciones no autorizadas sobre el patrocinio en el sentido de la ley de juegos de azar, o servicios que ofrezcan realizar juegos de azar prohibidos.

El proyecto preveía que el registro de las páginas web y los servicios ilegales fuera llevado en forma abierta por el Presidente de la Oficina de Comunicación Electrónica, un órgano en la órbita del sector de correos, telecomunicaciones y frecuencias.

En enero de 2010 se elaboró una nueva versión del proyecto que fue publicada en la página web del Ministro de Finanzas. Según esta nueva versión, el tribunal distrital de Varsovia decidirá sobre la incorporación al registro por medio de una resolución adoptada a solicitud de la policía, la Agencia de Seguridad Interior, el órgano de control fiscal o la autoridad aduanera. El pedido se puede

formular una vez que otros recursos demostraron ser insuficientes o cuando es „altamente probable que sean ineficaces o inútiles". En el proyecto ya no se habla de un bloqueo a páginas de Internet que promuevan regímenes fascistas o totalitarios. También quedaron excluidas disposiciones que se refieren al bloqueo de contenidos "cuya presentación admite el engaño con alevosía a fin de obtener ventajas materiales". El bloqueo de páginas web no permitidas en virtud de un fallo judicial sin duda es menos controvertido que un bloqueo sin intervención de la justicia. Por otra parte, el proyecto prevé que los operadores comuniquen a los usuarios de Internet el bloqueo de la página. En esa comunicación deberán mencionarse las razones jurídicas y el órgano competente que lleva el registro de las páginas web y de los servicios no permitidos. Sin embargo, esto no cambia en nada el hecho de que la posibilidad del cierre de muchas páginas genere controversias entre los operadores de telecomunicaciones, ya que los bloqueos también generan elevados costos.

El proyecto mencionado generó un acalorado y controvertido debate. Representantes de diferentes sectores, entre ellos titulares de portales de Internet, políticos, periodistas, empresarios y docentes plantearon serias objeciones al proyecto presentando. En particular se argumentó la inconstitucionalidad de la norma, ya que la Constitución garantiza la libertad de opinión y la libertad para preservar y difundir informaciones. Además, el Art. 54 de la Constitución establece que queda prohibida la censura previa de medios masivos y el otorgamiento de concesiones de prensa. Los autores subrayaron que el actual sistema jurídico prevé la posibilidad de perseguir autores de páginas web con pornografía infantil, propaganda nazi o que prediquen el racismo o el odio religioso, etc. Por lo tanto no sería necesario confeccionar un nuevo registro.

Se estima que la creación del registro costará un millón de euros. Sin embargo, se duda de su eficacia. Más de 80.000 personas firmaron una carta de protesta contra el registro. Opinan que este tipo de disposiciones podría afectar la libertad de opinión en la red. La presión ejercida por los usuarios de Internet motivó un encuentro con el Primer Ministro Donald Tusk. El debate tuvo lugar con la participación de usuarios de Internet y representantes de organizaciones no gubernamentales en la Oficina del Primer Ministro con transmisión simultánea en vivo por algunas redes de acceso general. Luego del encuentro, que duró más de tres horas, el gobierno retiró las disposiciones sobre la censura en Internet del proyecto de ley. No obstante, la iniciativa no está archivada y podría ser retomada en un futuro próximo.

También los proveedores comerciales bloquean ocasionalmente las páginas de sus clientes cuando constatan páginas con contenidos dañinos o cuando existe una amenaza sustancial. Desde la perspectiva de los proveedores, estas medidas tienen carácter preventivo para preservar su buen nombre. Sin embargo, ha ocurrido también que las páginas bloqueadas por los proveedores polacos fueron transferidas a servidores de operadores extranjeros. Esto derivó en la cooperación de la policía polaca con la policía del Estado afectado que incluye la búsqueda en territorio polaco de personas que han actuado fuera de la ley.

PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

La legislación actualmente vigente en Polonia garantiza la protección de la propiedad intelectual en dos campos esenciales: el derecho de autor consagrado en la Ley sobre Derechos de Autor y Derechos Conexos de 1994, y la protección de las patentes y derechos conexos como marcas, denominaciones geográficas y diseños industriales.

A fin de garantizar la protección de productos de propiedad industrial, se creó en 1918 la Oficina de Patentes de la República de Polonia con sede en Varsovia. La patente registrada allí cuenta con veinte años de protección a partir del año en el que ingresa la solicitud. La protección de modelos de utilidad rige diez años y para diseños industriales la vigencia es de 25 años. Es obligatorio el pago de aranceles periódicos para la protección de invenciones y modelos de utilidad. El arancel básico para la solicitud de una patente sobre una invención o un modelo de utilidad asciende en la actualidad a unos €120.

La protección de los derechos de autor surge automáticamente a partir de la creación de la obra y no requiere registro ni certificación. Abarca tanto a los derechos de autor materiales como inmateriales. Los derechos materiales pueden ser transferidos a otras personas por vía de herencia o celebración del contrato correspondiente (por ejemplo, contrato de transferencia de los derechos materiales).

Los casos más frecuentes de infracción a los derechos de autor son:

- registro (en la página web propia) de un texto ajeno que es firmado con el propio nombre y apellido,
- copia y uso comercial de obras,
- adquisición de los derechos de autor o de una licencia de una persona no autorizada a vender o a conceder una licencia,
- apropiación de un manuscrito o un *applet* ajeno.

La consecuencia legal de una violación a los derechos de autor y su uso no autorizado es una pena privativa de libertad y la responsabilidad penal de quien ha vulnerado el derecho.

El autor cuyas derechos se vieron avasallados puede recurrir a un tribunal civil y reclamar, entre otras cosas, indemnización por daños y perjuicios, omisión de las actividades que lesionan sus intereses y la publicación de un comunicado de prensa o un edicto público en el que se transcribe la decisión del tribunal en forma parcial o total.

Por otro lado se trata de una responsabilidad penal; en este caso se asume un tipo criminal. Este tipo de responsabilidad está previsto para el caso de un uso ilegal de materiales de terceros. Quien lesione un derecho puede ser sancionado con una pena pecuniaria o prisión de hasta 5 años.

Los derechos de propiedad intelectual también se impusieron gradualmente en la práctica. En ese sentido contribuyeron algunos juicios penales contra personas o instituciones que infringieron este derecho con notorio impacto aleccionador.

Además, en el caso de las marcas se puede recurrir a la protección en forma de marcas comunitarias (el registro se hace en la Oficina de Armonización para el Mercado Doméstico en Alicante, España) o también se puede solicitar la protección internacional de la marca (en este caso el registro se hace ante la Oficina de la Organización Mundial de la Propiedad Industrial - OMPI en Ginebra).

PROGRAMAS PARA GARANTIZAR LA DIFUSIÓN DE LA BANDA ANCHA EN TODO EL TERRITORIO NACIONAL

El gobierno polaco proyecta garantizar el abastecimiento de todo el territorio nacional con servicios de banda ancha para 2015. A la luz de los progresos alcanzados en los últimos dos a tres años el proyecto parecería ser realista. No obstante, debe considerarse la posibilidad de que el cumplimiento de la meta proyectada pueda situarse ligeramente por debajo del 100%.

Para 2012, el programa oficial "Polonia Digital" debe promover la difusión del acceso a Internet banda ancha en tres aspectos: por un lado se trata de elaborar mecanismos para incentivar las inversiones en la infraestructura de las telecomunicaciones. En segundo lugar se proyecta eliminar los obstáculos legales, administrativos y técnicos. La tercera medida sería la creación de condiciones que faciliten el uso de recursos de la UE destinados a tal efecto.

Como consecuencia de las actividades que viene desarrollando hace algunos años la Oficina de Comunicación Electrónica, los precios para servicios de Internet y telecomunicaciones han comenzado a descender. Además, se fueron desarrollando saludables mecanismos de competencia. Ambas cosas lograron reducir en los últimos años notablemente las barreras económicas que también dificultaban el desarrollo de Internet en Polonia.

Un paso sustancial en la implementación del programa de gobierno fue la sanción de la llamada Megaley sobre Apoyo al Desarrollo de Servicios de Redes de Telecomunicaciones aprobada en mayo de 2010. Esta ley fue recibida positivamente por expertos y operadores de Internet. Una de las ventajas fundamentales de la ley es la creación de condiciones institucionales y legales para inversiones en la conexión a Internet de las administraciones municipales y de los servicios públicos básicos. Otras disposiciones esenciales se refieren al acceso a la infraestructura de telecomunicaciones que se financia con fondos públicos. La realidad jurídica creada a partir de las medidas adoptadas permite la ampliación de las conexiones de banda ancha con aporte de recursos financieros de la UE.

La puesta en práctica del programa oficial se coordina en el marco de un grupo informal: el llamado Foro Nacional de Banda Ancha. Se trata de una plataforma de cooperación de todos quienes intervienen en la creación de una infraestructura de banda ancha de las telecomunicaciones en Polonia. Participan el gobierno, los órganos de gestión municipal, los operadores de las telecomunicaciones, instituciones financieras, organizaciones no gubernamentales y organismos de regulación del mercado. El foro cuenta con el soporte de un portal de Internet para la comunicación, transmisión de conocimiento e intercambio de experiencias entre los participantes de la iniciativa.

Sin embargo, el programa de gobierno también toma en consideración la competencia tecnológica global que lleva a parámetros técnicos más elevados para la banda ancha y que demanda inversiones permanentes en la infraestructura de las telecomunicaciones.

PARTICIPACIÓN DE LAS ASOCIACIONES DE LA SOCIEDAD CIVIL

Muchas de las medidas administrativas destinadas a promover una sociedad de la información han sido cuestionadas por los medios y la opinión pública por su escasa eficacia. Especialmente activa se muestra la comunidad de los usuarios de Internet que lleva adelante una gestión muy eficiente y que hace un uso eficaz de las redes sociales más populares. Existen numerosas organizaciones

como la Internet Society Poland o la Fundación para el desarrollo de la Sociedad de la Información (*Fundacja Rozwoju Społeczeństwa Informacyjnego*). El objetivo de estas organizaciones es promover el desarrollo de Internet y preparar a las personas para una vida en una sociedad de la información global. Estas organizaciones cooperan a gran escala con sus equivalentes internacionales.

Cabe mencionar algunas de las acciones llevadas a cabo por usuarios de Internet que buscan incrementar la presencia de las redes digitales en la vida social y económica. Estas acciones estaban referidas a los siguientes trámites públicos:

- Posibilidad de presentar la declaración impositiva por Internet, cosa que efectivamente se logró,
- Reconocimiento de las facturas que se envían mediante Internet y no sólo por correo por parte de las autoridades fiscales, una acción que también prosperó
- Celebración de elecciones generales *online*, una acción que hasta ahora no se ha puesto en práctica.

La mayor difusión de Internet en la vida social y económica es más el producto de la presión de los usuarios de Internet que de las medidas de carácter oficial. Especial importancia reviste la eficiencia de las actividades de actores de la sociedad civil a la hora de movilizar a la administración pública con el fin de imponer medidas socialmente beneficiosas. Durante la conferencia "Ciudades en Internet", celebrada en junio de 2010 y organizada por una alianza entre la Organización de la Gestión Territorial Autárquica y doce organizaciones no gubernamentales, se difundió una "Declaración sobre los cambios necesarios en la gestión de desarrollo de la sociedad de la información en Polonia". Uno de los temas tratados fue el programa de los llamados "analfabetos digitales" (cerca de 13 millones de polacos adultos). En su documento, los autores de la declaración convocaron a las autoridades a adoptar medidas más dinámicas para limitar el analfabetismo digital. Otro tema abordado en el documento es la brecha entre las competencias digitales de la mayoría de los alumnos de las escuelas primarias y medias, y el programa educativo tradicional que aplican las escuelas. Advierten los autores que deberá prestarse más atención a esta brecha.

INDIA

INTERNET EN INDIA – UN ESTUDIO DE CASO*

RAJAT KATHURIA | MAHESH UPPAL

I. INTRODUCCIÓN

El poder de Internet para contribuir a difundir el conocimiento, integrar los mercados y contribuir a acrecentar el compromiso de los ciudadanos con su comunidad y la sociedad en general, es ampliamente reconocido en India. Se sobreentiende también que el uso de Internet depende de su disponibilidad. Es evidente que lo primero no es factible sin lo segundo. No obstante, el uso de cualquier tecnología depende del ecosistema en su conjunto, incluido el marco jurídico que se desarrolla en torno a la tecnología en el contexto local. La demanda en la República de Corea, por ejemplo, fue impulsada inicialmente por la introducción de la banda ancha para operaciones bursátiles en línea, servicios educativos y juegos. Más tarde, el foco se trasladó a los servicios interactivos como compras *online*, correo electrónico y participación en comunidades cibernéticas. Actualmente, el énfasis está puesto en bajar música, juegos y gobierno electrónico. Otros factores importantes en Corea para la introducción de la banda ancha a gran escala fueron el gobierno electrónico, el comercio electrónico y el *e-learning*. En Estados Unidos, Internet se considera un servicio público como el agua y la electricidad, que se presta a toda la sociedad. El gobierno británico lanzó en 2009 el programa *Digital Britain* en vista de las posibilidades que ofrece la banda ancha para apuntalar la recuperación del país de una fuerte recesión económica. Por otra parte, algunos trabajos de investigación subrayan la influencia niveladora de Internet y sus posibilidades para una mayor democratización, en tanto que otros más bien hacen hincapié en la influencia del contexto local.

---

* Traducción al alemán: Sandra H. Lustig

El presente trabajo analiza la evolución del ecosistema Internet indio, con énfasis en el contexto local. En India, Internet está mucho menos difundida que la telefonía móvil de voz, a la que, en forma incesante y altísimo número, se agregan nuevos usuarios a la elevada cantidad ya existente. En contraposición, la difusión de Internet sigue siendo extremadamente baja e India casi no se menciona en trabajos de investigación internacionales.[77] De los 1.400 millones de usuarios de Internet en todo el mundo hacia fines de 2008, la mayor cantidad vivía en China (298 millones) seguida por Estados Unidos (191 millones) y Japón (88 millones). Por el contrario, ha merecido gran atención el éxito de India en la telefonía móvil de voz.[78]

No obstante, existe evidencia suficiente para afirmar que se avecina un cambio importante. En los últimos años, el uso de Internet ha aumentado y la licitación exitosa de servicios de 3G y banda ancha sin cable en abril de 2010 augura un promisorio futuro en cuanto a disponibilidad y uso de Internet en el país. En vista de la escasa ampliación de la infraestructura de redes fijas, el acceso inalámbrico a Internet prevalecerá en un futuro próximo. Por otra parte, la Autoridad Reguladora de Telecomunicaciones de India (*Telecom Regulatory Authority of India,* TRAI) se ha planteado como objetivo acelerar la difusión de Internet, sobre todo mediante una mayor difusión de la banda ancha.[79] El acceso a Internet por ese medio brinda la posibilidad de enfocar las cosas desde otro ángulo, obtener mejores resultados y garantizar el desarrollo social y económico. Adicionalmente existen iniciativas estatales, por ejemplo la proyectada Infraestructura de Información Pública (*Public Information Infrastructure,* PII), así como varias iniciativas en el marco del Plan Nacional de Gobierno Electrónico *(National E-Governance Plan,* NeGP) que prevé instalar

---

77 UNCTAD Information economy 2009: El número de usuarios de Internet en países en desarrollo creció hacia fines de 2008 cinco veces más rápido que en los países industrializados. No obstante, India no forma parte de los países en desarrollo del mundo o del sudeste asiático más dinámicos en términos de crecimiento de Internet.

78 ICT Development Index report 2009 de ITU: India mantuvo su lugar en el ranking y se ubicó en 2007 en el puesto 118 en comparación con el puesto número 117 en 2002. El país muestra una ligera mejora en el subíndice "Acceso" (la difusión de los teléfonos móviles ha crecido fuertemente, entre otras cosas), pero el ancho de banda por usuario de Internet sigue siendo limitado, además de que las tasas de crecimiento de PCs e Internet en los hogares siguen siendo bajas. Asimismo, India se ubica en el puesto número cinco de diez economías con la subcanasta "Telefonía Móvil" más económica, detrás de Dinamarca, Hong-Kong, Bangladesh y Macao.

79 La TRAI difundió en junio de 2010 un documento debate para desarrollar el Plan Nacional de Banda Ancha (*National Broadband Plan*) cuyo propósito es instalar la discusión sobre diferentes aspectos que constituyen desafíos para el crecimiento de la banda ancha en India y que van desde la definición del término banda ancha hasta la infraestructura y diversas cuestiones regulatorias.

quioscos de Internet a nivel local y distrital, además de aprobar una legislación moderna con el objeto de modificar la actual situación de Internet de manera permanente.

Cuando a mediados de la década de 1990 comenzó el *boom* de Internet, muchos pensaron que el medio electrónico mejoraría la transparencia de los precios, dejaría afuera a los intermediarios y haría más eficientes los mercados. Existe en India una evidencia rica en anécdotas y también científica que avala esta tesis. Por otro lado, existen procos trabajos de investigación en las áreas de seguridad, privacidad y protección en Internet. La presente contribución no puede cerrar esta brecha, pero intenta describir los principales aspectos del ecosistema Internet en India. El resto del trabajo ofrece la siguiente estructura: la Sección II brinda un breve resumen del marco institucional en el que se inserta Internet y el crecimiento de las prestaciones de este medio electrónico desde su liberalización hacia finales de la década de 1990. La Sección III analiza la importancia de los temas de Internet en el debate político, en tanto que en la Sección IV se analizan la forma y el impacto de la conservación de datos en India, incluido el proyecto de Identificación Única (*Unique Identity*, UID) para todos los ciudadanos. En la Sección V se debaten preguntas relativas a la protección y la seguridad de los datos, incluido el acceso público a ciertos tipos de datos. Otro tema de esta sección es el cierre de ciertas páginas de Internet. En la Sección VI se analiza el actual sistema de la propiedad intelectual y en la Sección VII se describen los proyectos destinados a generar una mayor difusión de la banda ancha en India, además de fortalecer el rol de la sociedad civil. En la Sección VIII, finalmente, se presentan las conclusiones.

II. MARCO INSTITUCIONAL PARA EL GOBIERNO DE INTERNET Y CRECIMIENTO DE LOS SERVICIOS EN LA RED

Las autoridades que constituyen el núcleo del marco institucional de los servicios de telecomunicaciones son el Departamento de Telecomunicaciones *(Department of Telecommunications*, DoT) y la Autoridad Reguladora de Telecomunicaciones (*Telecom Regulatory Authority of India*,TRAI), conocida en India también como "*the Authority*". La cartera competente es el Ministerio de Comunicaciones e Información (MoC&IT). El Departamento de Telecomunicaciones y la Autoridad Reguladora son los organismos responsables de la política y las medidas de regulación para los proveedores de Internet, respectivamente. El Departamento de

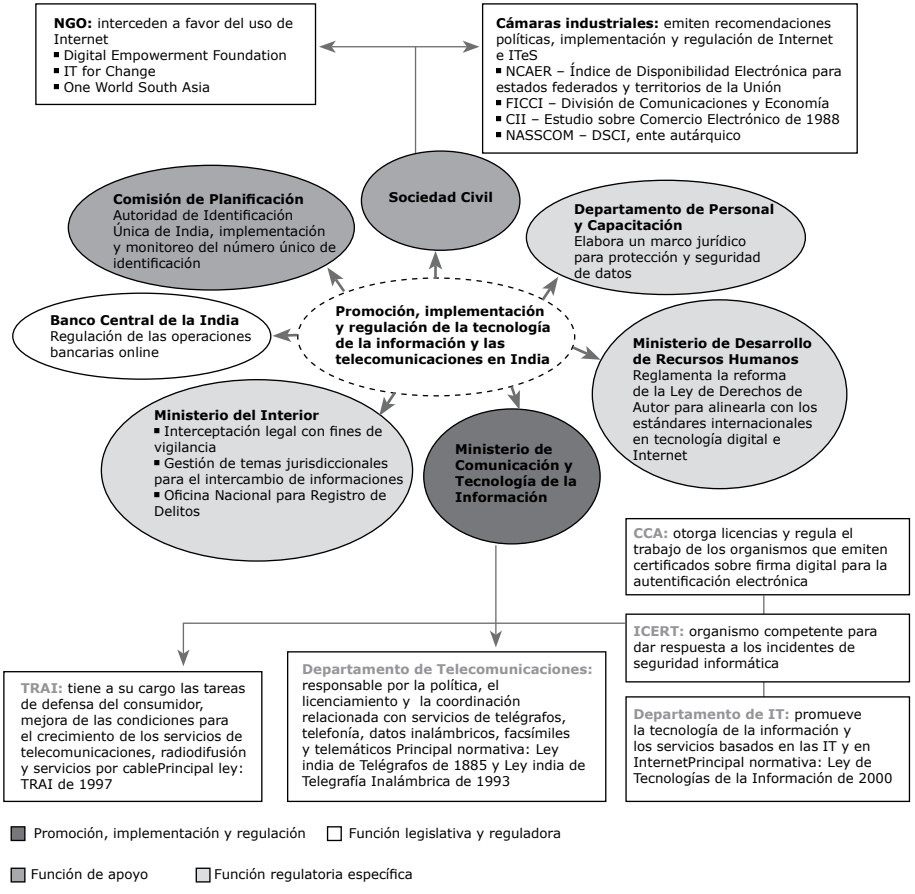
Tecnologías de la Información (DIT) del Ministerio homónimo elaboró la Ley de Tecnologías de la Información (*Information Technology Act, IT Act*), considerada la ley fundamental de la seguridad informática en India. El Ministerio de Desarrollo de Recursos Humanos supervisa las enmiendas a la Ley de derechos de autor (*Copy Right Act*), a fin de armonizarla con las normas internacionales en función de los nuevos desarrollos en Internet y la tecnología digital. El Departamento de Recursos Humanos y Capacitación define actualmente, y por primera vez en India, un marco jurídico para la protección y seguridad de datos. La Comisión de Planificación de la India es responsable por la puesta en práctica del proyecto UID para ciudadanos indios. El Ministerio del Interior, a su vez, administra la Documentación Nacional sobre Delitos (*National Crime Records*). Asimismo, el Banco Central indio regula las transacciones bancarias *online*. Existen, luego, una serie de organizaciones de derecho civil que intervienen en distintos aspectos de Internet. La Asociación Nacional de Compañías de Software y Servicios (*National Association of Software and Service Companies* - NASSCOM) creó una organización de protección de datos independientes, el Consejo de Seguridad de Datos de India *(Data Security Council of India* - DSCI,) con el fin de supervisar la protección de datos del sector de las IT. También buscan influir a través de un trabajo de *lobby* organizaciones no gubernamentales (ONG) como *IT for Change* y la *Digital Empowerment Foundation* (DEF). En la Fig. 1 se representa esquemáticamente el marco institucional y de gobierno en el sector de las IT.

La gran cantidad de organismos públicos intervinientes en la administración de Internet refleja la naturaleza multidimensional de la tarea. Temas tales como seguridad de datos, propiedad intelectual y firma digital son relativamente nuevos y complejos, y están asignados a diferentes organismos públicos. Como resultado de esta situación, algunos elementos del marco jurídico son relativamente nuevos y se encuentran aún en proceso de evolución. Estos aspectos serán abordados en las Secciones correspondientes de este trabajo.

En cuanto a la disponibilidad y el uso de Internet, los logros alcanzados hasta ahora son más bien limitados en razón de múltiples factores. En marzo de 2010 existían en India unos 16.000.000 de usuarios de Internet, un número que es claramente superado por las 584.300.000 de líneas de telefonía móvil existente en ese mismo momento. En ese sentido, Internet podría ser considerada la víctima del éxito de la telefonía móvil, dado que los proveedores se concentraron en el lucrativo negocio de la telefonía de voz. En India existen 104 proveedores de Internet, pero la mayor parte del mercado es dominada por cinco proveedores que, por otra parte, son también proveedores de telefonía

móvil.[80] Dado que el mercado de telefonía móvil muestra signos de saturación, en particular en regiones urbanas, es muy posible que los proveedores comiencen a dedicar más esfuerzos a la expansión de servicios de datos.[81]

Figura 1: Representación esquemática del marco institucional y de gobierno de Internet en India (Fuente: el autor)



80 *National Broadband Plan 2010*: Los diez principales proveedores de servicios de banda ancha proveen el 95% del mercado. De este 95% el 70% recibe los servicios de las estatales BSNL y MTNL. Más del 89% se reparten claramente en cinco proveedores que cuentan con una red nacional propia.

81 Ya han sido asignadas frecuencias 3G y BWA, lo que contribuirá a un mayor uso para la transmisión de datos. Además, las iniciativas gubernamentales, descritas en este trabajo, también llevarán a una expansión de los servicios de transmisión de datos.

Tabla 1: Uso de Internet y estadísticas demográficas

Año	Usuarios	Población	Difusión
1998	1.400.000	1.094.870.677	0,1
1999	2.800.000	1.094.870.677	0,3
2000	5.500.000	1.094.870.677	0,5
2001	7.000.000	1.094.870.677	0,7
2002	16.500.000	1.094.870.677	1,6
2003	22.500.000	1.094.870.677	2,1
2004	39.200.000	1.094.870.677	3,6
2005	50.600.000	1.112.225.812	4,5
2006	40.000.000	1.112.225.812	3,6
2007	42.000.000	1.129.667.528	3,7
2009	81.000.000	1.156.897.766	7,0

Fuente: Internet World Stats.

Actualmente, cerca del 7% de la población india usa Internet, lo que equivale a 81 millones de usuarios. No obstante, las cifras de usuarios se indican como múltiplo de las líneas;[82] las líneas reales están indicadas en la Tabla 2. Además, la difusión de Internet se concentra en las ciudades. Incluso aquellas personas que usan con frecuencia Internet tienen un acceso lento y poco confiable. Existen pocas PCs y laptops y el número de accesos móviles a Internet recién está comenzando a aumentar. Hay escasos 9.000.000 de accesos con una velocidad mínima de 256 kbps, valor orientativo para conexiones de banda ancha.[83] Para acceder a Internet, muchos usuarios dependen de computadoras de uso público en cibercafés o en el lugar de trabajo. Este hecho reduce la flexibilidad, disminuye la demanda y limita el uso de funciones y servicios que son de interés directo. Impide también que las personas investiguen las múltiples posibilidades que ofrece Internet para cambiar su vida. Dado que más mujeres que hombres están atadas a la casa y como el acceso a Internet en las zonas urbanas es más sencillo, el uso de Internet entre la población está distribuida en forma desigual a favor de los hombres residentes en zonas urbanas. En vista de que ni el gobierno y sus organismos, ni las empresas de servicios públicos cuentan por el momento con una presencia *online* importante,

82 Dado que una conexión es usada por muchos usuarios, en algunos años el factor incluso podría llegar a nueve. En promedio, en India se asume un factor seis.

83 TRAI, Definición de banda ancha: una conexión de datos "siempre encendida", capaz de ofrecer soporte a servicios interactivos, incluido el acceso a Internet, y que tiene la capacidad de una velocidad mínima de bajada de 256 Kilobits (kbps) por segundo desde el Point of Presence (POP) del proveedor que ofrece el servicio hasta la conexión particular, con la intención de proveer un servicio de banda ancha donde existe la agregación de múltiples de estas conexiones de banda ancha individuales y el usuario puede obtener acceso a estos servicios interactivos, incluida Internet, a través del punto de acceso.

los ciudadanos no tenían hasta ahora incentivos para invertir en una PC relativamente cara o para abonarse a una conexión a Internet.

Tabla 2: Suscripciones a Internet y banda ancha

Año	Suscripciones de banda ancha (en millones)	Total abonados de Internet (en millones)
Marzo 2010	8,75	16,18
Marzo 2009	6,22	13,54
Marzo 2008	3,87	11,09
Marzo 2007	2,34	9,27
Marzo 2006	1,35	6,94
Marzo 2005	0,18	5,55
Marzo 2004	0,02	4,55
Marzo 2003	0,01	3,6

Fuente: TRAI.

No obstante, existen indicios de que estamos en presencia de un cambio. La Tabla 2 muestra que la cantidad de líneas ha venido aumentando más rápidamente en los últimos años. En forma proporcional creció también el uso. Así por ejemplo, ha crecido el número de indios que usan Internet para comprar pasajes de tren online. La compañía india de *catering* y turismo ferroviario *Indian Railway Catering and Tourism Corporation Limited* (IRCTC), una empresa estatal, aprovechó el potencial de Internet para aumentar las cifras de venta y mejorar la transparencia. La venta de pasajes *online* subió en forma exponencial, pasando de unos 3.300 pasajes en agosto de 2002 a más de 2.400.000 en marzo de 2008.[84] Una ventaja enorme de este tipo de operaciones es que deja afuera a los intermediarios. El éxito del portal de IRCTC ha permitido aprender mucho acerca de la lucha contra la corrupción en la administración pública. El portal, uno de los más exitosos de India en el segmento del comercio electrónico, ha permitido que millones de pasajeros de tren pudieran evitar la corrupción prevaleciente con anterioridad a su introducción. Como los ferrocarriles indios son los más importantes en Asia y transportan a diario unos 20.000.000 de pasajeros, la venta de pasajes *online* ha tenido un efecto transformador.

Asimismo, el acceso a internet se utiliza con creciente frecuencia para establecer la conexión a las redes sociales, buscar empleo y amigos o parejas.[85] Con casi 600 millones de líneas de telefonía móvil y precios a partir de un

84 http://www.egovonline.net/articles-list/48-case-study/7262-helping-e-government-step-into-web-20.html.

85 Ver naukri.co, monster jobs, babajobs.com, bharat matrimony, shaadi.com usw.

centavo por minuto, las tecnologías inalámbricas son la principal posibilidad para tener acceso a muchos servicios de Internet, en particular aquellos en los que la pantalla chica resulta menos problemática, por ejemplo intercambio de información o música. Pese a que existen indicios de que aumenta el uso de Internet en localidades más pequeñas y zonas rurales, el ecosistema en torno a Internet en las regiones rurales sigue en pañales. A las brechas en el abastecimiento se suma la falta de contenidos locales.

En India existen 22 idiomas reconocidos por la Constitución y más de 1.600 dialectos regionales. Del total de la población alfabetizada, el 37% residente en las zonas urbanas domina el inglés, en tanto que en las zonas rurales lo habla el 17%. La población restante (es decir el 63% de las regiones urbanas y el 83% en las zonas rurales) no domina el inglés. Hindi ocupa el tercer y el bengalí el octavo lugar entre los idiomas más hablados, pero entre los diez idiomas más difundidos en Internet no se encuentra ningún idioma indio. Los usuarios en las ciudades más pequeñas se entusiasman empleando aplicaciones y servicios en el idioma local, pese a que en India sólo existen 1.249 páginas de Internet en idiomas locales.[86] Por el contrario, en países como China, Japón y Corea, las aplicaciones y los contenidos están en gran parte adaptados al medio local y el desarrollo en estos países se orienta hacia tecnologías más ambiciosas. De allí que sea imperativo desarrollar contenidos locales si se quiere que aumente el uso de Internet en las zonas subabastecidas.

III. LA IMPORTANCIA DE INTERNET EN EL DEBATE POLÍTICO

Para una sociedad democrática es indispensable contar con una amplia participación de los diferentes sectores de la población en los temas políticos. Los estudios de los países más avanzados industrialmente muestran que Internet fomenta una mayor participación cívica, ya que facilita el acceso a informaciones y noticias e incentiva las acciones colectivas. Además de los ciudadanos de activa participación política, hay ciudadanos políticamente pasivos que admiten que los *blogs* fomentan el intercambio online con otros ciudadanos. Permiten conversar ad hoc sobre temas políticos e intercambiar informaciones.[87] En India, el poder de Internet en la política y el trabajo de

---

86 Investigación de IAMAI e IMRB http://www.iamai.in/PRelease_Detail.aspx?nid=1744&NMonth=12&NYear=2008

87 Net gains in political participation: Secondary effects of Internet on community, Andrea Kavanaugh; B. Joon Kim; Manuel A. Perez-Qui Jones, Joseph Schmitz, Philip Isenhour en: Information, Communication and Society, vol. 11, Nro. 7, octubre de 2008, Routledge

lobby cobró protagonismo cuando el activista social Arvind Kejriwal lanzó una campaña de firmas contra los cambios propuestos a la Ley RTI (ver abajo).[88] Actualmente, las páginas de Internet sólo se utilizan como complementos de las fuentes de información tradicionales en soporte papel, y el uso de Internet en la política recién está en sus comienzos.[89] Todos los grandes partidos políticos y los dirigentes políticos más destacados tienen su propia página web, aun cuando algunas no son especialmente interactivas. Entre los partidos políticos con páginas web propias están el Partido *Bharatiya Janata* (BJP), el Partido Congreso Nacional Indio (INC), el Partido Comunista de India (Marxista) (CPI(M)), el *Samajwadi Party*, el *All India Anna Dravida Munnetra Kazhagam* (AIADMK), el *Shivsena*, el *Bahujan Samaj Party* (BSP), el *Rashtriya Janata Dal* (RJD y el Partido Humanista. Los tres partidos más importantes de India –el INC, el BJP y el CPI (M)– usan sus páginas web para concientizar a la población e informarla acerca de su agenda política, sus antecedentes históricos y su visión para el futuro. Facilitan un amplio arco de informaciones como antecedentes históricos, discursos públicos de los líderes partidarios, programas partidarios y otras publicaciones. El INC, uno de los partidos mayoritarios de la coalición de gobierno, usa sus páginas web también para facilitar informaciones acerca de iniciativas oficiales como la Ley sobre el Derecho a la Información (RTI), la Ley Nacional de Garantía del Empleo Rural (*The National Rural Employment Guarantee Act – NREGA*), el empoderamiento de minorías étnicas y el programa sobre condonación de deudas agropecuarias. Un estudio más reciente llegó, luego de analizar los portales web de los grandes partidos políticos en los últimos años, a la conclusión de que Internet puede ser un eficaz instrumento de comunicación, pero que hoy su uso es relativamente limitado.[90]

Obviamente, la dirigencia política es consciente de la importancia de Internet. En su discurso ante el parlamento en ocasión de asumir el gobierno, la actual presidente Pratibha Patil señaló, entre otras cosas, que el gobierno se ha fijado como meta ampliar la difusión de la banda ancha para conectar a todos los panchayats[91] dentro de los próximos tres años a una red

---

88 http://en.wikipedia.org/wiki/Arvind_Kejriwal#cite_note-8

89 Link analysis of Indian political parties web sites: a temporal comparison. Bhaskar Mukherjee. Assistant Professor, Department of Library & Information Science, Annals of library and Information studies Sept. 2009

90 *Op.cit.*

91 *Gram panchayats* son gobiernos ejercidos por el concejo municipal a nivel de pueblos y pequeñas ciudades. En 2002 había en India unos 265.000 *gram panchayats*. El *gram panchayat* constituye la base del sistema de *panchayat*s. Un *gram panchayat* puede establecerse en pueblos con un mínimo de 300 habitantes. En algunos casos en los que

de banda ancha.[92] Para alcanzar esta meta, el gobierno diseñó la Iniciativa sobre Infraestructura Informática Pública (*Public Information Infrastructure* - PII) con el propósito de unir el acceso a Internet con aplicaciones para el suministro de servicios públicos en una escala que ningún país del mundo hasta ahora siquiera imaginó. Pese a ser un plan muy ambicioso, tiene el potencial necesario para revolucionar de manera duradera las estructuras de información y gobierno en India si se los implementa adecuadamente.[93] Los principales componentes de la infraestructura informática pública son la instalación de cuatro centros de datos nacionales y habilitar paulatinamente conexiones de datos de alta velocidad para los 265.000 panchayats y jurisdicciones municipales que constituyen la columna vertebral de los gobiernos locales. La medida no sólo tendrá un importante impacto sobre el gobierno y el suministro de servicios públicos, sino también sobre la competitividad. Según señala Sam Pitroda, a cargo de la iniciativa PII,[94] su esencia es facilitar un mejor acceso a la información. Del mismo modo que el acceso a las telecomunicaciones es un importante catalizador para concretar una mejor productividad y eficiencia, el acceso a la información encierra el potencial necesario para modificar la forma en que se presentan los servicios públicos, lo que puede dar paso a una distribución más equitativa de las ventajas del crecimiento económico.[95]

El acceso a la información sigue teniendo la capacidad de cambiar la vida de la gente y la política, además de fortalecer la democracia de India. La actual versión de la Ley sobre Derecho a la Información (*Right to Information Act* - RTI) fue sancionada por el Parlamento indio en 2005 y otorga a los ciudadanos indios el derecho a acceder a documentos públicos. La ley permite a todos los ciudadanos de India recabar informaciones de organismos integrantes del

---

la población de los diferentes pueblos no llega a los 300 habitantes, dos o más pueblos contiguos pueden unirse y formar un *gram panchayat* grupal.

92 Alocución de la honorable Presidente de India, Shrimati Pratibha Devisingh Patil, ante el Parlamento, Nueva Delhi, 4 de junio de 2009.

93 Sam Pitroda es el responsable del proyecto. Es asesor del Primer Ministro en temas relacionados con información pública, infraestructura e innovación. Ya ha sometido el proyecto a consideración del Primer Ministro.

94 http://www.iii.gov.in/index.php.

95 En una única plataforma se facilitan datos públicos sobre salud, trabajo, alimentación, precios, población, transporte, nacimientos, fallecimientos, terremotos casamientos. Los usuarios pueden acceder con un clic a informaciones sobre ciudades y pueblos, así como infraestructuras claves como redes eléctricas, minas, diques, ríos y parques nacionales. En forma similar se pueden buscar datos referidos a pensiones, programas de asignación por hijo, justicia electrónica, sistemas de distribución pública, cárceles y policía, catastros y proyectos de beneficencia. A mapas, datos y análisis se tendrá acceso a través de un portal común.

gobierno central, de los gobiernos de los estados federados o de empresas e instituciones bancarias públicas respecto de casi cualquier cuestión relacionada con el trabajo del organismo o de las empresas, y eso en un plazo razonable y a un precio extremadamente bajo. Pese a que la ley no establece que determinados tipos de información, como las referidas a la seguridad, deben ser dados a conocer, su ámbito de vigencia es amplio y está poco regulado. Intentos por parte del gobierno de modificar la ley, una vez aprobada, para restringir su efectividad como instrumento de contralor generaron protestas entre los activistas sociales. En agosto de 2006, el gobierno retiró el proyecto de reforma a la Ley de Derecho a la Información y prometió respetar en cualquier acción futura el procedimiento democrático estipulado.

La ley sobre Derecho a la Información desencadenó muchas discusiones y debates públicos, algo poco habitual entre el común de los ciudadanos indios. Internet contribuyó sustancialmente a esta situación. La ley es ampliamente elogiada como instrumento para disminuir la corrupción en la vida pública, pero también es relevante porque podría mejorar la obligación del Estado de rendir cuentas sobre sus actos. Un gobierno democrático requiere una ciudadanía informada. La falta de transparencia en los actos del Estado tiene como finalidad ocultar la prioridad de intereses particulares sobre el interés público.[96] Al facilitar la participación pública en los actos de gobierno, la ley podría allanar el camino hacia una democracia más participativa. En consecuencia, en las discusiones públicas se plantea cada vez más la importancia de las tecnologías de la información y de Internet. En ocasión de las elecciones parlamentarias de 2009, el partido BJP elaboró por primera vez un manifiesto de las IT. La coalición de gobierno, por su parte, incorporó el rol de Internet a su programa nacional de acuerdo mínimo. Cabe esperar que el ambicioso programa de gobierno electrónico, descrito más arriba, destinado a facilitar la provisión *online* de los servicios públicos, transforme la vida de las personas y la política.

IV. NATURALEZA E IMPACTO DE LA CONSERVACIÓN DE DATOS APLICADA EN INDIA, INCLUIDO EL NÚMERO ÚNICO DE IDENTIFICACIÓN (UID)

El Ministerio del Interior ha creado una Oficina Nacional para Registro de Delitos *(National Crime Record Bureau* - NCRB,) a fin de llevar "un banco de datos a nivel nacional sobre delitos, delincuentes y propiedad

96 http://rti.aidindia.org/content/view/136/107/.

relacionada con la delincuencia".[97] Un ejercicio similar realizan los estados federados. Una de las metas explícitamente enumeradas por la NCRB es, „facilitar la recopilación, conservación, consulta, análisis y transmisión de datos e informaciones, así como fomentar el sistema integrado de datos de comisarías, distritos, oficinas jerárquicas estaduales y otros organismos/ oficinas, incluido el nivel nacional". Los datos almacenados comprenden huellas digitales así como informaciones personales y culturales y fotografías de individuos, entre otros datos. También forman parte documentaciones detalladas sobre propiedad de automóviles, inmuebles, etc. Por ahora, ni la NCRB misma ni su forma de trabajo o su efectividad han sido mayormente objeto de debate público.

Un enorme interés despertó, en cambio, el proyecto de identificación única UID. En enero de 2009, el gobierno de India creó la Autoridad India de Identificación Única *(Unique Identification Authority of India* - UIDAI), una oficina adscripta a la Comisión de Planificación. La misión de la UIDAI es crear "un número único de identificación" (UID) que pueda ser verificado y autentificado *online* y que sea de bajo costo y lo suficientemente robusto como para eliminar identidades mellizas o falsas".[98] El UID está concebido como un número único que almacenará tanto informaciones básicas sobre demografía e identidad de una persona, como así también informaciones biométricas (diez huellas dactilares, escaneo del iris y fotografía). El UID se considera crítico para la creación de una Base Nacional de Datos de Ciudadanos *(National Citizens Database*), un proyecto prioritario del plan de gobernanza electrónica (NeGP) lanzado por el gobierno.

La creación de la NCRB y de la UIDAI son medidas administrativas adoptadas por los organismos competentes. No existe una base legal para ninguna de las dos oficinas. No obstante, está en circulación un proyecto de ley que daría sustento a la creación de la UIDAI; por el momento no ha ingresado al Parlamento. Además, ambas oficinas entran dentro del ámbito de vigencia de la Ley sobre Derecho a la Información (2005).

Hasta ahora hubo pocas declaraciones públicas respecto de la NCRB. Más atención despierta, en cambio la UIDAI. Los medios y otros analistas apoyan mayoritariamente medidas tendientes a conferir una clara identidad a cada ciudadano. Los defensores de la medida argumentan que un número único de identificación ayudará a millones de personas, en particular a los más

---

97 http://ncrb.nic.in/index.htm.
98 http://www.uidai.gov.in/.

humildes que hoy no están condiciones de hacer valer su derecho recibir servicios porque no pueden identificarse. Estos sectores tendrán ahora acceso a muchas prestaciones como alimentos subsidiados por el Estado, asistencia para personas con capacidades diferentes, subsidios para diversas actividades económicas, llamadas de emergencia y muchas otras prestaciones que podrían morigerar las consecuencias de una pobreza salvaje, catástrofes naturales, discapacidades muy difundidas, muertes y destrucción de las bases existenciales.

No obstante, existe también una clara preocupación en algunos sectores de la sociedad civil. El 3 de septiembre de 2010 Jean Dreze y Aruna Roy, destacados miembros del Consejo Asesor Nacional *(National Advisory Council* - NAC), manifestaron serias objeciones al proyecto de introducir un número único de identificación. Sus objeciones se relacionan con el proyecto de unir la asistencia por desempleo en el marco del renombrado Programa Nacional para la garantía de empleo en el espacio rural "Mahatma Gandhi" (*Mahatma Gandhi National Rural Employment Guarantee Scheme* -MGNREGS) con el número único de identificación. En vista de las incertidumbres respecto del marco legal del proyecto UID consideran que sería particularmente peligroso e inapropiado tomar medidas tendientes a establecer esta vinculación ahora.

Muchas organizaciones de la sociedad civil consideran el UID un proyecto de seguridad.[99] Temen que un uso abusivo se constituya en una seria amenaza a la privacidad y las libertades civiles. Argumentan que los organismos de seguridad usarán el UID para observar a individuos con el propósito de impedir legítimos movimientos democráticos y de protesta. Existe el temor de que los datos del UID sean ingresados a la Red Nacional de Inteligencia (Natgrid), propuesta por el Ministro del Interior y con la que se busca prevenir amenazas provenientes de terroristas y otros extremistas. Por el momento existen pocas informaciones oficiales sobre creación, funcionamiento y facultades de esta Red Nacional de Inteligencia y cómo deberá rendir cuenta. Existe la preocupación de que el UID expanda el dominio el Estado sobre la vida del ciudadano y facilite la observación y vigilancia por parte de los organismos de seguridad que no siempre actúan en el marco de la ley.[100] Se ha afirmado que más que el ciudadano normal serán los usuarios del sector privado los que se beneficiarían con el número de identificación único.

---

99 Ver p. ej. la página web http://cis-india.org/events/unique-identity-project.
100 Usha Ramanathan, Economic & Political Weekly, 24 de julio de 2010.

La UIDAI se defiende argumentando que la obtención de un número único de identificación será voluntaria y que sólo se emitirá un documento de identidad. Usuarios de usuarios del sistema como bancos, compañías aéreas, organismos que soliciten informaciones sobre autentificación de la identidad de una persona, únicamente recibirán como respuesta un sí o un no. Se espera que la utilización del UID termine con la dilapidación de fondos públicos y contribuya a darle a los servicios públicos un destino más productivo. El programa UID es el ejemplo más destacado de los esfuerzos por incorporar gran parte de la población de la India al sector formal, pero demandará años hasta que sus efectos se hagan visibles. El primer número de identificación de 12 dígitos, basado en datos biométricos, fue emitido en el estado de Maharashtra, el 29 de septiembre de 2010 y el gobierno tiene previsto emitir hasta 2014 600.000.000 de números de identificación única.

Es probable que el impacto más importante del programa se haga sentir en otra iniciativa del gobierno que apunta a una mayor bancarización de la población. En efecto, los sectores humildes, tanto rurales como urbanos, en India muchas veces se ven impedidos de abrir una cuenta bancaria porque no pueden presentar un documento de identidad. Esto los excluye de las ventajas que ofrece el sistema financiero como el acceso a créditos para microemprendimientos. A pesar de que el número único de identificación es una condición necesaria, es posible que no sea suficiente. Se deberá sumar, además, la voluntad de los bancos de abrir cuentas bancarias para personas que posean un número de identidad. Será necesario, asimismo, abrir una gran cantidad de sucursales bancarias para que las transacciones puedan hacerse. A pesar de que el UID puede ser un instrumento vigoroso para ayudar a los sectores humildes a demostrar su identidad y cumplir con las normas "conoce a tus clientes" *(know your customer* - KYC,) de los bancos, las instituciones financieras indias deberán abrir cerca de 500.000.000 de cuentas bancarias, esto es cinco veces el número actual, si es que se quiere alcanzar un impacto interesante.[101]

V. PROTECCIÓN Y SEGURIDAD DE DATOS. ACCESO PÚBLICO A CIERTO TIPO DE DATOS

La cultura social y laboral en India no parece estar demasiado preocupada por la protección y seguridad de datos. La atención que estos temas reciben parece

101 http://www.livemint.com/2010/09/30214432/UID-programme-will-take-a-few.html?atype=tp

ser mucho mayor en Europa y Estados Unidos que en India. Una investigación realizada por el canal de televisión *Channel 4* en Gran Bretaña reveló en 2006 que en India supuestamente era posible comprar documentación sobre la situación financiera de cientos de miles de británicos. El caso mereció una amplia cobertura en los medios indios y se especuló sobre el tipo de amenaza que podría constituir este tipo de hechos para el próspero sector del *Business Process Outsourcing* (BOP) de India en particular, y de los servicios de las tecnologías de la información (IT) en general.[102] La Ley de Tecnologías de la Información de India (*IT Act*) contempla algunas normas que en mayor o menor grado fueron adaptadas a la Convención del Consejo de Europa sobre delincuencia Informática, pese a que India no adhirió a este tratado internacional. La ley, sancionada en 2000, es el principal instrumento legal de India en seguridad informática. En diciembre de 2008, el Parlamento aprobó una reforma a la ley, conocida como Enmienda a la Ley de Tecnologías de la Información (*IT Amendment Act*) de 2008. Algunas de las reformas introducidas fueron el producto de un diálogo de varios años con diferentes sectores interesados, en tanto que otras (entre ellas algunas de las nuevas medidas antiterroristas) fueron el resultado de los atentados cometidos en Mumbai en noviembre de 2008.

La Ley de 2008 establece: "En caso de que una persona jurídica que posea o procese cualquier tipo de datos o informaciones personales sensibles en un recurso informático que ella posea, controle o opere, sea negligente en la implementación y la preservación de las debidas prácticas y procedimientos de seguridad, y como consecuencia de ello cause a una persona pérdidas o ganancias indebidas, tal persona jurídica es responsable y deberá indemnizar a la persona afectada con una compensación". La ley especifica que "*debidas prácticas y procedimientos de seguridad*" se refiere a prácticas y procedimientos de seguridad destinados a proteger estas informaciones de un acceso no autorizado, daño, uso, modificación, revelación o discapacidad. Pueden estar especificadas en un acuerdo entre las partes o en una ley actualmente vigente o, a falta de semejante acuerdo o semejante ley, las debidas prácticas y procedimientos de seguridad que sean dictadas por el Gobierno Central y que éste considere adecuadas, previa consulta con las federaciones y asociaciones profesionales.

---

102 Ver p.ej. http://ibnlive.in.com/news/thursday-could-spell-doom-for-call-centres-in-india/23165-7.html (último acceso: 6 de septiembre de 2010)

La Ley criminaliza muchas actividades que constituyen delitos centrales de la Convención internacional sobre delincuencia cibernética del Consejo de Europa. El nuevo Art. 66 enuncia entre otras cosas:

- acceso no autorizado a una computadora, un sistema o una red de computación (el Art. 70 de la Ley de 2008 también criminaliza el acceso no autorizado a sistemas informáticos que los gobiernos estimen necesario proteger);
- introducción no autorizada de virus informáticos en una computadora o en un sistema o una red de computación;
- daños no autorizados en una computadora, un sistema o una red de computación, así como datos o software;
- interferencia no autorizada de una computadora, un sistema o una red de computación;
- denegación no autorizada de acceso a una computadora, un sistema o una red de computación; así como
- destrucción o modificación no autorizada de datos en una red de computación.

Estos nuevos delitos pueden ser sancionados con hasta tres años de prisión y/o pena pecuniaria de 500.000 rupias indias (unos 11.000 dólares), siempre que pueda demostrarse que los actos constituyen un "fraude" o fueron cometidos con "deshonestidad". Se argumenta que usuarios nuevos en un país en el que el uso de Internet es nuevo en sí, estos delitos pueden ser cometidos en desconocimiento de las leyes vigentes y que, por lo tanto, los usuarios no deben ser penalizados en forma demasiado severa por su curiosidad. El Departamento de Tecnologías de la Información (DIT) del gobierno indio creó el Equipo Indio de Emergencia Informática *(Indian Computer Emergency Response Team* - CERT-in) como respuesta a eventuales casos de infracción a la seguridad informática. El CERT-in también brinda apoyo a la implementación de medidas proactivas para reducir los riesgos de incidentes informáticos. CERT-in es la oficina central a la que deben ser comunicados los incidentes y administra una base de datos en la que están registrados los incidentes ocurridos en el pasado. La oficina analiza, además, tendencias y patrones de actividades invasivas de las redes informáticas.

La Ley India de Telégrafos (*Indian Telegraph Act)* de 1885 regula la supervisión de las comunicaciones en India y abarca tanto las escuchas telefónicas como la interceptación de correos personales. El Art. 5 permite al gobierno interceptar todo tipo de comunicaciones en cualquier red de telecomunicaciones. No obstante, la Corte Suprema de India constató en una decisión de principios de

1997 que el Art. 21 de la Constitución india, que concede al individuo el derecho a la vida y a la libertad, implícitamente garantiza un derecho a privacidad. En consecuencia, los organismos estatales no tienen derecho a interceptar las comunicaciones sin razón o facultad suficiente. La Corte Suprema ha restringido también cuándo y cómo el gobierno puede recurrir a las escuchas telefónicas: únicamente el Ministro del Interior de la Unión y sus pares de los estados federados pueden ordenar una escucha telefónica y en la orden deben dejar aclarado que la información requerida no puede obtenerse por otros medios. Pese a que los tribunales indios no consideran las llamadas telefónicas interceptadas evidencia primaria, las escuchas telefónicas no son una práctica poco habitual. En ese sentido, Privacy International ha constatado que sigue habiendo una brecha entre el orden establecido por la Ley de Telégrafos y su aplicación efectiva.

Por otra parte, la Ley de Telégrafos de 1885 criminaliza la interceptación ilegal de datos transmitidos por las redes informáticas. El Art. 26 criminaliza la interceptación de mensajes por parte de empleados de la compañía de teléfonos y algunos otros funcionarios. A su vez, el Art. 25 de la ley establece que es un acto punible cuando una persona, con la intención de escuchar el contenido de un mensaje "dañe, retire, manipule o toque" una línea telegráfica o "cualquier otro objeto que sea parte de un telégrafo o está incorporado a un telégrafo o se encuentra en la proximidad de un teléfono o sea utilizado para el funcionamiento de éste".

La responsabilidad corporativa en el sentido de la Ley de Tecnologías de la Información es particularmente grave para los directivos. En efecto, la responsabilidad por infracciones a la ley por parte de empresas es atribuida a los responsables de la compañía a menos que éstos puedan demostrar que la violación fue cometida sin su conocimiento (y que no actuaron con negligencia) o que actuaron con la diligencia debida para prevenir la contravención cometida (y que no hubo consentimiento tácito). Las implicancias prácticas de este artículo generaron revuelo internacional en diciembre de 2004 cuando el entonces director de eBay India (por entonces Baazee) fue detenido y encarcelado durante cuatro días porque en la página web de Baazee aparecía un videoclip objetable.

No sorprende demasiado constatar que la protección de datos y el acceso abierto a informaciones son, a menudo, antagónicos. Con la expansión de Internet también se tomó más conciencia de su poder de interferir con los espacios laborales, personales, sociales y políticos. Existe ahora creciente preocupación sobre la privacidad, la seguridad de los datos y la seguridad

online (especialmente cuando se trata de niños). Del mismo modo existe la preocupación de que sectores extremistas puedan usar redes seguras para llevar adelante actos ilegales, incluida la planificación y ejecución de ataques terroristas. Tal como ya se señalara, la Ley de Tecnologías de la Información fue reformada en 2008 con el fin de fortalecer las disposiciones concernientes a muchas de las preocupaciones actuales. La reforma del Art. 69 permite al gobierno nacional y a los gobiernos de los estados indios y a sus funcionarios autorizados a instruir a cualquier organismo público a interceptar, vigilar o descifrar (u ordenar que se intercepte, vigile o descifre) cualquier información generada, transmitida, recibida o guardada en una computadora. Los organismos pueden solicitar a intermediarios, usuarios o personas responsables de los recursos informáticos a asistirles en estas tareas. No prestar el apoyo solicitado es sancionado con siete años de prisión y una multa por un monto no definido.

La reforma de la ley introdujo también penas más severas para servicios que violan el derecho a la privacidad. El Art. 43 (2) versa sobre el manejo de datos personales sensibles. El Art. 67 (2) aborda el problema de la pornografía infantil y establece penas más severas para estos delitos. Recientemente se suscitó también un debate acerca del acceso *online* a informaciones sobre la situación patrimonial y las fuentes de ingresos de los servidores del Estado. Los candidatos en las elecciones parlamentarias a nivel nacional y estadual están obligados por ley a informar públicamente sobre su situación patrimonial. Considerables controversias generó la afirmación de que la ley no es de aplicación a los jueces por no ser estos "servidores públicos". Es probable que la enorme presión de la opinión pública determinara que varios jueces, entre ellos el presidente de la Corte Suprema, dieran a conocer su patrimonio y sus ingresos.

Además de las normas legales vigentes para la seguridad de datos, y luego de que informes aparecidos en la prensa señalaran que empleados de las exitosas empresas de procesamiento de datos indias entregaran indebidamente a otros usuarios datos personales procesados, el sector aprobó un sistema de autorregulación con el fin de mejorar la seguridad y proteger su imagen. En 2007, la NASSCOM creó el Consejo de Seguridad de Datos de India (DSCI, *Data Security Council of India*), una organización independiente dedicada a la protección de datos, con el propósito de institucionalizar los esfuerzos de sus miembros por cumplir las normas de seguridad de datos vigentes en los muchos países, en los que desarrollan actividades comerciales. El Consejo también asesora a sus miembros en temas de auditoría, formación de capacidades y

benchmarking. Sin embargo, por el momento el Consejo no es todavía una sociedad legalmente constituida.[103]

Una disputa entre el Departamento de Telecomunicaciones de India y la empresa canadiense Research in Motion (RIM), fabricante del *SmartPhone* BlackBerry, sobre el acceso a versiones no codificadas de mensajes tuvo mucha repercusión y plantea en forma elocuente el conflicto entre la protección de datos y la seguridad nacional. En tiempos de amenazas reales a la seguridad nacional, India seguramente no es el único país preocupado por estos temas. El gobierno indio instó a RIM a otorgarle acceso a sus servicios de correo electrónico y messenger codificados, amenazando con prohibir los servicios en India en caso contrario. La preocupación de los usuarios comerciales como generales de BlackBerry es que con esta medida el Estado contaría con la acumulación de informaciones más importante en todo el país, sin que los usuarios tuvieran una remota idea de cómo podría llegar a usar estas informaciones en un futuro. También hay quienes sostienen que una tecnología moderna, inserta en la red, muchas veces utiliza un sistema de codificación que por cada mensaje genera un nuevo código con lo cual sería casi imposible decodificar todo de modo tal de que el Estado lo pueda leer. El Departamento de Telecomunicaciones instó a todos los operadores de la red a reequipar sus redes de modo que pueda interceptar mensajes que son enviadas y recibidas a través de servicios de messenger del BlackBerry de RIM y le fijó a la empresa un plazo hasta octubre de 2010 para ofrecer una solución. En caso contrario, el gobierno emitirá una prohibición. Asimismo, India instó a Google, Skype y RIM a instalar servidores locales en India y permitir a los organismos de seguridad a monitorear el tráfico de datos.

---

103 DSCI es una entidad de bien común con un consejo de vigilancia independiente. Los objetivos declarados del organismo son:

- Ayudar a organizaciones indias de IT/ITeS en sus esfuerzos por cumplir un elevado estándar de seguridad y protección de datos, aplicando "mejores prácticas" [ITeS: *information technology enabled services*, servicios asistidos por tecnologías informáticas];
- Desarrollar, supervisar y aplicar un estándar de seguridad y protección de datos adecuado para el sector indio de las IT/ITeS que sea adecuado, eficiente en cuanto a costos, flexible y asimilable a los estándares globales;
- Crear capacida des para proveer la certificación de seguridad para organizaciones;
- Crear una plataforma común para fomentar el intercambio de conocimientos acerca de la seguridad informática y constituir una comunidad de especialistas y empresas de seguridad;
- Concientizar a profesionales de la industria y a otros sectores interesados sobre temas relacionados con la seguridad y protección de datos.

Tal como se señalara, los operadores de los servicios de telecomunicaciones como telefonía fija o móvil o los proveedores de Internet, son regulados según la Ley de Telégrafos de *1885* que estipula la concesión de licencias. El Art. 5 de la ley concede al Estado el poder superior de interceptar cualquier comunicación. El Art. 69 de la Ley de Tecnologías de la Información de 2008 reafirma esta facultad y obliga a todos los operadores de red a facilitar las interceptaciones aun cuando la correspondiente persona autorizada deba cumplir previamente con el procedimiento estipulado para este tipo de acciones. En algunos casos, el Estado usó esta facultad para bloquear el acceso a determinadas páginas web. El bloqueo de páginas web comenzó en 1996, cuando páginas de telefonía Internet fueron bloqueadas por la empresa VSNL que por entonces ostentaba en India el monopolio de las llamadas internacionales de larga distancia. En 2003, CERT-in desarrolló, bajo la supervisión del Departamento de Tecnologías Informáticas, directrices para el bloqueo de páginas web, confeccionando una lista de organismos facultados para efectuar los bloqueos y definiendo el proceso del bloqueo y las razones legítimas para hacerlo. En la mayoría de los casos que afectan el bloqueo de determinadas páginas, una oficina del Ministerio de Comunicaciones y Tecnologías de la Información escribe una breve nota confidencial al proveedor del servicio de Internet instruyéndolo para bloquear el acceso a la página en cuestión. Los proveedores deben confirmar la recepción de las notas y su cumplimiento.[104]

A título ilustrativo reproducimos de Internet el listado de las páginas web que en 2006 fueron bloqueadas a solicitud del Estado indio.

Tabla 3: Lista de las páginas prohibidas en India actualizada a 2006

www.soniamaino.com/	www.hinduunity.org
mypetjawa.mu.nu	pajamaeditors.blogspot.com
exposingtheleft.blogspot.com	thepiratescove.us
commonfolkcommonsense.blogspot.com	bamapachyderm.com
princesskimberley.blogspot.com	merrimusings.typepad.com
mackers-world.com	www.dalitstan.org
hinduhumanrights.org/hindufocus.html	nndh.com
bloodroyaltriped.com	imagessearchyahoo.com
imamali8.com	rahulyadav.com

Fuente: http://censorship.wikia.com/wiki/List_of_Sites_Banned_in_India.

104 El bloqueo de la página web del grupo separatista *Kynhun* desencadenó una discusión internacional. Hubo varios otros acontecimientos controvertidos en la historia de la gestión de contenidos y del bloqueo de URLs/páginas web.

Más recientemente se procedió a bloquear el acceso a direcciones IP específicas (p. ej. 173.194.36.104) en lugar de nombres de hosts (p. ej. www.google.com). Se ha especulado mucho acerca de las razones por las cuales se bloquean determinadas páginas. En la mayoría de los casos se asume que las páginas publican material antiindio, extremista o de otro tipo de incitación al odio. En algunos casos se cree que las páginas web lesionan los sentimientos indios en la forma de describir la sexualidad. No obstante, las listas parecen ser muy cortas como para enumerar a todas o a la mayoría de las páginas que probablemente difundan material similar. A menudo se señala que en el cierre de las páginas entra a jugar cierta arbitrariedad.

Entre las muchas leyes que fueron dictadas en los últimos años relacionadas con la seguridad de datos e información, la Ley sobre Derecho a la Información (*Right to Information Act*) aprobada en 2005 marca un hito en India. Su objetivo es garantizar a los ciudadanos el "acceso a informaciones que son controladas por los organismos públicos, a fin de promover la transparencia y la rendición de cuentas en el trabajo de todo organismo público". El concepto "información" en la ley se refiere a todo material en cualquier forma, incluidos registros, documentos, notas, correos electrónicos, opiniones, recomendaciones, declaraciones de prensa, circulares, instrucciones, hojas de ruta, contratos, informes, papeles, muestras, modelos y material de datos que exista en toda forma electrónica así como informaciones respecto de cualquier corporación privada a la que un organismo público tiene acceso de conformidad con cualquier otra ley vigente.

El derecho a la información comprende el derecho a:

- inspeccionar trabajos, documentos y registros;
- tomar apuntes o extractos o copias certificadas de documentos o registros;
- tomar pruebas de material certificadas; y
- obtener informaciones en forma de disquetes, *floppy disks*, cintas, videocasetes o cualquier otro modo electrónico o mediante impresiones, si estas informaciones están guardadas en una computadora o en cualquier otro equipo.

La ley satisface la necesidad de permitir a los ciudadanos obtener en forma adecuada informaciones de "organismos públicos". La ley comprende a organismos que en forma directa o indirecta son propiedad del gobierno o son controlados o financiados por éste. En general, los servicios secretos y los organismos de seguridad no están comprendidos por la ley, aunque tampoco

en estos casos la corrupción quede al margen del ámbito de vigencia de la ley. La Ley RTI establece que todos los organismos públicos deben catalogar e indexar adecuadamente todos sus archivos de manera tal de facilitar el derecho a la información en el sentido de la ley. A fin de facilitar el acceso a estos documentos, toda la documentación pertinente debe ser registrada informáticamente y todos los organismos estar conectados en red a nivel nacional. Quien en el sentido de esta ley desee obtener informaciones, deberá formular la solicitud correspondiente en forma escrita o por medio electrónico y pagar el arancel estipulado. Los solicitantes no necesitan indicar la razón por la cual desean obtener la información.

Se hace un uso considerable de la RTI. La Tabla 4 enumera los diez organismos públicos con mayor cantidad de consultas en términos de la RTI, indicando la etapa en la que se encuentran las consultas.

Tabla 4: Datos estadísticos de los diez organismos públicos con mayor cantidad de consultas en el período entre el 1 de enero de 2008 y el 12 de septiembre de 2010

Rango	Organismo público	Consultas en total	En trámite	Concluidos (%)
1	Department of Personnel & Training (Recursos Humanos y Capacitación)	5.581	2.074	3507 (62,84%)
2	Bharat Petroleum Corporation Limited (BPCL)	4.264	237	4027 (94,44%)
3	Ministry of Environment & Forests (Ministerio de Medio Ambiente y Silvicultura)	3.356	1.352	2004 (59,71%)
4	Central Vigilance Commission (Comisión Anticorrupción)	1.991	907	1084 (54,45%)
5	Steel Authority of India Ltd. (SAIL)	1.375	966	409 (29,75 %)
6	CSIR Hqrs., Nueva Delhi	1.156	82	1074 (92,91%)
7	Ministry of Mines (Ministerio de Minería)	921	104	817 (88,71%)
8	NHPC Ltd.	866	26	840 (97,00%)
9	Policía de Dehli	833	518	315 (37,82%)
10	Ministry of Civil Aviation (Ministerio de Aviación Civil)	691	11	680 (98,41%)

Fuente: http://164.100.42.72/rtistatus/RTIMISStatus.aspx

La Tabla 4 muestra que las informaciones recabadas con mayor frecuencia se refieren a empresas de servicios, puestos de trabajo y medios de vida,

prestaciones del Estado, infraestructura, construcciones ilegales, otros temas relevantes para el medio ambiente, así como investigaciones policiales. Las personas que solicitaron informaciones en el marco de la RTI documentaron en forma detallada varios cientos de casos que terminaron exitosamente. [105]

Pero también hubo reveces. Un activista del RTI, el ambientalista Amit Jethwa, fue muerto el 20 de julio de 2010, presumiblemente porque formuló preguntas incómodas sobre la minería en el estado de Gujarat. En enero también fue asesinado Satish Shetty, quien supuestamente había descubierto una serie de fraudes inmobiliarios en Maharashtra. Estas represalias extremas son poco habituales. No obstante, el éxito de los casos denunciados en el marco de la RTI, en algunas ocasiones puede depender del interés que tengan los capitales afectados en que ciertas informaciones sigan siendo confidenciales.[106] Por un lado, la RTI tiene por finalidad fortalecer la gobernabilidad, por el otro funciona también en el marco del actual sistema de gobierno distorsionado. De sumarse nuevos éxitos, es de esperar que sirvan para fortalecer, si no de un día para otro, al menos en forma gradual, la voluntad política de aplicar con más firmeza la RTI, protegiendo a aquellos que podrían verse perjudicados por hacer uso del derecho que les asiste.

VI. EL ACTUAL SISTEMA DE DERECHOS DE PROPIEDAD INTELECTUAL EN INDIA

India fue uno de los primeros defensores de la protección de los derechos intelectuales y también uno de los primeros signatarios tanto de la Convención de Berna como del Convenio TRIPS.[107] Sin embargo, no se encuentra entre los países signatarios del WCT[108] y del WPPT.[109] Las cuestiones referidas a los derechos de la propiedad intelectual están reguladas en la Ley de Derechos de Autor *(Indian Copyright Act*, 1957 (ICA)[110] y la reglamentación correspondiente *(Copyright Rules*)[111]. La ley fue reformada en varias oportunidades (1983, 1984 y 1994) con el objeto de adaptarla a los estándares internacionales. Actualmente (2010), una comisión parlamentaria está analizando un proyecto

---

105 http://www.rtiindia.org/forum/59746-success-stories.html.
106 http://www.thehindu.com/opinion/Readers-Editor/article698823.ece.
107 *Trade-Related aspects of Intellectual Property Rights*, aspectos comerciales de los derechos de propiedad intelectual.
108 Tratado de la OMPI sobre Derecho de Autor (WCT) de 1996.
109 Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT) de 1996.
110 http://www.copyright.gov.in/CprAct.pdf.
111 http://www.copyright.gov.in/CopyrightRules1958.pdf.

de reforma a la Ley de Derechos de Autor elaborada en la órbita del Ministerio de Desarrollo de Recursos Humanos.[112] La Ley de Derechos de Autor busca balancear los intereses legítimos de los titulares de derechos con el interés de los ciudadanos en tener un acceso justo y económico a material protegido. La ley especifica las penas aplicables a actos que infringen el derecho de autor. En determinados casos establece la obligación de licenciar la propiedad intelectual.

La mayoría de los países siguen el modelo de la *Digital Millennium Copyright Act* (DMCA) de Estados Unidos para hacer frente al desafío que implica proteger la propiedad intelectual ante el avance de la digitalización. Internet se convierte cada vez más en una fuente de piratería de datos como se aprecia claramente en el impacto sobre los sellos musicales y las editoriales. La industria cinematográfica de India posee y produce una cantidad considerable de material protegido por la legislación sobre propiedad intelectual como películas, música, etc. En los últimos años, la industria de la biotecnología y de las tecnologías de la información también ha generado una cantidad importante de material protegido. Por lo tanto, estas industrias son sectores fundamentalmente interesados en un régimen de propiedad intelectual que los proteja adecuadamente.

No obstante, en India existe un enorme mercado de copias piratas de música y películas. Los "Special 301 Reports",[113] que anualmente publica la oficina del *United States Trade Representative* (USTR, Representante de Estados Unidos en Cuestiones referidas al Comercio), sitúan a India entre los países que niegan a ciudadanos y empresas una adecuada protección de su propiedad intelectual. Se presume que Estados Unidos ha tratado de influir reiteradas veces para que el gobierno indio implemente un régimen de protección de la propiedad intelectual más estricto. En particular, la industria cinematográfica india solicitó el apoyo del gobierno para proteger sus producciones, muy populares en decenas de países. El sector afirma que estas producciones son publicadas y bajadas a gran escala de manera ilegal, provocando considerables pérdidas de ingresos a sus miembros. La industria cinematográfica india, conocida como Bollywood, produce más películas que Hollywood. Sin embargo, sus ingresos alcanzan apenas el 2% de lo que se gana en Estados Unidos. Un informe de Price Waterhouse Coopers de marzo de 2010 señala que la industria cinematográfica

---

112 copyright.*gov.in/Documents/*CopyrightAmendmentBill2010.pdf.
113 Ver p.ej.: http://www.ustr.gov/sites/default/files/Full%20Version%20of%20the%20 2009%20SPECIAL%20301%20REPORT.pdf.

india perdió cerca de 959.000.000 de dólares en 2008 y unos 571.000 puestos de trabajo por la piratería.[114]

La legislación india sobre propiedad intelectual puede ser calificada de débil. Se asume que las violaciones a los derechos de autor ocurren con tanta frecuencia que no se las pueda perseguir y, en general, se las ignora o tolera. Se argumenta que las diferentes instancias que intervienen en la cadena de creación de valor, por ejemplo los proveedores de Internet, tienen pocos incentivos para invertir en la tecnología y en el tiempo que demandaría bloquear las páginas que vulneran los derechos de autor. No obstante, en los últimos años fueron presentadas varias iniciativas importantes. En 2006, Business Software Alliance y Nasscom trabajaron en conjunto para lograr la persecución de la empresa de *software* Netflix. El acuerdo alcanzado incluye, entre otros puntos, el pago de una indemnización de 30.000 dólares, el retiro de todo *software* que no cuenta con la licencia correspondiente (o copias piratas) y el permiso de efectuar una auditoría de los sistemas informáticos.

En el contexto de un sistema jurídico en evolución, el sistema de Gestión Digital de Derechos (Digital Rights Management - DRM) es considerado el mejor instrumento para la protección de los derechos de autor. Comprende la aplicación de una serie de mecanismos técnicos y legales que permite a los titulares de los derechos controlar el acceso a sus obras, así como establecer los tipos de usos permitidos y la comercialización de sus obras en el mundo digital. En particular integra la identificación y la protección de la propiedad intelectual en formato digital mediante Medidas de Protección Tecnológica (*Technology Protection Measures* - TPM) y Sistemas Informáticos para la Gestión de Derechos *(Rights Management Information Systems* - RMI). Las TPM son sistemas y tecnologías que permiten a los titulares de los derechos controlar el acceso a sus obras y establecer los tipos y condiciones de usos legales así como la comercialización final de sus obras en el mundo digital. Los RMI son mecanismos para identificar las obras digitales que se utilizan para administrar la provisión de material a los clientes. Las reformas propuestas a la Ley de Tecnologías de la Información incluyen la incorporación del Art. 2(xa), que define los RMI, y el Art. 65B, que prevé la protección de estos sistemas. El propuesto Art 65A introduce la protección de medidas tecnológicas. Además, la Ley sobre Tecnologías de la Información de 2000 otorga al Organismo de Control de Entes Emisores de Firmas Electrónicas *(Controller of Certifying Authorities* - CCA) facultad para controlar las firmas digitales, una función

---

114 http://timesofindia.indiatimes.com/india/Piracy-cost-Bollywood-959m-Report/articleshow/5703165.cms#ixzz0zBmdOmw8.

que se hizo necesaria a partir del crecimiento del comercio y del gobierno electrónico.

No obstante, las estimaciones sobre el alcance de la piratería de datos y los perjuicios consiguientes no gozan de un consenso general. Voces críticas aducen que las estimaciones reflejan un desconocimiento de la realidad socioeconómica en India. Sostienen que muchas personas que bajan ilegalmente propiedad intelectual en cualquier caso no comprarían los productos por no estar en condiciones de pagar los altos precios exigidos, por lo que las pérdidas generadas serían simbólicas.[115] Sobre todo los defensores del *software* de código abierto (del inglés *Open Source Software*) sostienen que los derechos de propiedad no sólo no son aplicables sino también innecesarios y que incluso explotan a aquellas personas que pueden pagar los exorbitantes precios a los que se venden las películas, videos o *software* en el mercado legal. Organismos del gobierno indio, entre ellos la Comisión Nacional del Conocimiento (*National Knowledge Commission*), frecuentemente han manifestado su apoyo al *software* libre.

VII. PROPUESTAS PARA MEJORAR LA DIFUSIÓN DE LA BANDA ANCHA

La escasa difusión de la banda ancha preocupa a muchos sectores interesados, entre ellos usuarios, industrias, organismos reguladores y el propio gobierno. Con apenas 9.000.0000 de conexiones, lo que equivale a menos de una conexión por cada cien usuarios, India ha quedado muy por detrás de sus propias modestas metas. Ello tiene evidente implicancia para la gran mayoría de la población, en particular para aquellas personas que dependen del Plan Nacional de Gobierno Electrónico (*India National E-Governance Plan)*.

Afortunadamente existen importantes esfuerzos en el marco del plan citado por ampliar la conectividad. El plan prevé instalar conexiones de banda ancha en todos los panchayats mediante acuerdos entre el sector público y empresas privadas. Los Centros de Servicios Comunes dependientes del NeGP disponen de conexiones de banda ancha y contribuirán a facilitar una serie de servicios públicos *online*. El Estado utiliza una amplia infraestructura para apoyar los servicios en estos Centros de Servicios y espera alcanzar la eficiencia que normalmente se atribuye el sector privado.

---

115 Ver p.ej.: http://www.cis-india.org/advocacy/ipr/blog/consumers-international-ip-watch-list-2009/?searchterm=None.

La autoridad reguladora de las telecomunicaciones TRAI también reconoció la necesidad de acrecentar la difusión de la banda ancha y está en estos momentos finalizando un proceso de consultas para informarse acerca de los métodos más adecuados para acelerar el crecimiento de la banda ancha.[116] Sobre la base de temas planteados en el documento elaborado para efectuar las consultas, es probable que las recomendaciones cubrirán casi todos los aspectos relevantes, incluida la ampliación de la red, una mezcla de redes inalámbricas y fibra óptica, las ventajas de las diferentes tecnologías de banda ancha, equipos terminales, aplicaciones y otras medidas que contribuyen a la viabilidad económica de la banda ancha.

El Fondo para Servicios Universales (*Universal Service Obligation Fund* - USOF) fue creado en 2002 para financiar la infraestructura de las telecomunicaciones en zonas rurales. Su financiamiento proviene de un derecho del 5% sobre la facturación de todos los proveedores de servicios telefónicos de corta y larga distancia. Desde su creación ocho años atrás, el USOF acumuló ingresos por 5.500 millones de dólares, de los cuales ha desembolsado hasta la fecha menos de la mitad. Actualmente está abocado a la tarea de elaborar planes para mejorar el acceso a los servicios de banda ancha. Estos planes comprenden el subsidio a las conexiones sobre la base de la fibra óptica para tráfico por red de retorno (*backhaul*) que crecen aceleradamente en India gracias a la fenomenal expansión de los servicios de la telefonía móvil. Recientemente, el gobierno completó la subasta de radiofrecuencias para servicios de banda ancha 3G y acceso inalámbrico (BWA, por sus siglas en inglés). Los ganadores de las subastas, entre los que figuran actores viejos y nuevos en el mercado de los servicios inalámbricos, ya han abonado el monto total ofertado. El gobierno, por su parte, ha cumplido con la promesa de asignar a los ganadores el espectro acordado. Se trata de un cambio positivo. Todo parece indicar que los servicios de banda ancha inalámbricos, 3G y BWA estarán disponibles en 2010 o comienzos de 2011 y que darán un enorme impulso al crecimiento y al uso de estos servicios en India. Se espera que los proveedores de servicios móviles y de Internet que constituyen el emergente mercado indio para servicios móviles de valor agregado aprovechen la nueva capacidad de banda ancha para explotar las oportunidades que ofrece un mercado que está lejos de estar saturado.

---

116 Documento debate sobre el Plan Nacional de Banda Ancha, 10 de junio de 2010, acceso a través de www.trai.gov.in/WriteReadData/trai/upload/ConsultationPapers/202/consultationon10june10.pdf.

VIII. CONCLUSIONES

La clara presencia internacional de la industria de las IT india y su éxito comercial, la expone también a un riguroso examen por parte de sus clientes en cuanto a su capacidad de proteger los datos que la han sido confiados, además de demostrar su respeto por la propiedad intelectual. Esta nueva realidad dio lugar a una reforma de la legislación existente, pese a que algunos elementos del marco legislativo vigente aún no están plenamente consolidados. Atentados terroristas como el perpetrado en Mumbai también forzaron al gobierno a adoptar iniciativas legislativas para vigilar el tráfico de comunicaciones y las redes informáticas. Por otra parte, la escasa difusión de Internet y banda ancha, sobre todo en regiones rurales, obliga al Estado a concentrar sus esfuerzos en las diferentes posibilidades de impulsar su difusión en estas áreas. Como resultado de estos esfuerzos, el gobierno desarrolló un plan para dotar a los 265.000 panchayats con una infraestructura de banda ancha. El objetivo es prestar una cantidad importante de servicios públicos mediante Internet y ayudar a la inclusión social de los sectores populares. Al mismo tiempo, la Autoridad Reguladora de las Telecomunicaciones estudia las posibilidades que existen para destinar recursos del fondo USOF a la rápida creación de la infraestructura necesaria en las regiones subabastecidas. Todo esto implicó una mayor participación de organismos públicos y asociaciones del sector privado en temas relacionados con Internet. Consiguientemente, el marco de gobierno también ha experimentado profundas transformaciones hasta volverlo casi irreconocible.

La ligereza con la que este tema fue tratado en el pasado ha dado paso ahora a intensas consultas y debates, una situación a la que en buena medida contribuyó la propia Internet. Una característica distintiva de este debate es la participación de organizaciones de la sociedad civil. En India existe una activa cultura de organizaciones de la sociedad civil y activismo social. La sociedad civil india jugó un papel clave en la determinación e influencia de algunas de las grandes decisiones relacionadas con Internet, aunque por cierto no en todas. Uno de los primeros ejemplos fue la decisión de eximir a los proveedores de servicios de Internet del pago de licencias. Otro caso digno de mención es la Ley sobre Derecho a la Información de 2005 (un proyecto de 2002 fue retirado porque se consideró que su ámbito de aplicación era muy limitado) luego de años de activa intervención de los actores de la sociedad civil como la organización Trabajadores y Campesinos de la fuerza de la Unión (*Mazdoor Kisan Shakti Sangathan* - MKSS) dirigida por Aruna Roy, hoy miembro del influyente Consejo Asesor Nacional del gobierno. Anna Hazare, conocida activista de Maharashtra, abogó desde muy temprano por una mayor

transparencia de los actos del Estado. Varias acciones lanzadas por activistas, entre ellos la Campaña Nacional por el Derecho a la Información, influyeron sobre el proyecto de ley que finalmente fuera aprobado.

La influencia de Internet en la política y los *lobbies* se puso de manifiesto durante la campaña contra las enmiendas propuestas a la Ley sobre el Derecho a la Información (RTI). Intentos del gobierno de introducir modificaciones a la ley con posterioridad a su aprobación con el fin de restarle capacidad como instrumento efectivo para la rendición de cuentas, generaron importantes protestas entre los activistas sociales. En agosto de 2006, el gobierno retiró la propuesta de enmienda a la Ley de Derecho a la Información y prometió observar en adelante el proceso democrático en cualquier acción futura concerniente a este tema.

Arvind Kejriwal, un destacado activista en favor de la transparencia de los actos de gobierno, renunció a un empleo seguro en el sector público para crear la ONG *Parivartan* (Cambio), que ayuda a ciudadanos a aprovechar al máximo las posibilidades de la Ley RTI. *Parivartan* coopera en toda India con diferentes sectores interesados como las asociaciones de inquilinos. El propósito es ayudar a estas organizaciones a lograr, mediante la aplicación de los instrumentos previstos en la Ley RTI, una mejora en los servicios como asistencia sanitaria y provisión de agua, electricidad, construcciones, etc.[117] *Parivartan* también llevó a cabo importantes campañas de concientización para llamar la atención sobre las posibilidades que brinda la Ley RTI. La página web de *Parivartan* ofrece una serie de herramientas e informaciones muy valiosas en apoyo de los ciudadanos. La organización también instituyó premios para distinguir a funcionarios del gobierno especialmente eficaces en su labor relacionada con el derecho a la información.

Pese a que aún resta mucho para hacer, el sistema se está desarrollando en la dirección correcta. Una mayor disponibilidad y, por ende, un mayor uso de Internet generará mayor transparencia, mejorará la rendición de cuentas por parte del gobierno y naturalmente brindará también un mejor acceso a la información. Del mismo modo que el acceso a las telecomunicaciones se convirtió en un importante catalizador para mejorar la productividad y la eficiencia, el acceso a Internet y a la información alberga el potencial para mejorar la interacción entre ciudadanos y Estado.

---

117 http://www.parivartan.com/home.asp.

REFERENCIAS BIBLIOGRÁFICAS

- Bhartiya Janata Party, principal partido de oposición en India http://www.bjp.org/
- Confederation of Indian Industry (October 2010) http://www.cii.in/
- Controller of Certifying Authorities (CCA) http://cca.gov.in/rw/pages/guidelinesissuedbycca.en.do
- Department of Technology (DOT), (actualizado al 1 de octubre de 2010) http://www.dot.gov.in/
- Federation of Indian Chambers of Commerce & Industry (actualizado a octubre de 2010) http://www.ficci.com/events.asp
- Indian Computer Emergency Response Team (CERT-In), (actualizado al 30 de septiembre de 2010) http://www.cert-in.org.in/
- Indian National Congress, partido político mayoritario de India, http://www.congress.org.in/new/
- International Telecommunication Union (ITU), The ICT Development Index, 2009.
- International Telecommunication Union (ITU), United Nations agency for information and communication technology issues, (actualizado al 3 de octubre de 2010) http://www.itu.int/net/about/index.aspx
- Ministry of Information Technology (MIT), (actualizado al 29 de septiembre de 2010) http://www.mit.gov.in/
- NASSCOM (Oktober 2010) http://www.nasscom.in/
- National Sample Survey of India (NSSO), Census: Literacy and Levels of Education in India, 2001. http://www.mospi.gov.in/mospi_nsso_rept_pubn.htm
- RTI Gateway http://www.rtigateway.org.in/index.jsp
- Telecom Regulatory Authority of India (TRAI), National BroadBand Plan, Documento debate del 31 de Julio de 2010, (actualizado al 27 de septiembre de 2010) http://www.trai.gov.in/ConsultationPapers_content.asp

- Telecom Regulatory Authority of India (TRAI), (actualizado al 27 de septiembre de 2010) http://www.trai.gov.in/Default.asp
- Telecommunication Regulatory Authority (TRAI), Performance Indicators Report: The Indian Telecom Services Performance Indicators January-March 2010, (actualizado al 27 de septiembre de 2010) http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf
- World Bank, Building Broadband: Strategies and Policies for the developing World, enero de 2010, http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/BuildingBroadband_cover.pdf

COREA DEL SUR

LA ACTUAL POLÍTICA COREANA DE LA TECNOLOGÍA INFORMÁTICA. PERSPECTIVAS*

PROF. DR. SEONG-WOO JI

I. INTRODUCCIÓN: LA SOCIEDAD DE LA INFORMACIÓN DE COREA ASPIRA AL LIDERAZGO EN TECNOLOGÍA INFORMÁTICA. LA IDEA BÁSICA DE LA POLITICA DE LAS IT

Gracias a sus persistentes esfuerzos por reafirmar su liderazgo en el sector electrónico, alcanzado en los pasados diez años, Corea ocupa a enero de 2010 el puesto número uno en el Índice de Gobierno Electrónico –IGE– de la Organización de Naciones Unidas (*UN Development Index of Electronic Government*). Las medidas adoptadas por el gobierno coreano para promover desde la jerarquía gubernamental la sociedad de la información no sólo han merecido reconocimiento por los logros alcanzados en la planificación de la infraestructura, sino también en lo atinente al crecimiento del sector de los servicios.

No obstante, el país enfrentará en el futuro próximo una creciente demanda que le exige emprender un camino totalmente nuevo, si quiere consolidar en la próxima década una sociedad de la información que no esté dirigida por el gobierno. Por otra parte, estas evoluciones se ven aceleradas por las nuevas tendencias en las IT como la creciente fusión de los sectores de medios y comunicaciones, una mayor movilidad, un desarrollo basado en el *software* y una creciente personalización. El año 2010 constituye un punto de inflexión importante en el camino desde una "sociedad de la información 1.0" hacia una "sociedad de la información 2.0" y consagra nuevos sistemas de una estrategia orientada hacia la información.

Pese a las tendencias económicas negativas globales, la industria coreana de las IT muestra un saludable crecimiento en los últimos años. Hacia fines de 2008,

---

***** Traducción al alemán: Dr. Benedikt M. Helfer

la industria del país sufrió un estancamiento en el marco de la crisis económica mundial, del que pudo recuperarse gracias a los impulsos económicos dados por el gobierno en 2009, y actualmente continúa su tendencia expansiva. Los servicios que brinda la industria de las IT pueden ser considerados en sentido positivo un motor de la reactivación económica.

Desde 2010, la industria de la Tecnología de la Información y Comunicación comienza a recuperarse también gracias a los numerosos paquetes de apoyo a la economía aprobados por las naciones industrializadas más avanzadas. Según datos de la Unión de la Industria Coreana, de persistir la recuperación a lo largo de 2010, el atractivo de las marcas industriales coreanas aumentará considerablemente.

También IDC Corea prevé un crecimiento del mercado local de las IT del 3,9%, con lo que las ventas sumarían unos 15.000 millones de dólares. En tal sentido, el año 2010 será considerado el punto de partida para un nuevo florecimiento de la industria coreana. Por lo tanto, es necesario focalizar la atención más en la política de las IT que en las IT propiamente dichas, si es que se quiere abarcar las consecuencias económicas, y sociales, incluidos los efectos secundarios negativos.

Para el actual presidente Lee, alcanzar resultados concretos en el campo de la sociedad de la información es un imperativo. Cumplir con los objetivos de Lee en materia de tecnologías verdes (*Green IT)*, computación en la nube (*Cloud Computing*), etc. exige coordinar las propuestas y los planes destinados a promover la vida económica. Los planes anunciados en 2009 deben ser implementados en todas las áreas y sus resultados verificados periódicamente. En particular, la sociedad coreada queda convocada a activar la fuerza de esa sociedad de la información bajo el Consejo Presidencial para la Sociedad de la Información (*Presidential Council on Information Society*), recientemente creado, y diseñar un segundo plan nacional (*To-Be*-Plan).

Además, es necesaria una estrategia activa como respuesta a un mercado de Internet inalámbrico en rápido crecimiento. Se espera que las cifras de venta en este segmento superen las de la red por cable en vista de la vertiginosa difusión de los teléfonos inteligentes *SmartPhones* en 2010. Es importante perseguir una política sólida y ofensiva para superar la demora surgida en el cambio de la Internet inalámbrica. Se requiere un proyecto que englobe políticas para aspectos tales como acceso abierto, posicionamiento de los *smartphones*, bancos de datos de telefonía móvil sencillos y económicos,

asegurar los contenidos de alta calidad, además de incrementar las inversiones en Internet para el intercambio de datos móviles *offload*.

Finalmente, se deberá dar un trato prioritario a la cuestión de la seguridad en la red. La industria, sobre todo luego del Ataque de Denegación de Servicio Distribuido DDos (*Distributed Denial of Service-attack*) del año 2009, es muy consciente de la importancia de la seguridad, ya que se ven amenazados los ecosistemas de las IT de las empresas en su conjunto, así como su integridad comercial. Especial importancia reviste reaccionar a tiempo a la pregunta acerca de la seguridad en los nuevos segmentos emergentes como las áreas de realidad virtual, ARS (*Augmented Reality Systems*), sistema de computación en nube (*cloud computing)* y la telefonía móvil. Existe, además, una gran necesidad de instalar sistemas cooperativos mediante la cooperación entre el sector público y el privado, a fin de combatir la violencia y los delitos cibernéticos. Asimismo, cabe fomentar una mayor conciencia individual acerca de la seguridad.

II. LA SOCIEDAD DE LA INFORMACIÓN DE COREA Y EL ACTUAL ESTADO DE LAS IT

II.1. Coeficiente entre uso de Internet y número de usuarios

El uso de Internet en Corea crece en forma constante y según datos actualizados a 2009 cerca de 37.000.000 de personas, es decir el 77,2% de la población mayor a 3 años, hacen uso de Internet. Si el patrón demográfico se limita a la población mayor a seis años, el porcentaje se eleva a 77,6%, lo que equivale a unos 35.700.000 millones de usuarios.

II.2. Comportamiento de los usuarios de Internet

En promedio, el coreano usa Internet durante 13,9 horas por semana. El 48,3% de los usuarios usa la web durante más de 14 horas. El 80% de los usuarios de Internet usa las páginas web para recabar informaciones y resultados de investigaciones (89,4%) o para actividades relacionadas con música, juegos y entretenimiento (88,4%), así como para intercambiar correos electrónicos, enviar mensajes de texto y desarrollar otras formas de comunicación (87,0%).

II.3. Internet y comunicación

El 85,2% de los usuarios de Internet (incremento del 1,0% anual) hace uso del correo electrónico y ha usado esa función al menos una vez en los últimos doce meses. De este porcentaje a su vez el 68,3% hizo uso de esa función en el último mes. Y nuevamente un 51,0% de los usuarios de Internet (incremento del 1,1% anual) usó el Instant Messenger por última vez en los últimos doce meses y de éstos a su vez un 38,8% lo hizo en la última semana.

El 59,7% de los usuarios de Internet (incremento del 1,6% anual) son usuarios de *blogs* y han visitado el *blog* de otros usuarios durante el último año. De estos usuarios, un 44,6% (incremento del 1,5% en un año) son administradores de *blogs* que durante el último año visitaron y administraron su propio *blog*.

II.4. Internet y actividades económicas

Según indican los estudios realizados, el 62,3% de los usuarios de Internet (incremento del 1,7% respecto del año anterior) son "usuarios de Internet con intenciones de compra", que a lo largo de los últimos doce meses adquirieron al menos una vez productos del sector de los servicios (incl. reserva y compra anticipada). El 23,4% de ellos ha hecho uso de esa función en los últimos meses.

El 41,2% de los usuarios de Internet (incremento del 1,2% respecto del año anterior) efectuó una operación bancaria por Internet durante los últimos doce meses. El 31,6 % de ellos ha usado este servicio en los últimos meses.

En la actualidad, un 9,0 % de los usuarios de Internet mayores de 18 años (incremento del 1,8% respecto del año anterior) ha hecho alguna operación bursátil por Internet; ha usado este servicio de la web durante el último año.

II.5. El entorno de Internet

Según datos actualizados a 2009, el 81,2% (incremento del 0,6% respecto del año anterior) de los hogares cuenta con conexión a Internet. Esto implica un incremento del 9,0% desde 2004 (72,2%). Los posibles caminos de conexión a Internet desde la casa son el servicio xDSL con el 75,6%, seguido por una red LAN de fibra óptica (incluido el acceso a Internet a través de la tecnología de comunicaciones FTTH) con el 27,0%, cable módem con el 25,0% y tecnología LAN inalámbrica con 8,3%.

III. LA SOCIEDAD DE LA INFORMACIÓN, EL ESTADO ACTUAL DE LAS IT Y PLANTEOS RELACIONADOS

III.1. El campo de la sociedad de la información: la computación en la nube y las tecnologías verdes son los factores más dinámicos para impulsar el crecimiento verde

Tanto en Corea como en el mercado mundial, la computación en la nube adquirió gran relevancia como factor de las IT dada su capacidad de reducir los costos a través de la adopción de nuevos sistemas y formas de servicio rápidas.

La industria coreana aspira a liderar el mercado a partir de la ventaja de haber sido una de las primeras en aplicar esa tecnología al uso público. En virtud de toda una serie de proyectos como el del Ministerio para Administración Pública y Seguridad ("Introducción y difusión de la computación en nube para el uso público"), el Ministerio de la Economía del Conocimiento ("Estrategia para el uso de computación en nube en la vida comercial") o de la Comisión Coreana de Comunicaciones ("Propuesta para el fomento de un K-Cloud-Service") se impulsaron diferentes estrategias. En diciembre de 2009, las tres instituciones participantes presentaron, además, la llamada "Propuesta general para el establecimiento de la computación en nube".

También merece reconocimiento la Agenda *Green IT* del gobierno para promover un "Crecimiento Verde" (*Green Growth)*. En ese sentido, el Comité Presidencial para el Crecimiento Verde (*Presidential Committee for Green Growth*) resumió las medidas políticas de diferentes departamentos que desarrollan actividades relacionadas con las estrategias verdes promovidas en la Estrategia Nacional. Según la propuesta en general, el gobierno proyecta invertir hasta el año 2013 cerca de 2.000 millones de dólares para implementar diez catálogos de medidas diferentes en tres áreas distintas. En el marco de la implementación cabe esperar un impulso inicial para la producción de 5.000 millones de dólares, la creación de 52.549 puestos de trabajo y una reducción de las emisiones de carbono en unas 18.400.000 toneladas para el año 2010.

III.2. Internet: *Micro Blogging* y *Smart Search* entre candilejas

Gracias a la rápida difusión del teléfono inteligente (*SmartPhone*), el pasado año trajo un rápido aumento del servicio de redes sociales (SNS) móvil. El número de usuarios del SNS alcanzó en todo el mundo los 200 millones, esperándose para Corea un incremento a 8.000.000 para fines de 2010 (eMarketer, 2009).

Particularmente grande es la demanda de servicios de *Micro Blogging* como Twitter.

A partir de la introducción del iPhone en noviembre de 2009, en Corea aumentó notablemente el número de usuarios de *SmartPhone*. Según el informe presentado y publicado por la Agencia Nacional de Desarrollo de Internet (*National Internet Development Agenc*y), en junio de 2009 el uso del SNS móvil coreano se ubicaba en tan sólo un 5,4%. Sin embargo, un 47,8% de los usuarios indicaron su intención de usar este servicio.

III.3. Comunicación: creciente popularidad del SmartPhone en 2010 a partir del lanzamiento de iPhone

Se espera que 2010 sea el "año 1" de una creciente popularidad del *SmartPhone*. La introducción del iPhone hacia fines de noviembre de 2009 marcó la largada para un mercado importante de teléfonos inteligentes en Corea. Según el Instituto de Investigación Económica de Samsung (*Samsung Economic Research Institute*), el *SmartPhone* ocupó en 2009 el quinto lugar entre los productos más vendidos en el mercado doméstico.

También es notable el aumento de los App Stores, tiendas de aplicaciones abiertas para los teléfonos móviles. Apple lanzó el App Store en 2008, obteniendo más beneficios que con la venta de iPhones. Empresas coreanas como Samsung, LG y SK no tardaron en competir por ese segmento del mercado. También empresas web como Daum y Naver facilitan plataformas propias para diferentes aplicaciones de teléfonos móviles y aplicaciones móviles web.

III.4. Medios de comunicación: el comienzo de una era de millones de usuarios de IPTV y el ascenso de los medios mixtos (*Cross Media*)

Cuestiones jurídicas sin resolver causaron una demora de varios años en la introducción de servicios IPTV en el país. Recién cuando se reformó la legislación correspondiente y el gobierno apoyó decididamente el proyecto, estos servicios se instalaron en Corea. El número de usuarios se ubica, luego de tan sólo nueve meses, en más de un millón (10/2009). Asimismo, se observa un cambio en la dinámica de comercialización. Una agresiva campaña de marketing llevó a que un creciente número de hogares rescindiera los servicios analógicos a favor de servicios IPTV.

La conjunción de servicios por cable e inalámbricos sobre la que tanto se especuló, se hizo ahora realidad con una serie de fusiones corporativas de ambos sectores. En junio de 2009 se fusionaron las compañías KT y KTF y en enero de 2010 nació de las tres empresas de comunicaciones LG Telecom, G Dacom y G Powercom la LG Telecom "unida". A partir de esta fusión, las empresas de comunicaciones están en condiciones de ofrecer servicios más eficientes, uniendo la red de alta velocidad con servicios de IPTV, de telefonía de Internet y de telefonía móvil.

Como la tendencia más novedosa en el escenario corporativo coreano se van perfilando modelos comerciales basados en medios mixtos (*Cross Media*). *Chosun Daily*, por ejemplo, presentó una nueva cobertura de noticias que incluye la distribución de material tanto a través de medios tradicionales (diarios/radio y televisión abierta) como también a través de los nuevos medios (cable, satélite, Radiodifusión Digital Multimedia (**DMB)** e Internet).

III.5. Seguridad y función negativa: la creciente previsión ante el terror cibernético luego del ataque DDoS del 7 de julio

El Ataque de Denegación de Servicio Distribuido DDos (*Distributed Denial of Service-attack*) del 7 de Julio de 2009 causó importantes daños a empresas líderes, portales y organizaciones financieras en el interior y exterior, y fue una advertencia que obligó a las autoridades a prestar más atención al tema de la seguridad en Internet.

El incidente puso de manifiesto toda una serie de problemas como la falta de un sistema de control central, el funcionamiento deficiente de los sistemas de cooperación internacionales, el déficit existente en materia de expertos y equipamiento, así como un mantenimiento insuficiente de las PC por parte de usuarios de Internet.

Con la irrupción del *Phishing* en Internet y MSN "Messenger" que mantiene toda su agresividad y que día a día demuestra ser más sofisticado –ni que hablar de los códigos de virus y *hackers* maliciosos– se tomó también mayor conciencia de la necesidad de proteger la información personal ante eventuales situaciones de crisis. El *Voice Phishing* que típicamente se dirige a una determinada persona y que requiere de una comunicación por cable y una información personal específica quedó incorporado al Messenger *Phishing* y demuestra ser ahora más dañino que nunca. Se trata de un fraude basado en el robo de datos de identificación bancaria con los que luego se retira dinero indebidamente. El Messenger *Phishing* se ha vuelto más malintencionado y organizado y el monto

de dinero robado más elevado. El número de estafas aumentó de 109 en enero de 2009 a 810 en agosto de 2009.

IV. ESTRATEGIA PARA CONVERTIR A COREA EN UNA PROGRESISTA SOCIEDAD DE LA INFORMACIÓN, BASADA EN EL CONOCIMIENTO

IV.1. Un sistema de apoyo a la sociedad de la información

El Consejo Presidencial para la sociedad de la información (*Presidential Council on Information Society*) fue creado oficialmente en noviembre de 2009 con el objeto de abrir nuevas perspectivas para el desarrollo de una sociedad de la información, y asumir las tareas de difundir esta idea y preparar adecuadamente los ciudadanos.

El Consejo mismo, dependiente de la Oficina del Presidente y que actúa en sintonía con la cooperación entre el sector privado y público, surgió como organización ampliada y reestructurada del anterior Comité sobre Sociedad de la Información dependiente de la Oficina del Primer Ministro (*Committee on Information Society*). Su tarea como máxima entidad de intermediación consiste en formular consideraciones sobre propuestas de proyectos y medidas destinadas a coordinar las políticas correspondientes con el propósito de fomentar la cultura de la información y superar la brecha digital. Asimismo, es tarea del Consejo en calidad de instancia de control, desarrollar una agenda política para una sociedad de la información orientada al futuro.

En total, el Consejo consta de 31 miembros del Comité, incluidos el Primer Ministro y un experto civil (Kak-Beom Lee, profesor de la KAIST) que comparten su presidencia. Los restantes miembros son 15 funcionarios de gobierno y otros 14 expertos civiles.

La principal función del Consejo es la puesta en práctica de su rol como instancia de control que administra y armoniza las medidas políticas en general. Además, debe apoyar las medidas políticas claves del Estado como es el Crecimiento Verde por la vía táctica así como la activación de la economía, para de este modo llegar, a través del diseño de una agenda de futuro, a una progresista sociedad de la información basada en el conocimiento.

IV.2. Planes concretos para la sociedad de la información

IV.2.1. Elaboración de las bases para la conversión al IPv6

La Comisión Coreana de las Comunicaciones y la Agencia Nacional de Desarrollo de la Internet han definido un objetivo anual y un proyecto de conversión, para consagrar el IPv6 (*Internet Protocol Version 6*). El IPv6 fue concebido para el ISP nacional con el propósito de aplicarlo en 2009 a la red de uso general. A tal efecto se realizaron esfuerzos tanto en el área de capacitación como también de entrenamiento personal.

En total se destinaron 1.800.000 dólares a un proyecto modelo que en una primera instancia se abocó a la tarea de verificar la tecnología para luego aplicar el IPv6 a la red general operada por el ISP local. El proyecto fue administrado por un consorcio constituido por once organizaciones que habían asumido exitosamente el IPv6.

Actualmente son 43 las organizaciones nacionales que ya adoptaron el IPv6 en el marco de esta medida, lo que representa un incremento del 7% respecto del año anterior.

IV.2.2. Una próxima generación de Internet para el futuro

IV.2.2.1. La Giga-Internet

En abril de 2009, el gobierno sometió una "Propuesta para ingresar a la Giga-Internet" destinada a introducir la Gigared para uso general después de 2012. El área comercial piloto fue fomentada por la Agencia Nacional para la Sociedad de la Información. La propuesta abarca la creación de una red modelo en el período 2009-2012, prestaciones piloto, el desarrollo de la tecnología y la creación de un entorno adecuado. Con estas medidas se espera facilitar las prestaciones de la Gigared con una velocidad diez veces superior a la de la red de convergencia de banda ancha (BcN) a la mayor cantidad de hogares posible. Al mismo tiempo, se busca enfocar el desarrollo de futuras tecnologías de redes y proyectar la evolución de la demanda en el sector de los servicios.

IV.2.2.2. La Red de Convergencia de Banda Ancha
(Broadband Convergence Network, BcN)

El gobierno apoyó la creación de una red de convergencia de banda ancha (BcN), esto es una red combinada de la próxima generación, que permite usar sin problemas, en forma segura y en todo momento e independiente de su

ubicación, servicios multimedias de banda ancha de las áreas combinadas de comunicación, transmisión e Internet.

El objetivo fue la creación de una BcN, en condiciones de competir internacionalmente, como red de usuarios que prevé la disponibilidad de prestaciones de multimedios por banda ancha mediante un programa de lanzamiento de la BcN. Como resultado del programa se ofrece ahora un servicio completo de banda ancha de alta calidad para un total de 37.000.000 de abonados (12.000.000 de hogares con servicios por cable, 25.000.000 sin cable según datos actualizados a diciembre de 2009) mediante una red ampliada de abonados a la BcN.

La creación de una red BcN es fomentada con el fin de crear un entorno informático y de comunicaciones para todos, posibilitando el uso de una oferta cuádruple combinada de Internet, telefonía IP, televisión, video a la carta y telefonía móvil QPS (*Quadruple Play Service*) prácticamente en todo momento y en cualquier lugar, e impulsar, además, la ampliación de la red por cable y sin cable que en 2010 ya abarcaba a 40.000.000 de usuarios.

IV.2.2.3. La implementación de IP-USN

La red universal basada en IP IP-USN (*IP-Ubiquitous Sensor Network* – red universal de sensores basada en IP) es una tecnología que de manera práctica y segura permite recibir y trasmitir información. Es accesible en cuanto a costos y de gran alcance en términos de extensión y transferencia dentro de la conexión a una infraestructura de Internet como BcN y IPv6. Sus destinatarios son los usuarios mismos, pero también busca promover el uso de 2G/3G así como la tecnología WiBro. Podría ser usada como infraestructura clave para el desarrollo del "Crecimiento Verde" a efectos de reducir las emisiones de carbono, moderar el consumo de energía y crear un entorno menos contaminante. A ello se unirían aquellas redes de sensores que hasta ahora se pusieron en práctica esporádicamente en el caso de prevención de catástrofes u observación del tiempo, así como en meteorología marina, administración de bienes inmobiliarios y otras áreas.

IV.2.3. La activación del negocio de las IT

A raíz de la crisis económica global y la caída del consumo en las naciones líderes del sector como China y Estados Unidos, las exportaciones en el rubro de las IT que alcanzaron un valor de 120.900 millones de dólares, retrocedieron en un 7,8% respecto del año anterior. La exportación industrial en general cayó, en

comparación con el año anterior, un 13,9% equivalente a una contracción 1,8 veces mayor que la sufrida por el sector de las IT. Las exportaciones generadas por la industria de las IT alanzan el 33,3%, lo que implica un aumento del 2,2% respecto del año 2008.

El gobierno anunció una "Estrategia para el futuro de las IT en Corea" (*IT KOREA Future Strategy*) como medida para implementar el proyecto de gobierno del presidente Myung-Bak Lee. Su objetivo es desarrollar una industria de las IT que se convierta en la principal fuerza motriz de la nación emergente. La estrategia abarca cinco medidas claves: apoyar la asociación de diez compañías industriales consideradas estratégicas en el sector de las IT (1), impulsar el negocio del *sofware* como fuente de la competitividad en el sector industrial (2), crear una base mundial de suministro para el equipamiento líder de IT (3), crear un servicio de comunicaciones adecuado y de avanzada (4) así como una Internet más rápida y más segura (5).

IV.2.4. Protección de la información

En 2009, la Agencia de Desarrollo de Internet coreana recibió 10.395 informes (un promedio de 866 casos por mes) sobre gusanos informáticos. Esto implica un aumento del 22,7% respecto de 2008 (con un promedio de 706 casos por mes). El número de casos informados sobre ataques de *hackers* ascendió en 2009 a 21.230 casos en total, lo que implica un aumento del 33,2% respecto de 2008, año en el que se registraron 15.940 casos. El 56,4% de los casos corresponde a *spam relay,* el 4,2% a *hacking* y el 96% a manipulación de páginas web. Los casos registrados de páginas intercaladas con fines de cometer estafas por suplantación de identidad (*Phishing Scam*) y los ataques simples se redujeron en un 15% y un 13,6 %, respectivamente respecto del año anterior.

Códigos malignos como los que se utilizaron para perpetrar el ataque DDoS del 7 de julio de 2009 son cada vez más complejos y camuflados, de modo que la propia detección del código podría conllevar problemas. Tampoco puede descartarse su activación en un determinado momento o el uso de tecnologías complejas para su ejecución. Adicionalmente, los códigos de ataque más recientes no sólo se propagan automáticamente a través de puntos vulnerables como era típico en el caso de los antiguos gusanos de Internet, sino que también se difunden a través del sistema de las redes sociales, aprovechándose para ello de diversos medios como Internet, correos electrónicos, mensajería instantánea (IM) o mensajes cortos, de conformidad con las diferentes conductas de comunicación de los usuarios de Internet.

Bajo el impacto del llamado ataque DDoS, el R&D, organismo a cargo de la protección de la información, estuvo al menos hasta 2010 activamente involucrado en el desarrollo de tecnologías capaces de prevenir ataques violentos en Internet. En particular existen cuatro proyectos que buscan prevenir un nuevo ataque como el DDoS del 7 de julio de 2009: una nueva forma de descubrimiento y de reacción tecnológica para eliminar la fuente de ataque antes de que éste pueda cometerse; el análisis automático de un código inteligente maligno así como el desarrollo de una tecnología capaz de detectar páginas temporarias y en circulación; desarrollo de una tecnología de reacción rápida que con ayuda de una herramienta capaz de impedir la propagación de un código atacante minimice el daño en caso de producirse otro ataque DDoS; desarrollo de un sistema de control de seguridad combinado que transfiere informaciones sobre ataques a la red para prevenir otro incidente al estilo del DDoS.

Además, la Agencia de Seguridad Informática de Corea, KISA (*Korea Information Security Agency*), redobla sus esfuerzos destinados a mejorar la seguridad de páginas web vulnerables y solucionar los problemas existentes en el campo de la seguridad de los sitios web de los organismos gubernamentales, entre otros. Además desarrolla herramientas aptas para detectar el ataque de un *hacker* que luego facilita gratuitamente a los organismos mencionados.

En este momento existen tres tipos de programas disponibles para prevenir o contrarrestar ataques a páginas web: una tecnología para evitar ataques a páginas web (*castle*), una tecnología para detectar estrategias de *hackers* para atacar páginas web (*whistle*) y un Web-*Firewall* abierto (*ModSecurity*, *WebKnight*).

LOS AUTORES

Prof. Dr. Seong-Woo Ji es profesor de la facultad de derecho de la Universidad de Dankook, Jukjeon Campus, República de Corea.

Laura Johnson estudió historia en la Universidad de Leeds y actualmente es investigadora del Departamento de Estudios de Guerra del King's College de Londres.

Prof. Dr. Rajat Kathuria es profesora titular de la cátedra de Gestión, Economía y Estrategia en el Instituto de Management Internacional en Nueva Delhi, India.

Hans Günter Kellner es periodista independiente de medios gráficos y radio, entre los que cabe mencionar la agencia "Evangelischer Pressedienst" (epd) y el Deutschlandfunk. Vive y trabaja en Madrid.

Dr. Helmut Reifeld tiene a su cargo el asesoramiento en temas programáticos en el Departamento de Cooperación Internacional de la Fundación Konrad Adenauer en Berlín.

Roman Sehling es colaborador científico de la Fundación Konrad Adenauer en Washington, donde está a cargo de las áreas temáticas de política exterior y de cooperación para el desarrollo. Entre otras cosas es responsable del *blog* uspolitik.info. Estudió relaciones internacionales en la Escuela de Servicio Exterior de la Universidad de Georgetown y el Instituto Estatal de Relaciones Internacionales de Moscú, así como ciencias económicas en la Universidad de Denison.

Michael Thielen es Secretario General de la Fundación Konrad Adenauer desde 2008. Estudió ciencias políticas, historia moderna y filosofía. Entre 2006 y 2008 fue Secretario de Estado en el Ministerio Federal de Educación e Investigación.

Dr. Mahesh Uppal es asesor y analista en telecomunicaciones así como director de Com First (India) Ldt. en Nueva Delhi, India. Luego de obtener el Ph.D. en el India Institut of Technology en Kanpur obtuvo un MA in Communications Policy en la City University en Londres.

Tobias Wangermann se desempeña en el Departamento de Política y Asesoramiento de la Fundación Konrad Adenauer en Berlín.

Dr. Bohdan Wyżnikiewicz es vicepresidente del Instituto de Investigaciones sobre la Economía de mercado de Gdansk, Polonia. Entre 1991 y 1992 fue Presidente de la Oficina Principal de Estadísticas (CEI). Es autor de numerosos informes y ensayos científicos, publicista y docente invitado en universidades polacas, entre ellas la Universidad de Varsovia y la Universidad de Gdansk. Experto en diversos grupos de estudio polacos y extranjeros.

Aneta Zwolińska es jurista, estudiante del doctorado de la Facultad de Derecho y Administración de la Universidad de Varsovia, cursó el posgrado de derecho de Internet en la Facultad de Gestión y Comunicación Social en el Instituto de Derecho de Propiedad Intelectual en la Universidad de Jagiellonen. Es docente de la Facultad para Sistemas de Salud de la Universidad de Medicina en Łódź y autora de artículos sobre legislación de Internet.