CUADERNOS CGI.br Estudios

1

Lucha contra el *spam* en la Internet de Brasil

Historia y reflexiones sobre la lucha contra el spam y la gestión del puerto 25 coordinados por el Comité Gestor de Internet en Brasil

Coordinadores

Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen

cgi.br

Núcleo de Información
y Coordinación del Punto BR

Coordinación
Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen

Informe y entrevistas realizadas por
Carlos Affonso Pereira de Souza
Marília de Aguiar Monteiro

CUADERNOS CGI.br **Estudios**

Lucha contra el *spam* en la Internet de Brasil

Historia y reflexiones sobre la lucha contra el spam y la gestión del puerto 25 coordinados por el Comité Gestor de Internet en Brasil

Comité Gestor de Internet en Brasil
2017

Núcleo de Información y Coordinación del punto BR (NIC.br)

CEO
Demi Getschko
CAO
Hartmut Richard Glaser
CFO
Ricardo Narchi
CTO
Frederico Neves
Director de Proyectos Especiales y Desarrollo
Milton Kaoru Kashiwakura

Equipo Asesor para las Actividades del CGI.br

Asesores administrativos
Paula Liebert, Salete Matias
Asesores técnicos
Carlos Francisco Cecconi, Diego Rafael Canabarro, Jamila Venturini, Jean Carlos Ferreira dos Santos, Juliano Cappi, Marcelo Oliveira, Nathalia Sautchuk Patrício, Vinicius Wagner Oliveira Santos

Concepto & Producción

Coordinadores
Cristine Hoepers
Henrique Faulhaber
Klaus Steding-Jessen
Informe y entrevistas
Carlos Affonso Pereira de Souza
Marília de Aguiar Monteiro
Coordinación ejecutiva y editorial
Carlos Francisco Cecconi y Juliano Cappi
Producción editorial
Caroline D'Avo y Everton Rodrigues (Comunicação NIC.br)
Apoyo editorial para esta edición
Jamila Venturini
Jean Carlos Ferreira dos Santos
Juliana Nolasco
Traducción del español
Linnguagem Idiomas y Laureana Pavon
Revisión de la traducción al español
Laureana Pavon
Diseño gráfico
Pilar Velloso
Maquetado e ilustraciones
Milena Branco y Pilar Velloso
Fotografías
Omar Paixão, Gettyimages e Istockphoto

Esta publicación está disponible en formato digital en la siguiente dirección: <http://www.cgi.br>

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Lucha contra el spam en la Internet de Brasil [livro eletrônico] : historia y reflexiones sobre la lucha contra el spam y la gestión del puerto 25 coordinados por el Comité Gestor de Internet en Brasil / Núcleo de Informação e Coordenação do Ponto BR ; [tradução Linguagem Idiomas]. -- São Paulo : Comitê Gestor da Internet no Brasil, 2017. -- (Cadernos CGI.br estudos)
3,87 Mb ; PDF.
Título original: Combate ao spam na Internet no Brasil : histórico de reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil.
Vários colaboradores.
ISBN 978-85-5559-039-9
1. Internet - Medidas de segurança 2. Políticas públicas - Brasil 3. Redes de computadores - Medidas de segurança 4. Spam (Mensagem eletrônica) - Combate I. Núcleo de Informação e Coordenação do Ponto BR. II. Série.
17-02310 CDD-005.8

Índices para catálogo sistemático:
1. Segurança de redes de computadores : Combate ao spam : polítticas de Internet : Brasil
005.8

Comité Gestor de Internet en Brasil (CGI.br)

Composición en diciembre de 2016

Miembros del Comité

Representantes de organismos gubernamentales

Carlos Roberto Fortner
Francilene Procópio Garcia
Franselmo Araújo Costa
Igor Vilas Boas de Freitas
Luiz Carlos de Azevedo
Luiz Fernando Martins Castro
Marcelo Daniel Pagotti
Marcos Vinícius de Souza
Maximiliano Salvadori Martinhão

Representantes de organizaciones empresariales

Eduardo Fumes Parajo
Eduardo Levy Cardoso Moreira
Henrique Faulhaber
Nivaldo Cleto

Organizaciones sin fines de lucro y no comerciales

Carlos Alberto Afonso
Flávia Lefèvre Guimarães
Percival Henriques de Souza Neto
Thiago Tavares Nunes de Oliveira

Representantes de la comunidad técnica y científica

Flávio Rech Wagner
Lisandro Zambenedetti Granville
Marcos Dantas Loureiro

Experto en Internet

Demi Getschko

Coordinador

Maximiliano Salvadori Martinhão

Secretario Ejecutivo

Hartmut Richard Glaser

Prefacio

por HENRIQUE FAULHABER

> "Las iniciativas para mejorar la seguridad cibernética y enfrentar las amenazas de seguridad digital deben involucrar una colaboración adecuada entre los gobiernos, el sector privado, la sociedad civil, el sector académico y la comunidad técnica."
>
> *Declaración Multisectorial de NETmundial, San Pablo - 2014*

Estimado lector:

Esta publicación busca relatar los esfuerzos realizados por el Comité Gestor de Internet en Brasil y por diversas personas y organizaciones en la lucha contra el spam desde 2004. Los mensajes masivos no solicitados que llegan a nuestros buzones son uno de los primeros desafíos que enfrentan los usuarios, las empresas y toda la cadena involucrada en la infraestructura de acceso y de servicios de Internet.

Creada en el ámbito del Comité Gestor de Internet en Brasil (CGI.br) en 2004, la Comisión de Trabajo Antispam (CT-spam) tuvo como principal atribución la creación de una estrategia nacional para abordar el problema del spam. Dado que el spam es uno de los principales vehículos para la distribución de código malicioso y una grave amenaza para la seguridad de Internet, CERT.br ha sido un actor fundamental para el éxito de la Comisión de Trabajo Antispam.

La importancia de esta publicación, Lucha contra el spam en la Internet de Brasil, no se estima por tratarse de una tentativa de documentación histórica de las actividades desempeñadas a lo largo de los últimos diez años para luchar contra un determinado problema. Este informe surge de la necesidad de explicitar mejor la concepción de una de las principales atribuciones del CGI.br: la coordinación de múltiples partes interesadas de los actores con interés en la política nacional sobre Internet.

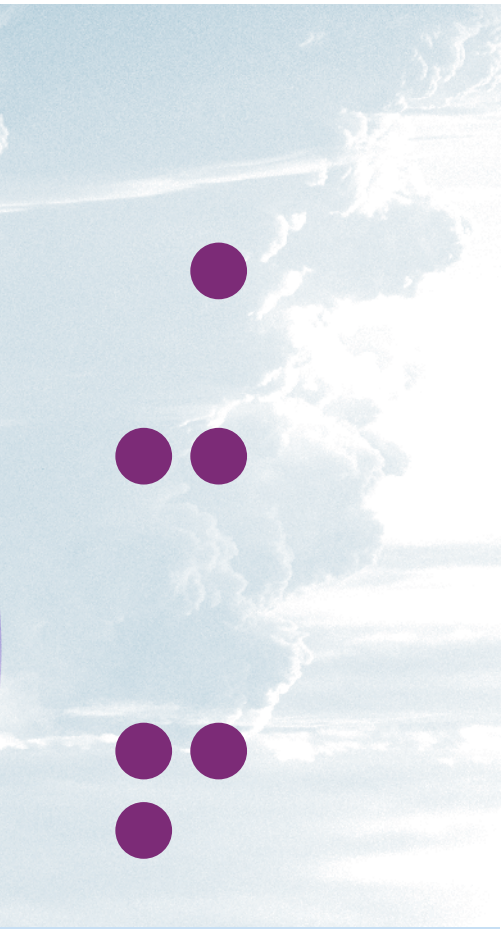
En el camino hacia una colaboración eficaz todavía quedan muchos desafíos. La educación y el compromiso de diferentes grupos descentralizados, entre ellos diversos actores gubernamentales, atraviesan dificultades que incluyen la dificultad de hacer entender la complejidad de la colaboración por medio de distintas competencias y desafiar modelos de gestión preestablecidos en favor de un compromiso multisectorial innovador y participativo.

Este trabajo fue más allá de la exclusión de Brasil de las principales listas de spammers a nivel mundial. Es el resultado de una correlación entre seguridad, libertad y gobernanza de la red a partir de un diálogo dinámico y complejo entre los distintos tomadores de decisiones.

¡Buena lectura!

Henrique Faulhaber
Consejero del CGI.br

Sumario



I
Informe
Gestión del puerto 25 en la Internet de Brasil

Introducción

Las cuestiones relacionadas con la seguridad de las redes de comunicación adquieren cada vez mayor importancia en los escenarios nacional e internacional a medida que las tecnologías de comunicación e información se vuelven esenciales para la realización de derechos como la libertad de expresión, la ampliación del acceso en términos de políticas públicas y, en general, para los procesos intrínsecos a diversas cadenas productivas.

Por afectar de forma significativa la vida cotidiana de los ciudadanos, la industria y el poder público, distintos actores están dirigiendo legítimamente sus esfuerzos para garantizar la seguridad y la confianza en las redes. Sin embargo, estas cuestiones están impregnadas de complejidad a diferentes niveles: político, técnico, regulatorio, económico y social. Parte de esta complejidad deriva de la naturaleza de la propia red: las decisiones regulatorias, tomas de decisiones empresariales o incluso decisiones jurídicas concernientes a la seguridad de la red deben considerar siempre su carácter mundial, su fundamento en la interoperabilidad y en la participación de diferentes actores.

Gran parte de las amenazas a la seguridad de la red son de naturaleza sistémica y afectan simultáneamente a diferentes actores, por lo que la cooperación entre estos distintos actores es la mejor manera de detectar y mitigar los efectos de tales amenazas.

Esto también se aplica a las amenazas que involucran *spam* y que, a su vez, también poseen sus particularidades que se relacionan, de forma puntual, con el desarrollo de las prácticas de seguridad de red.

El tema de la lucha contra el *spam* ha estado presente en los foros sobre gobernanza y regulación de Internet durante los últimos quince años. Los factores que llevan a la persistencia del tema son tan variados como las formas de investigar el problema, ya que los esfuerzos para impedir su envío se pueden desarrollar e implementar a través de perspectivas de naturaleza tecnológica, jurídica, política y social. El objetivo de este trabajo es presentar la labor de coordinación realizada por el Comité Gestor de Internet en Brasil en la gestión del puerto 25 como un importante estudio de caso exitoso, con iniciativas que apuntan hacia la colaboración de múltiples partes interesadas como la mejor estrategia para enfrentar los temas de seguridad cibernética.

Diversas iniciativas nacionales e internacionales y diferentes foros internacionales se basan en la cooperación entre diferentes actores para combatir incidentes y mitigar amenazas. A continuación mencionamos algunos ejemplos. En Holanda, el Consejo Holandés de Seguridad Cibernética (Dutch Cyber Security Council) cuenta con quince miembros que representan al gobierno, la comunidad científica, el sector privado y la industria. Este Consejo presta asistencia de oficio o a pedido de solicita la sociedad y el gobierno holandés y es responsable por la implementación de la Estrategia Holandesa de Seguridad Cibernética Doméstica. En 2013, el Consejo Holandés publicó una recomendación de buena práctica para una nueva estrategia de seguridad cibernética que resaltaba la importancia de la colaboración y la coordinación entre actores para alcanzar un nivel eficiente de protección, intercambio de información y respuesta a incidentes de seguridad:

> The advice specifically focused on the need for close cooperation and coordination in the field of incident detection and response. Only through active information sharing, timely response and seamless collaboration can a secure digital environment be established[1].

En Japón, el Cyber Clean Center (CCC) cuenta con la cooperación del gobierno, la industria del software y los proveedores de conexión de Internet para prevenir la infección de las computadoras de los usuarios, a través de una estructura que posee un Comité Gestor y grupos de trabajo especializados[2].

A nivel internacional, el Grupo de Trabajo Conficker (Conficker Working Group, CWG) fue una coalición entre investigadores de seguridad de red para combatir un software malicioso conocido como conficker que afectó a usuarios de todo el mundo. Este grupo de trabajo es reconocido como una cooperación sin precedentes entre organizaciones e individuos, a nivel global, de los sectores

1 "Las recomendaciones se enfocan específicamente en la necesidad de una estrecha cooperación y coordinación en materia de detección y respuesta a incidentes. Solo a través de un activo intercambio de información, respuestas oportunas y colaboración continua es posible establecer un entorno digital seguro". E. Van Den Heuvel G.K. Baltink, Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond, p. 122. Disponible en <https://www.ncsc.nl/english/current-topics/news/best-practices-in-computer-network-defense.html>. Consultado el 4 de julio de 2014.

2 Cyber Clean Center <https://www.ccc.go.jp/en_ccc>. Consultado el 4 de julio de 2014. Nota del Traductor: la dirección de la página web fue reemplazada por <https://www.telecom-isac.jp/ccc/en_index.html>. Consultado el 8 de marzo de 2017.

público y privado, para luchar contra una amenaza a la seguridad de los recursos críticos globales de la red:

> In an unprecedented act of coordination and collaboration, the cybersecurity community, including Microsoft, ICANN, domain registry operators, anti-virus vendors, and academic researchers organized to block the infected computers from reaching the domains – an informal group that was eventually dubbed the Conficker Working Group (CWG). They sought to register and otherwise block domains before the Conficker author, preventing the author from updating the botnet. Despite a few errors, that effort was very successful[3].

De la misma forma, el DNS-changer Working Group (DCWG) fue un grupo *ad hoc* creado para remediar los efectos de los servidores de DNS maliciosos de Rove Digital. La *botnet* operada por esta empresa alteraba los parámetros de DNS del usuario conectándolo a DNS maliciosos en diferentes países, promoviendo así una experiencia engañosa y peligrosa para los usuarios de Internet. La coordinación se dio entre Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics and Training Alliance, Neustar, Spamhaus, Team Cymru, Trend Micro y la Universidad de Alabama en Birmingham, en colaboración con el FBI de Estados Unidos, CERTs nacionales y proveedores de conectividad.

De esta forma, los trabajos del Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil (CERT.br) y del Comité Gestor de Internet en Brasil (CGI.br), a través su Comisión de Trabajo Antispam, figuran entre las iniciativas globales de colaboración y coordinación de múltiples partes interesadas exitosas para la promoción de temas de seguridad cibernética. Por más de veinte años, Brasil ha estado desarrollando un modelo de múltiples partes interesadas de gobernanza de Internet a través del trabajo del CGI.br. Como uno de los brazos que mantiene el Núcleo de In-

3 "En un acto sin precedentes de coordinación y colaboración, la comunidad de seguridad cibernética, incluyendo a Microsoft, ICANN, operadores de registro de dominio, proveedores de antivirus e investigadores académicos, se organizaron para bloquear las computadoras infectadas e impedir que llegaran a los dominios – un grupo informal que acabó recibiendo el nombre de Grupo de Trabajo sobre Conficker (CWG). Este grupo intentó registrar y de alguna forma bloquear los dominios antes que el autor de Conficker, impidiendo que el autor actualizara la botnet. Aunque hubo algunos errores, el esfuerzo fue muy exitoso". Conficker Working Group: Lessons Learned. Disponible en <http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf>. Consultado el 4 de julio de 2014.

formación y Coordinación del Punto BR, entidad sin fines de lucro responsable por la implementación de las decisiones y proyectos del CGI.br, la coordinación es uno de los elementos esenciales de sus actividades de seguridad y respuesta a incidentes en la red brasileña, junto con la comunicación y el apoyo a la comunidad brasileña en lo que se refiere a tendencias y amenazas.

El estudio y la documentación de la iniciativa de gestión del puerto 25 en la red de Brasil tiene como premisa principal demostrar, a partir de un caso concreto, el desarrollo de políticas de Internet en el país en los últimos veinticinco años.

De forma secundaria, este trabajo señala la importancia de la colaboración y la coordinación entre los diferentes actores como elemento clave para el desarrollo de políticas de seguridad efectivas y el establecimiento de confianza en Internet. Resultado de la convergencia de las experiencias de decenas de empresas de telecomunicaciones, miles de proveedores de servicios de Internet, representantes de la sociedad civil y de la comunidad académica con los técnicos del CGI.br, el proceso de gestión del puerto 25 produjo un amplio intercambio de conocimientos. La amplia discusión promovida por la coordinación del CGI.br fue de especial importancia para su realización, ya que exigía que primero los proveedores de e-mail ofrecieran enviar el correo electrónico por un puerto distinto, migrando por lo menos el 90% de los usuarios de diferentes empresas antes que los proveedores de conectividad pudiesen bloquear el tráfico de salida del puerto 25. Dado que la colaboración y la coordinación entre los diferentes actores es el principal eje de este estudio, sus testimonios son la fuente primaria de la narrativa de esta iniciativa más allá del pragmatismo teórico del modelo de múltiples partes interesadas en las políticas de Internet, este estudio se concentra en la experiencia y la colaboración de los actores en el proceso específico de coordinación de la gestión del puerto 25.

La coordinación de la gestión del puerto 25 en Brasil fue realizada por el Comité Gestor de Internet en Brasil (CGI.br), órgano de múltiples partes interesadas creado en 1995[4] por una iniciativa interministerial para tratar temas relacionados con las políticas de Internet en el país. Dentro del Comité Gestor, en 2004 se creó un grupo de trabajo específico sobre *spam*, una iniciativa del entonces

4 Puede consultar una historia del CGI.br en <http://cgi.br/historicos/>. Consultado el 2 de junio de 2014.

consejero Henrique Faulhaber, la Comisión de Trabajo Antispam (CT-Spam). Por lo tanto, la primera parte de este trabajo incluirá una breve historia de las actividades desarrolladas en el ámbito de este grupo de trabajo del Comité Gestor de Internet. Las actividades de la CT-Spam reflejan la cantidad de soluciones que puede requerir un problema de seguridad de red: necesidades jurídico-regulatorias, actividades empresariales y educación de los usuarios.

La segunda parte trata la gestión del puerto 25 en sí, mientras que la tercera muestra los aspectos jurídicos y regulatorios relevados durante el proceso. La cuarta y última parte trata la actividad de coordinación a partir de la historia de las regulaciones brasileñas para los servicios de telecomunicaciones e Internet. En esta etapa el lector verá una breve presentación del modelo regulatorio de telecomunicaciones brasileño, así como el modelo de múltiples partes interesadas de gobernanza de Internet desarrollado por Brasil en los últimos veinticinco años.

De forma breve, el estudio presenta las decisiones regulatorias brasileñas a partir de los procesos de privatización de la economía que se iniciaron en la década de los 90 y tuvieron su reflejo en el desarrollo de la gobernanza de Internet en el país. Por lo tanto, este estudio demuestra que las soluciones efectivas para las políticas de Internet se derivan a partir de la colaboración de los diferentes actores: proveedores de telecomunicaciones, proveedores de aplicaciones de Internet, organismos técnicos, sector académico, gobierno, entidades de la sociedad civil y representantes de los usuarios. El texto no pretende abordar con ahínco teórico el creciente debate global acerca del modelo de múltiples partes interesadas, sino que pretende ofrecer la perspectiva de los actores en un proceso exitoso de colaboración descentralizada, multiparticipativa y voluntaria.

Brasil, "Rey del Spam"

En 2009, Brasil ocupó el primer puesto en el ranking de la Composite Blocking List de los países que más enviaron *spam*, por lo que la prensa internacional lo calificó como el "Rey del *Spam*". La lista —que se actualiza todos los días— actualmente incluye a Brasil en el vigésimo quinto puesto[5]. El éxito brasileño es fruto de

5 Composite Blocking List. Disponible en <http://cbl.abuseat.org/country.html>. Consultado el 12 de octubre de 2013.

ocho años de implementación de políticas de lucha contra el *spam* por parte del Comité Gestor de Internet a través de su Comisión de Trabajo Antispam (CT-Spam)[6]. La CT-Spam se constituyó tanto para diseñar una estrategia nacional de lucha contra los abusos de la red perpetrados por *spammers*, como para articular medidas de lucha con los diversos actores involucrados.

El principal motivador de las acciones de la CT-*Spam* fue la reputación de la red brasileña. Se llegó a casos extremos en que bloques completos de IPs brasileñas fueron bloqueadas en el tráfico de entrada de otros países simplemente en base al criterio de su nacionalidad[7].

Lo que se percibió fue un abuso de la infraestructura de Internet por parte de los *spammers* y la necesidad de revertir este escenario, ya que los riesgos de la inercia eran sentidos directamente por el consumidor, entre ellos: (i) precarización del ancho de banda contratado por el consumidor; (ii) inclusión del consumidor en listas negras, lo que imposibilitaba el pleno goce de sus libertades en la red y, en casos extremos, podría llevar a limitar su libertad de expresión; (iii) costos de soporte técnico innecesariamente soportados por el consumidor infectado; y (iv) precarización de los servicios globales de comunicación, en la medida en que el trayecto del *spam* es internacional[8].

La CT-Spam trabajó en la sensibilización de los actores sectoriales involucrados tanto con respecto a su papel como con respecto a su importancia en la implementación de estas políticas, como así también en la educación y la construcción de capacidades entre los consumidores sobre el uso seguro y eficiente de los servicios de Internet. Entre otras, estas tareas convierten a los trabajos de la CT-Spam en un importante y crucial *leading case* del modelo modelo de múltiples partes interesadas del CGI.br de amplio éxito internacional y un rector temático de la historia de Internet en Brasil.

La tecnología y la política más eficientes intentadas para esta

---

6 Comisión de Trabajo Antispam del CGI.br. Disponible en <http://www.cgi.br/pagina/comissoes-de-trabalho-antispam/121#a4>. Consultado el 05 de mayo de 2014. La primera reunión de la CT-Spam se realizó el día 14 de enero de 2005 para definir la agenda del grupo e iniciar los trabajos.

7 Razón observada principalmente por Rubens Kuhl, Eduardo Parajo, Klaus Steding Jessen y Cristine Hoepers en diferentes entrevistas concedidas al Proyecto Memoria de la lucha contra el spam en Brasil.

8 MAAWG. MAAWG Recommendation: Managing Port 25 for Residential or Dynamical IP Space Benefits of Adoption and Risks of Inaction. Disponible en <http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf>. Consultado el 12 de octubre de 2013.

finalidad están en la gestión del puerto 25, "nombre dado al conjunto de políticas y tecnologías, implementadas en redes de usuarios finales o de carácter residencial, que trata de separar las [1] funcionalidades de entrega de mensajes de aquellas de [2] transporte de mensajes entre servidores"[9].

El largo proceso de ejecución de la gestión del puerto 25 refleja que no se trataba de un tema menor, ni desde el punto de vista técnico —incluso los sectores técnicos de las empresas desconocían las consecuencias y los impactos de la medida— ni desde el punto de vista regulatorio y jurídico. Fue necesario coordinar diferentes intereses, muchas veces contradictorios, en nombre de un resultado beneficioso para todos y, en este sentido, cuestiones como la protección del usuario y las garantías contractuales aparecieron como argumentos que volvieron el proceso más complejo y consecuentemente más prolongado.

El proceso de realización de la medida también fue afectado de forma tangencial por las discusiones acerca del Marco Civil de Internet de Brasil, actualmente Ley nº 12.965/2014. Esta ley fue el resultado de una consulta realizada entre 2009 y 2010 por el Ministerio de Justicia a través de un portal de Internet. El proyecto fue presentado al Congreso Nacional en 2011. Entre los temas centrales del Marco Civil, el que concierne a la gestión del puerto 25 es la cuestión de la garantía del principio de neutralidad de la red.

Metodología de este estudio

Antes de este trabajo se entrevistó a Henrique Faulhaber, coordinador de la CT-Spam, quien dijo que, además de la importancia técnica de la gestión del puerto 25 señalada por expertos nacionales e internacionales, en Brasil la gestión se dio gracias el papel individual de cada uno de los actores involucrados. Si no fuese por aquellas personas reunidas a favor de un deseo común, tal vez la gestión del puerto 25 no hubiese sido adoptada eficientemente[10].

El testimonio de estos actores constituye la principal fuente de este

9 C. Hoepers, K. Steding-Jessen. Gerência da Porta 25: Motivação, Importância da Adoção para o Combate ao Spam e Discussões no Brasil e no Mundo. Disponible en <http://www.cert.br/docs/ct-spam/ct-spam-gerencia-porta-25.pdf>. Consultado el 12 de octubre de 2013.

10 Henrique Faulhaber en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 17 de septiembre de 2013.

trabajo, lo que ha permitido desarrollar una documentación del proceso a partir de la comprensión de diferentes formas de articulación entre actores y grupos, revelando el impacto de las acciones de los individuos y de sus estrategias de actuación. Además, esta metodología también sirve para estudiar el modo en que las personas o los grupos elaboraron y llevaron adelante determinadas experiencias, incluyendo situaciones de aprendizaje y toma de decisiones estratégicas[11].

Por lo tanto, el objetivo de este trabajo es preservar la memoria de la lucha contra el *spam* en Brasil, a través de la realización de la gestión del puerto 25, a partir de una perspectiva de documentación histórica, no solo para que sirva de legado de un caso paradigmático y ejemplo internacional, sino también para que contribuya al registro del desarrollo de Internet en el país. Esta opción preserva detalles poco documentables del proceso, como la visión y el empeño personal de los individuos involucrados, propiciando un intenso y rico material de investigación para generaciones presentes y futuras interesadas en la historia de Internet en Brasil.

Se entrevistó a los principales actores representantes de los sectores involucrados en la cadena de Internet: gobierno, sociedad civil, sector privado y sector académico. Los informes permitieron aclarar no solo los esfuerzos de articulación para la toma de una decisión estratégica, sino también cuestiones jurídico-regulatorias encontradas por los individuos ante un escenario de ausencia de leyes específicas sobre el tema y considerando derechos fundamentales como privacidad, libertad de expresión, defensa del consumidor y competencia.

La primera parte de este trabajo presenta una breve historia de las acciones que llevaron a la realización de la gestión del puerto 25. Se destacan cómo se identificó el problema, los primeros abordajes para su resolución y el proceso de toma de decisión estratégica para el bloqueo del puerto 25. La segunda parte se desarrolla a partir de las narrativas recogidas y aborda la ejecución de la medida a partir de sus elementos políticos, jurídicos y regulatorios.

11 V. Alberti. Ouvir contar: textos em história oral. Rio de Janeiro: Editora FGV, 2004.


CT-Spam
UCE

1. Breve historia de las actividades de la CT-Spam para luchar contra el spam en Brasil

Comisión de Trabajo Antispam del Comité Gestor de Internet en Brasil (CT-Spam)

Conforme se detallará en la segunda parte de este trabajo, el Comité Gestor de Internet en Brasil es un órgano que se ocupa de la gobernanza de Internet en Brasil. Uno de los principales efectos de su constitución fue justamente garantizar un carácter multisectorial para la gobernanza de la estructura de Internet, es decir, los nombres de dominio y las direcciones de IP, separando esta atribución de la que usualmente se atribuye a la regulación estatal del sector de las telecomunicaciones.

Con el desarrollo de los temas de gobernanza de Internet, especialmente en 2004 con la Cumbre de la Sociedad de la Información, ya existía una demanda interna que abogaba para que el Comité Gestor discutiera otras capas de la gobernanza de Internet, no solo las capas de estructura[12].

La Comisión de Trabajo Antispam (CT-Spam) del Comité Gestor de Internet en Brasil se creó en 2005 como una de las iniciativas de profundización de la actuación del CGI.br más allá de la gestión de la estructura de la red. Por iniciativa del consejero Henrique Faulhaber, se comenzó a trabajar en la lucha contra el *spam* ante los problemas evidentes que este fenómeno traía a la red: en 2005, el 90% de los mensajes enviados eran correos no deseados, también llamados *spam*[13].

Además de lo molesto que resultaba para el usuario, también era necesario abordar la cuestión del uso indebido de la red brasileña, que afectaba no solo su credibilidad internacional sino también el desempeño de los operadores de telecomunicaciones y proveedores de servicios de Internet, perjudicando a los consumidores con poco ancho de banda contratado y, en algunos casos, causando pérdidas

12 Henrique Faulhaber en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 17 de enero de 2014.

13 Estimación aproximada revelada por Henrique Faulhaber en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 17 de enero de 2014.

financieras a través de mensajes con contenido fraudulento.

Se realizaron muchos esfuerzos buscando una definición de *spam* como forma de impulsar la lucha contra este problema[14].

La Cartilla de Seguridad del CERT.br incluye el concepto de no solicitación como elemento fundamental para la caracterización de lo que sería *spam*. De acuerdo con este texto, *spam* "es el término usado para referirse a los mensajes de correo electrónico no solicitados, que generalmente se envían a una gran cantidad de personas. Cuando este tipo de mensaje posee contenido exclusivamente comercial, también suele denominarse UCE (***U****nsolicited* ***C****ommercial* ***E****-mail*)"[15].

De esta forma, las definiciones —normativas o no— del término trabajan con aspectos subjetivos derivados de la utilidad o de la conveniencia del mensaje para el consumidor, con el agravante de la ampliación del tema a otras formas de mensajes electrónicos, como los SMS, la mensajería instantánea o los mensajes en las redes sociales. Dado que la subjetividad dificulta la definición de

---

14 El término "Spam" en sí es una marca norteamericana de carne procesada y enlatada de Hormel Foods. Su popularización y contextualización en el área de la informática son inciertas y una de las mayores curiosidades sobre el tema. Para muchos, el término fue acuñado primeramente por el célebre grupo humorístico Monty Python, en uno de sus episodios de la década de 70 que transcurre en una taberna donde todos los platos del menú se hacen con carne enlatada Spam. Mientras los consumidores deciden sobre el plato, un grupo de vikingos repite hasta el cansancio el término "Spam" entonando una canción y causando molestia generalizada. En los sistemas informáticos, la controversia es aún mayor, llegando al origen del envío de mensajes no solicitados a destinatarios en forma masiva, independientemente del término spam. De acuerdo con el sitio antispam.br: "Las controversias acompañan al spam desde su 'nacimiento', cuya fecha oficial puede ser considerada como el 5 de marzo 1994. Este día, dos abogados, Canter y Siegel, enviaron un mensaje sobre una lotería de Green Cards estadounidenses a un grupo de discusión de Usenet. El acto de enviar un mensaje de propaganda a un foro no relacionado con el tema causó espanto y revuelta entre quienes estaban suscriptos al grupo. Sin embargo, lo peor sucedería el 12 de abril de 1994, cuando los abogados enviaron el mismo mensaje a diversos grupos de discusión de Usenet. Para ello utilizaron un programa capaz de automatizar el envío masivo de mensaje de propaganda. Las reacciones no se hicieron esperar, fueron negativas y generaron denuncias sobre la violación de la netiqueta, un conjunto de reglas de buenos modales para los usuarios de la red. El gran número de mensajes intercambiados sobre el tema afectó el desempeño de la red, provocando así uno de los conocidos efectos secundarios del spam. Estos mensajes están disponibles en WebArchive.org: <http://web.archive.org/web/20011214024742/math-www.uni-paderborn.de/~axel/BL/CS941211.txt>. Durante las acaloradas discusiones sobre lo ocurrido, surgió la referencia al término spam, recordando una escena del programa de TV del grupo inglés Monty Python. Para leer más sobre el tema, puede dirigirse a <http://antispam.br/historia/>

15 CERT.br, Cartilha de Segurança para Internet: 5. Spam. Disponible en <http://cartilha.cert.br/spam/>. Consultada el 8 de marzo de 2014.

denominadores comunes, la CT-Spam realizó un estudio sobre los aspectos regulatorios del *spam* y estableció algunos criterios básicos para su identificación[16], entre ellos los siguientes:

(i) el carácter comercial;
(ii) el envío masivo;
(iii) la uniformidad de su contenido; y
(iv) el hecho de no haber sido solicitado por el destinatario.

En sus actividades a lo largo de los años, la CT-Spam desarrolló varias soluciones que ayudaron a revertir el panorama de Brasil como uno de los países que más *spam* enviaba en el mundo. Desde campañas educativas para la sensibilización de usuarios individuales y empresas hasta la producción del referido estudio, pasando por la construcción de un sitio que se ha vuelto una referencia sobre el tema y el estímulo a la autorregulación en el área, se podría analizar un universo bastante amplio de actividades de la CT-Spam.

Como el objetivo de este estudio es la gestión del puerto 25, comentamos aquí brevemente las iniciativas pertinentes de modo que se comprenda que su implementación no fue una actividad aislada, sino un paso más en los reiterados esfuerzos de la CT-Spam para atacar el problema del envío en masa de *spam* desde el país. De tal forma, indicamos cómo estas actividades se relacionan y se diferencian de los desafíos encontrados en el desarrollo de la gestión del puerto 25.

Código de Autorregulación del E-Mail Marketing

Una de las actividades que se incentivaron en la CT-Spam fue la creación de un código de autorregulación del *e-mail marketing*. Esta iniciativa surgió de la percepción dentro de la Comisión de que, además de acompañar las propuestas legislativas para regular la materia, sería necesario establecer estándares que pudiesen guiar a las empresas que se valen de los mensajes de correo electrónico como instrumento para dar publicidad a sus productos y servicios. En las palabras del exconsejero Jaime Wagner:

> Yo siempre digo que existen varios tipos de spam. Uno es el "spam bandido", que estaba siendo combatido mediante la

16 Lemos, R.; Doneda , D.; Souza, C.A.; et al. Estudo sobre a Regulamentação Jurídica do Spam no Brasil. Publicado originalmente en abril de 2007 <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Consultado el 12 de agosto de 2013.

> gestión del puerto 25; el otro es el "spam ingenuo", que se disfraza de marketing. Es el sujeto que compra una base de datos y envía mensajes a todo el mundo, con la mejor de las intenciones y tratando de vender más. Es el caso de múltiples pequeños comerciantes que ven a esta práctica como una forma de marketing barato. Estos comerciantes tienen un interés común legítimo, pero acaban volviéndose spammers[17].

El objetivo de la autorregulación del *e-mail marketing* era justamente evitar que una actividad comercial legítima, el envío de publicidad a los consumidores, disminuyese equivocadamente al tratar de luchar contra el *spam*, ya que en muchos aspectos esta práctica adquiere las características subjetivas del *spam*, como veremos más adelante.

En esta frente de lucha contra el *spam*, el exconsejero Jaime Wagner estuvo a cargo de la coordinación de los actores involucrados en la cadena de *e-mail marketing*. Las diferencias de coordinación entre los actores requerida por la autorregulación del *e-mail marketing* y aquella demandada por la gestión del puerto 25 residen en la profundización tecnológica y en el distanciamiento del consumidor.

En otras palabras, la autorregulación del *e-mail marketing* es una actividad desempeñada por actores que utilizan Internet apenas como un vehículo para la entrega de un producto o del servicio, en este caso la publicidad de determinado producto o servicio. Sumado a esto, la conveniencia y la utilidad del producto es percibida de forma clara por el consumidor, que identifica de manera casi automática el origen del problema —el proveedor—. A su vez, el esfuerzo de coordinación de la gestión del puerto 25 se amolda con la gestión de los recursos de la red y de los diversos agentes responsables por la provisión del servicio de Internet. Aquí, el consumidor no tenía una percepción obvia del problema ni de a quién se podía atribuir la falla del servicio.

Sitio antispam.br

La CT-Spam trató de actuar en diversos frentes contra el *spam*. Para promover la educación, tanto de los usuarios finales como de los proveedores y operadores, se creó el sitio *antispam*.br con materiales informativos para usuarios finales, administradores de red

17 Jaime Wagner en entrevista concedida al proyecto Memoria de la Lucha contra el Spam en Brasil el 11 de marzo de 2014.

y operadores de comunicación donde se presentan sugerencias de defensa e información general sobre *spam*. Dado que es producto de la Comisión de Trabajo Antispam, sigue en importancia al bloqueo efectivo del puerto 25, en virtud del legado que representa en términos de información y educación al consumidor y sus derechos básicos, conforme a las normas de defensa del consumidor pertinentes[18].

Conforme destaca Henrique Falhauber:

> "El sitio <antispam.br> dio soporte a toda esta sensibilización con respecto al problema del spam. (...) El spam no terminó; salimos de la lista de los países que más envían spam, pero el spam aún es un problema. Un problema inclusive en otros medios: redes sociales, SMS. Por lo tanto, este trabajo de educación, sensibilización y alerta a las personas es fundamental y es un subproducto que está ahí hasta el día de hoy. Hacemos campañas para divulgar este sitio que es una referencia y que acabó ayudándonos mucho en la implementación de la gestión del puerto 25."[19]

De tal forma, la relación entre el sitio antispam.br y la gestión del puerto 25 indica la necesidad de coordinar tanto actividades técnicas complejas (como la gestión en sí) como el desarrollo de una plataforma de carácter informativo que pueda transmitir al público objetivo las informaciones necesarias para su actuación, garantizando así mejores resultados. En este sentido, el sitio antispam parece haber funcionado no solo como herramienta de convencimiento de la importancia de gestionar el puerto 25, sino también como herramienta de movilización e instrucción para los más diversos agentes.

Proyecto de ley de lucha contra el spam

La CT-Spam promovió un estudio comparado de leyes mundiales sobre la lucha contra el *spam,* analizando las propuestas

---

18 De acuerdo con el Art. 6º del Código de Defensa del Consumidor:
"Son derechos básicos del consumidor:
(...) II – educación y divulgación sobre el consumo adecuado de los productos y servicios, garantizadas la libertad de elección y la igualdad en las contrataciones;
III – información adecuada y clara sobre los diferentes productos y servicios, con especificación correcta de su cantidad, características, composición, calidad, tributos incidentes y precio, así como sobre los riesgos que presenten (...)". (Brasil, Ley 8078 de 11/09/90).

19 Henrique Faulhaber en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 1 de enero de 2014.

legislativas en trámite en el Congreso Nacional que abordaban el tema en la esfera penal. Al final del mencionado estudio se presentó una propuesta de redacción para un eventual proyecto de ley. Elaborado por Ronaldo Lemos, Danilo Doneda, Carlos Affonso Pereira de Souza y Carolina Rossini en 2007, este estudio representó una de las primeras investigaciones sobre los desafíos jurídicos y regulatorios que se podrían enfrentar para implantar una política eficaz de lucha contra el *spam* en el país[20].

El trabajo propuso los siguientes criterios[21] para una técnica legislativa de lucha contra el *spam*:

> **1.** Adopción del sistema llamado opt-in (inclusión voluntaria) como modelo para la clasificación de los mensajes electrónicos en Internet —de esta forma no se legitima la práctica de envío de spam como medio de comunicación con los consumidores en Internet—. Antes del envío de la publicidad es necesario que exista una relación de consumo y que el consumidor opte por recibir publicidad del proveedor vía e-mail. Además, establecer el momento legítimo de envío permite una neutralidad tecnológica en relación con el medio por el cual se envía la publicidad: correo electrónico, telefonía celular y otras formas de comunicación electrónica;
>
> **2**. Posibilidad de tutela colectiva de los derechos para la lucha contra el spam, considerado el carácter difuso del daño que provoca esta práctica;
>
> **3.**Explicitación de parámetros para que el juez estime el daño en el contexto de una acción judicial relacionada con el spam. Ante definiciones subjetivas y la dificultad de valoración del daño en casos de responsabilidad, el proyecto desarrollado buscó incorporar mecanismos de ayuda para la toma de decisiones por parte del magistrado ante situaciones técnicas para la estimación del daño;
>
> **4.**Ampliación del delito de falsedad ideológica para abarcar los mensajes enviados a través de redes digitales o analógicas con la finalidad de obtener ventaja económica o causar daño.

El objetivo del trabajo no fue criminalizar la actividad de envío de

---

20 CGI.br. R.Lemos, D.Doneda, C.A. Souza, C. Rossini. Estudo sobre a Regulamentação Juridica do Spam no Brasil. Publicado originalmente en abril de 2007. Disponible en <http://www.cgi.br/media/comissoes/ct-spam-EstudoSpamCGIFGVversaofinal.pdf>. Consultado el 12 de octubre de 2013.

21 Idem, p. 62

publicidad al consumidor, sino desarrollar criterios legítimos compatibles con la defensa del consumidor y el desarrollo económico. Este trabajo subsidió la coordinación realizada en 2009 por Jaime Wagner, exconsejero de CGI.br, para desarrollar un código de conducta para el envío de publicidad electrónica, según lo descrito anteriormente. Consecuentemente, la autorregulación del *e-mail marketing* legitima esta forma de comunicación con el consumidor, creando límites relacionados con la privacidad y la conveniencia del consumidor.

Los proveedores de publicidad directa se mostraron muy resistentes y críticos con la propuesta de reglamentación desarrollada por la Comisión de Lucha contra el *Spam*. Por este motivo, los proveedores fueron incluidos en el debate de forma que fuera posible llegar a un consenso sobre una propuesta sectorial que no fuese perjudicial desde el punto de vista comercial y que satisficiera los estándares de defensa del consumidor.

> Por lo tanto, creamos una forma de tratar el problema que no fuese a través de la ley, sino mediante un consenso entre los actores involucrados en esta actividad.
>
> En lugar de intentar caracterizar qué es spam como venían haciendo los proyectos de ley, optamos por definir qué sería el e-mail marketing legítimo. Todo lo que quedara fuera sería spam y podría ser afectado por la ley que se aprobara. Incluso porque definir qué es spam es muy complejo."[22]

Es importante reconocer cómo la gestión del puerto 25 se relaciona con las actividades hasta aquí comentadas, ya que el esfuerzo de coordinación que representa está íntimamente relacionado con una secuencia de actividades realizadas en otras áreas, ya sea en la técnica jurídico-legislativa o bien en la coordinación sectorial. Sin entrar en este momento en un debate sobre la eventual preponderancia de los aspectos jurídicos sobre los tecnológicos o viceversa, para la construcción del mosaico de actividades desempeñadas por la CT-Spam es relevante percibir cómo el carácter multidisciplinario aparece de forma evidente en la conducción de medidas de ambos tipos.

Por más tecnológica que pueda parecer la gestión del puerto 25, ciertas cuestiones de naturaleza jurídica se impusieron notoriamente como elementos a ser considerados para su implementación. Aspectos contractuales y la defensa del consumidor son solo algunas

22 Jaime Wagner en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 11 de marzo de 2014.

de estas cuestiones. Por otro lado, comprender que la CT-Spam ya trabajaba con actividades de naturaleza jurídica para luchar contra el *spam* ayuda en la percepción de este carácter multidisciplinario.

Honeypots y spampots

Desde 2003, el Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil (CERT.br) mantenido por el Comité Gestor de Internet lleva adelante el proyecto Honeypots Distribuidos, que tiene por objetivo suministrar métricas e información sobre el abuso de redes y cuenta con cerca de 50 equipos distribuidos por la red brasileña. A través de equipos que simulan ciertos sistemas operativos y servicios de una computadora, permite ver cómo podrían ser abusados (por ejemplo, detección de intentos de robo de contraseñas)[23].

A partir del uso de esta técnica para la construcción de métricas sobre el abuso de redes, en 2006 se crearon los *spampots*, un tipo de especialización del sistema de *honeypots* dedicado al análisis específico de abusos promovidos por los *spammers*[24].

Para ello se instalaron diez *honeypots,* es decir, diez equipos configurados para simular computadoras de usuarios residenciales reales propensos a sufrir un abuso.

Voluntarios para medición en banda ancha

Para un centro especializado en incidentes de seguridad, el problema del *spam* era una cuestión estrechamente relacionada con la seguridad de la red. Sin importar el contenido circulado de forma no solicitada, el *spam* siempre será, antes que todo, un abuso de la estructura de Internet brasileña.

Con la cooperación de diez voluntarios, cinco de ellos parte de los propios consejeros del CGI.br, se instalaron sensores en el domicilio de usuarios de los cinco principales operadores brasileños. Además de capturar *spam*, estos sensores también detectaron la inestabilidad y baja calidad de la banda ancha suministrada. Tan grande era el consumo de ancho de banda de subida de los *spammers* que incluso los

---

23 CERT.br, Distributed Honeypots Project. Disponible en <http://honeytarg.cert.br/honeypots/index-po.html>. Consultado el 12 de octubre de 2013.

24 CERT.br, Spam Post Project. Disponible en <http://honeytarg.cert.br/spampots/>. Consultado el 12 de octubre de 2013.

servidores del propio CERT.br no lograban colectar datos[25].

Un *spammer* barre la red buscando puertos y *proxies* abiertos, donde hace diversas pruebas para averiguar si determinada computadora está dispuesta a realizar ciertas acciones, como por ejemplo encaminar tráfico de red. De esta forma, los *honeypots* enviaban una respuesta positiva al *spammer* indicando que su acción había ocurrido de forma válida y el *spammer* pasaba a enviar *spam* a los *honeypots*.

Durante 466 días, se recogieron 524.585.779 mensajes de correo electrónico provenientes de 165 países diferentes, destinados a más de cuatro mil millones de usuarios. Los dos principales destinos finales de estos mensajes ni siquiera eran Brasil, sino Taiwan y China. Un estudio de la Universidad de Minas Gerais (UFMG) encargado por la CT-*Spam* demostró que un 90% del *spam* recogido y que salió de Brasil tenía contenido en chino[26].

Por lo tanto, se concluyó que el *spam* y los *spammers* no eran brasileños, sino que eran computadoras de usuarios brasileños que estaban siendo sistemáticamente abusadas por *spammers* internacionales, comprometiendo el disfrute del servicio y la experiencia de conexión[27].

El trabajo de desarrollo de métricas promovido por el equipo del CERT.br —especialmente por Klaus Steding-Jessen y Cristine Hoepers— con el apoyo de Marcelo Fernandes, entonces consejero del CGI.br, fue fundamental para convencer a los actores que muchas veces juzgaban a los números y la información acerca del *spam* como simples manipulaciones de la industria del software *antivirus* y *antispam*.

A partir de todas las experiencias narradas en los párrafos precedentes, se decidió avanzar con la gestión del puerto 25 como la medida más eficiente para transformar la situación en la cual el país se encontraba en los rankings de envío de *spam*. El tema a seguir explora cómo se dio esta actividad.

---

25 Entrevista de Cristine Hoepers y Klaus Jessen concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

26 Entrevista de Cristine Hoepers y Klaus Steding-Jessen concedida al proyecto Memoria de lucha contra el spam en Brasil el 25 de septiembre de 2013.

27 Nic.br. Taiwan e China lideram ataques de spams ao Brasil. Disponible em <http://nic.br/noticia/na-midia/taiwan-e-china-lideram-ataques-de-spams-ao-brasil/>. Consultado el 12 de octubre de 2013. Según el comunicado de divulgación de los datos de la iniciativa SpamPots publicado el 11 de julio de 2007: "De acuerdo con los resultados preliminares, la lista de los diez países que más abusan de Brasil es liderada por Taiwan, con 281.601.310 de e-mails capturados (el 76% de las ocurrencias). China aparece en segundo lugar, con 58.912.303 de e-mails (el 16% del volumen analizado). Estados Unidos, Canadá, Corea y Japón, Hong Kong, Alemania, Brasil y Panamá completan el listado y juntos suman menos del 8%."

2. Gestión del puerto 25

El puerto 25 es el puerto estándar del protocolo TCP/IP utilizado para envíos de correos electrónicos entre servidores de e-mail que utilizan el protocolo SMTP (*Simple Mail Transfer Protocol*). El puerto 25 es un puerto implementado por una conexión lógica para transmisión de datos. Un puerto físico que transmite datos, por ejemplo, es la parte del dispositivo del usuario que se conecta a un cable de red. Conforme explica Rubens Kuhl:

> "El puerto 25 se utiliza para comunicación entre servidores de correo en Internet. Cuando un usuario envía un e-mail en Internet no es necesario que utilice el puerto 25. Después que el mensaje es enviado, el servidor al cual se envió utiliza el puerto 25 para entregarlo al servidor de destino."[28]

Dado que era un "camino abierto"[29], el puerto 25 estaba sujeto a cualquier tipo de abuso. En esta situación se considera un "abuso" la utilización de computadoras de usuarios brasileños, sin su conocimiento, para enviar mensajes de correo electrónico no solicitados que llegaban de remitentes extranjeros y en cantidades masivas a usuarios en todo el mundo de forma no identificable.

Los Principios para Gobernanza y Uso de Internet en Brasil[30] indican que la red debe ser libre, abierta e inimputable. Por lo tanto, la limitación del uso de funcionalidades abiertas se debe justificar no solo en base a requisitos técnicos sino también por la identificación objetiva de los abusos perpetrados que limitan la utilización de la red, su buen funcionamiento y el libre disfrute por parte de los usuarios. En palabras de Demi Getschko:

> "No sabíamos si había algún abuso o no. Empezamos a investigar qué sucedía con el *spam* brasileño. (...) El e-mail llegaba a la computadora y era reenviado incontables veces, dependiendo de la lista de destinatarios que tenía el mensaje. Vimos que el e-mail no era nacional: no tenía origen

28 Rubens Kuhl en entrevista concedida al proyecto Memoria de lucha contra el spam en Brasil el 17 de enero de 2014.

29 Demi Getschko en entrevista concedida al proyecto Memoria de lucha contra el spam en Brasil el 25 de septiembre de 2013.

30 CGI.br Resolução CGI.br/RES/2009/003/P Princípios para a Governaça eUso da Internet no Brasil, disponible em <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Consultado el 12 de octubre de 2013.

nacional ni destino nacional. Funcionábamos solo como reflector, por lo que el procedimiento más sencillo era cambiar ese puerto por uno que tuviese una contraseña."[31]

El proyecto SpamPots permitió comprobar el abuso y el CERT.br identificó la tecnología y la política más eficientes. Luego, para revertir este cuadro, la CT-Spam optó por la gestión del puerto 25. Esta iniciativa marcó los trabajos de la Comisión y significó un importante *leading case* para Internet en Brasil en términos de coordinación de múltiples partes interesadas.

Según lo explica Klaus Steding Jessen, gerente técnico del CERT.br y uno de los ingenieros responsables por la implementación de los *spampots*:

> "(...) algo que quedó claro como el agua. Pese a que varios puertos de proxy estaban siendo abusados, todos tenían un mismo objetivo: salir con destino al puerto 25. Esto es lo que el *spammer* quería. Entraba a través de un *malware*, de una mala configuración del e-mail del usuario. Intentaba de todo, pero todos tenían el mismo destino: el puerto 25. Allá donde había un servidor de correo electrónico, allí es donde efectivamente se dirigía el *spammer*. Esto fue algo grandioso de mostrar: en este caso la gestión del puerto 25 sería devastadora.
>
> Al comienzo, algunos operadores dijeron que sería mejor bloquear las conexiones entrantes con destino al proxy, pero nosotros lo desaconsejamos diciendo "¡Miren, hoy hay 30!". Y a veces el *malware* puede ser colocado en cualquiera, pero el destino del *spam* tiene que ser el puerto 25. Caso contrario, no logra interactuar con un servidor de *e-mail* en este puerto, que es estándar del SMTP[32].

El bloqueo del puerto 25 para usuarios residenciales ya era una práctica incentivada por el IETF (Internet Engineering Task Force), la organización internacional responsable por el desarrollo de estándares para diversos aspectos del funcionamiento de la red a través de sus RFC (Requests for Comments). Pese a que la adhesión es voluntaria, estos estándares son reconocidos por toda la comunidad internacional como los estándares de funcionamiento de la red, ya que se construyen

---

31 Demi Getschko en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

32 Klaus Stending-Jessen en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013. IETF. RFC 6409. Disponible en: <http://tools.ietf.org/htmlrfc6409>. Consultada el 14 de marzo de 2014.

a través del consenso entre los agentes participantes.

La RFC referente a la entrega de mensajes de correo electrónico presentaba la división de las tareas de entrega y transferencia de correo electrónico como una mejor técnica de administración efectiva de la red, identificando los principales beneficios: (i) disminución del envío masivo de e-mails no solicitados y (ii) inclusión de aspectos de seguridad y privacidad con la exigencia de autenticación:

> *Implement security policies and guard against unauthorized mail relaying or injection of unsolicited bulk mail; implement authenticated submission, including off-site submission by authorized users such as travelers; separate the relevant software code differences, thereby making each code base more straightforward and allowing for different programs for relay and submission; detect configuration problems with a site's mail clients; provide a basis for adding enhanced submission services*[33].

De forma simplificada, se puede afirmar que en todo servicio de correo electrónico existen dos funcionalidades principales: (i) el envío en sí, que involucra el envío del mensaje por el cliente al servidor de correo electrónico y (ii) el transporte, es decir, el acto de un servidor de correo electrónico de comunicarse con otro para trasmitir el mensaje enviado. Por lo tanto, la gestión del puerto 25 representa una clara distinción entre estas funcionalidades.

A partir de esta gestión, es decir, a partir de la distinción entre las funcionalidades del servicio de *e-mail*, el usuario residencial solo puede enviar correo electrónico a un servidor de *e-mail* y no directamente a otros usuarios, ya que la actividad de transporte debe ser realizada por los servidores.

Además, para los usuarios residenciales el envío queda bloqueado en el puerto 25, pasando a ser desempeñado por un puerto exclusivo para este fin (el 587/TCP), con autenticación, dejando el transporte típico del puerto 25 solo para entidades competentes. En la gestión del puerto 25 hay un control y un deber impuestos a los usuarios de redes residenciales que no se manifiestan por códigos jurídicos sino por el diseño de la arquitectura de la red.

---

33 - Implementar políticas de seguridad y proteger contra la retransmisión no autorizada de e-mail o la inyección de e-mail masivo no solicitado; implementar envío autenticado, incluyendo envío off-site por parte de usuarios autorizados como viajeros; separar las diferencias de código de software relevantes, haciendo así que cada base de código sea más directa y permitiendo el uso de diferentes programas para relé y envío; detectar problemas de configuración en los clientes de e-mail de un sitio; proveer una base para la adición de servicios de envío mejorados.

Por tratarse de un aspecto técnico de gestión de la red, la CT-*Spam* se acercó a quienes tenían la capacidad técnica para bloquear el puerto 25 y migrar los usuarios al puerto 587: los operadores de telecomunicaciones que prestan servicios de conexión a Internet y los proveedores de *e-mail*. Como aclaran Cristine Hoepers y Klaus Jessen:

> "Era una medida técnica, una acción compleja. Actualmente ellos [los operadores de servicios de comunicación multimedia] implementan diversos filtros en sus estructuras; ya participamos en diversas reuniones.
>
> Nuestra visión, tal vez en general, es que existen diversas buenas prácticas de red que ellos han adoptado y que eran la misma implementación de una buena práctica: impedir que las computadoras de los usuarios residenciales fuesen infectadas y enviasen *spam*. Imaginamos que con media docena de reuniones con el personal más técnico quedaría claro que esto implicaba un desperdicio de los recursos de red y del ancho de banda, algo malo para ellos, y harían que se sumasen a la iniciativa. Pero ocurrió todo lo contrario, inclusive cuando tratamos con el personal más técnico."[34]

La coordinación solo entre los actores técnicos no cumplió con los objetivos esperados por la CT-Spam. Se percibió cierto temor, principalmente por parte de los actores afectados por las reglamentaciones en el área de las telecomunicaciones, entre ellos los proveedores de servicios de comunicación multimedia[35], independientemente de ser una implementación técnica internacionalmente aceptable y con una RFC específica del IETF. Esto hizo con que algunos actores responsables por la coordinación sugirieran que a la negociación de la gestión del puerto 25 ingresaran los dirigentes de las empresas en lugar de los técnicos.

El fracaso de las articulaciones iniciales y de las recomendaciones técnicas hizo que en 2009 Brasil recibiese el título de "Rey del

---

34 Cristine Hoepers y Klaus Steding-Jessen en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

35 Servicio de Comunicación Multimedia es la expresión utilizada por ANATEL (Agencia Nacional de Telecomunicaciones) para designar la prestación de servicios de "oferta de capacidad de transmisión, emisión y recepción de informaciones multimedia, permitiendo inclusive la provisión de conexión a Internet", de acuerdo con el art. 3º de la Resolución nº 614/2013 de la ANATEL. La relación entre el servicio de comunicación multimedia, que es un servicio de telecomunicaciones, y el servicio de conexión de Internet, que es un servicio de valor agregado, se explicará con mayor detalle en el Capítulo 4.

Spam" en la prensa internacional[36], ya que figuraba en el primer puesto en varias listas mundiales de averiguación sobre *spam*, incluso cuando la solución del problema ya había sido identificada. La información causó conmoción y permitió que, de hecho, las actividades de la CT-Spam fueran impulsadas.

En 2009 también ocurrieron otros dos hechos relevantes para la CT-Spam. Primero, en la composición representativa del CGI.br, el representante de los operadores de telecomunicaciones, que hasta ese entonces era una persona con una gran especialización en el sector de la TV por cable, fue reemplazado luego de la elección por Eduardo Levy, quien aceleró la articulación con los proveedores de servicios de comunicación multimedia. Además, en 2009 se inició el debate legislativo que llevó a la creación de la ley nº 12.965/2014, el Marco Civil de Internet en Brasil. Entre otras cosas, esta ley incluía un artículo específico sobre la reglamentación de la neutralidad de la red en el país. Esto implicó la incorporación de representantes jurídicos de las empresas en el debate para aclarar las dudas sobre la neutralidad de la red y de qué forma se relacionaba con las actividades de gestión del puerto 25.

La presencia de diferentes actores sectoriales en las reuniones de la CT-Spam fue algo natural para el Comité Gestor de Internet en Brasil, algo intrínseco a su forma de actuación. Como se puede comprobar con la lucha contra el *spam*, la gestión de los recursos de red implica un abordaje multisectorial. El desarrollo de soluciones concretas y efectivas depende de la cooperación entre los actores esenciales, poseedores de conocimientos y competencias críticos para la puesta en funcionamiento de la medida.

En la implementación de la gestión del puerto 25, la separación de las funcionalidades de envío y transporte de mensajes exigió un acuerdo entre los operadores de telecomunicaciones, los provee-

---

36 Responsable por el envío de 7.7 billones de mensajes de spam, de acuerdo con el reportaje de la revista Forbes, con información de la empresa Cisco. "El auge del spam en Brasil no es ningún misterio. Según Patrick Peterson, investigador en seguridad de Cisco, el país está sufriendo la misma epidemia de basura electrónica que experimentaron otras naciones en rápido crecimiento al conectarse a Internet. (...) Ni Brasil ni India son responsables directos por la cantidad de spam emanada de los dos países con el surgimiento de sus economías digitales. Ambos países son propensos a ser vulnerados por criminales virtuales globales que ven en los dominios baratos y el gran número de computadoras personales desprotegidas una oportunidad de canalizar basura electrónica hacia todo el mundo". FORBES. Brazil: The New Spam King. Disponible en <http://www.forbes.com/2009/12/08/spam-china-cisco-technology-cio-network-brazil.html>. Consultado el 4 de octubre de 2013.

dores de servicios de comunicación multimedia[37] (Internet banda ancha), los proveedores de servicios de Internet (específicamente los proveedores de alojamiento y correo electrónico, además de la actuación de ANATEL en su rol de agencia reguladora de los operadores de telecomunicaciones, el Ministerio de Justicia a través del Departamento de Protección y Defensa del Consumidor (DPDC), y las asociaciones civiles integrantes del sistema nacional de defensa del consumidor. Todo ello sin dejar de mencionar el papel del sector técnico en el proceso inicial de recolección de datos y de los investigadores del área en la construcción de métricas, además de su trabajo de capacitación y educación durante todo el proceso.

Pese a la aparente facilidad de la cuestión técnica para los técnicos involucrados, en especial dada la experiencia internacional en la implementación autónoma por los proveedores de *e-mail*, la realidad brasileña hacía que la solución fuese más compleja. Los operadores de telecomunicaciones de SCM, primeros actores a ser abordados por la CT-Spam, no llevaban control, por ejemplo, de cuántos de sus usuarios utilizaban servicios de *webmail* o programas como Outlook o Thunderbird. Es decir, cada operador de SCM poseía múltiples proveedores e *e-mails* en su estructura.

Por este motivo, la coordinación de todos los agentes involucrados demostró ser una estrategia crucial para la realización de la gestión del puerto 25. Era necesario oír a todos los interesados y lograr que acompañasen el proceso paso a paso para así evitar que un número significativo de usuarios de Internet en Brasil se viesen impedidos de enviar mensajes de correo electrónico justamente por no haber alertado a las partes interesadas sobre el cierre del puerto 25 y la necesidad de reconfiguración para el envío de mensajes. En este sentido, primero fue necesario migrar los proveedores y los usuarios a un puerto con autenticación para después realizar el efectivo bloqueo del puerto 25. Por lo tanto, los operadores de telecomunicaciones no podrían actuar antes que los proveedores de *e-mail*.

La coordinación de los proveedores de servicios de comunicación multimedia, un sector regulado, hizo que fuera ser necesario incluir al gobierno en la legitimación de la colaboración y en 2010 la CT-Spam

37 En Brasil, según la Ley General de Telecomunicaciones y la Norma del Ministerio de Comunicaciones nº 004 de 1995, el Servicio de Conexión a Internet (SCI) es un Servicio de Valor Agregado (SVA) que no depende de una concesión, permiso o autorización de Anatel, por lo que el proveedor de SVA es un usuario de un servicio de telecomunicaciones que le da soporte, en este caso, el Servicio de Comunicación Multimedia (SCM). Esta relación se explicará luego en el Capítulo 4.

firmó un acuerdo de cooperación con la Agencia Nacional de Telecomunicaciones (Anatel) para implementar la recomendación de la gestión del puerto 25. El acuerdo preveía la adopción de la medida por parte de los operadores después de la migración del 90% de la base de usuarios de los proveedores de servicios de *e-mail*.

El oficio nº 195/2010-PR-Anatel sobre la cooperación con las actividades de lucha contra el *spam* de CGI.br hizo que los operadores se comprometiesen con un cronograma de adopción, siguiendo a los proveedores de servicios de Internet. Como veremos a continuación, el documento de cooperación firmado con Anatel desempeñó un papel crucial en la legitimación de las actividades de la Comisión y en el logro de un compromiso efectivo por parte de los operadores de telecomunicaciones.

En 2011, el Departamento de Defensa y Protección al Consumidor del Ministerio de Justicia (DPDC/MJ)[38] fue otro órgano del gobierno incluido en el debate, por exigencia tanto de los operadores de telecomunicaciones como de los servidores de *e-mails*, que temían una interpretación negativa de la implementación de la medida por parte del Sistema Nacional de Defensa del Consumidor[39].

Luego el DPDC/MJ expidió una Nota Técnica (NT nº 65 CGSC/DPDC/SDE[40]) sobre las consecuencias y beneficios de la gestión del puerto 25 para el consumidor y la aclaración para los Procons de todo Brasil. Habiendo eventualmente quejas sobre la conexión a Internet, se debería verificar si el problema en la conexión a Internet estaba relacionado con el bloqueo del puerto 25. Consultado el operador y existiendo una prerrogativa legítima para el uso del puerto 25 para ese consumidor en particular, el puerto podría permanecer abierto para atender esta necesidad concreta y legítima.

---

38 En aquella época, el Departamento de Defensa y Protección al Consumidor formaba parte de la Secretaría de Defensa Económica. A partir de 2012, el Departamento pasó a formar parte de la Secretaría Nacional del Consumidor, creada por el Decreto nº 7.738 del 28 de mayo de 2012.

39 El Sistema Nacional de Defensa del Consumidor abarca los Procons (estaduales y municipales), el Ministerio Público, la Defensoría Pública y entidades civiles de defensa del consumidor, que actúan de forma articulada e integrada con la Secretaría Nacional del Consumidor.

40 Antispam.br. Nota Técnica nº 65/CGSC/DPDC/SDE disponible en <http://www.antispam.br/porta25/brasil/notatecnica65.pdf>. Consultada el 5 de marzo de 2014.

El entendimiento del DPDC/MJ[41], abarcado por todo el Sistema Nacional de Defensa del Consumidor, se reveló de crucial relevancia para conferir seguridad ante el cumplimiento de las normas de defensa del consumidor tanto para los operadores de telecomunicaciones como para servidores de *e-mail*.

Con el Acuerdo para la Implementación de la Gestión del Puerto 25 y la Nota Técnica arriba citados, el camino estaba abierto para la implementación de esta iniciativa de lucha contra el *spam* en Brasil. Los entrevistados para este estudio destacaron que la elaboración de los mencionados documentos y la coordinación desempeñada por el CGI.br fueron fundamentales para que los diversos interesados tuviesen seguridad para desarrollar las actividades necesarias para la gestión del puerto 25.

En este sentido, es importante destacar que tanto Anatel como el Ministerio de Justicia desempeñaron papeles extremamente relevantes para ofrecer el confort jurídico necesario para que las partes interesadas y sometidas a su área de actuación pudiesen proceder con las actividades demandadas. En el CGI.br recayó entonces la misión de conectar los sectores involucrados, asegurando el cumplimiento de las fases del proceso y proveyendo un foro de discusión y acompañamiento constante del proceso de gestión del puerto 25 ya implementado.

Al indagar a los entrevistados para este estudio si existía alguna otra entidad que pudiese haber coordinado la iniciativa de gestión del puerto 25 en Brasil, se puede destacar que en muchas entrevistas se mencionó el papel determinante, tanto de Anatel como del MJ, en el convencimiento de las empresas, asociaciones y demás actores pertinentes a su sector específico de actuación. Pero los entrevistados estuvieron de acuerdo en que la existencia de una instancia de múltiples partes interesadas como el CGI.br fue de inestimable valor para que el proceso pudiese ser conducido de modo que las diferentes partes involucradas pudiesen entrar en contacto con la realidad de

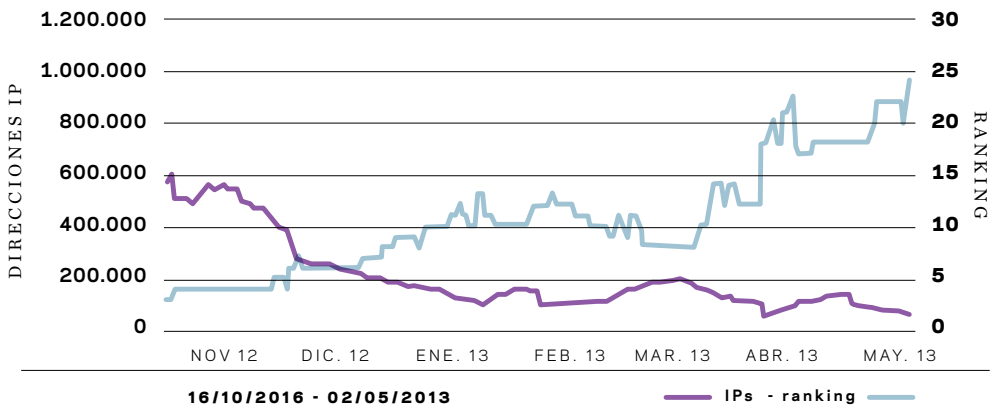
41 La CT-Spam no contactó primero al DPDC/MJ, pero sí a los Procons y a las entidades civiles, que exigieron el entendimiento del Departamento sobre el asunto: "La CT-Spam busco órganos de defensa del consumidor y nos llegó una demanda para que nos manifestásemos al respecto de la viabilidad o no de proceder con la gestión del puerto 25 y verificásemos de facto los potenciales impactos sobre los consumidores, si había realmente algo que temer. Fue en ese momento que llegó a nuestro conocimiento todo el trabajo realizado por la CT-Spam, todas las cuestiones técnicas y también las ingenierías de implementación relacionadas con la gestión del puerto 25". Danilo Doneda, Coordinador General de Estudios y Monitoreo de Mercados del DPDC/MJ en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 27 de septiembre de 2013.

otros agentes y, en el debate sobre sus diversos intereses y preocupaciones, tomar decisiones estratégicas que ayudasen a alcanzar la meta pretendida por todos: la reducción del volumen de *spam* enviado desde computadoras de Brasil mediante la gestión del puerto 25.

La implementación de la gestión del puerto 25 fue responsable —indudablemente entre los actores involucrados— por la drástica reducción del volumen de *spam* enviado por computadoras brasileñas. El país abandonó la posición de liderazgo que ocupaba en 2009 en el ranking de la Composite Blocking List para pasar al puesto 25 en 2013, como se puede ver en el gráfico aquí debajo[42].

BRASIL (BR) EN LA CBL

IPs Listados y evolució9n en el ranking



fuente: CBL / by Highcharts.com

Este resultado se logró a través de debates en diversas reuniones técnicas, la sensibilización de órganos representativos de los sectores interesados sobre la relevancia de la medida, la realización de una amplia campaña de información al público en general y un acompañamiento cuidadoso del proceso de implementación e inclusión de las instancias gubernamentales competentes. A continuación se destacarán aspectos regulatorios y jurídicos relevantes de esta iniciativa, para luego analizar las peculiaridades identificadas y los desafíos que enfrenta por la gestión de múltiples partes interesadas en los modelos adoptados por el CGI.br.

42 CERT.br. Port 25 Management in Brazil: Overview and Results, disponible en <http://www.cert.br/docs/palestras/certbr-lac-csirts-medellin2013-1.pdf>. Consultado el 12 de octubre de 2013.

3 • Cuestiones jurídico-regulatorias

La dificultad de la articulación sectorial no se dio por cuestiones que afectaban a los individuos o con problemas de convergencia de intereses. Todos los actores involucrados estaban convencidos de que la implementación de la medida era de interés público. Lo que para todos resultaba controvertido eran los problemas jurídicos y regulatorios que se debían enfrentar. De esta forma, la articulación sectorial resultó ser un recurso crítico para aportar experiencia a los agentes gubernamentales y privados ante cuestiones relacionadas con tecnologías y prácticas sociales emergentes.

Uno de los primeros obstáculos jurídicos comentados en las reuniones de la CT-Spam fue la posibilidad de que la gestión del puerto 25 recibiera oposición bajo el argumento de que hería la libertad comercial. Con el desarrollo de los trabajos de la Comisión se comprobó que la medida sugerida sería la migración del tráfico de *e-mails* al puerto 587, que requiere autenticación y mucho menos la limitación de una liberalidad. Además de ofrecer mayor seguridad (requiere el uso de contraseña), esta autenticación desestimularía el envío indiscriminado de *spam,* ayudando así a reducir el volumen de este tipo de mensajes enviado desde computadoras brasileñas hacia la Internet global. Esta medida no afectaba el envío de mensajes ni imponía ninguna limitación indebida[43].

Los perjuicios a los consumidores por causa del uso indebido del puerto 25 para enviar *spam* todavía se podían detectar en diversos frentes. Para comenzar, profundizando en la cuestión de su vulnerabilidad técnica, los consumidores raramente atribuían el pobre desempeño de sus computadoras y la mala calidad de la banda ancha contratada a un abuso de sus dispositivos por parte de los *spammers*. Aunque esta era la razón del bajo desempeño de su computadora, el consumidor tendía a relacionarlo con problemas de orden general de la red y frecuentemente preferían incurrir en costos adicionales de mantenimiento o cambio de computadora, software y contratación de mayor velocidad de conexión. Por lo tanto, el *spam* primero es percibido por el usuario como un costo en

43 Entrevista de Cristine Hoepers y Klaus Steding-Jessen al proyecto Memoria de la lucha contra el spam en Brasil, concedida el 25 de septiembre de 2013.

su tiempo, no como algo que afecta toda su experiencia de conexión.

La banda ancha es un recurso asimétrico, lo que significa que un usuario posee capacidades de bajada y subida limitadas. Se percibió que los *spammer*s internacionales consumían toda la capacidad de subida de los usuarios brasileños, es decir, todo el tráfico de salida, haciendo imposible una conexión estable e impidiendo que el usuario enviase, por ejemplo, contenido a las redes sociales[44].

El Ministerio de Justicia, a través de su departamento especializado en defensa del consumidor, consideró que la implementación del puerto 25 era beneficiosa para el consumidor, ya que no solo existe información previa sobre el proceso, sino que también se garantiza un vehículo de comunicación para el saneamiento de cuestiones técnicas acerca de la implementación. Fueron identificados y considerados los riesgos para los consumidores que usasen clientes de *e-mails* desactualizados u otros medios de comunicación con la red que dependerían del puerto 25. Un análisis de mercado reveló que el número de estos consumidores era francamente residual con relación a la masa que no sería afectada por la gestión del referido puerto[45].

De esta forma, el DPDC/MJ consideró que el número de personas perjudicadas sería considerablemente menor en comparación con la cantidad total de consumidores que se beneficiarían de la medida. Además, al ser alertados sobre un eventual problema, los consumidores perjudicados tendrían la posibilidad de remediar la situación a través del contacto con su proveedor de Internet o buscando orientación con los órganos de defensa del consumidor.

Conforme explica Danilo Doneda:

> El Código de Defensa del Consumidor incluye un artículo que suele dejarse de lado: la defensa del consumidor tiene que adecuarse, adaptarse al desarrollo tecnológico. Y fue justamente este artículo el que ofreció una fundamentación casi ontológica para nuestra Nota Técnica en el sentido de que permitiríamos este cambio técnico, la gestión del puerto 25. Aunque pudiese alcanzar a un número pequeño de consumidores, era esencial para la creación de un ambiente más favorable para todos. Los

44 Entrevista de Cristine Hoepers y Klaus Steding-Jessen concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

45 Antispam.br. Nota Técnica 65-CGSC/DPDC/SDE/MJ. Disponible en <http://www.antispam.br/porta25/brasil/notatecnica65.pdf>. Consultado el 13 de octubre de 2013.

> eventuales perjuicios para algunos consumidores —que en el fondo no serían perjudicados en nada dado que podrían revertir esta situación— eran francamente un problema fácilmente superable por los beneficios que el bloqueo del puerto 25 podría representar para la generalidad de los consumidores[46].

Los departamentos jurídicos de algunos proveedores todavía cuestionaban eventuales impedimentos contractuales para la gestión del puerto 25. Este argumento fue descartado después de que la CT-Spam realizara un análisis detallado de cada contrato de servicio y concluyera que los contratos permitían este tipo de gestión, siempre que fuera notificado el consumidor.

Otros argumentos comentados durante los trabajos de la CT-Spam fueron los costos de implementación para los operadores de la gestión del puerto 25 y la posibilidad de eventuales procesos administrativos contra los mismos por incumplimiento de las reglamentaciones. Después de la participación de Anatel, con la firma del Acuerdo de Cooperación este argumento perdió sentido, ya que el propio órgano regulador apoyó la iniciativa de cerrar el puerto 25. En lo que se refiere a los factores económicos, la gestión del puerto 25 permitió incluso que los operadores ahorraran ancho de banda, que anteriormente se utilizaba de forma injustificada para el envío de *spam*[47].

Consideraciones sobre la neutralidad de la red

Para lograr reducir sustancialmente el volumen de *spam* enviado por las computadoras en Brasil, la gestión del puerto 25 coordinó esfuerzos para el cierre del referido puerto. Esta medida, que alcanzó de forma evidente los objetivos buscados, también trajo una reflexión importante para la maduración del debate sobre el llamado principio de neutralidad de la red en el país.

El debate sobre el principio de neutralidad de la red ha ocupado un puesto de destaque en los foros internacionales y nacionales sobre gobernanza y regulación de Internet, por lo menos en los últimos diez años, con interés creciente tanto por parte del público especializado

46 Danilo Doneda en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 27 de septiembre de 2013.

47 Eduardo Parajo, Consejero del CGI.br y Director de ABRANET, en entrevista concedida al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

como de los formadores de opinión y de la prensa en general.

En una síntesis bastante citada, Carlos A. Afonso, consejero de CGI.br, definió el principio de neutralidad de la red como el precepto que determina que "todos los datagramas son iguales ante la red"[48].

De esta forma, la regla es que el tráfico de datos en la red no debe ser discriminado, evitando así que los operadores puedan dar preferencia a determinados tráficos de datos en detrimento de otros por los motivos más diversos. La regla en sí busca combatir la lucha contra las discriminaciones que podrían suceder en base a factores comerciales (privilegiar un contenido propio y al mismo tiempo bloquear o perjudicar la calidad del acceso al contenido del competidor) o incluso políticos, religiosos o culturales (prohibiendo la circulación en la red de un tipo de discurso).

El CGI.br eligió la neutralidad como uno de sus diez Principios para la Gobernanza y Uso de Internet en Brasil. Este principio fue previsto de la siguiente forma:

> **"6.** Neutralidad de la red. Los filtros o privilegios de tráfico deben respetar criterios técnicos y éticos, no siendo admisibles motivos políticos, comerciales, religiosos, culturales o cualquier otra forma de discriminación o favoritismo."[49]

Muchos son los expertos que defienden el principio de neutralidad de la red como un elemento fundamental para la conservación de Internet como un espacio abierto e innovador, garantizando la potenciación de libertades y transformaciones en la forma de comunicación, el acceso al conocimiento, la formación de la identidad de los individuos y grupos, además de modelos de negocio para empresas en las más diversas áreas de actividad.

Si bien por un lado parece haber consenso entre gran parte de los interesados en el debate sobre la importancia de este principio, la necesidad de intervenciones puntuales que puedan generar excepciones a la regla de la neutralidad ha generado debates en todo el mundo.

Lo opuesto al principio de neutralidad sería la liberación, de manera que todos los intermediarios que hacen posible el tráfico

---

48 CGI.br. C. A. Afonso, Todos os Datagramas são Iguais Perante a Rede! Disponible en <http://www.cgi.br/publicacao/todos-os-datagramas-sao-iguais-perante-a-rede/>. Consultado el 13 de octubre de 2013.

49 CGI.br. Resolução CGI.br/RES/2009/003/P: Princípios para a Governança e Uso da Internet no Brasil. Disponible en <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Consultado el 12 de octubre de 2013).

de datos en la red puedan adoptar los criterios que entiendan para discriminar lo que se envía a través de Internet. En contraposición a este escenario, Vint Cerf, reconocido como uno de los "padres" de Internet, sostiene que "permitir que los proveedores de banda ancha controlen lo que las personas ven y hacen en línea puede erosionar los principios que hicieron de Internet un éxito."[50]

Además:

> "Se creó una serie de justificaciones para apoyar el control de los operadores sobre la decisiones del consumidor en línea, pero ninguna resiste un análisis más detallado. Dar a los operadores la opción de discriminar de forma amplia el tráfico de datos no es necesario para proteger a los usuarios contra los virus, bloquear el spam, preservar la integridad de la red, hacer que el tráfico de VoIP o video funcionen correctamente, ni para garantizar que los operadores sean remunerados por sus inversiones en banda ancha. En particular, estamos firmemente convencidos de que los operadores serán capaces de definir los precios de mercado del acceso a Internet y recibir una buena remuneración por sus inversiones, como lo han hecho exitosamente operadores de banda ancha en otros países."[51]

Especialmente en Brasil, la Ley 12.965 de 2014 identifica la neutralidad como uno de los principios fundamentales de Internet en el país. El artículo 9º de la ley está redactado de la siguiente manera:

> **Art. 9o** El responsable por la transmisión, conmutación o enrutamiento tiene el deber de tratar de forma isonómica cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación.
>
> **§ 1o** La discriminación o degradación del tráfico será reglamentada en los términos de las atribuciones privativas del Presidente de la República previstas en el inciso IV del art. 84 de la Constitución Federal, para la fiel ejecución de esta Ley, oídos el Comité Gestor de Internet en Brasil y la Agencia Nacional

---

50 U.S. Senate Committee on Commerce, Science, & Transporation. Prepared Statement of Vinton G. Cerf. Disponible en <http://www.commerce.senate.gov/pdf/cerf-020706.pdf>. Consultado el 12 de octubre de 2013. Presentación en la Audiencia Pública sobre "Neutralidad de la Red" realizada ante el Comité de Comercio, Ciencia y Transporte del Senado de los Estados Unidos el 7 de febrero de 2006.

51 Ídem.

de Telecomunicaciones, y solo podrá resultar de:

I – requisitos técnicos indispensables para la prestación adecuada de los servicios y aplicaciones; y

II – priorizar los servicios de emergencia.

§ 2o En la hipótesis de discriminación o degradación del tráfico prevista en el § 1o, el responsable mencionado en el título debe:

I – abstenerse de causar daño a los usuarios, de acuerdo con el art. 927 de la Ley no 10.406 del 10 de enero de 2002, Código Civil;

II – actuar con proporcionalidad, transparencia e isonomía;

III – informar previamente de modo transparente, claro y suficientemente descriptivo a sus usuarios sobre las prácticas de gestión y mitigación de tráfico adoptadas, incluso aquellas relacionadas con la seguridad de la red; y

IV – ofrecer servicios en condiciones comerciales no discriminatorias y abstenerse de practicar conductas anticompetitivas.

§ 3o En la provisión de conexión a Internet, onerosa o gratuita, así como en la transmisión, conmutación o enrutamiento, está prohibido bloquear, monitorear, filtrar o analizar el contenido de los paquetes de datos, respetando lo dispuesto en este artículo[52].

La discusión sobre la gestión del puerto 25 podría aparecer en este contexto, ya que, al coordinar las actividades para el cierre del referido puerto, se está impidiendo un determinado tráfico de datos. El propio relator del proyecto de ley, diputado Alessandro Molon, diagnosticó esta cuestión e hizo referencia a la misma en el informe que acompañó el texto sustitutivo propuesto por el diputado a la redacción original del proyecto:

> "En el propio § 1º enumeramos la posibilidad de la existencia de discriminación o degradación del tráfico, si y solo si se da como resultado de requisitos técnicos indispensables para el disfrute adecuado de los servicios y aplicaciones.
>
> Por lo tanto, admitimos que en casos específicos, y siempre que resulten de requisitos técnicos indispensables para un disfrute adecuado por parte del usuario de los servicios y aplicaciones, puede haber discriminación o degradación del tráfico, siempre y cuando se respete lo previsto en los párrafos siguientes, como por ejemplo no provocar perjuicios injustificados a los

52 Brasil. Ley 12.965 de 2014 – Marco Civil de Internet

usuarios, el respeto a la libre competencia y a la transparencia. Así, combinando con los demás párrafos del mismo artículo, el § 1º hace posible que el spam no sea direccionado hacia el buzón de entrada del usuario. En caso de ataques a la seguridad, siempre que se respeten los requisitos del artículo 9º, también podrá haber un tratamiento diferenciado que propicie el disfrute adecuado de los usuarios. Por ejemplo, el tratamiento diferenciado de los videos en tiempo real o inclusive la VoIP pueden ser otros motivos justificables a priorizar, pero sin que haya violación al principio de neutralidad, siempre que se satisfagan los demás requisitos del artículo 9º."[53]

En este sentido, tanto el texto del Marco Civil de Internet como el propio Decálogo del CGI.br parecen indicar que las excepciones admitidas al principio de neutralidad de la red deben ser "criterios técnicos". Bajo esta visión, la gestión del puerto 25 se encuadraría perfectamente como un ejemplo de excepción técnica adoptada en el país a través de un amplio consenso logrado con todos los agentes interesados y el montaje de una estructura técnica, jurídica y reguladora capaz de amparar esta toma de decisión.

Entre los entrevistados para este estudio se observó que la mayoría interpreta la gestión del puerto 25 como un ejemplo exitoso de excepción a la neutralidad de la red, adoptada con los debidos recaudos y siguiendo un riguroso proceso de acompañamiento y toma de decisión estratégica de múltiples partes interesadas.

Algunos entrevistados también destacaron que fue justamente pensando en situaciones como la gestión del puerto 25 que el Decálogo del CGI.br restringió las excepciones al principio de neutralidad a "criterios técnicos y éticos", descartando así la discriminación por motivos "políticos, comerciales, religiosos, culturales, o cualquier otra forma de discriminación o favoritismo "[54].

En entrevista para la elaboración de este estudio, Demi Getschko, consejero del CGI.br y director y presidente del Núcleo de Información y Coordinación del Ponto BR (NIC.br), resaltó que la gestión del puerto 25 "no elimina ninguna característica de Internet sino que,

53 Informe del diputado Alessandro Molon al Proyecto de Ley nº 2126/2011 con fecha 4 de julio de 2012.

54 Entrevista concedida por Rubens Kuhl, gerente de productos de NIC.br, al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

por el contrario, el mensaje se continúa enviando, por lo que esta medida solo es una dificultad que se presenta para quien pretende abusar del puerto 25 para enviar mensajes no solicitados."[55]

Asimismo, Carlos Afonso señala que: "los cambios de puerto lógico para un mismo servicio no afectan el tráfico de los respectivos paquetes; o sea, el servicio se continúa usando de la misma forma, bastando cambiar el puerto en las configuraciones (algo siempre transparente en el *webmail*, lo que quiere decir que el usuario no tiene por qué preocuparse con qué puertos el proveedor presta el servicio)."[56]

La cuestión de no discriminar con base en el contenido aparece en varios testimonios recogidos para este estudio. También vale la pena destacar la reflexión de Cristine Hoepers y Klaus Steding-Jessen del CERT.br al evaluar si la gestión del puerto 25 realmente se podría encuadrar como un tema pertinente para la neutralidad de la red. "Lo que parece existir es un juego de palabras. Neutralidad de la red es no privilegiar un tráfico en detrimento de otro. El problema que se busca combatir es la ruptura de isonomía. En el caso del puerto 25, la misma regla sirve para todos. Además, no se investiga el contenido del paquete."

Ampliando sobre la cuestión de la inspección del contenido, que consistiría en una ruptura indebida de la neutralidad de la red, los entrevistados también argumentan lo siguiente:

"El modelo de encapsulamiento de datos del TCP/IP nos obliga a tener sobres dentro de sobres. Las metáforas sobre correos son siempre controvertidas porque Internet no es correo, pero en este caso son de ayuda: ¿Cuál es el contenido del bolso de un cartero? Las cartas. Pero para repartir estas cartas es necesario abrir la valija. Yo no abro las cartas, solo miro la dirección para poder encaminarlas a su destino. No existe un análisis del contenido de la carta o del *e-mail* para saber si se trata de propaganda o de cualquier otro contenido. No existe un análisis del contenido o de la información. Y es justamente por esto que la gestión del puerto 25 funciona tan bien."[57]

La preocupación con el argumento de la neutralidad de la red en

55 Entrevista concedida por Demi Getschko al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre 2013.

56 Entrevista concedida por Carlos A. Afonso al proyecto Memoria de la lucha contra el spam en Brasil el 8 de octubre de 2013.

57 Entrevista concedida por Cristine Hoepers y Klaus Steding-Jessen al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

la gestión del puerto 25 se justifica para que, por buenos que hayan sido los resultados obtenidos, esta iniciativa no se utilice como ejemplo para abogar a favor de excepciones cada vez más amplias y que puedan, en última instancia, vaciar el propio contenido del principio de neutralidad.

En el debate sobre el Marco Civil de Internet en Brasil esta cuestión se incluyó con frecuencia y, en la oposición entre entendimientos contrarios sobre cómo el actual artículo 9º de la ley debe disponer el principio y sus excepciones, la gestión del puerto 25 y la lucha contra el *spam* surgen como ejemplos en forma recurrente.

En entrevista con el sitio Convergencia Digital, Eduardo Levy, consejero del CGI.br y actual director ejecutivo de SindiTeleBrasil, afirmó que "en la cuestión de la neutralidad tenemos una palabra ['monitorear'] que nos gustaría suprimir, porque es importante gestionar una red que ofrezca la mayor calidad por el menor costo final. Significa que dentro de ella tenemos elementos por los que podemos hacer alguna interferencia por el bien de todos, como hicimos en el puerto 25"[58].

Aunque reconozca los beneficios de la adopción de la gestión del puerto 25 para la colectividad y lo encuadre como una excepción al principio de neutralidad, el consejero cuestiona si valdría la pena tener este mismo principio incluido en la ley. De acuerdo con la entrevista concedida a este proyecto:

> "(La gestión del puerto 25) es un buen ejemplo de cómo casos semejantes o incluso casos nuevos que surjan en el futuro y en los cuales se demande alguna acción bajo la red se pueden desarrollar de modo de obtener un beneficio para la sociedad como un todo.
>
> Nuestro temor en el sector de las telecomunicaciones es la propia existencia de una ley rígida. Nos gusta mucho el Decálogo, pero muchas veces entendemos que puede haber una dicotomía entre aquello que predicamos —que la red debe ser más libre, más simple, más libre realmente para todos— y la existencia de una ley, algo que puede tener con-

58 Convergencia Digital. L. O. Grossmann, L. Queiroz. Teles tratan neutralidade de rede como tema prioritário. Disponible en <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34357&sid=4#.Ulh-XmQ0i1Q>. Consultado el 13 de octubre de 2013.

secuencias que salgan del control de esta libertad.

Entiendo perfectamente que el grupo que más actúa en Internet reaccione al exceso de reglamentación. Yo también reacciono y el sector de las telecomunicaciones está extremadamente regulado por Anatel. Porque la sociedad debe obtener un beneficio de esto, no puede dejar que las empresas actúen sin reglamentación. Pero Internet tiene un grado de libertad mucho mayor. Eliminar este grado de libertad a través de una ley hecha en el congreso puede ser un contrasentido con respecto a aquello que se predica sobre la libertad de Internet."

En una presentación realizada durante una audiencia pública en la Cámara de Diputados el 12 de junio de 2012, SindiTeleBrasil defendió la necesidad de modificar la redacción sobre neutralidad de la red en el Marco Civil como forma de viabilizar iniciativas como la gestión del puerto 25 y la presentación de proyectos de banda ancha a precios asequibles para los usuarios que no utilizan todos los recursos de Internet. En esta presentación, la gestión del puerto 25 se menciona como una de las formas de "bloqueo o discriminación de tráficos razonables"[59].

Si bien el cierre del puerto 25 no es necesariamente una novedad desarrollada en Brasil puesto que otros países[60] ya han adoptado la medida y grandes proveedores y operadores internacionales también lo hacen[61], el debate sobre la neutralidad tiene ribetes especialmente relevantes en el país, dado que sus eventuales excepciones se encuentran próximas a ser reglamentadas, tal como consta en el Marco Civil de Internet.

Como mencionado anteriormente, este estudio sobre la gestión

---

59 Cámara de Diputados de Brasil. La visión de los proveedores de acceso fijo y móvil: Audiencia pública – Comisión Especial – PL 2126/11. Disponible en <http://www2. camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/54alegislatura/pl-2126-11-principios-do-uso-da-internet/reunioes-1/audienciaspublicas/apresentacoes-digitais-das-audiencias-publicas/apresentacao-eduardolevy-12.06.2012>. Consultado el 13 de octubre de 2013.

60 Ver, por ejemplo, el trabajo del Japan E-mail Anti Abuse Group: <http://jeag.jp/index.html>, consultado el 13 de octubre de 2013. Sobre la práctica adoptada en otros países, ver también Neil Rubenking, Port 25 Block Stalls Spam After All, <http://securitywatch.pcmag.com/spam/290791-port-25-block-stalls-spam-after-all>, consultado el 13 de octubre de 2013.

61 Beverly; R. Bauer, S. ; Berger, A., The Internet's not a Big Truck: Towards Quantifying Net Neutrality. Disponible en <http://www.akamai.com/dl/technical_publications/truck-pam07.pdf>. Consultado el 12 de octubre de 2013.

del puerto 25 procura, a través de testimonios y del análisis de las cuestiones presentadas por esta iniciativa, reflexionar sobre su proceso de implementación, impacto y lecciones que pueden ser aprendidas para un momento de intensa transformación en el escenario de la gobernanza y la reglamentación de la red.

Justamente por ser percibida por los actores de este proceso como una excepción al principio de neutralidad de la red, fue necesario dejar claro lo siguiente (i) los motivos que llevaron a su adopción; (ii) el proceso de múltiples partes interesadas empleado para garantizar que la toma de decisión no fuese arbitraria, unilateral o causase perjuicios a terceros; y (iii) el constante acompañamiento del proceso para promover evaluaciones de sus impactos.

En este sentido, es importante acompañar la evolución de los debates para poder mapear la forma en que una exitosa estrategia de coordinación de múltiples partes interesadas será apropiada en otros frentes en el futuro. El debate sobre neutralidad de la red es un ejemplo de la importancia de la gestión del puerto 25 y de la necesidad de conocer en profundidad iniciativas como esta.

4. Una gestión de políticas públicas de múltiples partes interesadas

Las actividades de la CT-Spam reflejan, primordialmente, el modelo de gobernanza de Internet implementado por el Comité Gestor de Internet en Brasil. De forma práctica, fue una de las primeras veces que se aplicó este modelo a la gestión de una política de Internet en el país.

En cuanto se implementó esta política se observó la necesidad de incluir a los actores no técnicos en el debate y la importancia subsidiaria y complementaria del gobierno en este proceso. Además, fue un ejemplo de cómo las características de la arquitectura de la red son relevantes para los debates políticos sobre la propia red, dada la influencia de la gestión del puerto 25 en las discusiones sobre el Marco Civil de Internet.

El proceso se demoró, algo que sus participantes atribuyen a diversos factores, desde la forma inédita de la coordinación hasta la postergación innecesaria de ciertos actores. Sin embargo, indudablemente todos destacan el éxito y la relevancia del proceso para el futuro de la gobernanza de Internet en el país.

Entender cómo se creó este modelo de múltiples partes interesadas es de gran importancia para comprender cómo fue posible la implementación de la gestión del puerto 25 y para poder reflejarlo sobre el futuro de nuevas iniciativas multisectoriales para el desarrollo de políticas públicas.

Gobernanza de Internet en Brasil y el modelo de múltiples partes interesadas

En 1995, el Ministerio de Comunicaciones, durante el periodo de privatizaciones en Brasil que empezó por los servicios de telecomunicaciones, expidió la Norma nº 004/95 que definió la relación entre los proveedores de servicio de conexión a Internet y los servicios de telecomunicaciones prestados por las "Entidades Explotadoras de Servicios Públicos de Telecomunicaciones". Válida hasta hoy, esta norma determina que la provisión de conexión a Internet no constituye un servicio de telecomunicaciones, sino un servicio de valor agregado, definido como:

> (...) el servicio que añade a una red preexistente un servicio de telecomunicaciones, medios o recursos que crean nuevas utilidades específicas o nuevas actividades productivas,

relacionadas con el acceso, almacenamiento, movimiento y recuperación de información[62].

El servicio de conexión a Internet quedó definido de la siguiente forma:

(...) nombre genérico que designa al Servicio de Valor Agregado, que posibilita el acceso a Internet a Usuarios y Proveedores de Servicios de Información[63]

Décadas después su creación, estas definiciones aún constituyen una incógnita para la reglamentación y gobernanza de la red en Brasil. Según la entrevista concedida por Marcelo Bechara a este proyecto:

"(...) la norma que conceptúa los servicios de valor agregado dice que la relación entre los proveedores de servicios de valor agregado y los proveedores de servicios de telecomunicaciones es definida por Anatel. Por lo tanto, existe realmente un ambiente poco claro. Y es comprensible que así sea, dado que este ambiente se ha modificado intensamente desde 1995 hasta hoy en cuanto hasta dónde debe llegar Anatel. En relación con este asunto, hubo una regulación específica —la Regulación del Servicio de Comunicación Multimedia[64]

---

62 Brasil. ANATEL, Decreto nº 148 del 31 de Mayo de 1995 que aprobó la Norma nº 004/95 sobre el Uso de la Red Pública de Telecomunicaciones para acceso a Internet. Disponible en <http://legislacao.anatel.gov.br/normas-do-mc/78-portaria-148>. Consultada el 5 de marzo de 2014. Nota del Traductor: la dirección de la página web fue reemplazada por <http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148>. Consultado el 8 de marzo de 2017.

63 Ídem.

64 Según el análisis del consejero Marcelo Bechara en un informe sobre la Propuesta de Modificación del Reglamento del Servicio de Comunicación Multimedia (SCM) y el Reglamento de Cobranza de Precio Público por el Derecho de Explotación de Servicios de Telecomunicaciones y por el Derecho de Explotación de Satélite, después de sometida a los comentarios de la sociedad, a través de la Consulta Pública nº 45 de 08/08/2011:2. Por tratarse de un servicio amplio y dotado de innumerables aplicaciones, incluso el soporte a la banda ancha, el SCM se presenta como uno de los instrumentos de democratización del acceso a las tecnologías de información, de reducción de las desigualdades en este acceso e instrumentalización de garantías fundamentales como la educación, la salud, la información y la comunicación. (...)
El SCM creado por la resolución 272 de 2001 como resultado de la velocidad de la innovación tecnológica en el sector de tecnologías de la información y de la convergencia entre los servicios de telecomunicaciones e Internet.
(...)
5.2. De este modo, el SCM surgió con la finalidad de ampliar los servicios de transmisión de datos, entre ellos el Servicio Limitado Especializado en las submodalidades de Red Especializada y Circuito Especializado, así como también las autorizaciones del Servicio de Red de Transporte de Telecomunicaciones (SRTT), incluidos el Servicio por Línea Dedicada, el Servicio de Red Conmutada por Paquete y el Servicio de Red Conmutada por Circuito.

— que fue hacia donde acabaron yendo los proveedores, los antiguos proveedores de conexión. Hoy en día ellos todavía son proveedores de servicios de valor agregado y de servicios de telecomunicaciones. A veces la misma empresa dentro de una estructura empresarial."[65]

Por lo tanto, tan importante como las definiciones de servicio de valor agregado y servicio de conexión a Internet, la Norma nº004/95 fue el primer paso descentralizador del desarrollo de Internet en el país al establecer una relación de autonomía entre los proveedores de servicio de conexión a Internet y la entidades explotadoras del servicio público de telecomunicaciones, estimulando la competencia y la iniciativa privada.

Ese mismo año, el Ministerio de Comunicaciones y el Ministerio de Ciencia, Tecnología e Innovación presentaron una Nota Conjunta sobre el desarrollo de la red brasileña, marcando el fin del suministro estatal de conexión, así como la creación de un comité gestor para organizar Internet en Brasil con la presencia de representantes de ambos ministerios, de los operadores de *backbone*, de los proveedores de conexión, de los usuarios y de la comunidad académica. Entre los puntos de la nota se destacan:

"1.4 La participación de las empresas y órganos públicos en el suministro de servicios de Internet se dará de forma complementaria a la participación de la iniciativa privada, y se limitará a las situaciones donde sea necesaria la presencia del sector público para estimular o inducir el surgimiento de proveedores y usuarios.

(...)

7.1 Para efectivizar la participación de la Sociedad en las decisiones que implican la implantación, administración y uso de Internet, se constituirá un Comité Gestor de Internet, que contará con la participación del MC y el MCT, de entidades operadoras y gestoras de columnas vertebrales, de representantes de proveedores de acceso o de información, de representantes de los usuarios y de la comunidad académica.

7.2 El Comité Gestor tendrá como principales atribuciones:

a) fomentar el desarrollo de servicios de Internet en Brasil;

b) recomendar estándares y procedimientos técnicos y operacionales para Internet en Brasil;

c) coordinar la distribución de direcciones de Internet, el re-

65 Entrevista concedida por Marcelo Bechara al proyecto Memoria de la lucha contra el spam en Brasil el 17 de marzo de 2014.

gistro de nombres de dominios y la interconexión de columnas vertebrales;

d) recoger, organizar y diseminar información sobre los servicios de Internet."[66]

Aunque el entorno regulatorio para Internet en Brasil no se desarrolló a través de una centralización política, estuvo lejos de ser un descontrol. La creación del Comité Gestor de Internet en Brasil suplió la falta de un agente regulador específico, asumiendo las principales características de la red: descentralización y colaboración, tecnicidad y política.

Luego de la Nota Conjunta, el Decreto Interministerial nº 147[67] del 31 de mayo de 1995 creó el Comité Gestor de Internet en Brasil con la atribución de acompañar la disponibilización de servicios de Internet en el país, establecer recomendaciones relativas a la estrategia de implantación e interconexión de redes, analizar y seleccionar opciones tecnológicas y papeles funcionales para las empresas, instituciones educativas, de investigación y desarrollo (IEPD); recomendar estándares, procedimientos técnicos y operativos y un código de ética de uso para todos los servicios de Internet en Brasil; coordinar la distribución de direcciones IP (Internet Protocol) y el registro de nombres de dominio, y recomendar procedimientos operativos para la gestión de redes, entre otras.

Por consiguiente, la representación de múltiples partes interesadas del CGI.br inicialmente se configuró de la siguiente forma: (i) un representante del Ministerio de Ciencia y Tecnología, que estaría a cargo de la coordinación; (ii) un representante del Ministerio de Comunicaciones; (iii) un representante del Sistema Telebrás; (iv) un representante del Consejo Nacional de Desarrollo Científico y Tecnológico, CNPq; (v) un representante de la Red Nacional de Investigación; (vi) un representante de la comunidad académica; (vii) un representante de los proveedores de servicios; (viii) un representante de la comunidad empresarial; y (ix) un representante de la comunidad de usuarios del servicio de Internet.

---

66 Brasil. Nota Conjunta del Ministerio de Ciencia y Tecnología y el Ministerio de Comunicaciones, 15 de mayo de 1995. Disponible en: <http://www.cgi.br/legislacao/notas/nota-conjunta-mct-mc-maio-1995>. Consultada el 5 de marzo de 2014.

67 Brasil. Decreto Interministerial nº 147 del 31 de mayo de 1995. Disponible en <http://www.cgi.br/regulamentacao/port147.htm>. Consultado el 7 de marzo de 2014.

Marcelo Carvalho destaca la importancia de los Grupos de Trabajo en el ámbito del Comité Gestor de Internet en Brasil para el desarrollo de sus atribuciones:

> Para desarrollar sus acciones y aumentar la participación de la sociedad en sus actividades, atendiendo a uno de los objetivos definidos en su creación, desde su primera reunión, el CGI empezó a crear y perfeccionar la organización de Grupos de Trabajo (GTs) cuyas actividades buscaran fomentar el desarrollo de servicios en Internet en Brasil[68].

Ante este contexto, hay unanimidad entre los actores involucrados en el proyecto de gestión del puerto 25 con respecto a la esencialidad del protagonismo del Comité Gestor, es decir, de su rol como coordinador de la sociedad en la toma de decisiones e implantación de las políticas de Internet. Aún no hay consenso en la determinación específica del principio del multilateralismo.

DeNardis y Raymond indican que el multisectorialismo no se debe aplicar como un principio en sí mismo, sino como la determinación de una gestión que busque un punto óptimo, promoviendo equilibrio y estabilidad entre los objetivos y prioridades involucradas. Según los autores:

> "(...) multisectorialismo no debe ser visto como un valor en sí mismo a ser aplicado de forma homogénea en todas las funciones de gobernanza de Internet. Por el contrario, el abordaje apropiado para generar una gobernanza más eficaz y responsable de la red demanda una reflexión sobre cuál sería el sistema que mejor equilibra innovación, interoperabilidad, libertad de expresión y estabilidad operacional en cada contexto funcional y político."[69]

Además, para los autores, el legado del modelo de gobernanza basado en órganos estandarizados y decisiones empresariales genera modelos de gobernanza de Internet con dos características principales: (i) no intervención de los gobiernos en el proceso de toma de decisión y (ii) el proceso de toma de decisión en gober-

---

68 M. S. Revoredo de Carvalho. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição de mecanismos de governança. COPPE/UFRJ, Rio de Janeiro, 2006, p.142.

69 De Nardis, L.;Raymond, M. Thinking Clearly. Social Science Research Governance. 14 de noviembre de 2013. Disponible en <http://ssrn.com/abstract=2354377>. Consultado el 8 de marzo de 2014.

nanza de Internet considera solo aspectos técnicos y decisiones de mercado. De esta forma, se observa que los problemas de coordinación son más comunes que los problemas de cooperación.

Vemos, por lo tanto, que lograr un nivel satisfactorio de coordinación es tan complejo como las amenazas que la red enfrenta todos los días. Por otra parte, lograr un nivel estandarizado de coordinación no solo es inviable, sino también indeseable. Además de lograr un modelo óptimo de coordinación, algunas premisas básicas son incuestionables, como las mencionadas por el Conficker Working Group en su documento "Lessons Learned" publicado en 2011. Estas premisas no mencionan precisamente un modelo de múltiples partes interesadas, pero destacan la cooperación entre diversos niveles de actores y la participación y apoyo de los gobiernos ante la volatilidad y la velocidad de las amenazas y la necesidad de una comunicación rápida, fácil y efectiva.

Independientemente del término, el proceso de gestión del puerto 25 ha estado marcado por un intenso proceso de colaboración entre los actores en busca de un bien público, coordinados por el Comité Gestor de Internet en Brasil. Por lo tanto, en este punto, no hay dudas en cuanto al éxito de la implementación del modelo de gobernanza de múltiples partes interesadas y multiparticipativo de Internet en Brasil. Este resultado fue reconocido por el consejero Eduardo Levy, quien en una entrevista concedida a este proyecto dijo:

> "Esto es complejo; es bonito desde el punto de vista de la democracia y de las diversas fuerzas que actúan y es más mucho bonito por el resultado final cuando la sociedad es quien sale ganando. No hubo nada muy fuerte que impidiese que la sociedad saliera ganando. Por esto creo que, para mí personalmente y para el sector de las telecomunicaciones, fue un orgullo muy grande formar parte de este proceso y poder difundirlo de la forma como se ha hecho.
>
> Creo que la acción del CGI.br fue fundamental desde el punto de vista *multistakeholder* y de la participación de todos. Pero si no fuese así y si todas las partes no estuviesen presentes, probablemente aún estaríamos patinando. Aún faltaba la parte de las telecomunicaciones, que podía ser la menos o la más importante, dependiendo del momento de que se tratara, ya que en distintos momentos su importancia puede ser más o menos significativa. La discusión dentro del Comité es de una gran

riqueza gracias a las características que tienen los segmentos."[70]

Para los actores del proceso de la gestión del puerto 25, la actuación del Comité Gestor demuestra que en el país no existe un vacío de poder en cuanto a política de Internet. La identificación técnica de un problema, la toma de decisión colaborativa y la coordinación eficaz de los actores para la resolución del problema hicieron del modelo implementado por el CGI.br el sistema democrático posible para una gobernanza sustentable de la red. Para algunos, este ejemplo debe ser seguido en futuras coordinaciones de políticas de Internet. Conforme señala Marcelo Bechara:

> "Pienso que el puerto 25 fue la primera vez que el Comité Gestor actuó más como Comité Gestor y menos como NIC[71], porque el NIC tiene vida propia e incluso la gestión de las direcciones IP y los nombres de dominio no es realizada por el Comité Gestor. (...) Pero el Comité se trata mucho más de debate y menos de gestión. En esta ocasión fue un comité de gestión. Solo que esto es una cosa que no forma parte de su rutina, aunque en mi opinión sí debería hacerlo. Esto ha sucedido de forma bastante gradual."[72]

La característica multisectorial del CGI.br en la coordinación de la gestión del puerto 25 no revela la imposición de un modelo en sí, pero, como se puede deducir de los relatos presentados, el modelo de múltiples partes interesadas deriva de las características de la propia red. Sin la coordinación de los actores, no se habría desarrollado el proceso y su imposición gubernamental quizás no sería efectiva, ya que una de las principales características de Internet que se revela en el proceso de múltiples partes interesadas es su democratización y descentralización.

En este contexto, Rubens Kuhl subraya que:

> "el resultado de un proceso de múltiples partes interesadas siempre será mejor visto porque tiene una adopción de to-

---

70 Entrevista concedida por Eduardo Levy al proyecto Memoria de la lucha contra el spam en Brasil el 17 de enero de 2014.

71 El Núcleo de Información y Coordinación del Ponto BR - NIC.br fue creado para implementar las decisiones y los proyectos del Comité Gestor de Internet en Brasil - CGI.br, que es el responsable de coordinar e integrar las iniciativas y servicios de Internet en el país. Más información disponible en <http://nic.br/about-nic-br/>. Consultado el 2 de junio de 2014.

72 Entrevista concedida por Marcelo Bechara al proyecto Memoria de la lucha contra el spam en Brasil el 17 de enero de 2014.

dos los proponentes, de todos quienes discutieron el proceso. Por lo tanto, sin importar si es mejor o peor, siempre va a ser mejor percibido. Esto es una ventaja desde el punto de vista político, es decir, en este proceso del puerto 25 también existe un aprendizaje de todos los actores de no defender solamente un punto específico o una adecuación específica que cada uno tenga. Así, el hecho de que este proceso haya sido lento demuestra cuál era nuestra madurez política para tomar este tipo de decisión"[73].

5. Conclusiones

El Comité Gestor de Internet en Brasil trabaja diariamente con temas relacionados con Internet, un recurso compartido por varias partes de forma intrínseca. En línea con estas características, el CGI.br no solo construyó su estructura, sino también adaptó su proceso de toma de decisión.

La gestión del puerto 25 puede parecer un tema árido, demasiado técnico y de difícil comprensión. Este informe intentó arrojar luz tanto sobre el proceso como sobre las reflexiones fundamentales que se pueden extraer de la experiencia de la lucha contra el *spam* en Brasil hasta el momento. La democratización de la sociedad pasa necesariamente por la democratización de la toma de decisiones de interés público y una entidad como el CGI.br puede servir de ejemplo para demostrar el potencial de este proceso.

En este sentido, con el trabajo de la CT-Spam, sobretodo con la implementación del puerto 25, se puso en práctica este modelo de toma de decisión y gestión de un recurso de forma multisectorial de forma bastante exitosa, en que todos los interesados convergieron para mejorar un interés público.

Justamente por desempeñar este rol, el CGI.br está en una posición privilegiada para coordinar nuevos desafíos multisectoriales con el objetivo de perfeccionar el uso y la gobernanza de Internet en el país. Según lo indicado en una entrevista concedida para este estudio, la transición de IPv4 a IPv6 parece ser una de las iniciativas que, aprendiendo de la experiencia de la gestión del puerto 25,

73 Entrevista concedida por Rubens Kuhl al proyecto Memoria de la lucha contra el spam en Brasil el 17 de enero de 2014.

sigue el mismo camino para generar otro desafío de coordinación de múltiples partes interesadas para la entidad para la entidad[74].

En lo que se refiere a los proveedores y a los operadores de telecomunicaciones, la experiencia de la gestión del puerto 25 representó una iniciativa importante para evidenciar cómo diferentes empresas se pueden organizar en torno a distintos intereses en relación con un mismo tema de gobernanza y regulación de la red. Con el desarrollo cada vez más presente de un discurso que incentiva la toma de decisiones a través de procesos de múltiples partes interesadas, es muy importante percibir las diferentes perspectivas que pueden existir dentro de un mismo sector y cómo estas perspectivas se presentan y resuelven para lograr un consenso que permita avanzar en la discusión.

Observando el problema desde la perspectiva del consumidor, vale destacar que el Código de Defensa del Consumidor de Brasil orientó los trabajos del sistema nacional de defensa del consumidor en su colaboración en la toma de decisión estratégica de múltiples partes interesadas. En este sentido, la Política Nacional de las Relaciones de Consumo debe atender a las necesidades del consumidor, mejorando su calidad de vida, adecuándose a la protección del consumidor y a las necesidades del desarrollo tecnológico[75].

Aunque este nuevo diseño técnico pudiese afectar negativamente a un número pequeño de consumidores, era esencial para la creación de un ambiente más favorable para todos. Los eventuales perjuicios a consumidores —que en el fondo no se verían perjudicados en nada porque podrían revertir esta situación— significaban francamente un problema que sería fácilmente superado

74 Entrevista concedida por Eduardo Parajo al proyecto Memoria de la lucha contra el spam en Brasil el 25 de septiembre de 2013.

75 De acuerdo con el Art. 4º del Código de Defensa del Consumidor: La Política Nacional de las Relaciones de Consumo tiene por objetivo el atendimiento de las necesidades de los consumidores, el respeto a su dignidad, salud y seguridad, la protección de sus intereses económicos, la mejora de su calidad de vida, así como la transparencia y armonía de las relaciones de consumo, teniendo en cuenta los siguientes principios: (Redacción dada por la Ley nº 9.008, de 21.3.1995) (...) II – Armonización de los intereses de los participantes de las relaciones de consumo y compatibilización de la protección del consumidor con la necesidad de desarrollo económico y tecnológico, de modo de viabilizar los principios en los cuales se basa el orden económico (art. 170, de la Constitución Federal), siempre con base en la buena fe y equilibrio en las relaciones entre consumidores y proveedores.

por los beneficios que el bloqueo del puerto 25 podría traer para los consumidores en general[76].

Lo que se concluye principalmente de la gestión del puerto 25 en las redes brasileñas es lo imprescindible que resulta la coordinación de múltiples partes interesadas para las políticas de Internet. La coordinación por parte del CGI.br de los actores de los sectores empresariales, técnico, gobierno, sociedad civil y académico no tiene equivalente. De acuerdo con los testimonios recogidos, ante la necesidad de una solución altamente técnica y especializada, sería poco probable que un órgano público pudiese hacerlo. De tal forma, la alianza público-privada derivada de la colaboración de los actores demuestra ser la mejor vía para obtener respuestas efectivas en cuestiones de seguridad y políticas de red.

Por lo tanto, a partir de las entrevistas realizadas y las reflexiones resultantes, se espera que, además de los frutos ya cosechados en cuanto a la reducción del volumen de *spam* enviado por el país, la memoria de este proceso pueda servir para impulsar los debates sobre gobernanza y regulación en Brasil, de forma que se produzcan experiencias multisectoriales como esta tanto a nivel nacional como a nivel internacional, ayudando a fortalecer el papel del país en el escenario global de gobernanza de la red.

Además, la documentación de este proceso debe servir también para perfeccionar las iniciativas de coordinación a nivel nacional e internacional sobre temas de gobernanza de Internet. Es importante destacar una vez más las recomendaciones de la estrategia del Dutch Cyber Security Council, en su segunda fase, que hacen hincapié en la importancia de las coaliciones nacionales e internacionales para la realización de estándares establecidos internacionalmente, el diálogo permanente, la transparencia, la regulación (autorregulación o regulación institucional) y la creación de conocimiento.

Por todo lo expuesto, la coordinación y la colaboración efectivas entre las partes interesadas para los temas de gobernanza de Internet operativizan pilares democráticos fundamentales, entre ellos el diálogo, la apertura, la transparencia, la cooperación y una constante construcción de información y conocimiento colaborativos.

---

76 Entrevista concedida por Danilo Doneda al proyecto Memoria de la lucha contra el spam en Brasil el 27 de septiembre de 2013.

II
Entrevistas
Entrevistas realizadas por

Marília de Aguiar Monteiro

Bachiller en Derecho por la Escuela de Derecho de Rio de Janeiro, de la Fundación Getulio Vargas, con intercambio académico en el Institut d'Etudes Politiques de Lille, Francia. Coordinadora de Consumo y Sociedad de la Información en la Secretaría Nacional del Consumidor del Ministerio de Justicia. Investigadora del Instituto de Tecnología y Sociedad de Rio de Janeiro (ITS/RJ).

Carlos Affonso Pereira de Souza

Doctor y Máster en Derecho Civil por la Universidad del Estado de Rio de Janeiro (UERJ). Director del Instituto de Tecnología y Sociedad de Rio de Janeiro (ITS/RJ). Profesor de los cursos de grado y de postgrado de la UERJ, PUC-Rio e IBMEC. Investigador Visitante del Information Society Project, de la Facultad de Derecho de la Universidad de Yale. Miembro de la Comisión de Derecho Autoral de la OAB/RJ. Consejero electo del GNSO/ICANN como representante de los usuarios no comerciales de Internet (2008-2009) y Miembro electo del Comité Ejecutivo del NCUC (Non-Commercial Users Constituency). Policy Fellow de la ONG Access y miembro del Consejo Consultivo del Instituto NUPEF.

1. Entrevista con Henrique Faulhaber

Realizada en Río de Janeiro el 12 de febrero de 2014

Carlos Affonso Pereira de Souza: Para comenzar con una perspectiva histórica, ¿podría explicarnos cuáles fueron las razones para la creación de la CT-Spam dentro del Comité Gestor de Internet en Brasil?

HF: El Comité Gestor de Internet en Brasil es un órgano que se ocupa de la gobernanza de Internet en Brasil. Desde el inicio hubo mucha preocupación con la gobernanza relacionada con la estructura, es decir, con los nombres de dominio y las direcciones IP.

Después de 2004, con la Cumbre de la Sociedad de la Información[1], llegué al CGI.br en 2005 para mi primer mandato y ya había una crítica masiva en el sentido de que el Comité Gestor debía discutir no solo las capas de la estructura sino también otras capas de la gobernanza de Internet.

1 Sobre la Cumbre Mundial de la Sociedad de la Información, ver los Cuadernos del CGI.br que contienen los documentos de Ginebra y Túnez. Disponible en <http://nic.br/about-nic-br/>.

En esta perspectiva, propuse que formásemos el grupo de trabajo *antispam* en el Comité Gestor de Internet. ¿Por qué? Porque es un problema que aflige y afecta a todos los internautas; porque en aquella época, en 2005, un 90% de los mensajes electrónicos que llegaban a través de *e-mail* eran mensajes no deseados y era un vector importante de inyección de virus y programas maliciosos o *botnets* o programas que trataban de robar contraseñas.

El *spam* era un vehículo importante para infectar las computadoras de los usuarios. Por un lado, había una dificultad muy grande en separar la paja del trigo, de ver si el mensaje que llegaba era algo que le interesaba al destinatario, o si era un mensaje de propaganda que también traía un virus. Y también era un desperdicio para toda la cadena, en especial para los proveedores de acceso que tenían que gastar muchos recursos para filtrar para el usuario, desechar todo el *spam*; pero incluso así se entregaba un volumen muy grande de *spam* a los usuarios. También para las empresas de telecomunicaciones, ya que 90% del tráfico de *e-mails* es spam. Se está gastando, pagando por un gran ancho de banda que la persona podría estar utilizando para navegar en Internet, hacer otras cosas. Con toda seguridad, el *spam*, que ya era un problema cuando se creó Internet, fue aumentando. Era un tema que merecía la preocupación del Comité Gestor, discusiones, estudios. Y así empezó este grupo. Fue una iniciativa que yo tomé y luego los colegas adhirieron.

Empezamos realizando seminarios para discutir dentro de Brasil qué se podría hacer para disminuir la cantidad de *spam*, cuál sería el comportamiento del usuario al recibir estos mensajes indeseados y si era necesario algún tipo de legislación nacional, ya que algunos países (la Comunidad Europea, Estados Unidos, Canadá) ya tenían legislaciones para evitar la práctica del *spam*; examinar aspectos de seguridad, en qué medida podríamos mejorar la calidad de la seguridad de Internet luchando contra el *spam*. Estudiamos iniciativas internacionales, la OCDE (Organización para la Cooperación y el Desarrollo Económicos), la propia UIT (Unión Internacional de Telecomunicaciones), con el fin de elaborar un programa nacional de lucha contra el *spam*. Estas iniciativas se desarrollaron por caminos independientes.

Realizamos charlas, creamos un sitio importante que allá por 2006-2007 (antispam.br) dirigido a usuarios finales y administradores de red, explicando problemas, dando sugerencias sobre cómo defenderse; explicando lo que es y lo que no es *spam*. En aquella época

creamos un proyecto junto con el Centro Tecnología y Sociedad de la Fundación Getúlio Vargas en Río de Janeiro para realizar un estudio de la legislación internacional sobre *spam* y proponer un texto que pudiese ayudar al Congreso Nacional a colocar la lucha contra el *spam* en una ley brasileña, a la altura de lo más moderno que existía, que fuera actual y pertinente para la lucha contra el *spam*.

De forma paralela, solicitamos a la Universidad Federal de Minas Gerais (UFMG) un estudio para verificar por qué Brasil estaba primero o segundo entre los países que más enviaban *spam*. Además de las molestias en nuestros buzones de entrada, todo usuario brasileño recibía una gran cantidad de *spam*. Esto no era solo en Brasil, sino que ocurría en todos los lugares del mundo, pero Brasil era conocido como el "rey del s*pam"*. De acuerdo con los indicadores internacionales, Brasil era uno de los países que más enviaba *spam*: como mencioné, siempre figuraba entre los primeros puestos de los que más enviaban. Y este estudio comprobó que de hecho la red brasileña enviaba mucho *spam* hacia el exterior, pero no eran los brasileños quienes lo hacían. La red brasileña fue utilizada como un *hub*, es decir, en la red brasileña había muchas computadoras infectadas por virus, muchas computadoras brasileñas formaban parte de *botnets*. Así, los *spammer*s del exterior utilizaban la red brasileña para direccionar *spam* hacia otro país. Por lo tanto, había una cantidad enorme de *spam* escrito en chino mandarín que venía de los países asiáticos, pasaba por Brasil y regresaba a Asia.

Esto que constatamos era inequívoco. El trabajo de SpamPots comprobó que estábamos siendo usados, que el *spam* era un vehículo importante para transportar virus y contaminar otras computadoras, pero también que el *spam* brasileño venía de otro lugar.

Por todo esto —nuestros estudios, iniciativas de otros países, discusiones de leyes, esta investigación—, nos llevó a la conclusión que teníamos que tener un medio técnico para hacer que la red brasileña dejase de enviar esta cantidad tan grande de *spam*.

Ya había una recomendación adoptada en otros países de bloquear el puerto 25 para evitar que el *spam* saliese de la red en su origen. Es decir, en vez de combatir el *spam* después de su llegada al buzón del usuario, filtrando, seleccionando, desechándolo; buscamos un método que ya había sido recomendado por otros pero que aún no habíamos probado en Brasil para hacer que las computadoras de los usuarios finales, incluso si estaban contaminadas, no pudiesen enviar *e-mails* directamente usando el puerto 25. Esto es el llamado bloqueo

del puerto 25 que, entre las ideas discutidas por el grupo Antispam brasileño del Comité Gestor, la idea en la que más invertimos recursos y la que trajo un resultado final bastante bueno, porque ahora, en 2013, salimos de la lista de los tres que más envían *spam* y hoy estamos en una posición mucho mejor, variando entre el puesto 25 y el 30 de la lista de los países que más envían *spam*.

CAF: ¿Cómo lo lograron?

HF: En cuanto percibimos que una medida técnica de este tipo podía disminuir la incidencia de *spam* en la red brasileña y la cantidad de *spam* que el país enviaba al exterior, empezamos a conversar con los segmentos involucrados en la cadena de Internet. Porque el *spam* salía de la casa del usuario, pasaba por el proveedor, pasaba por los canales de comunicación de los operadores de telecomunicaciones, de diferentes tipos, ¿verdad? Podían ser de Internet fija, DSL, Internet móvil, TV por cable o Internet móvil, telefonía celular. Entonces formamos un grupo de trabajo en 2008 para discutir cómo implementar este tipo de bloqueo. Esto significaba que los usuarios de un cliente de correo electrónico —Outlook, Thunderbird, etc.— tendrían que cambiar, que no podrían usar el puerto 25 porque este iba a ser bloqueado por el operador. Así, el proveedor tenía que instruir a los usuarios para que cambiaran su programa de *e-mail* del puerto 25 a otro puerto, en este caso el 587. Y el operador de comunicación de estos diversos medios —cable, celular, etc.— debería bloquear la red, impedir que un *e-mail* que saliera del puerto 25 de estos usuarios siguiese adelante. Esto solo afecta al usuario residencial, no a la empresa. Para enviar un *e-mail* a otra persona, el usuario residencial utilizaba necesariamente un proveedor de correo electrónico, como Gmail o cualquier otro. No podría instalar en su computadora un servidor para disparar *e-mails* a todo el mundo. En realidad, las personas no hacían esto; quienes hacía este envío masivo de *e-mails* desde la casa del usuario eran programas que se instalaban en la computadora del usuario, sin su conocimiento, a través de virus. Y la computadora quedaba enviando miles de *e-mails* por día, sin conocimiento del usuario, degradando el ancho de banda del usuario, colocando a Brasil en el tope de la lista de *spam*. Esta medida era principalmente para evitar que las computadoras infectadas conectadas a la red nacional brasileña —que en aquella época eran muchas (alrededor de 1 millón de computadoras)— lograsen enviar *spam* a todo el mundo por medio de estos programas maliciosos.

A partir de 2008, empezamos a conversar con los diversos segmentos involucrados en el problema: (i) Anatel, porque, como Anatel regula a las empresas de telecomunicaciones, el bloqueo del puerto 25 debía contar con la ayuda de la institución, algo que luego demostró ser realmente necesario; (ii) los proveedores de acceso; (iii) las propias empresas de telecomunicaciones; y (iv) los usuarios a través de los órganos de defensa del consumidor. Esto llevó a la conclusión de que para mover a tantos actores —estamos hablando de 2 mil proveedores, 40 empresas de telecomunicaciones, Anatel— debíamos seguir algunas formalidades, digámoslo así, había algunos pasos que debíamos seguir de ahí en adelante. Por esto, en 2009 el Comité Gestor emitió una resolución indicando que los usuarios ya no debían utilizar más el puerto 25 para comunicarse por *e-mail*, sino que debían utilizar el puerto 587 a través de los servidores de *e-mail*. Los proveedores debían ayudar a los usuarios a hacer esta migración y las empresas de telecomunicaciones a hacer el bloqueo del puerto 25. Todo esto amparado por las buenas prácticas para disminuir la salida de *spam* a través de la red brasileña.

Adoptamos la resolución y empezamos a reunirnos mensualmente de forma más intensa con la participación de quince a veinte personas que representaban a estos diversos segmentos. Ahí notamos que, a pesar de que los proveedores ya estaban dando las instrucciones para que los usuarios cambiasen al puerto 587, los proveedores de servicios de comunicación aún no habían tomado la decisión de hacerlo, porque esto dependía de una regulación de Anatel. Como ellos eran regulados por Anatel, podrían recibir una multa o sanción en caso de que ellos hiciesen algo fuera de la reglamentación.

Demi y yo fuimos a Anatel para conversar con su presidente. A pesar de que Anatel formaba parte del Consejo, en esa época se estaba produciendo una migración: salía el Dr. Plínio Aguiar y llegaba el embajador Sardenberg. Fuimos a conversar con el embajador Sardenberg y le dijimos que , siguiendo el ejemplo del Comité Gestor, Anatel debía emitir un decreto comunicando a las empresas y operadores de telecomunicaciones que debían bloquear de forma efectiva el puerto 25 para el bien de Internet en Brasil y de su seguridad.

Esto se logró, aunque con cierta demora: los trámites dentro de la agencia pasan por el Consejo Directivo y por un cuerpo de técnicos.

Sin embargo, en 2010, a través de su Consejo Directivo, Anatel recomendó también que las empresas de telecomunicaciones debían cerrar el puerto 25, tal como lo recomendaba el Comité Gestor. Las

cosas salieron bien, este era un paso realmente necesario. Como mencioné anteriormente, los grandes proveedores de acceso ya habían migrado por completo su base. Por ejemplo, Terra y Uol ya no estaban usando más el puerto 25. Ellos habían hecho un trabajo óptimo, pero no servía de nada si el usuario no enviaba más por el puerto 25; las computadoras contaminadas, incluso en aquellos proveedores, ya eran muchas. Varios proveedores ya habían hecho este cambio, pero continuaban enviando *spam* por el puerto 25, que no estaba cerrado.

Esta resolución de Anatel fue un gran paso, pero nos equivocamos en el paso siguiente. En las reuniones los abogados de las compañías de telecomunicaciones dijeron lo siguiente: "Miren, Anatel nos dice que debemos cerrar, pero ahora estamos preocupados por nuestros contratos. ¿Qué van a hacer los consumidores, las asociaciones de consumidores, los Procons, con este bloqueo que estamos haciendo al puerto 25? El contrato no dice que el puerto 25 va a ser bloqueado; el puerto 25 ya se encontraba abierto". Entonces incursionamos en el Ministerio de Justicia, en el Departamento de Protección y Defensa del Consumidor, que en aquella época tenía a Juliana Pereira como Secretaria Nacional del Consumidor, y la tratamos de convencer diciendo que esto realmente beneficiaría al consumidor y a la seguridad de la red. Después de un tiempo, aproximadamente en 2012, el Departamento de Protección del Consumidor redactó una Nota Técnica diciendo que el bloqueo del puerto 25 sería beneficioso para la Internet en Brasil, aportando así la comodidad que los abogados querían y a la cual ninguna ONG de defensa del consumidor se podía oponer: ni siquiera el propio Ministerio podría multar al operador por el hecho de estar bloqueando.

Esto ayudó a que en 2012 firmáramos el Acuerdo de Cooperación en que el Comité Gestor, Anatel, los proveedores, proveedores de telecomunicaciones, apoyados por el Ministerio de Justicia y por el Departamento de Defensa del Consumidor se comprometiesen a bloquear el puerto 25 en un plazo de 12 meses.

El proceso se inció en marzo de 2012 y demoró un año. Nosotros nos quedamos un poco preocupados, porque este trabajo sería hecho de forma progresiva: ciudad por ciudad, central por central, simultáneamente por varios operadores (fijos, móviles, TV por cable, etc.). ¿Cómo afectaría esto al usuario final? Porque un día alguien que no estuviese informado sobre el puerto 587 no podría enviar más sus mensajes de correo electrónico. Fue así que montamos una operación de guerra para descubrir si no estaba habiendo problemas, porque no

queríamos que el proceso se detuviera a mitad de camino. Y el acuerdo incluía una cláusula que indicaba que en caso que se produjera un problema muy grande el proceso se podría detener.

Sucedió lo siguiente: como nosotros habíamos empezado mucho antes con el sitio, la divulgación, la prensa y las charlas, cuando se empezó a implementar el bloqueo propiamente dicho, las personas más técnicas de Internet, los administradores de redes, quienes tienen mayores conocimientos técnicos ya estaban enterados de la operación. Pero siempre había el temor de que las personas que viviesen en sitios más distantes, en ciudades del interior de Brasil, empezasen a reclamar que no podían enviar *e-mails*. No obstante, en la propia red había instrucciones sobre qué hacer y, para nuestra sorpresa y la de los operadores, los *call centers* de los operadores y de los proveedores prácticamente no fueron congestionados por este cambio. Sinceramente, fue mucho menos traumático. Estábamos preparados para un cambio mucho más traumático de lo que realmente fue. Tuvimos éxito, porque en el plazo se logró cerrar a todos los operadores y efectivamente verificamos que, de una semana para la otra, Brasil fue cayendo en los rankings. Pasamos del puesto 3 al puesto 15 y pasamos a seguir con mucho cuidado la cantidad de *spam* que salía de nuestra red en estas listas.

CAF: Pensando en los orígenes de la gestión del puerto 25, ¿cómo se desarrollaron los spampots de la alianza con la UFMG que mencionó? ¿Nos puede hablar un poco más sobre cómo se desarrolló esta fase?

HF: Ya existía un proyecto en el Comité Gestor, manejado por el CERT, que cuidaba los incidentes de seguridad. Este proyecto de *antispam* y puerto 25 solo fue posible porque fue manejado operacionalmente por el CERT.br. El equipo que se ocupaba todo el tiempo de los aspectos técnicos era un equipo de seguridad de la información. Ellos ya tenían en Brasil un proyecto que se llamaba HoneyPots, con el mismo modelo aplicado en el exterior. ¿Qué dijeron ellos? HoneyPots significa botes de miel, es decir, son computadoras puestas en la red especialmente para ser atacadas y recoger información sobre el ataque, información que luego se utiliza para perfeccionar nuestra defensa. Esto es un HoneyPot. Basado en el proyecto HoneyPots, una experiencia internacional ya aplicada en Brasil, el personal del CERT.br contrató al departamento liderado por el profesor Wagner Meira, en la UFMG, para hacer la depuración de los datos de lo que pasó a ser conocido como s*pampots* —computadoras listas para ser atacadas, computadoras zombi para enviar *spam* a todo el mundo.

Se instaló una serie de s*pampots* por todo Brasil en diversas redes y computadoras preparadas para recoger datos sobre cómo actuaba el *spammer* y a dónde se dirigía el *spam*. A partir de estas bases de datos y de las informaciones recolectadas por diversas computadoras especialmente preparadas, luego de este experimento se concluyó que las computadoras brasileñas eran utilizadas en la red internacional para servir de pasaje para un *spam* que se dirigía a otro lugar. Este fue el principio del proyecto SpamPots, en el cual la UFMG se involucró básicamente en los algoritmos de depuración de los datos de identificación (de dónde vienen, hacia dónde van, en qué idioma están escritos, etc.).

CAF: ¿Diría que la característica de múltiples partes interesadas del Comité Gestor se reflejó en este proceso? En caso afirmativo, ¿cuáles son las ventajas y los retos de esta característica?

HF: Bien, antes que nada esta experiencia brasileña de lucha contra el *spam*, particularmente la gestión del puerto 25, fue un ejemplo clásico de cómo un ambiente de múltiples partes interesadas o *multistakeholder* puede funcionar para proveer o mejorar la gobernanza de Internet. Es decir, este proyecto muestra típicamente cómo el sector académico, el sector técnico (porque la gestión del puerto 25 es una solución técnica), los usuarios, la sociedad civil y el segmento de la cadena de valor de Internet, los proveedores de acceso y los proveedores de servicios de comunicación, junto con el gobierno, tienen que trabajar juntos para resolver un problema que nos afecta a todos.

¿El gobierno podría hacer esto por sí solo? Podría, pero de una forma impositiva y no en forma de diálogo, como fue el caso. De hecho, nosotros involucramos al gobierno porque en algún momento se vio la necesidad de la regulación, tuvieron que participar Anatel y el Ministerio de Justicia, pero el proyecto ya estaba en marcha. La cuestión del *spam* es un problema nacional. Brasil no lo podía resolver externamente, debía ser una solución creada dentro de nuestras fronteras. Y efectivamente se requirió la cooperación de todos: el sector académico estudiando el problema, proponiendo las mejores prácticas, los proveedores y los operadores haciendo su parte también. Por esto yo creo que es un ejemplo de cómo la gobernanza de Internet también se debe ejercer en las capas de servicio y la razón por la cual tiene sentido una gobernanza multisectorial.

CAF: ¿Cómo relaciona el proceso de gestión del puerto 25 con el debate sobre la neutralidad de la red?

HF: La cuestión de la neutralidad de la red relacionada con la ges-

tión del puerto 25 surgió bien al inicio, incluso antes del decreto del Comité Gestor, planteada por el propio representante de Anatel en el Consejo. Anatel ya se preocupaba por esta discusión, ya que se iba a bloquear algo que normalmente estaba abierta y la aplicación de este criterio podía ser visto como una ruptura de la neutralidad. Resulta que la conclusión en aquella época —en ese momento el tercer sector también ya se había posicionado tratando de entender si había una ruptura de neutralidad o no— fue que la gestión del puerto 25 era una medida técnica que se justificaba por el beneficio para la operación y la seguridad de la propia red. Por lo tanto, si se entendía como algo que alteraba la neutralidad, podría ser caracterizada como una excepción, como una medida que de común acuerdo, algo que todas las partes aceptaban que sería una buena práctica.

De hecho, hasta es discutible que el bloqueo del puerto 25 produce una ruptura de la neutralidad, dado que se analiza el encabezado del mensaje pero no el mensaje propiamente dicho, no tiene que ver el mérito del contenido del mensaje que está siendo enviado. Es simplemente un direccionamiento. El puerto 25 es un campo de direccionamiento que tiene que debe ser verificado por los *routers* para entregar el mensaje.

Incluso la ruptura de la neutralidad es un punto polémico. Algunas personas ni siquiera consideran que haya una ruptura de la neutralidad. Con seguridad, si hubiese tal ruptura de la neutralidad por haber sido analizado el encabezado del paquete, el asunto fue tan discutido, tan negociado y profundamente estudiado que no habría dudas sobre que es algo para el bien de todos. Esto significa que no tuvo nada a ver con un filtrado o una priorización del tráfico de una forma no transparente en beneficio de alguien.

En relación con la neutralidad de la red, lo que nosotros defendemos es la transparencia de las prácticas de gestión de redes y que no haya privilegios sobre los paquetes o contenidos. Esto no fue el caso. Objetivamente, en verdad, esta cuestión era una falsa cuestión. No hubo ruptura de la neutralidad y esto no afecta en nada lo que defendemos sobre ella.

CAF: En relación con la gestión del puerto 25, algunos gobiernos optaron simplemente por una decisión administrativa, ejecutiva, a ser cumplida por el sector privado y que bastaría para coordinar la gestión del puerto 25. En Brasil no sucedió así y tuvimos este largo proceso, que tuvo las ventajas de haber sido diverso pero demoró más de lo que seguramente hubiera demorado una simple orden ejecutiva. ¿Cree que el proceso de

múltiples partes interesadas, incluso demorando más, logra un mejor resultado? ¿Podría elaborar un poco más sobre esta cuestión y lo que implica la calidad de un proceso de múltiples partes interesadas aplicado a la gestión del puerto 25?

HF: El ejemplo que me viene a la mente cuando usted menciona otros países que adoptaron esta medida pero de diferente forma es el de Japón. Ellos efectivamente tomaron una decisión gubernamental. Bloquearon el puerto 25: allí no había ninguna excepción. Los japoneses vinieron a Brasil, conversamos con ellos mientras estábamos en proceso de entender qué se podía hacer. Pero la cultura y la realidad de mercado brasileñas son muy diferentes.

En Brasil tenemos una multiplicidad de partes interesadas, tanto desde el punto de vista de la provisión de acceso, como desde el punto de vista de los proveedores de comunicación, por lo que me parece mucho más complicado lograr el mismo objetivo a través de una medida gubernamental.

En Europa o Estados Unidos, donde esto se hizo de manera global sino a través de iniciativas de algunos operadores, se obtuvieron efectos semejantes a los nuestros sin que haya habido un esfuerzo de una entidad *multistakeholder* de gobernanza de Internet como es el Comité Gestor. Yo creo que, para el mundo en desarrollo y para los países que aún figuran en la lista de los que más envían *spam*, el enfoque *multistakeholder* sería el mejor porque es bastante complicado hacer esto de arriba hacia abajo, mediante *enforcement* gubernamental, en un ambiente de alta competencia donde hay actores de tamaños diferentes. En nuestro caso demoró mucho porque tuvimos que involucrar al gobierno. Si hubiese habido un convencimiento puramente técnico de las razones por las cuales se podía hacer, todo se habría resuelto mucho antes. Demoró más porque tuvimos que seguir todos estos trámites gubernamentales, pero creo que es un buen camino para los países que aún no cerraron el puerto 25 y hoy son los campeones en nuestro lugar.

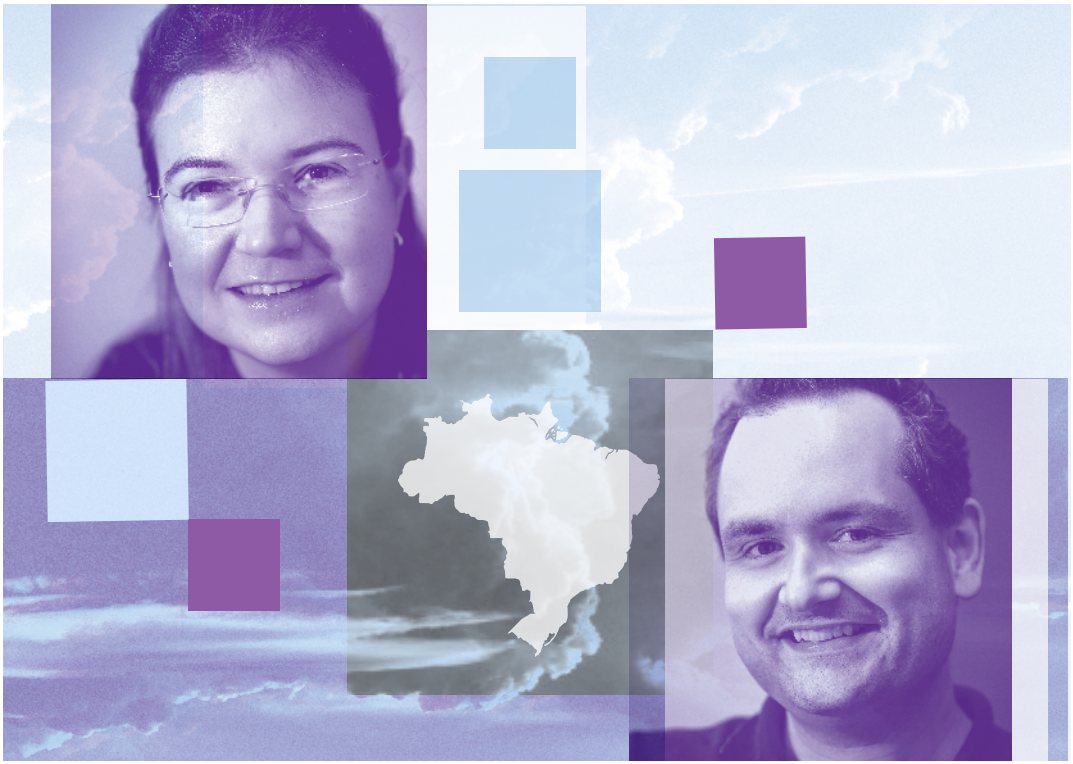
Para concluir, aunque la gestión del puerto 25 haya sido un proyecto que tuvo éxito y es lo que más aparece en el trabajo de este grupo del Comité Gestor, el Antispam, en realidad todas las cosas se sumaron y se ayudaron mutuamente. De nuestro proyecto de ley antispam salió una iniciativa importante que aún se encuentra en curso y que es la autorregulación del *e-mail marketing*. Los mensajes comerciales no deseados que reciben los usuarios comerciales son inconvenientes, pero también la gente del ámbito del *e-mail*

marketing necesita vender sus productos. Nosotros siempre sostenemos que no se debería enviar el primer *e-mail* antes de haber entablado una relación comercial o que el usuario haya indicado que desea recibir el *e-mail*, pero seguramente el *e-mail marketing* es una actividad importante para dar soporte a varias actividades en la red. Por esto, la gente de *e-mail marketing* se reunió en torno a la discusión sobre si debía haber o no haber una reglamentación. Nuestro colega Jaime Wagner, quien ayudó mucho en el proceso como representante de los proveedores en la época de 2009 a 2010, se puso al frente de un proceso interno entre los proveedores de *e-mail marketing* para crear el código de conducta para el envío de mensajes electrónicos. Este código de ética regiría el buen comportamiento y los malos publicistas que enviasen mensajes electrónicos no solicitados, caracterizando así un *spam,* serían castigados o advertidos por esta asociación interna. Creo que este resultado aún se está probando, pero fue una buena iniciativa. Pasamos a aceptar que el *e-mail* sea usado como propaganda, pero se han establecido límites relacionados con la privacidad y a la voluntad del individuo, creándose así un buen efecto que este grupo acabó por producir.

Otra cosa que fue fundamental es la educación. El sitio <antispam.br> dio soporte a toda esta sensibilización con respecto al problema del *spam*.

El problema del *spam* no terminó. Salimos de la lista de los países que más envían *spam*, pero aún es un problema. Un problema inclusive en otros medios: redes sociales, SMS. Por lo tanto, este trabajo de educación, sensibilización y alerta a las personas es fundamental y es un subproducto que está ahí hasta el día de hoy. Hacemos campañas para divulgar este sitio que es una referencia y que acabó ayudándonos mucho en la implementación de la gestión del puerto 25.

Por lo tanto, el balance que yo hago es bastante positivo, ya que logramos nuestros objetivos en esta cuestión del *spam* hacia fuera. Y todo este trabajo dejó, vamos a decirlo así, reflexiones interesante para cuestiones futuras, para que sepamos que, a través de proyectos que involucren a los diversos sectores, es posible hacer que las cosas cambien. Cuando empezaron los problemas con el *spam* todos decían que sería un problema intratable y demasiado complicado. Realmente es complicado —sigue siendo complicado— pero probamos que se puede hacer algo y de esta es mi conclusión sobre todo el proceso.



2. Entrevista con Cristine Hoepers y Klaus Steding-Jessen

Realizada en São Paulo el 25 de agosto de 2013

Marília de Aguiar Monteiro: ¿Podrían presentarse e indicar cuáles son sus funciones en el CERT?

CH: Mi nombre es Cristine Hoepers y soy actualmente gerente del CERT.br. Ingresé aquí como analista de seguridad. Al principio nos ocupábamos de incidentes más técnicos, pero con el paso del tiempo se fue volviendo más político. Hoy en día trabajo asesorando al Comité Gestor, en la capacitación de nuevos profesionales en el área, en algunos proyectos, en la parte de sensibilización. En aquella época de la CT-Spam mi actuación era más en el área técnica, pero también fue una participación muy grande para entender el problema y convencer a los actores de que la solución propuesta sería efectiva y tratar de explicar exactamente qué era a todos los actores que no eran del área. Creo que esta fue la mayor dificultad en aquel momento.

KJ: Mi nombre es Klaus Jessen, soy gerente técnico del CERT.br.

También empecé en 1999, en la época en que no era el CERT sino el NBSO, lo que significa que estoy aquí en el CERT hace tiempo. Sobre mis actividades, actualmente tengo mayor interacción con nuestro equipo que se ocupa de los incidentes, pero la mayor parte del tiempo trabajo con proyectos, análisis de tendencias, analizando las amenazas a Internet en Brasil, instalando algunos sensores. SpamPots es uno de estos sensores. Tenemos otros tipos de sensores. También estoy involucrado en la parte de capacitaciones, nuevos equipos de respuesta a incidentes, proyecto que empezó en 2004, y también en el asesoramiento a los grupos del CGI.

En relación a la gestión del puerto 25, mi participación fue principalmente en reconocer que era de suma importancia y que tenía que ver con la parte de seguridad. Al comienzo se escuchaba mucho "¿esto qué tiene que ver con la seguridad?" y para nosotros esto siempre estuvo muy asociado al abuso de la infraestructura, al abuso de la red. Independientemente de lo que está circulando en el contenido del *spam*, antes que nada, esto es un abuso de nuestra infraestructura y un abuso de nuestra red. Fue así que empezamos a involucrarnos con el asunto del *spam*, antes que esto llegase a Henrique. En aquella época, yo también estaba haciendo mi doctorado y algunas cosas de ahí ayudaron en el proyecto. Un primer prototipo de estos sensores para capturar *spam* empezó por ahí. Luego, conversando con los consejeros, con Marcelo Fernandes, quedó claro que este era un proyecto que podíamos desarrollar en el Comité Gestor; había un "sensorcito" que detectaba qué sucedía en términos de *spam*. Esto fue creciendo y contribuyó, desde el punto de vista del proyecto como un todo, produciendo números. Al principio, como dijo Cristine, nadie estaba muy convencido de que esto realmente estaba sucediendo, hasta que mostramos números chocantes. "¡Miren! Capturamos quinientos millones de mensajes de *spam* con apenas 10 sensorcitos en redes brasileñas". Una reacción típica de la época era oír que se trataba apenas de un problema teórico. Creo que nuestra mayor contribución fue justamente salir del problema teórico y mostrar que estábamos hablando de números palpables.

CH: Complementando esta parte de números, una cosa que oíamos antes de nuestra investigación era que los números disponibles venían de los fabricantes de software *antispam* y *antivirus*. Por lo tanto, por más que supiésemos que había algún problema, necesitábamos tener una métrica, un dato que fuese neutro y que mostrase que el problema existía; que hiciese salir del problema teórico y mostrar lo que realmente sucedía en Internet en Brasil. Esto fue un punto que surgió en una charla con Marcelo Fernan-

des. Él dijo: "si logramos ver que este problema existe, entonces vamos a hacer un proyecto que muestre el tamaño del problema y cómo está sucediendo". Y empezamos con esto en 2006.

KJ: En 2006 empezamos con los *spampots*.

MM: Hablando de *spampots*, me gustaría que explicasen cuál es el perjuicio que el *spam* ocasiona y, principalmente, los resultados de este proyecto inicial —el proyecto SpamPots— que luego originó el proyecto de implementación de la gestión del puerto 25. También les pido si pueden explicarnos qué es la gestión del puerto 25 y por qué fue escogida como la principal medida para combatir los resultados.

KJ: Mi percepción es que la imagen de Brasil en el exterior siempre nos ha afectado mucho, es algo que siempre nos ha orientado. Brasil estaba en el Top X de varias listas negras por ahí. Esto siempre fue algo que nos motivó: mejorar la imagen de Brasil. Siempre había alguna conferencia de seguridad a la que íbamos, creo que desde 1999, donde alguien acababa diciendo: "ah, pero Brasil envía mucho *spam*. ¿Qué está sucediendo? Se encuentra en los top no sé cuánto..." Desde 1999. Y lo mismo sucedía con los incidentes de seguridad "ah, pero muchos incidentes de seguridad salen de Brasil." Año tras año vimos una mejora en esta parte de los incidentes, a través de nuestros esfuerzos para crear más grupos de respuesta a incidentes. Esto fue sucediendo poco a poco, pero no veíamos esa mejora desde el punto de vista del *spam*. Era la misma letanía de siempre sobre que Brasil era el rey del *spam*. No sé qué crees tú, Cris, pero uno de nuestros principales motivadores era "cómo mejorar la imagen de Brasil en el exterior." Otro motivador era que ni siquiera se trataba de *spam* de Brasil. Era lo peor de dos mundos. Si ya estaba mal un negocio, un *spammer* de fuera estaba abusando de las redes brasileñas.

CH: Creo que este es el principal punto. Nosotros no estábamos atacando "Ah, estoy recibiendo mucho *e-mail*, voy a hacer un filtro mejor". La cuestión no era solo que estábamos perdiendo tiempo sino que estábamos perdiendo ancho de banda aquí en Brasil. Estaba todo el problema operativo del personal que tenía que lidiar con el exceso de tráfico; todos los proveedores de Internet de Brasil estaban entrando en redes de bloqueo alrededor del mundo; todas aquellas *blacklists*, en algunas de ellas ya se podía leer "quiero bloquear cualquier *e-mail* que llegue de Brasil", ni siquiera se especificaba más la red. Entonces llegamos a un punto en que todo el mundo estaba reaccionando, bloqueando las cosas que llegaban de Brasil. Esto era un impacto muy grande que sufríamos y era necesario probar que el origen estaba fuera de Brasil, en elementos que abusaban de las computadoras infectadas

en Brasil para enviar *spam* fuera del país. Y ahí está el mayor problema: ¿cómo saber qué están haciendo? Nosotros, que luchamos todos los días en el frente, veíamos aquello, pero realmente faltaba un número, un proyecto didáctico para convencer a las personas. Los desafíos eran dos: convencer al personal técnico, que era una combinación de no saber que las decisiones de diseño de red que habían tomado podían encarecer la implementación de la gestión del puerto 25. Notábamos esto, pero no estábamos seguros. No teníamos mucha explicación del motivo por qué no adoptar; entonces, si ellos no pensaron en la gestión de la red, podría haber más dificultades en la implementación.

Pero, desde el punto de vista del impacto, creo que era esto: la imagen de Brasil. Creo que fue el mayor impacto político que tuvimos; lo que originó la visita de la delegación japonesa. Ellos vinieron a cobrarnos porque no estábamos atacando el problema. Éramos los "testaferros" del *spam* mundial. Y el resultado de la gestión nació de esto.

KJ: En realidad hay un contexto en esta historia que es importante. El CERT.br mantiene otro proyecto llamado Honeypots Distribuidos, que existe desde septiembre de 2003 y busca medir otras cosas en Internet en Brasil, como ataques, computadoras infectadas en general que no entraban en el ámbito del *spam*. Es un proyecto que existe hasta hoy; cumplió 10 años en septiembre de 2013 y tiene cerca de 50 sensores esparcidos por la red brasileña.

Entonces ya teníamos *know-how* con los *honeypots*. Sabíamos colocar una máquina que emulara ciertas medidas, que no fuera manipulada por el abusador pero que le permitiera practicar ciertos ataques, como forzar una contraseña, que es un ataque de fuerza bruta. SpamPots fue, vamos a decirlo así, una especialización de este proyecto. Olvidemos todo el resto de los ataques y concentrémonos en algunos ataques específicos intentados por los *spammer*s: configuraciones incorrectas del proxy, configuraciones incorrectas de los servidores de *e-mail*.

La primera encarnación del proyecto SpamPots era apenas una modificación de lo que ya teníamos del proyecto anterior, que usaba algunos servicios como el software HoneyDe y algunos *sripts* que escribí y que básicamente emulaban esto.

El *spammer* salía barriendo Internet, buscando puertos. Hacía un conjunto de pruebas para ver si la computadora estaba dispuesta a realizar ciertas acciones, como encaminar tráfico de red. Y nuestro sistema ofrecía respuestas al *spammer* dando a entender que "sí, funcionó". Básicamente, indicaba en esos puertos de proxy abierto

la computadora a conectar o el servidor de *e-mail* en el destino X, devolvíamos que "sí, funcionó su comando, ¿qué desea hacer ahora?"

Es claro que jamás se conectaba a ningún lugar, mantenía al *spammer* en una especie de *loop*. Y cuando el *spammer* creía que había llegado a su destino, empezaba a inyectar *spam*. Esta fue la primera encarnación, que empezó como una prueba y después, conversando con Marcelo Fernandes, se pasó a instalar en computadoras con banda ancha. Realmente queríamos recrear ese escenario de un usuario residencial usando su Windows infectado en una conexión de banda ancha. Y así fue. Escogimos cinco operadores en aquel entonces, y para cada uno de ellos escogimos una modalidad —IP fija, residencial y otra residencia, IP dinámica... y así tuvimos cinco operadores.

CH: La idea era tener seis, pero nunca logramos activar las conexiones en Oi, que en ese entonces era Brasil Telecom.

KJ: Sí, era un trabajo 100% voluntario. Algunos consejeros del CGI.br pusieron computadoras en su casa. Fue el caso de Carlos Alfonso, de Henrique Faulhaber y también de Marcelo Fernandes. Teníamos una computadorita donde instalamos un *Unix*, un *OpenBSD*. El voluntario cogía esa computadorita, la ponía en su conexión de banda ancha y la dejaba conectada. Y tenía que soportarme llamándole cuando se perdía allí la conexión.

CH: ¿Por qué escogimos hacer esto? Los operadores no sabían que estábamos midiendo. Queríamos hacer una medición sin que el operador supiera. Y el segundo punto es que queríamos emular una situación real, una banda ancha real, en la casa del usuario, donde falta luz, donde la empleada desconecta el cable, una computadora real, pero sin tener a alguien efectivamente enviando *spam*. Queríamos eliminar la mayor cantidad posible de influencias del experimento y hacerlo lo más creíble posible. En aquella época, empezó a aparecer el problema de la calidad. Aún no existía el proyecto de la Banda Ancha, el SIMET, pero ya teníamos algunos informes.

KJ: Fue con el CA, en Río, con el Velox que quedó claro. No era posible permanecer así en el aire 15 minutos. Y era la banda ancha que caía. Lo llamaba y le decía: "Reinicia el módem, haz eso,..." y así... Fue el precursor de la calidad... ¿Recuerdas a Mariana? ¿Era cuál? ¿AJato? ¡Nunca caía! Era más estable que muchos *datacenter*.

CH: En el fondo, pensando bien en el proyecto, ¿qué queríamos medir ahí? Exactamente una computadora que no tuviera un *spammer*. Ya que se habló sobre el proxy, es importante recordar que era muy difícil explicar qué puerto, qué servicio, estábamos emulando. Uno

que era un servicio de proxy: se tiene una computadora en casa y se quiere compartir la banda ancha, entonces hay un montón de revistas que dan consejos, configura aquí, allí; el puerto está abierto y cualquiera en Internet puede acceder a su banda ancha. Hoy, la mayoría de los códigos maliciosos infecta la computadora, principalmente los *botnets*, que exploran diversos servicios. Y uno que hacen siempre, pueden alquilar, abrir un puerto de proxy que es específicamente un servicio para quedarse haciendo esto.

Nosotros emulábamos eso. No es que emulábamos una técnica para enviar *spam*, sino que lo usábamos para permanecer ocultos. Entonces podemos decir que el problema existía y que no era pequeño porque el volumen, con solo 10 computadoras, dejó a todos conmocionados. Creo que hoy, después que haber hecho nuestro plan interno, lo hicimos en escala mundial.

KJ: Por más grandes que fueran los problemas, fueron 10 computadoras, 15 meses de recolección y 500 millones de *spam* capturados.

CH: ¡*Spam* entrando! Esto habría alcanzado un promedio de personas 10 veces mayor, pues cada *spam* tenía un promedio de 10 destinatarios.

KJ: A veces era un problema hasta para nosotros. Era tanto el consumo de ancho de banda del *spammer* que muchas veces nuestro servidor no lograba capturar la información. Tuvimos que desarrollar un esquema de cola para dar mayor prioridad a la recolección que a los *spammers*, caso contrario no lograríamos capturar los datos.

CH: Y hubo algo que se planteó mucho en la discusión del puerto 25: el ancho de banda es asimétrico. Esto es, hay un ancho de banda de bajada, pero los operadores tratan siempre de no decir cuánto es la subida, que hoy en día casi siempre va a ser como máximo de 1 mega. Veíamos que el límite que los *spammer*s tenían era el ancho de banda de subida, porque son cosas que salen de su computadora. En realidad, esto afectaba toda la experiencia del usuario. El usuario no lograba mantener una conexión estable, no lograba subir nada a una red social. Esto ahogaba completamente el ancho de banda del usuario.

Y ahí es que entra un poco lo que se discutió como otro efecto: el efecto de banda. Los *spammers* consumían más que apenas el ancho de banda de subida del usuario. Y ahí estuvo el trabajo de la UFMG. Ellos hicieron *data mining* en los *e-mails* y un trabajo a partir de los idiomas de los *e-mails*. No solo vimos que un 99% de las conexiones de IP venían del exterior, sino también que con seguridad un 90% iba para destinatarios fuera de Brasil, en chino. Quedó claro que se trataba de personas del exterior que estaban abusando de nuestra estructura.

KJ: China y Taiwan.
CH: Cerca de un 70%. ¿Qué sucede hoy? Estamos viendo un proceso internacional que está cambiando. Vemos que se está abusando menos de Brasil, pero está migrando. Y es la misma historia, una medida que va a hacer que el *spam* sea más caro cuando todos los países la implementen. Para ellos es ahora mucho más costoso permanecer anónimo. El objetivo de todo *spammer* es evitar ser rastreado, siempre se está corriendo atrás de las víctimas.

Todos sufren en esta cadena: la IP del proveedor que se bloquea, el usuario que se queda con luces intermitentes en el módem, el disco, y no sabe qué está pasando en su banda ancha... Es un conjunto de cosas. Entonces, si logramos hacer que sea más difícil para los *spammers* abusar de esta manera, ellos tendrán que utilizar técnicas más costosas, no necesariamente en dinero, pero sí en tiempo, efectividad, en cantidad de *spam* que logren enviar.... Van a tener que crear una contraseña o una cuenta fácilmente detectable.
KJ: Quiero enfatizar algo que usted mencionó y que no solo fue importante para destacar el volumen de los abusos, sino que fue algo que quedó claro como el agua. Pese a que varios puertos de proxy estaban siendo abusados, todos tenían el mismo objetivo: salir con destino al puerto 25. Esto era lo que el *spammer* quería. Entraba a través de un *malware*, de una mala configuración del *e-mail* del usuario. Intentaban de todo, pero todos tenían el mismo destino: el puerto 25. Allá donde había un servidor de *e-mail*, allí es donde efectivamente se dirigía el *spammer*. Esto fue algo grandioso para mostrar: en este caso la gestión del puerto 25 sería devastadora. No solo se mostró que existía el abuso, sino también que todos tienen en común ese mecanismo: destino al puerto 25.

Al comienzo algunos operadores dijeron que sería mejor bloquear las conexiones entrantes con destino al proxy, pero nosotros lo desaconsejamos diciendo "¡Miren, hoy hay 30!" Y a veces el *malware* puede ser colocado en cualquiera, pero el destino del *spam* tiene que ser el puerto 25. Caso contrario, no logra interactuar con un servidor de *e-mail* en este puerto, que es estándar del SMTP.
CH: En 2005, cuando empezó la CT-Spam, pensado con Rubens Kuhi, redactamos un documento técnico de lo que se podría mejorar. En aquella época esto se había hablado sin que lo llamásemos gestión del puerto 25, porque era algo que estaba empezando a ser discutido entre los ISP (Internet Service Provider – Proveedores de Servicio de Internet) en el mundo y aquí en Brasil fuimos los pri-

meros a recomendar en un documento. Poco después, en 2005 salió unarecomendación dando a esto el nombre de "Port 25 Managing"[2].

MM: ¿De dónde vino esta recomendación?

CH: Esta recomendación es del MAAWG (Messaging Anti-Abuse Working Group, un gran grupo de trabajo de ISPs de Europa y de Estados Unidos), pero la nomenclatura varía. Japón lo llama OP25B (Outgoing Port 25 Blocking). El primer desafío era definir un tema que no asustase a los gestores: un bloqueo siempre asusta. Aquel asunto del término técnico vs. el término no técnico. En definitiva se trata de una gestión y no de un bloqueo. Si se bloquea, se acaba con el *e-mail*. Era necesario diferenciar el usuario de quien era el servidor que estaba transportando, intercambiando el mensaje.

MM: ¿Nos podrían explicar la gestión?

KJ: Esto fue una experiencia que tuvimos en todas nuestras reuniones con periodistas. Fue increíblemente difícil explicar lo que era.

CH: Una de las partes más difíciles del trabajo fue explicar la gestión del puerto 25.

KJ: Yo lo diría así: en todo esquema de *e-mail* existen básicamente dos servicios que debemos entender: envío, que es el cliente enviando el mensaje al servidor, y un segundo servicio que es el transporte, es decir, servidores hablando con servidores. En la gestión del puerto 25, es evidente esta división de características y se aplica que en ciertas redes, como en las redes residenciales, solo puede haber envío. Básicamente, lo que la gestión del puerto 25 hace es impedir el transporte —no tiene sentido hablar en transporte en una red residencial, ya que no hay servidores de *e-mail* allí... Es garantizar que en las redes de carácter residencial, 3G, IP dinámico y similares solo habrá envío; y que el transporte será hecho por el resto. Básicamente es obligar a que esto suceda así.

Antes de la gestión del puerto 25, en las redes comportadas esto no sucedía; en las redes no comportadas había computadoras que en el fondo estaban haciendo transporte, queriendo hablar con el servidor y no con alguien a mitad de camino para hacer el envío —y envío implica autenticación—. Separación y un *enforcement* entre actividades muy distintas que son el envío y el transporte, eso creo yo.

---

2 MAAWG, MAAWG Recommendation: Managing Port 25 for Residential or Dynamical IP Space Benefits of Adoption and Risks of Inaction. Disponible en <http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf>. Consultada el 12 de octubre de 2013.

Carlos Affonso Pereira de Souza: Yo comprendo por qué los periodistas se asustaron.

KJ: Hablábamos de puerto todos se preguntaban: "¿qué es el puerto?"

CH: Creo que tratamos ir mejorando nuestra definición de gestión del puerto 25 a lo largo de los años. Cada vez que había una reunión con alguien no técnico y cada vez que cambiaban los representantes en el grupo sobre gestión del puerto 25 teníamos que explicar todo nuevamente.

Y hay una cosa que no sé si ya mencionamos o no, pero es algo que fue el eje de todo este grupo de trabajo. Estábamos recomendando en 2005/2007 y aún estábamos trabajando. Tratábamos de llevarlo a la gente del CGI y decir que esto se debía implementar de una forma más política, mientras ellos argumentaban que se trataba de una decisión técnica.

De hecho, las reuniones empezaron en 2009. Creo que un punto importante fue la publicación de "Brasil, the king of spam", que tuvo un impacto muy grande. Se publicó en varios periódicos norteamericanos, en la prensa, y ahí nos dimos cuenta de la dimensión del problema. Todos cayeron en sí pensando "¿por qué no hacemos algo?" Me acuerdo que el coordinador del CGI en ese entonces me pidió que escribiese un artículo desmintiendo este hecho.

En aquella época llegó del CGI la indicación de que debíamos desmentir esa información. Fue en ese entonces que tuve que escribir un artículo explicando que no teníamos *spammers*, que se trataba de un abuso de la red y ya mencionaba los resultados de los s*pampots*. Aquello dio el empujón que faltaba para organizar una reunión interna en el CGI, solamente con los consejeros. Se decidió hacer una reunión formal para ver qué sucedía, por qué se había salido del control, estábamos entre los top 10 y de repente pasamos al primer puesto en todas las listas. Seguramente ese "Brasil, el rey del *spam*" fue un punto de inflexión en la postura general.

Técnicamente, la verificación sería sencilla para nosotros: separar el envío del transporte. Separar el envío del transporte nunca generó problemas para nadie. Para bajar los *e-mails* del proveedor se utiliza un protocolo, IMAP o POP. Se usa algún otro mecanismo para buscar los *e-mails* y la parte del envío fue la que generó más estrés. Pero tener esta división y cambiar los usuarios del puerto 25 para autenticación en el puerto 587 solo sería efectivo si el proveedor de conectividad lograba bloquear la salida del puerto 25. Este elemento dio mucho trabajo por aquello de que primero se debía

migrar el usuario, después las empresas implementando. Porque aquí en Brasil no se tiene este concepto de que quien provee conectividad también provee *e-mail*. En algunos países que vimos —en el propio Estados Unidos, Comcast fue la primera en implementar, en 2003, luego AT&T— y ellos decían "Mira, eres nuestro cliente. ¿Quieres enviar *e-mail* a través de nosotros? Puedes hacerlo, pero usa el puerto 25, pero si tienes otro, te las arreglas".

Aquí en Brasil era un poco más complejo porque los operadores decían que no podrían servir *e-mail*, que no tenían como bloquear. Los clientes de Telefônica tienen "n" proveedores, clientes de Vivo, de Oi, clientes de proveedores de radio en el interior. Por lo tanto, esta coordinación era necesaria para no generar un impacto en Brasil y que nadie lograse enviar *e-mails*. Era algo lógico: primero migrar los proveedores y sus usuarios a un puerto nuevo, que es básicamente abrir el lector de *e-mail* y cambiar el puerto, nada muy complejo. Y luego efectivamente implementar el bloqueo. Además, también está toda la parte que solo sabemos de las reuniones — porque no puedo, porque no voy a hacer... Una dificultad especifica de nuestro modelo regulador era esta: no había manera de que un operador lo hiciera mucho antes que otro y era necesario tener esta coordinación entre los actores (quien era proveedor del servicio de *e-mail* y quien era proveedor de la conexión, sea radio, 3G y etc.).

KJ: Quiero añadir que en el entendimiento del proceso en la prensa veíamos "¡Entonces vamos a bloquear el puerto 25!" y nosotros decíamos "No, mira, el puerto 25 se sigue usando en el transporte". Y ahí llegaba la opinión de un experto, una persona que no entendía muy bien lo que se estaba proponiendo, y decía "¡Esto es un absurdo! ¿Quieren bloquear el servicio del puerto 25? ¡Esto mata el servicio de *e-mail*!" Sí, mata el transporte, ¿verdad?

Esa diferenciación entre envío y transporte no estaba clara para todos. Esa diferenciación de quién hace cada cosa, a partir del acceso al servicio de *e-mail,* en esas discusiones había una gran dificultad para entender los números. Quien proveía la conectividad no sabía cuántos proveedores de *e-mail* había por ahí. El razonamiento era el siguiente: No sabemos quiénes están involucrados, no vamos a salir por ahí a bloquear si no estamos seguros de que nuestro usuario tiene alternativas para el envío".

Y había otra duda relacionada con el *webmail*. Dijimos desde el inicio que el *webmail* no se vería afectado. Incluso para los grandes proveedores, como Terra, no estaba claro quién usaba *webmail* y

quién usaba otro servicio. Entonces, para ellos, la cuestión se resumía diciendo que no iban a hacer el cambio si sus competidores no lo hacían y si todos los usuarios no estaban migrados.

CH: Y fue ahí que empezó: si las empresas de telecomunicaciones no lo hacen, nosotros no migramos a los usuarios.

KJ: Cada uno esperando al otro y la cosa no caminaba.

MM: La próxima pregunta es sobre la coordinación entre los actores. Inicialmente empezó entre los proveedores de conexión y las empresas de telecomunicaciones; ellos fueron los primeros en ser contactados a partir de la implementación de la CT- Spam. ¿Se pensó desde el inicio que sería una coordinación entre actores de diferentes sectores o solamente entre actores técnicos?

CH: Creo que nuestra esperanza era que no hubiera tanta burocracia. Era una medida técnica, una acción compleja; actualmente ellos implementan diversos filtros en sus estructuras; ya participamos en diversas reuniones.

KJ: Nuestra visión, tal vez en general, es que existen diversas buenas prácticas de red que ellos han adoptado y que eran la misma implementación de una buena práctica: impedir que las computadoras de los usuarios residenciales fuesen infectadas y enviasen *spam*. Imaginamos que con media docena de reuniones con el personal más técnico quedaría claro que esto implicaba un desperdicio de los recursos de red y del ancho de banda, algo malo para ellos, y harían que se sumasen a la iniciativa. Pero ocurrió todo lo contrario, inclusive cuando tratamos con el personal más técnico.

CH: Pero yo creo que ahí usted está entrando en los problemas, en esa parte inicial de los actores. En verdad, antes de empezar la CT-Spam ya habíamos tenido una reunión con el personal más técnico de los operadores y ellos decían "Yo me convencí, pero tengo que hablar con la gente de mi departamento jurídico y del área comercial" o "¿Voy a tener que incluir en mi presupuesto el cambio de los equipos?" Eran varias las dificultades y el tema no avanzaba.

Muchos decían que solo lo harían si Telefônica o NET también lo hacían. Este impasse se fue generando incluso en reuniones 100% técnicas. A partir de las reuniones con Henrique Faulhaber ya no participaba más el personal más técnico, sino que enviaban la invitación a los administradores.

KJ: Haciendo un paréntesis en esta parte de las dificultades y en relación con la definición del puerto 25, sinceramente creo que muchos personas, incluso los técnicos, tenían dificultades. Creo

que muchos no entendían cómo funciona el *e-mail* o no entendían parte de lo que estábamos diciendo. Muchos salían diciendo "¡Ustedes están locos! ¿Quieren que bloqueemos el puerto en el *backbone*?" Incluso en las reuniones más técnicas se demoró en comprender que no era en el *backbone,* era solo en la red, en las redes residenciales y en las conexiones salientes.

CH: Fue ahí que comenzó esto de traer al personal jurídico y de regulación. Con la incorporación de personal de regulación, comercial y jurídico, las discusiones se mezclaron con las del Marco Civil. Llegó el momento en que todas las discusiones llegaron a un punto muerto y se toparon con diferentes obstáculos. "Nosotros solo vamos a hacerlo si el equipo jurídico da su OK" era algo que se escuchaba con frecuencia. Después los equipos jurídicos dieron su OK.

Los argumentos esgrimidos pasaron a ser "Nosotros solo podríamos hacer esto si estuviesen involucrados los grandes de contenido o los Procons". Telefônica dijo que tenía que involucrar a los 600 Procons de Brasil, pero, como nadie se manifestó, sugerimos que fuese solamente el Procon de São Paulo.

Entonces empezó a discutirse que tendría que estar presente el IDEC (Instituto Brasileño de Defensa del Consumidor), la Proteste (Asosiación Brasileña de Defensa del Consumidor) y alguien mencionó al Ministerio Público. Para nosotros nunca quedó claro hasta dónde llegaba la insistencia de traer a todos o si solo querían ganara tiempo. Llegó un momento en que alguien en la mesa siempre decía que era regulado por Anatel.

Con Anatel se firmó un Acuerdo de cooperación, primero solo en relación con los operadores de telecomunicaciones, después con otros actores.

Siempre existía el argumento de que, si se defiende la neutralidad de la red, no se puede hacer la gestión del puerto 25. Nadie se va a beneficiar, la regla será igual para todos, ningún servicio se va a ver impedido, no se favorece a nadie en detrimento de otro. Incluso después de su firma, se demoró su la implementación de este acuerdo de cooperación.

El MAAWG ya estaba implementando la gestión del puerto 25. Yo conversaba mucho con el *chair* y preguntaba si él no tenía un estudio de caso que mostrase los beneficios de la implementación, beneficios económicos para los proveedores, y ellos decían que no, porque eso era obviamente beneficioso para los proveedores.

Mientras que aquí solo había problemas: "Esto va a tener un costo de implementación, ¿será que ustedes no tienen un estudio?" La

cuestión financiera nunca se planteó mucho; para tener métricas era necesario que los propios operadores generasen estadísticas, algo que no querían hacer. Por casi un año se discutió sobre métricas y estadísticas, pero nadie quería liberar ninguna información.

Carlos Affonso Pereira de Souza: Cristine, ¿por qué relacionas ese momento con el Marco Civil?

CH: En verdad lo que veíamos era más una cuestión retrospectiva, de *timing* de las cosas, ¿cuándo el Marco Civil fue presentado al congreso?

CAF: La discusión pública fue en 2009 y el proyecto se envió al congreso en 2011.

CH: ¿2011? En aquel momento veíamos las mismas discusiones que hasta hoy suceden: Anatel queriendo regular Internet. Veíamos una influencia muy grande de los operadores diciendo que solo lo harían si estaba regulado por Anatel. Incluso, hasta el final con el acuerdo de cooperación, muchos decían que no harían nada sin antes una reglamentación de Anatel. Era una forma en que ellos querían que Anatel regulase Internet.

KJ: En esta fase, muchos de los que participaban eran los operadores responsables por el sector regulador. Mostraban una mezcla de miedo a los reclamos de los usuarios y a ser castigados por Anatel.

CH: No sé si fue el Marco Civil, pero quedó mucho más claro después de 2010, después de la discusión pública, la necesidad de un reglamento de Anatel. Esto se podría ver como una forma de obligar a tener reglamentos de Anatel sobre Internet. ¿Pero por qué un reglamento? El departamento jurídico decía que si un usuario reclamaba a los operadores, ellos tendrían que ir hasta Anatel.

A partir de ahí hubo varias fases: algunos decían que bastaba una carta del presidente de Anatel e incluso había quienes querían un reglamento propiamente dicho. Sardenberg fue quien hizo la carta, pero para algunos no fue suficiente. Como siempre, la parte regulatoria de Anatel era reclamada por SindiTeleBrasil o por algún operador aislado; eran ellos quienes querían que Anatel regulase esto.

MM: Pero este estudio sobre el *spam* forma parte del análisis de red de las empresas de telecomunicaciones, ¿verdad?

CH: Es TCP/IP. Pasa por el *router*, pero algunos operadores implementaron el bloqueo de la salida del puerto 25 en el CPE (Customer Premises Equiopment), en el módem en la casa de los usuarios; otros lo implementaron en el concentrador; no sé si algunos lo hicieron en *router*, pero de cualquier forma este es un filtro TCP/IP, no es la base de Internet que es la telecomunicación.

KJ: Durante la discusión había esta distinción bien demarcada

entre telecomunicaciones y, ahí sí, entra Anatel y la parte de Internet, TCP/IP y otros protocolos, que no son telecomunicaciones. No entendí muy bien su pregunta. ¿Usted cree que esto es parte de las telecomunicaciones o...

MM: Si era por esto que las empresas estaban forzando una anuencia de Anatel...

KJ: Hablando técnicamente, eso es TCP/IP, puertos, capa 3.

CH: Si llega por celular, por señales de humo, lo mismo da.

KJ: Es Internet. Como dijo Cristine: da igual en qué los medios donde está implementada. También creo que la discusión se refería a la red, TCP/IP y no guardaba relación con Anatel. Esta prerrogativa de Anatel en el asunto es otra discusión.

CH: ¿Si hay usuarios con problemas en la red llamando a Anatel? Sí, los hay. Incluso nosotros en el CERT recibimos mensajes: "Envié un *e-mail* a Anatel, mi banda ancha está recibiendo muchos ataques y me dijeron que hable con ustedes". No está muy definido qué hace Anatel con los reclamos sobre Internet que le llegan.

Pero podría ser un usuario con un problema llamando a Anatel, al operador o incluso al Procon. Un punto realmente afectado fue este de involucrar a los actores.

Hubo aquél asunto, en 2009, cuando ya estábamos pidiendo la participación de alguien más político. Pero hubo un punto en que ellos empezaron a quedarse muy firmes en la cuestión económica de no implementar porque era muy costoso. Y en esa fase en que se hablaba en perjuicio al consumidor empezamos a mantener reuniones para explicar la parte técnica. Un momento clave en que las cosas se empezaron a destrabar fue cuando ingresó el DPDC (Departamento de Protección y Defensa del Consumidor).

KJ: Pero hubo un momento, Marília, que nos sonaba como una medida para ganar tiempo. Cuando se acercaba aparecía el obstáculo, como lograr el porcentaje de usuarios migrados. Parecía que esto nunca iba a suceder, hasta que UOL dijera que habían migrado el 100% de los usuarios. Pero, siempre llegaba alguien y decía: "no, hay que tener la carta de Anatel". Por este motivo, a nosotros siempre nos parecía una medida dilatoria, incluso sabiendo que no es justo generalizar.

CH: Incluso cuando trajimos a defensa del consumidor, ellos dijeron que tenía que estar el DPDC, trajimos el DPDC y nos dijeron que debía haber una nota técnica. Y nunca era así: "Usted tiene este abanico de cosas a resolver". Siempre nos traían un problema nuevo después que resolvíamos el anterior.

KJ: También parecía que estaban mal asesorados. Ni todo el personal

técnico estaba convencido de que el problema sería resuelto, pero no hablaban de eso.

CH: Llegó un punto en que todos los obstáculos estaban resueltos y solo faltaba la firma del Acuerdo de Cooperación, que ya estaba listo. Y los operadores se sentaron alrededor de la mesa y dijeron que querían un reglamento de Anatel. Esto sucedió cuando Levy ingresó al Comité Gestor, abrazó la causa y la llevó hasta el fin. Eso fue en 2010.

Llegamos a una reunión de SindiTeleBrasil con todos los vicepresidentes de regulación de todos los operadores y oímos aquellas frases célebres: "La gestión del puerto 25 es como el jarabe "Biotonico Fontoura": no va a hacer mal, pero sí puede hacer bien". Entonces el vicepresidente de un operador dijo: "Pero esto parece ser algo muy bueno, ¿por qué aún no fue implementado? Aquello para mí fue el auge.

KJ: Esto era muy frustrante para nosotros. El documento que escribimos en 2005, proponiendo buenas prácticas...

CH: Fue el primer país que formalmente propuso...

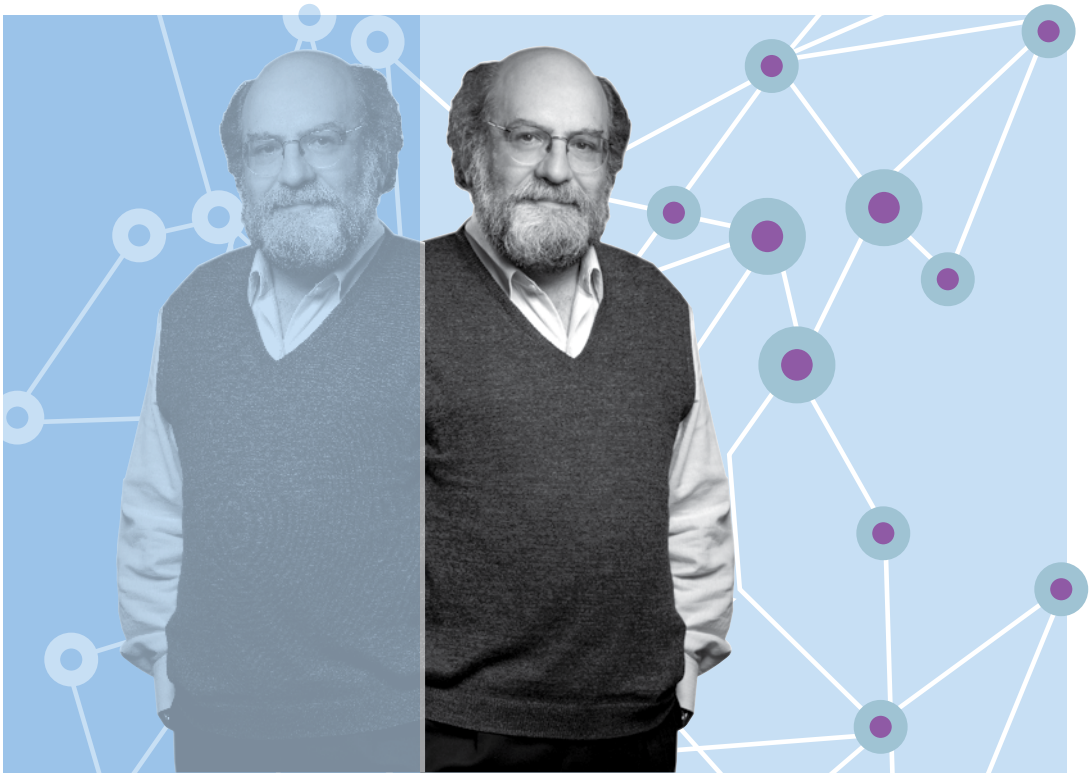
KJ: Oír a Japón cuestionando en una reunión por qué no implementábamos el texto cinco años después de escrito. Ahí Japón se decidió y en seis meses lo implementó. Es verdad que es una forma diferente de cómo Internet está instituida en Brasil. El caso Comcast fue mucho más sencillo: si se dan los medios y se suministra el servicio, es mucho más fácil tomar la decisión.

CH: Interesante es ver cómo funciona en Noruega. Hicimos una investigación dentro de nuestro grupo, entre los CERT de todo el mundo, quienes dijeron que habían escuchado hablar de esto. Recordaron que habían recibido un comunicado de los operadores diciendo que lo iban a implementar porque el problema del *spam* era muy grande.

En el fondo, es lo que ingenuamente esperábamos: porque es un asunto técnicamente sencillo, barato de implementar, y trae enormes beneficios. Por ejemplo, durante una reunión un operador que dijo que estaba implementando toda un área de gestión internacional para establecer cooperaciones para sacar a los proveedores de las listas de bloqueos. Nos preguntaron si no teníamos algún consejo para salir de las listas de bloqueo.

¡Y ellos estaban aquí desde hace dos años! Presentábamos razonamientos y métricas, pero nada. Y ellos estaban gastando dinero, creando una gestión con costos internacionales.

La única excepción clara fue Sercomtel, que la implementó en 2006, después que nosotros lo recomendamos en 2005 e incluso presentó un informe indicando por qué lo habían hecho.



3. Entrevista con Demi Getschko

Realizada en São Paulo el 25 de septiembre de 2013

DG: Mi nombre es Demi Getschko, soy ingeniero electricista graduado de la Escuela Politécnica de São Paulo en 1975, donde realicé mi maestría y mi doctorado. Trqabajo en redes desde mediados de la década de los ochenta, en especial en la Fapesp, donde realizamos las primeras conexiones de Internet, y desde entonces estamos involucramos con temas de Internet. La gestión del puerto 25 fue un tema que empezó cuando nos quedamos molestos con la posición que Brasil ocupaba en los rankings mundiales de generadores de *spam*, por lo que decidimos zambullirnos en el problema, ver los motivos y cómo eventualmente podía evitarse.

Carlos Affonso Pereira de Souza: ¿Nos podría explicar qué sería el puerto 25?

DG: El puerto 25 es un puerto usado en el protocolo conocido como SMTP. SMTP es Simple Mail Transport Protocol —protocolo simple de transmisión de *e-mail*—, Como todo en Internet,

este protocolo es simple y de alguna forma emula este proceso de colaboración que tiene Internet.

¿Qué es el puerto 25? En el puerto 25 cualquier computadora puede acceder otra, la computadora saluda y pide enviar un *e-mail*, es decir, usted le va a pedir ayuda para enviar un *e-mail* a alguien. Esto era perfectamente aceptable en Internet —apoyarse en alguien a mitad de camino para enviar un *e-mail*—; esta es la base del SMTP. Solo que evidentemente este es un puerto abierto, una puerta de entrada para los abusos. No sabíamos si había algún abuso o no. Empezamos a investigar qué sucedía con el *spam* brasileño. Esto ya lo habrán contado todos, pero nosotros descubrimos que el *spam* brasileño no era en portugués. Ahí vimos claramente que había *spam* por medio de computadoras que atraen este tipo de relación, llamados *honeypots* o botes de miel. Vimos que las computadoras eran usadas para enviar, en gran cantidad, *spam* que llegaba de algún lugar de Oriente y volvían hacia Oriente. El *e-mail* llegaba a la computadora y era reenviado incontables veces, dependiendo de la lista de destinatarios del *e-mail*, y luego regresaba.

Vimos que el *e-mail* no era nacional: no tenía origen nacional ni destino nacional. Funcionábamos solo como reflector, por lo que el procedimiento más sencillo era cambiar ese puerto por uno cuyo uso tuviese una contraseña. A un puerto con contraseña también se le puede pedir que envíe un *e-mail*, pero, como no conoce la contraseña, digamos que el abusador va a buscar una máquina que no necesite contraseña; es decir, uno se vuelve un blanco más antipático, deja de ser el primer blanco escogido, en la medida en que el puerto sin contraseña es el puerto 25. Quiere decir que dejamos de ser el blanco, lo que nos colocó por debajo del puesto 20, una posición proporcionalmente mejor dado que Brasil estaba siempre en el puesto 8 o 10. Estamos mejor que el promedio, lo que era de esperarse dado nuestro tamaño y nuestra gran participación en Internet. Esta es una descripción resumida del proceso.

Al hacerlo, se está sugiriendo algo que puede ser considerado una restricción a las cosas que en Internet estarían abiertas. De forma más dura, se estaría quebrando la neutralidad de Internet que contiene, desde su origen, en varias RFCs (Requests for Comments) la posibilidad de ser quebrada. La respuesta es sencilla: de hecho, estamos sugiriendo un quiebre de la neutralidad. Porque, de hecho, no hay neutralidad, pero sí un abuso. En realidad, al cerrar el puerto 25 no eliminamos ninguna característica de Internet, por el contrario. El

envío sigue siendo colaborativo, solo estamos dificultando un poco la vida de quienes pensaban abusar del puerto 25 para enviar mensajes no solicitados. Esto es una saludable excepción al principio de neutralidad, con una amplia justificación de beneficio general. Esto puede se puede usar en una eventual discusión sobre neutralidad, Marco Civil y otros asuntos similares para mostrar que las reglas se justifican más por sus excepciones que por sus formulaciones.

CAF: Algunos interlocutores sostienen que no se trata de un quiebre de la neutralidad de la red, porque no se accede al contenido en sí. Lo qué habría sería simplemente un análisis del direccionamiento.

DG: Por ejemplo, si se cierra el puerto oIP, no se entra en el mérito del mensaje, aunque se evita que el individuo haga esto. O si cierra el puerto telnet o TCP. En suma, es una ruptura de la neutralidad porque se está eliminando el acceso a un puerto estándar... Eliminando, no. Solicitando que no sea accedido un puerto estándar en Internet por algún motivo. Por lo tanto, no se trata de una ruptura de la neutralidad en el sentido de que se analizó y vetó el contenido de algún mensaje, porque incluso cuando luchamos contra el *spam* creemos que esto nunca se debe hacer por la definición del contenido, ya que, si vamos a luchar contra el *spam* sobre la base del contenido, ingresaríamos en un terreno movedizo y peligroso. Definimos *spam* por el comportamiento del mensaje, no por su contenido. Creo que ahí lo que sucedió fue una ruptura de la neutralidad, ya que se solicitó que no se utilizase un puerto estándar de Internet en beneficio general.

Marília de Aguiar Monteiro: ¿Esto significa que no analizar el contenido sería una cuestión de privacidad?

DG: El no análisis es una cuestión que establece que el contenido nunca debe ser analizado en las instancias intermedias. El único que tiene el derecho de acceder al contenido es el receptor. Por ejemplo, como receptor, yo tengo derecho de no querer recibir mensajes de contenido adulto e instalar un filtro para ello. Durante la intermediación, nadie tiene el derecho de decir "Ah, ese mensaje no es bueno para ti". Solamente yo, como destinatario final, que puedo ser padre o madre de familia, puedo impedir que mis hijos vean esto en casa. Pero esta es una decisión del usuario final, ya sea una familia o el responsable por una familia. Este sujeto puede hacer un filtro a partir de lo que considere razonable —no quiero contenido prejuicioso, no quiero contenido adulto, no quiero chistes—. En resumen, esta es su decisión; nadie a mitad de camino puede imponer este tipo de filtros, salvo que tenga una autorización suya para hacerlo.

MM: ¿Esto quiere decir que la cuestión de la privacidad no fue planteada en relación con la lucha contra el *spam* y la gestión del puerto 25?

DG: No, la cuestión de la privacidad nunca se planteó. Nunca definimos el *spam* según su contenido fuera comercial o no comercial. Consideramos que *spam* es algo que se recibe sin haberlo solicitado, sin que nos interese. De repente hay algo que nos interesa. Luego, al comienzo del *spam*, en los comienzos de la red, decíamos "Este asunto del *spam* es muy bueno; nunca recibo nada y de repente llega algo divertido, a veces llega una sugerencia de una compra interesante". Así, en los inicios de la red, cuando era más tranquila y no recibíamos *e-mail* de nadie, en esa época había quienes decían que querían un poco de basura, porque a veces podía ser interesante, etc. Claro que, con el tiempo, esto se transformó en una gran cantidad de basura y dejó de gustar. Pero definimos *spam* como algo que no es solicitado, independiente si el mensaje es óptimo o pésimo.

MM: Entonces, ¿el bloqueo del puerto 25 no es una limitación a una libertad comercial?

DG: Podría ser una limitación a una libertad comercial, pero en verdad, si se piensa bien, como este uso es abierto y gratuito, el puerto 587 es tan barato como el 25, solo necesita de contraseña, entonces no hay ninguna limitación comercial al proceso. Por ejemplo, creo que las campañas de *e-mail marketing* sin *opt-in*, sin que el usuario opte por recibir los mensajes, forman parte de la categoría de *spam*. No se debe enviar publicidad a nadie sin que antes la persona haya concordado recibirla. Por más que se caracterice una actividad comercial como *spam*, ésta ya se encuentra en una zona gris y cabe al usuario estimularla o no. El usuario tiene el derecho de no ser molestado, más de lo que yo tengo el derecho de enviar *e-mail*. Claro que tengo el derecho de enviar *e-mail* o a quien yo quiera, pero la otra persona tiene el derecho de no querer recibir mis mensajes.

MM: ¿Los costos de implementación de esta medida fueron vistos de alguna forma como una barrera a la implementación de la lucha contra el *spam*?

DG: No. En general las personas no notan que se ahorra al hacer esto. Con seguridad los operadores despdician mucho ancho de banda enviando *spam* para todos lados, entonces ya hay un costo injustificado. La primera cuestión que se tiene es el ahorro. En la última milla, el usuario final también tiene un ahorro si no es asumido por la empresa con la que contrató. Aquí, claro, el peligro cuando se cierra un puerto de este tipo es que se debe notificar a los usuarios que usan interfaces para bajar y subir *e-mail*, *emap* y otras cosas de este tipo. Al usuario

se le debe notificar que debe cambiar el puerto en la definición. De esta forma, si los usuarios no toman las medidas pertinentes, existe el riesgo de que dejen de recibir *e-mail* por un tiempo y después reclamen. Justamente por esto hicimos la gestión con gran cuidado, con campañas de esclarecimiento. Y los proveedores lo comunicaron a los usuarios. Llamamos también para participar a la gente del Procon, del Ministerio de Justicia, porque los proveedores querían tener la seguridad de que no serían procesados por sugerir a los usuarios que cambiaran un puerto y se perdiera algún *e-mail* en medio de este proceso. El riesgo era que fueran criticados por esto, pero sucedió lo contrario: finalmente fueron elogiados por esto. Creo que este temor no se justifica, pero hay que prever todos los riesgos.

MM: ¿Por qué se demoró la implementación? ¿A qué se atribuye la demora?

DG: Primero, esto no se puede implementar rápidamente. Digamos que se tiene 200 mil usuarios y 50 mil usan *emap* u otra forma de correo. Uno por uno, tienen que configurar un puerto antes de poder cerrar el puerto anterior. Existe este tiempo de configuración.

Después hubo una fase más jurídica en que los proveedores empezaron a preocuparse por si serían considerados responsables ante esto. Un consumidor podría ir a un Procon, reclamar "me obligaron a hacer esto, pero yo no sé hacerlo...", entonces garantizamos la comunicación vía el Ministerio de Justicia, Procons, etc. Había un ritmo, se podría haber hecho más rápido, pero también es necesario todo un proceso de cautela. Primero vimos los resultados de quien lo implementó y esto estimuló a otros. Algunos operadores empezaron antes —operadores de correo brasileños, operadores de contenido de Internet—. Vimos que no era complicado y todos fueron actuando cada vez más rápido, hasta que se produjo una avalancha. Esta es nuestra esperanza para IPv6, pero no creo que suceda.

CAF: ¿Y cómo va el proceso de implementación de IPv6? ¿Alguna información?

DG: En el proceso de IPv6 tenemos a nuestro favor que no somos el primer lugar del mundo donde se agota IPv4. Ya no hay más direcciones IPv4 disponibles en el registro asiático, que es APNIC; en Europa creo que fue en Abril de este año (2013) que RIPE anunció el fin de ese bloque. Por lo tanto, en este proceso fuimos precedidos por los asiáticos y los europeos. El próximo en quedarse sin direcciones será América Latina o América del Norte. Es difícil saber quién será el próximo en quedarse sin IPv4, porque, además de tener un fuerte stock de direcciones legadas,

América del Norte es una gran consumidora. El último será África, que tiene una reserva grande y poco consumo.

Tenemos siempre que pensar que estas cosas no son interoperables. IPv4 e IPv6 son diferentes. Aquí va a haber IPv4 para acceder al mundo IPv4 y va a haber IPv6, para acceder al mundo IPv6. En verdad, no se va a obligar a nadie a tener IPv6, pero cuando las direcciones IPv4 se acaben las direcciones IPv6 serán obligatorias. Esto quiere decir que los nuevos usuarios ya van a tener IPv6. Si ellos no encuentran un mundo que comprenda su idioma —IPv6—,van a tener una experiencia fraccionada, truncada, una mala experiencia de Internet.

Voy a dar un ejemplo. Todos declaran el impuesto a la renta en marzo o abril usando receitafazenda.gov.br. Se accede y funciona. Si se es un usuario nuevo y accede en enero o febrero por un PNBL, sea lo que fuera, y recibe un IPv6, porque no existe más IPv4, si accede a receitafazenda.gov.br, ¿será posible hacer la declaración? Hoy no. Quiero decir que pocos sitios brasileños funcionan con IPv6. Un ejemplo: hoy tenemos a la Universidad Federal de Santa Catarina, otro lugar que funciona bien es la UNESP, creo que Ceará tiene un sitio del gobierno que funciona bien. Nosotros tenemos un programa llamado "Validador" donde se puede escribir el nombre del sitio y verificar si contestan vía IPv6 o no.

Los grandes portales ya responden vía IPv6. Si utiliza UOL, UOL contesta. Terra, también. Todos los servicios internacionales, Google, Facebook, porque esta gente no está durmiendo.

Tenemos un problema bastante importante que se debe abordar y que son los sitios que ofrecen servicios a la ciudadanía, sitios del gobierno federal, estatal, municipal, y que, en general, no están atentos a esto. Hay un decreto del CGI que ha salido ahora y que tiene por objetivo estimular a las personas para que presten atención: el reloj de arena no se detiene y el tiempo de IPpv4 se está agotando.

CAF: ¿Existe un paralelo entre el proceso de gestión del puerto 25 e IPv6 en relación con la comunicación, la educación, las alianzas?

DG: En realidad no veo paralelo entre ambas cosas. En definitiva, hay que convencer a la gente que no lo ve. En este punto los procesos son iguales. Existe la impresión de que "estamos muy bien; ¿para qué necesitamos esto?" Yo espero, en este caso, que los paradigmas internacionales sean incluso más importantes que nuestra presión. Si continuamos insistiendo que esto es importante, la adopción será lenta; si se observa que afuera algo está cambiando, será diferente.

MM: ¿Usted cree que sucedió lo mismo con la gestión del puerto 25, que desde 2005 el CERT sugiere como buena práctica realizar el bloqueo, pero solamente a partir de 2010, con la llegada de un grupo de Japón que dijo que Brasil debía implementar la medida, los actores brasileños aceleraron el proceso?

DG: En realidad, cuando estuvieron aquí, nosotros le mostramos al gobierno japonés la diferencia que significó para Brasil haber cerrado el puerto 25. Ellos no nos dijeron que Brasil tenía que hacerlo, sino que querían dar el ejemplo de cómo se había hecho en su país. Y nosotros usamos esto para decir "Miren, por allá han logrado resultados". Logramos algo interesante: la primera cosa que los operadores decían era que no podían hacer nada que no estuviese regulado por Anatel, que eran operadores de telecomunicaciones y rendían cuentas a Anatel. En aquella época preparamos un texto firmado por Sardenberg, que era el coordinador de Anatel, y por Gadelha, que era coordinador del CGI, enfatizando este problema. En seguida llegó Levy, representante de las empresas de telecomunicaciones, y se hizo cargo del tema: "Si las empresas de telecomunicación no firman esto de forma individual, yo voy a firmar por Sindi Telecom, SindiTelebrasil", etc. Y acabó firmándose y todos los argumentos contra se vinieron abajo en el sentido de que no habría exposición a riesgos sino que, por el contrario, habría elogios. Al fin, todos se quedaron felices y esta parte fue vencida.

Ahora estamos oyendo un argumento en contra: "¿Ven? Si tuviéramos el Marco Civil no se podría haber hecho esto, ya que esto viola la neutralidad". Es algo sin pies ni cabeza, pero todo argumento es un argumento.

CAF: Incluso con "Si el Marco Civil se aprueba, vamos a eliminar los controles del puerto 25".

DG: Exactamente. Van a abrir el puerto 25 con la aprobación del Marco Civil y dicen que no va a suceder nada. Si se libera el puerto 25, lentamente va a volver a empezar el *spam.* No va a ser inmediatamente, porque en las máquinas se cambió por 587. Si ellos amenazan, pueden hacerlo, no hay problema. Pero está claro que no queremos que lo hagan.

Pero con IPv6 estamos esforzándonos para lograr algún progreso. No es algo trivial. El problema con Internet, tanto algo bueno como algo malo, es que siempre se defiende en el sentido de que logra arreglar imprevistos. IPv4 se debería haber agotado en 2001. ¿Por qué no se agotó en 2001? Porque se creó algo llamado NAT,

que es algo que se usa en redes enrutables. Por ejemplo, la red 10. Todos usan la red 10 en las redes sociales. La red 10 se eliminó del enrutamiento a mano mediante una RFC del IETF. ¿Qué significa esto? Usted tiene ocho millones de direcciones repetidas por el mundo y deja solamente tres o cuatro en el puerto. Se logra un buen ahorro de direcciones. En vez de necesitar ocho millones, se toman ocho direcciones y se dejan 8 millones escondidas en estas ocho. Esto permitió que IPv4 sobreviviera doce años.

Ahora hay otra maniobra que es el doble NAT. En este método, en vez de echar un mar de direcciones únicas, se toman estas direcciones únicas y se hacen varios puertos en ellas para la misma traducción. Se toma una IPv4 simple y, además de esconder detrás toda una red IPv4, también se puede mapear a IPv6 usando puertos diferentes. El método se llama doble NAT y no es muy bueno. Pero es una forma de prolongar un poco más la vida de IPv4. Lo ideal hubiera sido implementar un doble abordaje IPv4/IPv6 mientras todavía quedaba espacio IPv4, en cuyo caso la migración hubiera sido absolutamente indolora y trivial. Ahora van a faltar direcciones IPv4 para esta doble migración, por lo que vamos a tener que usar doble NAT. Pero esto es un detalle técnico que no es necesario; hay varias alternativas...

CAF: Nos gustaría destacar en este trabajo la participación de diversos sectores, diversos actores, diversos agentes. Entre los representantes gubernamentales que participaron en este tema de la gestión del puerto 25, ¿recuerda alguna entidad o representante gubernamental que haya sido particularmente relevante?

DG: Anatel no es propiamente gobierno sino agencia reguladora. Pero apoyó la iniciativa del CGI prontamente. Sardenberg firmó esto con Gadelha, diciendo que recomendaba a los operadores que hiciesen esfuerzos para cerrar el puerto 25.

CAF: ¿Algún otro órgano gubernamental?

DG: Que yo recuerde, no. No recuerdo la participación del Ministerio de Comunicaciones, porque eran solamente los operadores. Básicamente, quienes estaban involucrados eran proveedores de acceso y de información, grandes portales, Uol, Terra, proveedores de correo electrónico que iban a tener que enseñar a los usuarios y a las empresas de telecomunicaciones que, en general, tienen en sus manos la última milla de la banda ancha.

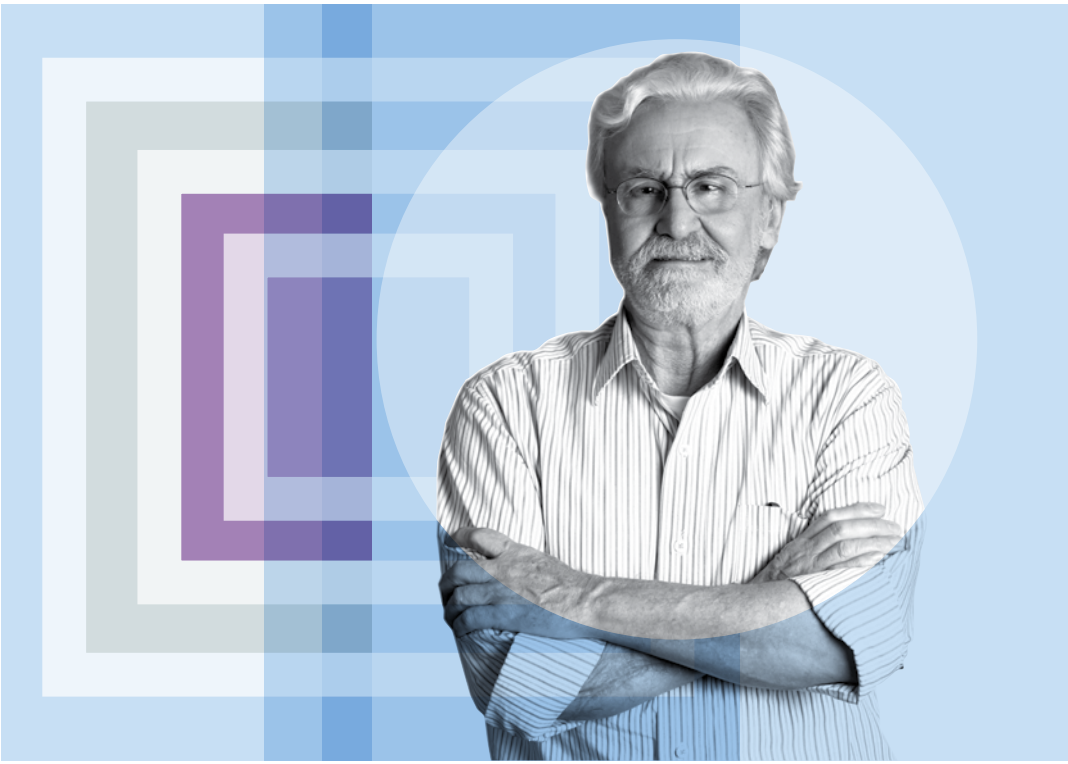
CAF: Además del debate sobre libertad comercial, ¿recuerda algún debate sobre libertad de expresión? Porque son dos debates distintos.

DG: El debate sobre libertad de expresión solo apareció cuando em-

pezaron las discusiones sobre la definición de *spam*. Inclusive, esto también surgió un poquito en Dubai, porque en Dubai apareció una redacción un poco rara de lo que sería *spam*, que después fue retirada, y tuvo contraataque y no sé en qué estado se encuentra hoy. Existe siempre el riesgo de tener una definición de *spam* que lleve a alguien a tener que leer los *e-mails* para decir si son *spam* o no. Eso sería abrir una puerta que nunca más se podrá cerrar. "Yo voy a leer para ver si esto es *spam* o no" —ahí se abre la privacidad de una forma inadecuada. Por lo tanto, creo que fue el único momento en que apareció este debate, en la definición del *spam,* porque podría causar estragos.

MM: ¿UCcree que algún otro órgano que no fuese el CGI.br hubiera sido capaz de implementar la gestión del puerto 25?

DG: El problema es que nos pasamos todo el día discutiendo temas de Internet. No existen otras personas dedicadas exclusivamente a esto. La Agencia de Telecomunicaciones discute sobre espectro, Anatel discute sobre la distribución de frecuencias, cada uno tiene su foco. Y tenemos ael CERT, nuestro personal que tal vez debiese discutir un poco más sobre los *honeypots* que ellos tienen allí y que no solo capturan *spam* sino también software malicioso, nuevos virus. Entonces ya teníamos una tradición en esta área de discutir estadísticamente o investigar cualitativamente cuáles eran los ataques que estábamos sufriendo, es decir, cuál era el nuevo virus que había surgido. Por ejemplo, hay una discusión sobre *spam* y denegación de servicio que va más o menos en la misma línea. Quiero decir máquinas que son cooptadas para ser zombis en un ataque de denegación de servicio. El *spam* no es tan grave, porque existe un puerto para prestación del servicio, pero es la misma cosa: se busca una debilidad en la máquina del internauta y se trata de explotar esta debilidad para el propio interés. La solución que encontramos fue la gestión del puerto 25.



4. Entrevista con Carlos Afonso

Realizada en São Paulo el 24 de enero de 2014

Carlos Affonso Pereira de Souza: ¿Podría explicar didácticamente qué es el puerto 25 y por qué fue importante que el CGI.br coordinara su proceso de gestión?

CA: El puerto 25 es el puerto estándar usado por los servidores de *e-mail*. Este puerto es el puerto de envío de mensajes. Es el protocolo SMTP, Simple Mail Transport Protocol. Los servidores de *e-mail* usan este estándar para dialogar entre sí. Se puede cambiar si todos deciden cambiarlo, pero esa es la convención. Como el FTP tiene el puerto 21, que es la copia de archivos etc. El usuario del servicio que envía mensajes a partir de un programita de *e-mail* como Thunderbird o Outlook no puede usar cualquier puerto predefinido entre él y su proveedor. Nada de esto afecta la facilidad que tiene para enviar y recibir mensajes de correo electrónico. Y no tiene nada que ver con la recepción sino que tiene que ver con el envío

¿Cuál es el problema de dejar el puerto 25 abierto para cualquier usuario en el extremo? Es que, como la inteligencia de Internet se encuentra en los extremos, en teoría, cualquier máquina conectada a Internet puede correr un servidor de *e-mail*. Funcionar como un servidor de *e-mail*. Y esto es usado por los *spammer*s, porque se contrata una conexión de banda ancha, se conecta una *laptop* con servidor de *e-mail*. Una computadorita Windows, Linux, puede ser, y esa computadorita se queda ahí automáticamente enviando mensajes por el puerto 25 como si fuese un servidor de *e-mail*. Allí la comunidad de servidores de *e-mail* la va a reconocer como un servidor de *e-mail* más.

Y ahí está el problema: facilita enormemente el envío de *spam*. Si alguien quiere enviar *spam* y necesita usar su proveedor de *e-mail* todo organizado, todo es más difícil porque hay controles, hay reglas operativas, inclusive éticas, entre los proveedores que buscan minimizar todo esto. Pero si se tiene una conexión a Internet propia, casera, puede correr el servidor allí, no se está bajo el control de nadie. La idea es cambiar la dirección lógica del puerto para que el usuario en el extremo envíe *e-mails* al servidor de *e-mail*. Y este puerto, por convención, ya existía antes y por estándar también es siempre una conexión cifrada; utiliza el estándar starttls, que es el puerto 587 y solo sirve para eso: enviar un mensaje a su servidor como un usuario, a través de la cuenta de *e-mail* propia. Para el usuario final nada cambia. Para el *spammer* cambia, porque ya no puede actuar como un servidor de *e-mail* en el extremo. Esta es la importancia de cambiar este puerto. Para el usuario final, en lugar de usar el puerto 25, usa el puerto 587. Si se tiene una conexión de banda ancha y si es una empresa o una organización, se puede solicitar la apertura de este puerto 25 para usar su propio *e-mail*.

No hay nada de prohibido ahí. Esto fue una propuesta colaborativa para minimizar el *spam* a partir de este recurso que consiste en instalar un servidor en el extremo y dejarlo enviando *spam* a gusto. El efecto de esto fue muy bueno. Hubo una reducción de los mensajes de correo electrónico. Porque, al menos en Brasil, los proveedores de servicio de *e-mail* conocidos siguen reglas estándares para evitar el *spam*. Es lógico, ya que la banda ancha en Brasil es muy costosa. El proveedor tiene una conexión, digamos de 100Mbs, un pequeño proveedor. No va a querer que 30% o 40% de esa máquina, de esa conexión, sea usada por *spammer*s. De este modo ahorra en ancho de banda, lo que le significa una ventaja.

Es muy importante recordar el principio número seis entre los

diez principios para la gobernanza y el uso de Internet del CGI. Después de años de discusión, cuando aprobamos este principio de neutralidad de la red, tuvimos el cuidado de decir "excepto por razones técnicas". Todo el resto, como yo solía y suelo decirlo aún: "todos los datagramas deben ser iguales ante la red".

Esta es una razón técnica; es el cambio de un número de puerto. Se sabe que existen miles de puertos que se pueden utilizar para todos los servicios. Si existe un acuerdo entre un extremo y otro para utilizar un puerto, se lo utiliza. Se puede utilizar cualquier puerto siempre y cuando estén configurados. Por ejemplo, el envío de archivos no es el puerto 21; es el puerto 2221. Se tiene que poner de acuerdo con otra persona. Si se ponen de acuerdo, funciona de la misma forma.

El problema es seguir estándares para que toda la red pueda darse cuenta que lo que se está enviando es un *e-mail* o que lo que se está transfiriendo es un archivo. Estos son los protocoles estándares.

CAF: También me gustaría oír sus comentarios sobre la participación de múltiples partes interesadas (y el rol del CGI.br) y el tema de la neutralidad. Vamos a continuar con el tema de la neutralidad. Bueno, el cierre del puerto 25 sería una razón técnica para analizar, investigar el encabezado de un mensaje y por esta causa este mensaje no seguiría. La pregunta es: ¿podemos decir que el cierre del puerto 25 es una excepción al principio de neutralidad de la red conforme a lo previsto en la reglamentación del CGI.br o esto no entraría en la discusión sobre la neutralidad de red porque no se estaría privilegiando un tráfico en detrimento de otro? Esta es una discusión que aparece bastante en las entrevistas realizadas hasta el momento.

CA: Entra en la discusión, pero como una excepción. Y permíteme decir algo: todos los encabezados de todos los paquetes se analizan automáticamente. ¿Por qué? Porque el *router*, el *switch* que decide para dónde enviar determinado paquete necesita conocer los datos, los metadatos de este paquete para conocer el número de puerto; para saber para dónde enviar el paquete, para saber si es FTP, SMTP, etc. Toda la información se encuentra en este *header*, en este encabezado que se lee automáticamente porque, si no lo fuera, los paquetes no viajarían. Necesita esta información para poder encaminarlos. Esto no es una violación de la neutralidad de red; por el contrario, se tiene que leer el encabezado para justamente poder usar el principio —uno de los principios originarios de Internet— que es el menor esfuerzo para entregar el paquete hacia el otro lado. Por lo tanto, leer el encabezado no es un problema; por el contrario, siempre es leído automáticamente. Esto no es lo mismo que leer el

encabezado para poder extraer otras informaciones para intentar hacer *profiling*, impedir que este paquete sea entregado en la forma debida, tal como está definido en el puerto, en la dirección IP. Esto es diferente: se estaría interfiriendo con lo que el *router* decide automáticamente para enviar este paquete. Es diferente.

CAF: En todo este proceso la participación del CGI.br fue muy importante para coordinar a los diversos actores. ¿Podría explicar qué papel desempeñó el GGI.br en esta coordinación?

CA: Esto fue algo importante, de nuevo, no solo porque refuerza los principios que hicimos, sino también por este trabajo que el CGI.br viene haciendo de ser un facilitador de problemas de la red. Vamos a resumirlo de esta forma. Nosotros no tenemos autoridad, pero sí tenemos la posibilidad de proponer recomendaciones para el mejor desempeño de la red. Y en este sentido —incluso antes de esto— hicimos un esfuerzo de desagregación de la red en el puerto para que más de un de proveedor de banda ancha pudiese usar la misma infraestructura física; y no lo logramos con Anatel simplemente porque los operadores dijeron que no. Pero esto es parte de nuestras tareas: hacer recomendaciones. Como esto del llamado *umbundling*, una desagregación de la red para conseguir más opciones de banda ancha en el extremo, más opciones en la conexión de telefonía fija equivalente.

Con el trabajo sobre el puerto 25 pasa lo mismo: identificamos un problema que no es solo nuestro, es un problema mundial y propusimos una discusión con los principales operadores de banda ancha para que tomasen la decisión de bloquear este puerto. Recordando que el usuario puede solicitar el desbloqueo; aquí el usuario se está responsabilizando, ¿verdad? No significa que está prohibido usar el puerto 25. El operador lo bloqueará —y ni siquiera estará bloqueado siempre—. Pero supongamos que todos lo bloquean. No es obligatorio, no existe un decreto sobre esto, fue un acuerdo colaborativo. Nosotros actuamos como facilitadores técnicos con conocimiento del problema. Tenemos un sector de seguridad que opera aquí analizando este problema y está calificado para decir: "Si este puerto se bloquea en el extremo del usuario final, habrá una reducción significativa del *spam* e inclusive del tráfico een la red" y todo lo demás. Y fue así. Por eso demoró tanto. Demoró mucho. Pasamos años trabajando en este asunto. Es así: el CGI tiene un papel muy específico y no tiene poder de regulación o legislación sobre todos estos asuntos. Solo tiene algunos poderes muy específicos sobre los nombres y los números: la distribución de los nombres y

la distribución de los números de dominio bajo el ponto br. Solo eso.

CAF: El proceso del puerto 25 es visto como un proceso de múltiples partes interesadas y como una experiencia que se puede llevar al público en general. Aquí está el trabajo de traducir aspectos que son muy técnicos para el público en general, además del debate sobre gobernanza de Internet, también es importante que aparezcan ejemplos de prácticas multisectoriales como esta.

CA: Esto es interesante, en el ámbito de lo que podríamos llamar "definidores de reglas" para la definición de la red en sí. Existe una organización internacional abierta que se llama IETF (Internet Engineering Task Force, Grupo de Trabajo de Ingeniería en Internet) que desde el inicio de Internet trabaja a través de recomendaciones llamadas RFC (Request for Comments, Solicitudes de Comentarios). A través de estas RFC este Grupo de Trabajo recomienda estándares para el funcionamiento de todos los aspectos de la red. Se puede decir que esta es una institución pluralista, *multistakehloder.* Cualquier persona puede ingresar, cualquiera puede ir hasta allí y discutir e inclusive elaborar estas RFC para que luego sean discutidas por el IETF. Allí, según el caso, podrán pasar a formar parte del acervo de las RFC, que son miles. Allí se encuentran las RFC que definen estos puertos estándares, las RFC que definen los servicios, cómo ellos funcionan en los *routers*, cómo distinguir el tráfico de una página web del tráfico de mensajes de correo electrónico, incluso si el puerto lógico cambia. Por ejemplo, se puede consultar un sitio web en el puerto 8085 y no en el puerto 80, que es el estándar de la web.

Todas estas características de funcionamiento de la red son definidas de forma pluralista por la IETF y desde el punto de vista técnico. ¡Técnico! De los *routers*, *switches*, etc. Esto sería un ejemplo de acuerdo colaborativo. No es la UIT (Unión Internacional de Telecomunicaciones) que hace una reglamentación cualquiera. Esta es una característica de Internet. El IETF sigue el estándar Internet de trabajo colaborativo. Lo mismo que hacemos aquí.

En este trabajo del puerto 25, ya somos por naturaleza una organización pluralista: el CGI.br es una comisión donde los miembros no gubernamentales son elegidos por sus comunidades. Significa que tenemos esta representación. Si no hacemos bien esta representación, ese es otro problema, pero tenemos esta representación. Cuando trabajamos con una empresa de telefonía o con un proveedor de acceso, trabajamos trayendo esta representación a la discusión e informando a las comunidades sobre esta decisión

de incentivar el bloqueo de un puerto o de incentivar la desagregación de la red. Por eso creo que es una experiencia importante que es seguida en otros modelos para Internet como es el IETF.

CAF: ¿La Internet en Brasil se encuentra mejor después del cierre del puerto 25?

CA: Indudablemente está mejor. Basta con ver las estadísticas del CERT.br sobre los países que más envían *spam*. Definitivamente hubo una diferencia muy grande y, en cuanto hubo una adopción más amplia del bloqueo por parte de los grandes operadores, la caída fue significativa. Es un poco como las hormigas, porque Internet es muy compleja y esta es una de las maravillas de Internet. No se pueden exterminar hormigas, se las puede minimizar. Si alguien va a enviar *spam* desde Rusia o desde Arabia, está bien, pero aquí en Brasil, en este territorio, logramos un acuerdo tácito de que por aquí no pasa.

CAF: ¿Alguna otra consideración?

CA: Sobre este tema del puerto 25 me gustaría decir una frase clásica: *no big deal*. Algunos lobistas de los operadores suelen decir "esto es una violación de la neutralidad de la red que ustedes tanto defienden". "¿Pero cómo? ¿Qué contradicción es esta?" Creo que ya expliqué que esto no tiene sentido. Por el contrario, con esto estamos mejorando el desempeño de la red.

5. Entrevista con Marcelo Bechara

Realizada en São Paulo el 24 de enero de 2014

Carlos Affonso Pereira de Souza: ¿Nos podría comentar sobre su participación en la gestión del puerto 25?

MB: Pese a ser miembro del Comité Gestor de Internet en Brasil por seis o siete años, diría que mi participación fue mucho más como profesional de Anatel que del CGI.br. Digo esto porque el Comité Gestor venía tratando con grupos específicos en los que no participé y manteniendo un debate más técnico sobre la gestión del puerto 25. En verdad nos molestaba mucho el hecho de estar en el segundo puesto del *ranking* mundial de *spammer*s.

Mi participación se dio en el marco del diálogo necesario entre el Comité Gestor y Anatel. En ese entonces, yo recién había ingresado a Anatel y aún era representante del Ministerio de Comunicaciones en el Comité Gestor. Fue un proceso interesante, incluso tuvo que ser llevado al Consejo Directivo de la Agencia, al final el director de la Agencia firmó un documento del propio CGI.br, con

empresas y, si no me equivoco, con el propio Ministerio Público. En verdad era un documento bastante importante, ya que involucraba a diversos actores. Por esta razón tuvo que ser sometido a la presidencia de la. Yo acabé siendo la voz del proyecto dentro de Anatel. Esto fue algo bastante importante; a fin de cuentas, fue un buen ejemplo de producción colaborativa.

CAF: Hablando de Anatel, CGI.br y csus ompetencias, ¿podría comentar de forma sucinta, de forma bien didáctica, las competencias de Anatel para regular a los proveedores de conexión y la Norma 4? Solo un paréntesis antes de hablar sobre el Puerto 25.

MB: La Norma 4 es anterior a la propia Anatel, que se creó en 1997. El proceso de licitación sucedió en 1998 y en 1995 se dictó el decreto que instituyó la Norma 4, que trataba sobre la relación entre los proveedores de conexión y las empresas —aún se llamaba así a las empresas públicas de infraestructura de telecomunicaciones—. Eran públicas por un motivo muy sencillo: eran estatales, aún no había ocurrido el proceso de privatización y el modelo de conexión a Internet era totalmente discado. Yo diría que hasta poco después de 2006, 2007, aún había más conexiones discadas que de banda ancha.

Esto solo cambió con la banda ancha móvil y obviamente, según los números que recuerdo, las conexiones discadas llegaron casi a un 10%, aunque este número debe estar cayendo. Y así esperamos que suceda.

Entonces, ¿cuál fue el papel de Anatel? Cuando asumió la regulación del sector de telecomunicaciones, Anatel pasó a ser responsable por la estructura de telecomunicaciones, que es donde funciona Internet. Y tratar sobre las funcionalidades de la red. Es que hay un dispositivo que dice así: servicio de valor agregado, que algunos llaman valor añadido; no es un servicio de telecomunicaciones, o sea, "Anatel, no se entrometa en esto".

Pero la norma que conceptúa los servicios de valor agregado dice que la relación entre los prestadores de servicios de valor agregado y los prestadores de servicios de telecomunicaciones es establecida por Anatel. Por lo tanto, existe realmente un ambiente poco claro. Y es comprensible que así sea, dado que este ambiente se ha modificado intensamente desde 1995 en cuanto hasta dónde debe llegar el papel de Anatel.

En relación con este asunto, hubo una regulación específica —la Regulación del Servicio de Comunicación Multimedia— que fue hacia donde acabaron yendo los proveedores, los antiguos provee-

dores de conexión. Hoy en día ellos todavía son proveedores de servicios de valor agregado y de servicios de telecomunicaciones. A veces la misma empresa dentro de una estructura empresarial. Hoy son más de cuatro mil prestadores.

El tema de la neutralidad de red ya se encuentra en el reglamento de servicio de comunicación multimedia como un valor no detallado. ¿Y por qué no está detallado? Porque existe la expectativa de que esto sea hecho por el Poder Legislativo y que no haya ningún conflicto entre lo que Anatel reguló y lo que el Poder Legislativo decidió y Anatel va a tener que cumplir.

CAF: Volveremos a hablar sobre neutralidad más adelante. Volviendo al papel de las empresas de telecomunicaciones, ¿podría hablar sobre la relación entre las empresas de telecomunicaciones y el CERT del CGI.br? ¿Cómo nació esta relación entre las empresas de telecomunicaciones y los informes sobre incidentes de seguridad?

MB: Lo desconozco, pero si existe alguna comunicación, no debe ser por iniciativa de Anatel sino del propio CERT y de las empresas. ¿Qué papel desempeñó Anatel en todo este proceso? Si para hacer esto de la administración y la gestión del puerto 25 no se necesitase de la actuación de los proveedores de servicio de telecomunicaciones, que son los dueños de la infraestructura y que también prestan servicios de comunicación de datos, Anatel no estaría en este acuerdo. ¿Por qué Anatel está en este acuerdo? Por una razón muy sencilla: las empresas de telecomunicaciones son reguladas por nosotros, son administradas por nosotros; esto está muy claro, inclusive en el acuerdo. O sea, cuando firma Anatel y firman las empresas de telecomunicaciones, las cosas suceden así en el universo de estos dos agentes: "Si no se cumple con esto, como regulador puedo tomar medidas administrativas y hacerlo cumplir, incluso con la aplicación de multas". Es una idea que, además de dar mayor legitimidad a nuestra propuesta, genera un *enforcement* específico, una obligación de cumplimiento, un deber de hacer de las empresas de telecomunicaciones. Creo que ese fue el papel.

En esta área más de seguridad, de usabilidad de Internet en sí, Anatel aún es bastante tímida en relación con su propia actuación, incluso porque es un tema que se ha puesto en duda. El Marco Civil de Internet pone en duda el papel de Anatel. Yo suelo decir que no existe un vacío de poder. El puerto 25 es un ejemplo positivo de ausencia de vacío de poder. ¿Por qué? Nosotros teníamos un problema real causado por la actuación de extranjeros, porque nuestras

máquinasa estaban siendo consideradas zombis. Es decir, aunque la gran mayoría de los usuarios brasileños no sabían que estaban siendo usados como un instrumento para la diseminación y proliferación de *spam*, Brasil ya se encontraba en un puesto extremadamente incómodo. Esto incluso ya fue probado. Hubo consecuencias nocivas para la navegabilidad, para la propia economía y para la mayoría de las personas a quienes no les gusta convivir con esto. Y la adopción de *software* no fue muy eficiente. El puerto 25 demostró ser un proceso extremadamente eficaz. El CGI.br comprendió que, para que esto sucediera, los propios usuarios, consumidores e internautas debían tener una visión más sofisticada del derecho del consumidor en Internet. Debían saber que un derecho del consumidor se vería perjudicado al recibir un mensaje o publicidad por la cual no tenían interés y que se repetiría exhaustivamente incluso sin haber autorizado la participación en aquella lista.

¿Cómo se articula este modelo? ¿Quién es el responsable? No hay un único responsable. Generalmente, cuando no se tiene un representante, el MP actúa. Pero para actuar el MP utiliza herramientas que demandan procesos más lentos, pasa por la Justicia, por ejemplo. ¿Cómo podíamos resolver esto? Tomamos un poco de cada uno y ahí pasó a ser efectivo. Desde su adopción hace 2 o 3 años, ya bajamos en este *ranking*. Gracias a Dios, ya no estamos más en este puesto que dejaba al país con una pésima imagen ante la comunidad internacional.

CAF: En cuanto al proceso en sí, una crítica frecuente a esta iniciativa es que demoró demasiado. ¿Cuál fue la causa?

MB: Nada. Los procesos en los que ya existen estándares de adopción y que ya son de rutina, muchas veces son extremadamente lentos. Así es la burocracia. En el caso de Anatel, puedo decir que tenemos el instrumento de consulta pública, pasa por una asesoría jurídica y existe un instrumento de tramitación. El Comité Gestor de Internet en Brasil del cual formo parte también es lento. Puedo decir esto: ¡es lento! ¿Por qué? Pienso que el puerto 25 fue la primera vez que el Comité Gestor actuó más como Comité Gestor y menos como NIC, porque el NIC tiene vida propia e incluso la gestión de las direcciones IP y los nombres de dominio no es realizada por el Comité Gestor. El CGI tiene una visión jerárquica del Comité Gestor, pero las operaciones ya se encuentran en el NIC, que tiene vida propia desde el punto de vista de sus procesos.

Al Comité le gusta más el debate que la gestión. Esta vez fue un comité de gestión. Solo que esto no es algo que forma parte ni que,

en mi opinión, debería formar parte de su rutina. Esto sucedió de forma bastante gradual. Hasta hace poco, las resoluciones del Comité Gestor no se publicaban, no se subían a Internet. El puerto 25 es un caso típico de "necesitamos hacer". Quizás también haya sido un caso traumático, por la cuestión de la unanimidad, empezamos de esta forma. Por lo tanto, convencer internamente al Comité Gestor sobre cómo hacer esto, cómo adoptarlo, ya sería un proceso lento de por sí, y más aún teniendo que involucrar a otros actores. ¿Se imagina? Tener que pasar por el área jurídica de Anatel, tener que pasar por el área jurídica del Comité Gestor, por el NIC.br, tener que llamar al Ministerio Público, a defensa del consumidor y luego llegar a un texto final. Mire, yo sé lo difícil que fue llegar a un texto final. Las empresas de telecomunicaciones fueron extremadamente meticulosas y cuidadosas, como lo es el estándar que tienen, por eso realmente creo que no había otra forma de hacerlo, muy difícilmente podría haber sido algo rápido. No se puede perder lo aprendido: a medida que algo que se trata de una forma más sistemática, se tienden a encontrar mecanismos que vuelven más ágil y rápido este proceso.

CAF: Vamos a abordar la parte de las empresas de telecomunicaciones dentro del proceso del puerto 25. Hubo una demanda muy fuerte por la presencia de Anatel. ¿Puede explicar cuál fue la demanda y por qué se exigía la presencia de Anatel? En su opinión, ¿por qué fue importante que Anatel también participara en este proceso?

MB: Las empresas de telecomunicaciones ya están habituadas a lidiar con diferentes organismos. A pesar de nuestros conflictos con las empresas, ellas prefieren lidiar con quien ya conoce cómo funciona el procedimiento, es decir, ya sabe cómo es la multa, ya sabe cómo funciona, qué es Anatel, que es el organismo con el cual están vinculados desde el punto de vista regulatorio, que, por ejemplo, con organismos de defensa del consumidor, con quienes están en eternos y constantes conflictos. Es natural. Ellos son los usuarios y los proveedores de servicios. Anatel cumple un papel más de intermediario, pero a favor del usuario, no somos un Procon, no somos parte del sistema brasileño de defensa del consumidor. Nos ocupamos de mercados con agentes económicos. Los consumidores y las empresas son agentes económicos y nosotros nos ocupamos del equilibrio de este mercado.

En un ambiente en el que existen defensa del consumidor, el Ministerio Público y el CGI.br, de repente se promueve el ingreso de las empresas a este proceso y estas empresas se preguntan "¿Cómo vamos a asumir compromisos sobre cuestiones de gestión de red,

siendo que el órgano que nos regula, inclusive sobre la funcionalidad de la red, es Anatel?" Por eso creo que Anatel surge en este proceso como una forma inclusive de viabilizar, de hacer de puente y legitimar la participación de las empresas de telecomunicaciones y también la de los usuarios. No significa que los usuarios necesitasen de esto. No lo necesitaban porque los usuarios tienen una legitimidad, una representatividad muy propia; con el Ministerio Público a su lado quedaba más formalizada. Pero creo que para los propios usuarios la presencia de Anatel ofreció legitimidad, porque se pasó a tener una institución que incluso tiene una superintendencia solo para tratar del usuario y que tiene sus procesos específicos para imponer sanciones, en fin, las imposiciones que sean necesarias para estas empresas.

CAF: Después de implementada la gestión del puerto 25, ¿supo si Anatel o las empresas de telecomunicaciones dieron algún *feedback* sobre la mejoría de la calidad de la banda ancha?

MB: Creo que sí. Porque evidentemente nosotros tenemos un grupo solo para tratar la banda ancha, tanto de banda ancha móvil como la banda ancha fija. En este grupo dse consideran varios elementos, inclusive es un grupo formado por la propia agencia, con empresas y expertos. Se crearon herramientas para evaluar la calidad. No me cabe la menor duda de que elementos como el *spam* interfieren mucho, porque acaban sobrecargando excesivamente la red y esto acaba generando impactos. Entonces, yo creo que sí, que debemos tener algún nivel de información. No sé si con una mirada al puerto en sí, pero tal vez con una mirada a todo el sistema.

CAF: Algunas empresas sostenían que el proceso de gestión del puerto 25 implicaría costos. ¿Cómo se solucionó este tema? ¿Cómo fue que se acabó incluyendo en el debate y se decidió que era importante proceder de esta forma, incluso si tenía un costo?

MB: El argumento sobre los costos es un argumento que las empresas usan en todos los casos. O sea, lo usan ante toda y cualquier medida de mejoría, de calidad, ya sea que afecte a las inversiones o no. Porque a veces no se requieren todas estas inversiones. A veces se pueden tomar medidas que afecten la prestación del servicio mucho más que el tema de las inversiones que se deben hacer para lograrlo.

Sinceramente no sé si ellos tuvieron que hacer toda esta inversión. Creo que no, aunque siempre usan este argumento.

Anatel hizo algo muy bueno —algo que en la época aún no existía, porque el reglamento interno era anterior al que está vigente hoy en día— que fue volver obligatoria la adopción de las medidas de gran

porte para los análisis de impacto regulatorio. No sé si sería el caso, porque no era una regulación sino que era un acuerdo, pero incluso si se pudiese realizar un AIR (Análisis de Impacto Regulatorio), ¿qué se demostraría? ¿qué es un AIR? Es la relación costo-beneficio de la regulación. Creo que en este caso no se necesita ser economista para verificar que el beneficio ha sido realmente extraordinario. Incluso si hubiera sido necesario incurrir en costos y realizar inversiones, creo que es parte del juego de su negocio y de nuestro interés de que las cosas funcionen. Creo que se trató con bastante naturalidad y normalidad, ya que estamos acostumbrados a lidiar con estas cosas.

CAF: ¿Cómo relaciona el debate sobre el puerto 25 con el debate sobre la neutralidad de la red?

MB: Yo tengo una visión realmente muy propia sobre la neutralidad de la red. Tengo una visión de la importancia de la neutralidad, porque todos están a favor de la neutralidad. No hay nadie que ande diciendo: "Estoy en contra la neutralidad de la red". La neutralidad de la red es un principio, un valor; creo que nunca se planteó la "no neutralidad" como una opción.

El debate se vuelve más interesante al hablar de qué es la neutralidad. Este concepto ha ido evolucionando. Creo que hoy se atribuye a la neutralidad de la red cosas que no son temas de neutralidad de la red. Por ejemplo: para mí, los paquetes de velocidad y capacidad no son una cuestión de neutralidad de la red. Si yo tengo un paquete y pago más por tener mayor capacidad, esto es una cuestión de perfil de consumo, no de neutralidad de la red. Para mí, neutralidad de la red presupone una gestión en la red, independiente de la velocidad o de la capacidad que uno tenga. Yo puedo tener la mejor banda ancha del mundo, con capacidad ilimitada, si es que existe. Incluso así, mi red podría ser degradada para que yo no tenga acceso a un determinado tipo de información. A esto yo le llamo neutralidad de la red.

Yo creo que la gestión del puerto 25 tiene sentido dentro de la neutralidad de la red. ¿Por qué? Guste o no, se están creando mecanismos para bloquear o dificultar contenidos indeseables, que son contenidos. Aquí tenemos que entrar en el concepto de calidad del contenido del *spam*, ya que esto no está en discusión, pero puedo decir que determinado contenido es prioritario en relación a otro.

Creo que el puerto 25 es un gran ejemplo de que no todos los contenidos son iguales y de que no todos deben tener necesariamente la misma prioridad. Internet ya lo hace. Hay algunas aplicaciones que son determinísticas, algunas de mayor esfuerzo. Por ejemplo, 2

o 3 segundos en una charla en Skype marcan una diferencia en una comunicación, mientras que 3 o 4 segundos al recibir un *e-mail* no marca la misma diferencia, o tal vez no marca ninguna diferencia.

Mi temor con respecto a la neutralidad de la red es que, en lugar de preocuparse por preservar la neutralidad de la red, el Marco Civil intente avanzar sobre conceptos tecnológicos. Porque la tecnología tiene una dinámica muy propia. Ni hablemos de Internet. Estamos entrando en una era a la cual ya no llamo la Internet de las Cosas, sino la Internet de Todo. ¿Qué es la Internet de Todo? Mi refrigerador va a estar conectado a Internet, ¿pero será que mi refrigerador tiene que recibir el mismo tratamiento de neutralidad que la telemedicina? Sinceramente no lo sé. Mi refrigerador está ahí, es una máquina conectándose con otra máquina; pero mi interacción es solo en la programación, no estoy ahí navegando. Estamos en el camino de la Internet de las Cosas a la Internet de Todo.

Sobre la discusión de la neutralidad de red, temo que la pregunta es: ¿será que si el Marco Civil de Internet hubiese salido antes que el acuerdo sobre el puerto 25 hubiéramos logrado este acuerdo? Esta es una pregunta que necesita ser contestada. A decir verdad, no sé si lo hubiéramos logrado, porque iba depender, porque aún existe un vacío, continúa existiendo un vacío. Es mejor que se diga que va a ser el CGI.br, Anatel, la Presidencia de la República, no importa. Pero es importante definir quién va a cuidar de esto, porque alguien debe cuidarlo, ya que, caso contrario, vamos a tener un vacío como el que ya tuvimos y, tal vez, existiendo amarras, no logremos exactamente la misma solución que tenemos, incluso siendo lenta.

Por eso creo que este es un debate bastante importante y que se deben tomar otras medidas importantes como esta. También creo que el Comité Gestor de Internet en Brasil debe ser realmente más gestor de Internet en aquello que Internet realmente necesita.

CAF: ¿Alguna consideración final que quiera hacer sobre aspectos técnicos o sobre aspectos políticos de este proceso?

MB: Sobre aspectos políticos. No voy a atreverme a hablar sobre asuntos técnicos, ya que ustedes deben haber conversado con expertos renombrados. Yo creo que, desde el punto de vista político, lo obvio es decir que fue un aprendizaje, claro, pero este aprendizaje bajo el aspecto político demostró lo siguiente: es posible. Esta fue la gran respuesta: es posible. Existe un camino para hacerlo posible, un grupo de trabajo de múltiples partes interesadas o no, no importa. Un grupo de trabajo que en algunos momentos puede

ser de múltiples partes interesadas y en otros puede no serlo, dependiendo del asunto. Ahora es posible encontrar caminos para tomar decisiones que tengan resultados efectivos. Y es lo que debe hacerse. Y sobre Anatel, a quien represento, no en vano Anatel tiene un lugar en el Comité Gestor de Internet, una representación. Esto no es en vano, sino que tiene un sentido, un significado que es exactamente esto: es tener una interacción que no solo sea desde el punto de vista del debate, sino también desde el punto de vista operativo para la implementación de las cosas. Porque esto es política. Política es diálogo. Y presupone diálogo en un ambiente en que se tiene algunas indefiniciones desde el punto de vista de la competencia. Espero que podamos usar este modelo como un proceso de maduración del debate político y que, en mi opinión, en cierta forma fue una revolución silenciosa. Nosotros tuvimos ni bombos ni platillos durante las negociaciones sobre el puerto 25. Después que se cerró el acuerdo, hubo una gran y amplia divulgación. Creo que este fue el mejor ejemplo de que es posible trabajar en silencio, no con falta de transparencia, pero sí en silencio, que es diferente, para que las cosas sucedan, incluso porque el tema es muy técnico y tal vez un 99% de los internautas brasileños no tenga la menor idea de lo que es el puerto 25 ni la menor idea de lo que se hizo, pero con seguridad está marcando la diferencia en la vida de estas personas mientras usan Internet.

6. Entrevista con Eduardo Parajo

Realizada en São Paulo el 24 de enero de 20144

Carlos Affonso Pereira de Souza: ¿Puede explicarnos qué es el puerto 25?

EP: Voy a tratar de presentarlo esto en un lenguaje bien sencillo. El puerto 25 es el puerto que hasta ese entonces se utilizaba cuando el software de cliente de correo electrónico iba a enviar un correo a otra persona en Internet. El problema es que el software de cliente y los servidores de correo también utilizan este puerto para enviar mensajes. Empezó a haber una abuso de computadoras de clientes enviando *spam*, transformando a las máquinas de clientes en mini-servidores, muchas veces sin que el usuario tuviera conocimiento de ello. Fue así que acabamos teniendo una inundación de *spam* enviado por computadoras brasileñas hacia todo el mundo.

CAF: ¿Cuál fue el efecto de esta infestación de máquinas brasileñas?

EP: Efectos devastadores para la Internet brasileña. Primero, cuando la computadora de un usuario era capturada por un *spammer*, se

agotaba la capacidad de procesamiento de la máquina y el ancho de banda de tanto estar enviando *e-mails*. A veces el usuario notaba una lentitud enorme en su computadora para acceder a Internet. A veces le echaba la culpa a la computadora, al *software* o incluso al proveedor que le ofrecía la conexión a Internet. Al final, era que alguien estaba utilizando sus recursos. Este sería el primer efecto, que yo diría que era bastante devastador para el usuario.

El segundo efecto es bastante complicado y es que la reputación internacional de la calidad y de la seguridad de la Internet brasileña empezó a verse fuertemente afectada. Brasil empezó a figurar en una lista de grandes *spammer*s mundiales; muchas IP brasileñas empezaron a circular en estas listas con graves consecuencias: a partir del momento en que estas IP o estos rangos de IP empezaron a figurar en estas listas de *spammer*s, también empezaron a surgir bloqueos por parte de diferentes servidores de *e-mail* del mundo cuyo objetivo era bloquear el recibimiento de mensajes de Brasil. Y tuvimos casos más radicales. Por ejemplo, en una época Europa bloqueó todos los correos enviados desde Brasil a cualquier servidor ubicado por allá. Ahí empezó un trabajo en esta línea para tratar de desarrollar el proyecto del puerto 25.

CAF: ¿Nos puede explicar este proceso?

EP: Constatados todos estos hechos y la utilización indebida de las computadoras de los usuarios, el Comité Gestor estableció el Grupo de Trabajo que estaba justamente buscando minimizar estas cuestiones.

Al comienzo apareció una cuestión muy técnica, que era modificar la forma en que el usuario encaminaba el *e-mail*, el puerto por el cual el usuario enviaba *e-mail.* Esto no fue una invención brasileña, ya que se había desarrollado una RFC con el objetivo de crear un puerto llamado 587, que es bastante utilizado. El grupo creado por el CGI.br empezó a involucrar a los actores de Internet de Brasil —proveedores de acceso, grandes operadores de *backbone* de Internet y grandes proveedores brasileños de *e-mail*—. Se empezó a reunir a estas personas para sensibilizar a todos sobre la necesidad de hacer este cambio de configuración en sus servidores, en el *software* de cliente para el envío de *e-mails*.

Fue un trabajo largo que llevó mucho tiempo, pero el objetivo era el siguiente: evitar que los *spammers* capturaran las máquinas de los usuarios y las transformaran en servidores de *e-mail*.

CAF: ¿Cuáles fueron los agentes llamados para desarrollar la gestión del puerto 25?

EP: Básicamente los proveedores que daban acceso a los usuarios y también los operadores de telecomunicaciones que daban estructura a este usuario. ¿Por qué? Era necesario realizar un trabajo conjunto en tres líneas. La primera se refiere a los grandes proveedores de *e-mail* que debían modificar esta RFC para empezar a aceptar y recibir *e-mails* por el puerto 587 y ya no por el puerto 25. Un segundo aspecto también relacionado con estos proveedores era informar al usuario que había una nueva configuración, que esta nueva configuración se debía realizar en los clientes de *e-mail* de los proveedores para que lograsen continuar la comunicación con el usuario. También hay otra característica de los proveedores de acceso, que daban conectividad a Internet. al usuario Estos eran quienes generalmente tenían contacto con el usuario final, por lo que también tendrían la función de informar al cliente: "Mira, estamos haciendo una configuración de seguridad, una modificación importante que va a tener que realizar ahí en su cliente". Por último, los operadores de telecomunicaciones que suministraban el cable de conexión al usuario a partir de un determinado momento en que constatásemos que una gran mayoría de estos usuarios ya estaba migrada a este otro puerto. Efectuar un bloqueo físico de este puerto específicamente para los usuarios residenciales en el extremo. Significa que, incluso si el malware ya hubiese infestado la computadora de la persona y quisiese continuar enviando *e-mail* por el puerto 25, existiría un bloqueo físico del puerto 25 que impediría que el *e-mail* saliese.

Y esta conjunción de actores involucrados —proveedores, operadores de telecomunicaciones, proveedores de *e-mail*— fue fundamental en la instrucción del usuario. Obviamente también involucramos a Anatel en el proceso por causa de los operadores, quienes estaban muy temerosos con relación a hacer el bloqueo. En este proyecto también involucramos a las entidades de defensa del consumidor. Realmente hubo una participación muy grande de estos actores para llegar al final de este proyecto.

CAF: El final de este proceso demoró cierto tiempo. ¿A qué le atribuye esta demora en la conclusión del proceso?

EP: En verdad creo que fueron varios factores, desde, por ejemplo, el hecho de que el operador de telecomunicaciones no efectuaba el bloqueo, que el usuario no estaba preparado, y el aumento del volumen de reclamos a su *call center*. Lo mismo sucedió con los proveedores de *e-mail* y los proveedores de conectividad. Llevó bastante tiempo, yo diría, para que este grupo encontrara una interlocución, prin-

cipalmente por parte de los operadores, en el sentido de dar gran importancia a este proceso. Del lado de los proveedores, tanto de conexión como de *e-mail*, esta conciencia ya existía y el trabajo se empezó a realizar, pero se estaba hablando con millones de usuarios de *e-mail*. Voy a dar un ejemplo: uno de los actores tiene más de 10 millones de cuentas de *e-mail*, ¿cómo iba a hacer esta comunicación? Era como el cuento del huevo y la gallina: ¿qué está primero? ¿Quién nació primero? Y fue ahí, en ese momento, que los grandes proveedores de *e-mail* y los grandes proveedores de conexión lógica empezaron a dar los primeros pasos y ahí sí los operadores empezaron a moverse de su lado. Creo que hubo un elemento importante para los operadores que fue el hecho de haber acertado un canal de comunicación de este grupo con su representación, aquí inclusive en el Comité Gestor. A partir de allí, el proceso empezó a fluir.

CAF: ¿En qué medida analiza la importancia de que este procedimiento haya sido multisectorial? ¿Se hubiera podido hacer de otra forma?

EP: De ningún modo. Ceo que Internet como un todo es un proceso multiparticipativo. No depende de un segmento y no es un segmento quien va a solucionar el problema. Puede tener una idea, pero no va a lograr ponerla en práctica si no hay otro para ayudar. Por esta razón, este proyecto *multistakeholder* es muy necesario.

Internet es un ambiente colaborativo. Existe una estructura básica que es suministrada por los operadores de telecomunicaciones, pero, si no tiene una interacción en la parte del negocio en sí, las cosas que circulan en el proceso no andan. Desde el usuario hasta un gran operador, un proveedor de conectividad, un proveedor de *e-mail*, el sector empresarial. Por lo tanto, hubo efectivamente participación para que el proceso pudiese ser exitoso.

CAF: Una de las cuestiones de contenido que se señala con respecto al puerto 25 es cómo este proceso se relaciona con la neutralidad de la red. ¿Puede decirnos algo sobre el cierre del puerto 25 y la neutralidad de la red?

EP: Creo que el proceso no tiene nada que ver una cosa con la otra. Mi opinión es muy clara —y hubo una preocupación de este grupo desde el inicio para que quedase muy claro— que este proceso no es una interferencia en la neutralidad de la red.

En realidad, el trabajo del grupo fue una recomendación técnica para la cuestión de la seguridad de Internet en Brasil. En ningún momento hablamos de discriminar un *e-mail* de Fulano que es más lento ni de Mengano que es más rápido. Por lo tanto, no hubo ninguna interferencia en el proceso de neutralidad. Entiendo que

hay 1uienes sostienen lo contrario. Tal vez el foco de la pregunta sea si el bloqueo estaría efectivamente influenciando el debate sobre neutralidad. Si verifica el propio decálogo del CGI.br, la gestión del puerto 25 no afectó el Decálogo en ningún momento, porque el propio Decálogo menciona que no es recomendable bloquear, filtrar, monitorear por motivos comerciales, culturales, religiosas, etc. No afectó de ninguna forma al decálogo. Por el contrario. Fue una decisión tomada incluso dentro de un modelo participativo, trayendo toda la sociedad a la discusión. El propio principio fundador de Internet es el principio colaborativo, no individualista de un único solo sector.

CAF: Analizando el Marco Civil y el proceso de cierre del puerto 25, ¿es posible incluir una posible cláusula de neutralidad de la red?

EP: Vamos a separar un poco la cuestión del Marco Civil y de la neutralidad. La neutralidad, específicamente, es que nadie quiere que exista ninguna discriminación o prioridad en el tráfico de datos. Creo que es este uno de los fundamentos básicos que estamos defendiendo en el tema de la neutralidad. Que no existan filtros, bloqueos ni prioridades con intereses comerciales, políticos o religiosos. Esto se tiene que dejar y preservar este proceso. Y esto también se aplica al Marco Civil. Sin importar cuál sea el texto aprobado, creo que se debe inspirar mucho más en el texto del Decálogo antes que crear una nueva nomenclatura para lo que se denomina neutralidad de la red. Creo que el Comité Gestor tuvo un gran acierto en las palabras del Decálogo y en la forma como ha quedado definida la neutralidad de la red. Creo que el Marco Civil o cualquier proyecto de ley deben extraer este texto y colocar el principio en la ley.

CAF: Pensando en el proceso del puerto 25, ¿qué lecciones se pueden aprender del modelo de múltiples partes interesadas que puedan ser consideradas en futuros procesos?

EP: Es un proceso difícil en cuanto a los plazos. Es un proceso que empezamos pero no sabemos bien cuándo va a terminar. Esta es una lección que aprendimos en este proceso. Su resolución demoró 5 a 6. Puedo dar otro ejemplo que está sucediendo ahora mismo y que es un proceso que ya lleva tres años: la implementación de IPv6. En general las cosas suceden en Brasil a los cuarenta y nueve minutos del segundo tiempo. Esta es una lección aprendida en este proceso que podemos tener en cuenta para tratar que no sea así. Existe un esfuerzo muy grande de parte de los actores involucrados en este proceso, no es algo muy sencillo.

Por ejemplo, mucho se dijo sobre el puerto 25 y sobre el proceso de comunicación del proveedor con el usuario, que realmente es complicado, porque a veces el usuario de la computadora no entiende absolutamente nada. Por eso, creo que tenemos todo este aprendizaje adquirido con el puerto 25 para no demorar tanto en otros procesos que puedan surgir.

Creo que vamos a tener un trabajo enorme ahora en abril y mayo, cuando produzca el agotamiento de IPv4, un proceso que ya está en curso. Creo que no debemos ser radicales al extremo para no dejar que el proceso suceda de cualquier forma. Pero tampoco posponerlo indefinidamente. Creo que esta es la principal lección. Que primero tenemos que unir a todos y teneos que tratar de hacerlo lo más rápidamente posible.

CAF: ¿Esto quiere decir que el saldo final del cierre del puerto 25 es positivo?

EP: Recuerdo la última vez en que miré y estábamos más allá del trigésimo puesto en la lista de *spammer*s del mundo, en una de las listas más conocidas. Creo que la experiencia fue extremadamente positiva para la Internet en Brasil, para la calidad de Internet en Brasil, porque imagínese millones y millones de usuarios infectados, usando el 100% de su capacidad, en el mismo momento, enviando basura en forma de *spam* hacia el interior del propio Brasil y hacia fuera de Brasil. Este es un costo absurdo que el usuario acaba pagando, que las propias empresas están asumiendo.

Desafortunadamente no es posible transformar o cuantificar esta cuenta en dinero, por lo que no es fácil hacer un paralelo, obtener un resultado objetivo de cuál fue el impacto. Por ejemplo, había empresas, principalmente los grandes operadores, que tenían todos sus bloques IP listados. Imagínese el perjuicio para estos usuarios que no lograban enviar correos a diversos lugares. Tal vez sería interesante hacer un estudio para tratar de cuantificar el costo o la cantidad de recursos que se obtuvo en este proceso.

7 • Entrevista con Rubens Kuhl

Realizada en São Paulo el 24 de enero 2014

Carlos Affonso Pereira de Souza: ¿Podría explicarnos qué es el puerto 25?

RK: El puerto 25 se utiliza para comunicación entre servidores de correo en Internet. Cuando un usuario envía un *e-mail* en Internet no es necesario que use el puerto 25. Después que este mensaje es enviado, el servidor al cual se envió utiliza el puerto 25 para entregarlo al servidor de destino.

CAF: ¿Cuál es la importancia del cierre del puerto 25?

RK: El puerto 25 estaba siendo usado por personas que querían entregar *e-mails* indeseados, por lo que hacían que el usuario, sin su conocimiento, enviase correos para que ellos, los verdaderos remitentes, no fuesen identificados por esta actitud nefasta que era entregar correo electrónico a las personas que no querían recibirlo.

CAF: ¿Cómo explota la persona esta vulnerabilidad de la máquina?

RK: Esta vulnerabilidad se explota enviando desde esa máquina el mensaje de correo que luego se entrega al servidor de *e-mail* que normalmente utiliza y que reenviará el correo.

CAF: ¿Cuál fue el efecto del cierre del puerto 25?

RK: Brasil, que se encontraba entre los países que más enviaban *spam*, que más enviaban correos indeseados, bajó muchos puestos, decenas de puestos, hasta uno más razonable, más compatible, digámoslo así, con las prácticas internas.

CAF: ¿Cuál fue su participación en el proceso del puerto 25?

RK: Junto con Cristine Hoepers y Klaus Steding-Jessen, fuimos los primeros en proponer esto. Ellos estaban en el CERT.br y yo había salido recientemente de un gran proveedor de correo electrónico. Y ya notábamos lo difícil que se estaba volviendo entregar mensajes porque Brasil tenía una fama de emisor de *spam*.

CAF: ¿Cómo relaciona el debate sobre la neutralidad de la red y el puerto 25?

RK: El puerto 25 se relaciona con la neutralidad de la red porque, desde el punto de vista técnico, es una violación de la neutralidad. Y así como están previstos en algunos marcos regulatorios que aún deben ser aprobados, existen buenos motivos para una ruptura de la neutralidad técnica de la red. En el caso de Brasil, un objetivo que es interesante para todos es ganar confiabilidad en el uso de la Internet mundial.

CAF: Volviendo al proceso del puerto 25, ¿cómo ve el papel del CGI.br en todo este proceso?

RK: El papel del CGI.br en el proceso de gestión del puerto 25 fue fundamental porque el CGI.br era el único ambiente en que todas las partes involucradas — usuarios, proveedores de telecomunicaciones, proveedores de acceso y proveedores de servicio de Internet— podían reunirse, debatir y llegar a una conclusión sobre si debían hacer esto o no. Cualquier actitud solamente del Poder Ejecutivo habría sido vista como una intrusión de la Administración Pública en los asuntos de estos actores del mercado. Dado que fue tomada dentro de un ambiente de múltiples partes interesadas donde todos los actores involucrados estaban representados, esta decisión permitió una adhesión más espontánea y efectiva a esta iniciativa.

CAF: ¿El cierre del puerto 25 era la mejor solución?

RK: El cierre del puerto 25 era la mejor solución para este problema de confiabilidad. Era la solución que ya se había adoptado en otras grandes redes de otros países. Desafortunadamente, demoramos en adoptarla, pero era la mejor y posiblemente la única solución para el tema del *spam*. Todavía tenemos que trabajar sobre otras cuestiones como la confiabilidad de la red, pero para la credibilidad de la entrega del correo electrónico era la única salida.

CAF: ¿Cómo compara la experiencia brasileña con la experiencia de otros países?

RK: La experiencia brasileña repitió la de las grandes redes norteamericanas, como la de Comcast, porque cuando se implementó se logró disminuir bastante el índice de reclamos sobre *spam* recibido y se logró mejorar la confiabilidad de la entrega. Pero en el caso de Brasil había algo más grave: Brasil estaba clasificado como un país entero. Había mucha gente en las listas de bloqueos, bloques enteros de direcciones IP brasileñas, algo que no sucedía en las redes norteamericanas, es decir, nadie bloqueaba todas las direcciones de correo de Estados Unidos. Pero esto sí sucedía con Brasil. Por esta razón, este tipo de iniciativa benefició no solo a las redes en que se implementaron, sino también a todas las redes brasileñas.

CAF: ¿Hay algo que quiera añadir sobre este proyecto, sea sobre el aspecto técnico o el aspecto político?

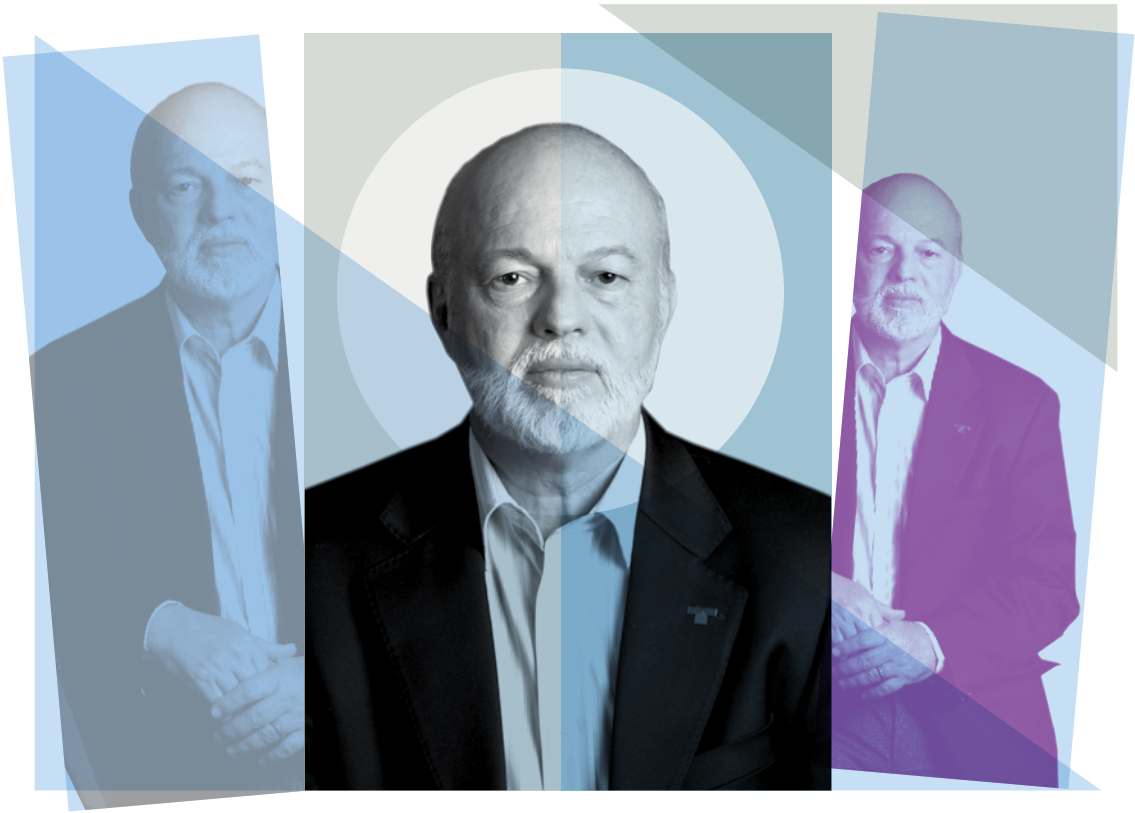
RK: La implementación del puerto 25 fue efectiva, pero llevó mucho tiempo más de lo que se había previsto. Creo que una lección para los actores involucrados fue que a veces es posible agilizar alguna iniciativa una vez que se vuelven claras, pero incluso así algunos actores posponen este tipo de adopción. Esto es una lección para las próximas veces que tengamos que implementar procesos políticos.

CAF: ¿Pero esto no es algo inherente al proceso de múltiples partes interesadas?

RK: Es inherente al proceso de múltiples partes interesadas que sea un poco más lento. Lo que necesitamos es volverlo un poco menos lento. Va a continuar siendo un proceso que involucra largos debates, pero puede llevar menos de lo que llevó esta vez.

CAF: Si se ponen en la balanza la duración de un proceso de múltiples partes interesadas que parece ser más largo y los resultados alcanzados, ¿el resultado de un proceso de múltiples partes interesadas es necesariamente mejor?

RK: El resultado de un proceso de múltiples partes interesadas siempre será mejor visto porque tiene una adopción de todos los proponentes, de todos quienes discutieron el proceso. Por lo tanto, sin importar si es mejor o peor, siempre va a ser mejor percibido. Esto es una ventaja desde el punto de vista político, es decir, en este proceso del puerto 25 también existe un aprendizaje de todos los actores de no defender solamente un punto específico o una adecuación específica que cada uno tenga. Así, el hecho de que este proceso haya sido lento demuestra cuál era nuestra madurez política para tomar este tipo de decisión.



8. Entrevista con Eduardo Levy

Realizada en São Paulo el 24 de enero de 2014

Carlos Affonso Pereira de Souza: ¿De qué forma sus atribuciones en el CGI.br se relacionan con el proceso que originó la gestión del puerto 25/TCP?

EL: Me parece importante empezar contando mi historia dentro del CGI.br. No solo la mía, sino la historia del sector de telecomunicaciones. El proceso de elección en el CGI.br nunca había despertado interés por parte del sector de telecomunicaciones, tanto que efectivamente nunca tuvo una representación dentro del Comité. Esta no representación del sector de telecomunicaciones dejaba un cabo suelto porque el trabajo que estaba siendo realizado de forma brillante por Henrique Faulhaber, a quien yo no conocía. De hecho, yo apenas conocía al profesor Glaser, pero asolo supe del trabajo brillante que estaba realizando cuando, después de la elección en que por primera vez el sector de las telecomunicaciones tuvo representación en el CGI.br, participé en una reunión en la que, si bien recuerdo, tuvimos la presentación de Henrique sobre el punto en que se encontraba el

proceso del puerto 25 y donde también dijo que una de las cuestiones, la principal quizás, en la que había que poner manos a la obra era la participación del sector de telecomunicaciones.

Yo no conocía muy bien el proceso. Mi vida no estaba dentro de las telecomunicaciones, no estaba involucrado en el puerto 25 y cosas así. Miré, pensé y dije "Creo que no estoy entendiendo, porque me parece tan obvio que esto se debe hacer, tan obvio". Pero como yo recién estaba llegando, decidí estudiar mejor el tema para poder tomar una posición en una próxima reunión. Así empezó a existir el proceso para el sector de telecomunicaciones y tal vez esto sea una demostración de que el sector debe estar representado en un Comité, por la importancia del sector en este asunto, no solo en el puerto 25, sino también en el tema de Internet en general.

Volví a conversar con las personas que estaban más familiarizadas con el proceso... Aquí vamos a hacer una conexión con la neutralidad. Las preguntas eran "¿Por qué?", "¿Cuáles eran las grandes reacciones a esta iniciativa?" Existía una reacción, incluso con una cierta lógica, que era desde el punto de vista de lo que habíamos relacionado con Anatel y con el Procon: ¿se le va a quitar a un determinado cliente la libertad de usar un puerto que tiene a su disposición dentro de su computadora? El Procon puede reclamar. ¿Por qué se está limitando la libertad? Si se limita la libertad, el Procon puede reclamar y presentar una demanda judicial contra las empresas y contra Anatel. Por otro lado, Anatel puede interpretar también que estamos actuando de una forma no autorizada y nos puede multar por estar interfiriendo con la libertad del ciudadano. Pero hay un mayor entendimiento y para nosotros esto es más fácil si paramos para reflexionar y decimos: "Lo que se encuentra a disposición de la sociedad tiene que servir a la sociedad; no es la sociedad la quien tiene que servir a alguna cosa. Por lo tanto, el cierre del puerto 25 es un beneficio innegable para toda la sociedad. Tenemos que trabajar en esta dirección e ir eliminando las aristas".

No voy a decir que mi parte haya sido la más fácil, porque el mayor trabajo fue de quien participó en el grupo coordinado por Faulhaber, pero me tocó un trabajo interno de convencer a las empresas y que culminó en una firma formal entre todos. Mantuvimos una gran reunión a la que traje más abogados que técnicos porque los abogados querían estar seguros no sobre el proceso técnico —esa no es su especialidad— sino que querían tener la seguridad de que en el futuro no serían penalizados por dejar que el sector firmase

un documento por el cual podría recibir multas posteriores. Esto es complejo; es bonito desde el punto de vista de la democracia y de las diversas fuerzas que actúan y es mucho más bonito por el resultado final cuando la sociedad es quien sale ganando. No hubo nada muy fuerte que impidiese que la sociedad salira ganando. Por esto creo que, para mí personalmente y para el sector de las telecomunicaciones, fue un orgullo muy grande formar parte de este proceso y poder difundirlo de la forma como se ha hecho y poder ver a Brasil ir bajando en el ranking mundial de *spam*.

En lo que a mí respecta, no había cómo lograr cerrar este proceso, no por el mérito de las personas sino porque el sector de telecomunicaciones no participaba en las reuniones.

El tema de la neutralidad de la red, para mí, tiene el mismo razonamiento: la sociedad tiene que beneficiarse de aquello que se pone a su disposición. Entonces, cuando hablamos de neutralidad de la red, creo que es casi como decir que se es hincha del Flamengo: nadie se opone (risas). ¿Usted está a favor o en contra de la neutralidad de la red? No imagino alguien que diga que se opone a la neutralidad de la red a partir de la hipótesis de que la red no puede interferir en algo que yo quiera hacer. Pero también es algo que se pone a disposición de la sociedad. El cierre del puerto 25 hizo que un grupo de clientes, de personas, perdiesen la oportunidad de utilizar algo que estaba a su disposición. En aquel momento, desde nuestra perspectiva, la red no estaba siendo neutra, pero existe algo más arriba de esto y que es el beneficio para la sociedad. Lo que estaba pasando por allí tiene que ser retirado, hay que evitar que pase, porque para empezar no es un cliente quien lo está usando. Partamos del principio que su computadora no sabe que en aquel momento está consumiendo ancho de banda y generando *spam* porque probablemente allí había sido introducido un virus que estaba consumiendo el ancho de banda del cliente. Por este motivo hicimos aquel acuerdo que involucró al Ministerio de Justicia, a Anatel. Pese a que en teoría estaríamos quitando una libertad o un poco de libertad, en realidad no es la persona que está haciendo aquello y sí un tercero de mala fe que está usando la banda que no fue hecha para el mal. Lo que se está haciendo es un beneficio para la sociedad.

Pero es un buen ejemplo de cómo casos semejantes o incluso casos nuevos que surjan en el futuro y en los cuales se demande alguna acción bajo la red se pueden desarrollar de modo de obtener un beneficio para la sociedad.

Nuestro temor en el sector de telecomunicaciones es la propia existencia de una ley rígida. Nos gusta mucho el Decálogo, pero muchas veces entendemos que puede haber una dicotomía entre aquello que proclamamos —que la red debe ser más libre, más simple, más libre realmente para todos— y la existencia simultánea de una ley, algo que puede tener consecuencias que salgan del control de esta libertad.

Entiendo perfectamente que el grupo que más actúa en Internet reaccione al exceso de reglamentación. Yo también reacciono y el sector de telecomunicaciones es extremadamente regulado por Anatel. Porque la sociedad debe obtener un beneficio de esto, no puede dejar que las empresas actúen sin reglamentación. Pero Internet tiene un grado de libertad mucho mayor. Eliminar este grado de libertad a través de una ley hecha en el Congreso puede ser un contrasentido con respecto a aquello que se predica sobre la libertad de Internet.

También entiendo perfectamente que, de la misma forma que se regula el sector de telecomunicaciones, debemos evitar posibles abusos de quien detenta un poder económico fuerte. Pero para esto tenemos a CADE (Consejo Administrativo de Defensa Económica), defensa de la competencia, los propios reglamentos de Anatel. Hasta desde este punto de vista, creo que la libertad sería mayor si solo nos quedáramos con el Decálogo, que es lo que existe actualmente en la Internet brasileña y es un ejemplo para el mundo.

CAF: Me gustaría oír su opinión sobre la importancia del Comité Gestor en este proceso. ¿Cómo ve el papel del Comité Gestor en la gestión del puerto 25 y cómo esto impacta acciones futuras, ya que mucho se discute sobre multisectorialismo y pocas son las prácticas y evidencias para que se pueda llevarlo a los foros internacionales?

EL: Yo también tengo críticas. Creo que la acción del CG fue fundamental desde el punto de vista *multistakeholder* y de la participación de todos. Pero si no fuese así y si todas las partes no estuviesen presentes, probablemente aún estaríamos patinando. Aún faltaba la parte de las telecomunicaciones, que podía ser la menos o la más importante, dependiendo del momento de que se tratara, ya que en distintos momentos su importancia puede ser más o menos significativa. La discusión dentro del Comité es de una gran riqueza gracias a las características que tienen los segmentos. El único problema que yo veo es cierto desequilibrio entre quien invierte y quien consume. El CGI está formado por una extensa mayoría de consumidores de banda, posee solo un representante de quienes que invierten. En una actividad que depende básica-

mente de inversiones sólidas, siempre es necesario tener en cuenta a quien va a pagar la cuenta del almuerzo. Entonces, quien va a pagar la cuenta del almuerzo no puede ser quien lidera y domina la discusión, pero debe ser siempre una voz activa e importante, porque paga la cuenta del almuerzo. ¿También obtiene talgo? Obtiene. Pero debe haber algún equilibrio. Con nuestra regulación —y tenemos mucha experiencia con la regulación en Anatel— ella siempre tiene en consideración el equilibrio económico-financiero de quien está practicando el negocio.

Cuando Anatel establece una regulación, principalmente para la concesión de un servicio, tiene en consideración los beneficios que va a obtener la sociedad, pero también tiene en consideración quién va a tener que invertir en aquello, obtener de aquello algo que le permita vivir y que no puede ser deficitario, porque no habría cómo existir, pero que tampoco explote a la sociedad obteniendo lucros fantásticos. Ella trabaja con el equilibrio.

Con mi experiencia de venir aquí todos los meses durante tres años, nunca participé de ninguna reunión en que hayamos cuestionado "¿Quién va a pagar?, ¿Quién va a invertir en esto? ¿Quién está recibiendo demasiados recursos?", "¿El ciudadano está siendo explotado?" Equilibrio es algo que echo de menos aquí en las discusiones, porque implica inversiones extraordinarias en la red brasileña.

9. Entrevista con Danilo Doneda

Realizada en Brasilia el 27 de septiembre de 2013

Marília de Aguiar Monteiro: ¿Podría describir sus actuales atribuciones en SENACON (Secretaría Nacional del Consumidor) y cómo se relacionan con las actividades de gestión del puerto 25?

DD: Soy coordinador general de estudios y monitoreo de mercado en Senacon. En mi coordinación me ocupo de los temas que se refieren al comercio electrónico, las comunicaciones e Internet. Hacemos estudios, análisis regulatorios, análisis de impacto, eventualmente con intervenciones para contribuir en políticas públicas que puedan colaborar con la defensa del consumidor en estas áreas.

En la época de la CT-Spam, acompañé de forma paralela el trabajo y específicamente participé del acuerdo que buscaba implementar la gestión del puerto 25 y la participación de los órganos de defensa del consumidor. Algunos participantes del acuerdo —empresas de telecomunicaciones, asociaciones de estas empresas— identificaban a los reclamos de los consumidores que serían afectados por esta gestión

como un eventual obstáculo a la gestión del puerto 25.

Dado que, por ser un problema de naturaleza jurídica, al principio este problema no había sido igualado técnicamente, la CT-Spam buscó a los órganos de defensa del consumidor y llegó a nosotros una demanda para que nos pronunciásemos al respecto de la viabilidad o no de proseguir con la gestión del puerto 25 y verificásemos, de hecho, los potenciales impactos a los consumidores; si realmente había algo que temer. Y fue en este momento que nos enteramos de todo el trabajo realizado por la CT-Spam, todas las cuestiones técnicas y también ingenierías de implementación que rodean a la gestión del puerto 25.

Creo que esto sucedió en 2010, incluso antes que yo estuviese aquí en Senacon. Para ser sincero, hubo un problema de comprensión técnica de lo que se trataba, ya que era un universo completamente nuevo. Defensa del consumidor tiene un problema crónico justamente por abarcar todos los mercados, todas las situaciones de consumo. Aquí, donde hay algunos datos técnicos que no son obvios para quien no es del área, hubo al principio una curva muy grande a recorrer. Esto lo sé porque me contaron sobre cuando esta demanda primeramente llegó a Senacon, antes que yo estuviese aquí.

En agosto de 2011, cuando yo llegué a trabajar aquí, el asunto fue retomado y nos llamaron para participar de una reunión del Comité Gestor, específicamente de la CT-Spam. Me recuerdo que participaron varios miembros del gobierno: Anatel, el MDIC y el propio Comité Gestor, empresas de telecomunicaciones, y en ese momento nos enteramos específicamente cuál era la naturaleza técnica del problema y cuál era la respuesta que se buscaba de nosotros, es decir, de qué forma la gestión del puerto 25 podía ser un problema para el consumidor o no.

La CT-Spam y el CERT se pusieron por completo a nuestra disposición para que aclarásemos dudas sobre esto. Hubo una reunión muy importante aquí en la secretaría, en aquella época departamento, si no me equivoco en 2011, en la que participaron Henrique Faulhaber, Cristine y Klaus del CERT y ofrecieron una explicación técnica de la gestión del puerto 25 y de lo que era la implementación. En aquel momento participó todo la directiva del entonces Departamento Nacional de Defensa del Consumidor.

La cuestión iba a ser examinada técnicamente por mi coordinación general —que era competente para apreciar la materia— y verificaríamos si el proceso sería de beneficio para el consumidor,

aunque tangencialmente pudiese acarrear algún pequeño problema, necesitando aquí de información. Si esto fuera verificado conforme había sido expuesto por la CT-Spam, trataríamos de informar al Sistema Nacional de Defensa del Consumidor, que está formado por los Procons y que oiría los reclamos si de hecho hubiese algún problema con un consumidor al respecto.

Se decidió que analizaríamos el tema e informaríamos a los órganos del Sistema Nacional de Defensa del Consumidor. Y a partir de esto, en los meses siguientes, estudiamos el tema, elaboramos una NT al respecto. Esta NT decía que, en vista de la naturaleza del problema, el *spam*, que afecta al consumidor tanto por las molestias, la pérdida de tiempo y las pérdidas de privacidad que provoca, como porque muchas veces el consumidor debe pagar, ya sea en dinero o en tiempo, para utilizar servicios que serían más simples y más baratos si gran parte del tráfico de la red no fuese *spam*, verificamos que una reducción específica y significativa del tráfico de *spam* en la Internet de Brasil representaría una ganancia concreta para el consumidor.

Llegar a esta conclusión fue bastante más fácil por el hecho de que yo había participado personalmente de un estudio comisionado por el CGI.br al Centro de Tecnología y Sociedad de la FGV en Rio de Janeiro justamente sobre la lucha contra el *spam*, perspectivas y una eventual redacción de un proyecto de ley. Recuerdo que en la parte de este estudio por la que fui responsable mi conclusión fue clara, algo que después transformé en un artículo personal: los instrumentos jurídicos serían incapaces de resolver de forma significativa los problemas relacionados con el *spam*. Por varios motivos. Porque los agentes directamente involucrados en la actividad del *spam* se encuentran debajo de una línea de civilidad o de legitimidad, incluso del alcance del brazo de la ley; por su ahorro de costos bastante particular, el *spam* es algo que no va a ser inhibido por mandato legal o formal, sino que se requiere un abordaje jurídico complementado por un abordaje técnico e incluso por un abordaje económico. Ante este cúmulo de experiencias y la verificación del resultado de la gestión del puerto 25, decidimos elaborar la Nota Técnica con nuestra conclusión, que es que también existía la posibilidad de que algunos usuarios/consumidores tuviesen algún problema. Especialmente aquellos que usaban ciertos equipos antiguos, algunas terminales no tradicionales como una computadora o *tablet* de uso médico, equipos particulares que tuviesen conexión

a Internet con estándares en cierta forma ya obsoletos y que aún podrían encontrarse en uso eventualmente, podrían ser afectados por una política de gestión del puerto 25.

En este sentido, la Nota Técnica trató de aclarar a los Procons de todo Brasil que, si hubiese eventualmente reclamos sobre esto, sería necesario verificar si el problema en la conexión a Internet tiene que ver con el bloqueo del puerto 25. Si fuese así, tendrían que buscar a los agentes del CERT —y otros que ahora no recuerdo y que figuran en la nota— para que indicaran cómo solucionar los problemas o llamar directamente al operador o al proveedor de Internet para verificar si existe una prerrogativa legítima del uso del puerto, que se podría abrir para las personas que tuviesen la necesidad concreta y legítima de utilizarlo.

La información que tenemos actualmente del tiempo que lleva la gestión del puerto 25 e incluso de la Nota Técnica es que absolutamente cero problemas llegaron a nuestro conocimiento en la Senacon. Eventualmente llegaron algunos problemas, en los Procons, oí decir, ni sé decir si fueron reclamos o denuncias ya que no hay una estadística cerrada sobre esto y, hasta donde consta, no hubo ningún problema que prosperara, ningún reclamo específico ni disputa entre consumidores y proveedores por causa el bloqueo del Puerto 25.

Por lo tanto, valoramos nuestra acción en todo este procedimiento y esperamos que haya sido útil en lo que se refiere a descartar el temor de que esta medida pudiera tener un efecto contrario, nocivo para los consumidores, capaz de bloquear o dificultar esta implementación que, a nuestro parecer, le trajo muchísimos beneficios al consumidor.

MM: Antes de la implementación de la gestión del puerto 25, ¿llegó alguna queja sobre *spam* al Sistema Nacional de Defensa del Consumidor?

DD: No es natural que un consumidor presente una queja sobre *spam* en Internet ante un Procon. Es un problema que veníamos monitoreando. Teníamos y tenemos una visión contraria, de que el *spam* es nocivo para el desarrollo de Internet o para el consumidor. Pero es un tipo de problema que se revela en un análisis sistémico y no en un análisis de datos del Procon. Las personas acuden a los Procons porque tienen un problema que les afecta directamente, que les impide comprar algo, impide que gocen de algún servicio, en fin, algo que influye directamente en su bolsillo, de forma concreta y tajante.

El problema del *spam* es un enfado crónico, que aflige a muchas

personas, pero que por su propia naturaleza no suele ser suficiente para hacer que una persona salga de la tranquilidad de su hogar y vaya hasta un Procon. Entonces, cualquier denuncia en de *spam* que eventualmente haya existido un Procon no influyó en nuestro análisis. Nosotros desarrollamos nuestro análisis de mercado en base a otros indicadores, un análisis más específico de un mercado, de aspectos de funcionamiento del mercado, que autorizó a Senacon a intervenir aunque no afectase directamente al consumidor.

MM: Durante la elaboración de la NT, ¿se identificó y desestimó algún perjuicio al consumidor?

DD: ¿Si se desestimó? Bueno, se consideraron eventuales riesgos identificados para personas que utilizaran agentes de *e-mail* desactualizados, personas que utilizaran sistemas conectados a Internet que no fueran computadoras en general y que eventualmente utilizasen el puerto 25 para su comunicación. En este punto habría un problema potencial para estos consumidores. Por otro lado, un análisis de mercado también revela que el número de estos consumidores es francamente residual en relación a la gran masa de consumidores que no utiliza estos sistemas. ¿Qué consideramos al respecto? Que el número de personas perjudicadas sería considerablemente pequeño en comparación con la cantidad total de consumidores que se beneficiarían de la medida. Y estos pocos consumidores eventualmente perjudicados serían consumidores que, al ser alertados sobre un eventual problema, tendrían la posibilidad de remediar la situación comunicando a su proveedor de Internet, entrando en contacto con los órganos de defensa del consumidor. Con la NT tratamos de aclarar al respecto, para que tuviesen rápidamente la información de que el problema que eventualmente podrían tener con la gestión del puerto 25 no era un problema de conexión, de calidad, de continuidad del servicio, sino un caso específico, casi que, entre comillas, un problema creado artificialmente por una nueva arquitectura de red y que podría ser subsanado y efectivamente lo fue. Nosotros tenemos contacto con el CGI.br, a través de quienes supimos que varios operadores abrieron el puerto 25 para los consumidores que reclamaron de manera de tratar de estabilizar un nivel prácticamente insignificante de personas afectadas. Aquí en Senacon, desde el comienzo del bloqueo directamente no recibimos ningún reclamo al respecto. Solo supimos de reclamos ante operadores que identificaron el problema y lo corrigieron para el consumidor.

MM: En cuanto a eventuales violaciones a los derechos del consumidor, ¿se identificó alguna potencialidad?

DD: Mire, el CDC (Código de Defensa del Consumidor) tiene un artículo que suele dejarse de lado: la defensa del consumidor tiene que adecuarse, adaptarse al desarrollo tecnológico. Y fue justamente este artículo el que ofreció una fundamentación casi ontológica para nuestra Nota Técnica en el sentido de que permitiríamos este cambio técnico, la gestión del puerto 25. Aunque pudiese alcanzar a un número pequeño de consumidores, era esencial para la creación de un ambiente más favorable para todos los consumidores. Los eventuales perjuicios para algunos consumidores —que en realidad no serían perjudicados en nada dado que podrían revertir esta situación— eran francamente un problema que fácilmente superable por los beneficios que el bloqueo del puerto 25 podrían representar para la generalidad de los consumidores.

MM: ¿Las actividades de educación y sensibilización realizadas en el ámbito de la CT-Spam fueron eficientes y percibidas por los órganos de defensa del consumidor?

DD: La única indicación que tendría para evaluar esto sería algún reclamo al respecto, algún comentario que nos hubiera llegado sobre el material educativo. Esto no sucedió. Desde el primer momento en que tuvimos contacto con la CT-Spam, uno de los aspectos que más realzamos y mantuvimos como punto firme fue la necesidad de que alguien nos apoyase con la educación, que nos aclarase las dudas, en caso que hubiese algún problema, porque dejamos en claro que, antes de nuestra actuación, sería imposible entrar en detalles minuciosos sobre el funcionamiento específico de la red. Y desde el principio la CT-Spam se mostró disponible e incluso contenta de poder contribuir en algo que nos pareció estar muy cerca, en nuestro ADN, que es el esclarecimiento, la producción de material informativo, etc. Este material llegó a nuestro conocimiento y lo enviamos a algunos Procons. Tal vez el Procon más sensible haya sido el Procon de San Pablo, donde seguramente se concentraría un número más grande de personas, de usuarios de Internet, tal vez de usuarios de servicios dedicados, especializados, que a lo mejor podrían encontrar algún tipo de problema. Hasta donde yo sé, esto sucedió y fue como dije. La única métrica que tendríamos sería la buena voluntad de comunicar el reclamo. Esto no ocurrió, por lo que, desde nuestro punto de vista, este flanco de la CT-Spam fue plenamente exitoso.

MM: Se considera que el proceso de implementación de la gestión del puerto

25 se demoró, que se trató de una implementación demorada. ¿Se podría decir que la entrada de otros organismos del poder público además de Anatel, entre ellos el propio Ministerio de Justicia, que mencionó anteriormente fueron lo que acabó prorrogando el proceso?

DD: Esta evaluación no nos corresponde a nosotros. Lo que nos pareció es lo siguiente: eventualmente muchas personas usan el nombre del consumidor en vano. Me pareció que esto estaba presente en la reunión que tuvimos con la CT-Spam. De todas formas, nuestro análisis del problema es que los problemas específicos para el consumidor eran puramente residuales. La práctica demostró que esto era realmente así. Hasta el momento no tuvimos ningún reclamo, ningún problema de porte que no haya sido fácilmente solucionado. Y en este contexto, nuestra actuación fue, espero —y me sentiría muy feliz si pudiera confirmarlo— en cierto sentido exorcizar algunos fantasmas que decían que el consumidor debía ser protegido de alguna manera para evitar que algunas ganancias de escala se revirtieran a favor del consumidor.

Tal vez una de las primeras actuaciones que presencié aquí en la Secretaría y en la cual se notó cierta madurez fue el hecho de enfrentar el problema no solo desde la óptica de algo que debe ser reparado sino de algo que debe ser sopesado por sus eventuales beneficios. Y en este contexto, solo estamos haciendo un cálculo de riesgo que es plenamente coherente con el CDC.

Carlos Affonso Pereira de Souza: ¿La experiencia del puerto 25 fue una ruptura de la neutralidad de red? ¿Cómo evalúa este tema?

DD: Bueno, la neutralidad de la red no es un valor absoluto en el sentido de que debe servir para algún propósito ontológico claro. En nuestra opinión, la neutralidad de la red sirve para privilegiar a Internet, a la comunicación sin limitaciones en cuanto a la libertad de expresión, en cuanto al libre flujo de información y consentimiento. Las medidas de gestión técnica que comprobadamente tengan como objetivo potenciar la libertad de expresión, el acceso al conocimiento y la libre comunicación no pueden ser caracterizadas propiamente como una forma de condicionar la neutralidad de la red, sino como excepciones cuidadosamente implementadas y estudiadas; excepciones que van a reforzar el carácter, el núcleo duro de la neutralidad de la red. Por esta razón, con el Marco Civil estamos siendo coherentes con otras definiciones de neutralidad alrededor del mundo, en el sentido de no confundir la neutralidad con un término absoluto que deje de lado la necesidad de gestión técnica para que la propia Internet sirva

a sus funciones. En fin, la función para la cual está destinada, una red libre y abierta a la comunicación para todas las partes integrantes.

MM: ¿Y en cuanto a la privacidad?

DD: ¿En cuanto a la relación de la privacidad con la gestión del puerto 25? Bueno, Senacon no identificó ningún problema relacionado con la privacidad que estuviese relacionado estrictamente con la gestión del puerto 25. Cualquier problema se enmarcaría dentro de otro espectro y Senacon no identificó nada en este sentido.

CAF: Una de las razones de este proyecto es entender la gestión del puerto 25 como una experiencia *multistakeholder* en Brasil. Como representante del gobierno llamado a participar de este asunto, ¿usted vio la gestión del puerto 25 como una iniciativa *multistakeholder*? ¿Cuál sería su evaluación de la participación de los demás agentes en este proceso?

DD: Mire, personalmente yo puedo haber llegado a esta fórmula, pero institucionalmente Senacon tenía poca experiencia con la gobernanza *multistakeholder*. En un primer análisis, lo enfrentó, como le comenté a Marília... Lo que llegó aquí incluso antes que yo estuviese en el Ministerio, en primer lugar lo enfrentó como un pedido a un órgano público, no necesariamente enfrentando la cuestión a través de un prisma más sofisticado, que el propio órgano encargado de la implementación era un órgano que ya contenía a los polos divergentes. Todos estaban representados. Entonces, dentro de esta mezcla de representación *multistakeholder,* participamos en una primera reunión en la CT-Spam y ahí quedó claro que había una divergencia de opiniones que se podía a través del posicionamiento de algunos de nosotros.

Verificamos que tal vez nuestro posicionamiento con la NT —si se me permite— con una tecnicidad tal vez inédita en las manifestaciones oficiales de Senacon, fue una NT que, a nuestro entender, —quedamos felices de verlo—, contribuyó a encaminar las posibles conclusiones que podía alcanzar aquel órgano.

A modo de paréntesis, hasta el día de hoy, en algunos Procons me conocen como la persona que habla sobre cosas incomprensibles, desde del día en que participé en una reunión con más de 150 Procons y el órgano de defensa del consumidor donde expliqué la gestión del puerto 25. Y algunas personas tal vez se hubiesen quedado menos sorprendidas si un marciano hubiese bajado a la tierra en vez de oírme hablar sobre SMTP y el puerto 25, el interés del consumidor, etc. Pero lo importante es que nadie reclamó, todos comprendieron el fondo del mensaje y consideran que hasta

aquí fue un procedimiento satisfactorio.

CAF: Considerando al consumidor técnicamente hiposuficiente en estas relaciones, ¿cómo ve el papel de Senacon como mediador de cuestiones técnicas como esta?

DD: Generalmente, cuando la relación de consumo tiene una gran complejidad técnica, para decidir sobre cuál es la mejor opción a tomar, la mejor opción a comprar, entra el papel que vemos como regulador, que en este caso somos nosotros, de funcionar como un "consumidor sustituto". Es decir, un ente que va a traducir técnicamente los términos del problema teniendo en cuenta los intereses del consumidor para ayudar en la toma de decisiones. En este sentido, como ya dije, la gestión del puerto 25 es algo un poco más moderno en el sentido que incluye aspectos regulatorios de naturaleza bien profunda; en el sentido de que nos pusimos en el lugar de consumidores sustitutos para tratar de prever riesgos, en una situación en que el propio consumidor no tendría conocimientos técnicos suficientes. ¿Qué hicimos? Funcionamos como un consumidor final, no solo ante el consumidor si no también ante los demás órganos de defensa del consumidor, que tienen la noble función de atender al consumidor en el mostrador diariamente, pero que por eso mismo tienen una dificultad muy grande para estudiar e investigar sobre temas casi esotéricos como este.

10. Entrevista con Jaime Wagner

Realizada telefónicamente el 11 de marzo de 2014

Carlos Affonso Pereira de Souza: ¿Qué recuerdos tiene sobre la gestión del puerto 25 en la CT-Spam?

JW: El Código de Autorregulación del *E-Mail Marketing* surgió como una derivación del trabajo de la Comisión Antispam del Comité Gestor de Internet. Durante el tiempo en que estuve en el Comité Gestor, la CT-Spam desarrolló dos importantes actividades: la gestión del puerto 25 y la elaboración del Código de Autorregulación del *E-Mail Marketing*.

Con respecto a la gestión del puerto 25, es importante destacar que todo empezó con la iniciativa de los llamados *honeypots* desarrollada por el personal del CERT. Las conclusiones a las que se llegó a partir de los datos generados por los *honeypots* fueron las que acabaron sentando la base técnica para lo que se hizo después. Pero hasta entonces se trataba de cuestiones eminentemente técnicas y que implicaban diálogo entre técnicos.

Cuando ingresé al CGI.br en 2008, el personal del CERT estaba listo para "tirar la toalla" en relación a la gestión del puerto 25. ¿Por qué estaba sucediendo esto? A mi entender, estaba claro que había una oposición por parte de las telefónicas en querer seguir con el proyecto. En las reuniones que se estaban realizando incluso existía la impresión de que esto no iba a funcionar.

Entonces sugerí a Henrique Faulhaber, quien coordinaba la CT-Spam, la estrategia de traer a las reuniones sobre el puerto 25 no solo al personal técnico sino también a los directivos de los operadores, además de también intentar atraer a las entidades representativas en lugar de las empresas. Hasta entonces, la estrategia consistía en mantener un diálogo entre técnicos pero hasta ahí nos topábamos con en el obstáculo de que la gestión del puerto 25 iba a dar mucho trabajo y que por esto sería mejor no seguir adelante.

El jaque mate en este tema fue justamente cuando los directivos de las empresas empezaron a asistir a las reuniones y a entender que no solo estaba el aspecto técnico. A fin de cuentas, acabó resultando una combinación en que Henrique y yo íbamos a las reuniones, yo decía lo que quería mientras Henrique adoptaba un tono más conciliador. Al final funcionó.

Yo decía que no quería hablar con los técnicos y sí con los directivos. Decía que quería hablar con quien iba a decidir y no con quien sentía pereza de trabajar. Mi argumento era: "¿No ven que el costo que esto va a generar para las empresas no se compara en nada con la pérdida de ancho de banda que está generando la situación actual?" A fin de cuentas, las empresas estaban aumentando la capacidad, pero parte de la banda era desperdiciada. "Bastaba mostrar a los accionistas", decía. Y mire que también soy accionista de Telefônica, por ejemplo. Mi punto era que este trabajo iba a permitir aumentar las ganancias.

Además de este cambio de discurso, también intentamos traer al diálogo a las entidades representativas. Pero aquí existía un problema que era el grado de correspondencia que las asociaciones encontraban en su representante en el CGIbr. A esta altura, las empresas de telecomunicaciones no consideraban al representante en el CGI.br como una persona próxima, sino que estaba más cerca del mercado de la TV por cable.

El asunto solo avanzó de verdad cuando logramos vencer la barrera técnica y en el CGI.br cambió el representante con el ingreso de Eduardo Levy. Cuando salí del CGI.br, recuerdo que él tomó el

proceso y lo llevó a un buen término. Sin él no habríamos llegado al mismo resultado.

Inicialmente él también mostró resistencia, pero notó que (la gestión del puerto 25) era lo mejor que se podía hacer. Observó que la situación que había en aquella época generaba un ahorro despreciable. Desde el punto de vista de las empresas, quedarse atado en el discurso de los técnicos generaba un ahorro despreciable, se ahorra trabajo, pero el perjuicio es mayor.

En verdad, en la conversación con las empresas de telecomunicaciones teníamos dos obstáculos. El primero eran los técnicos y el segundo eran los abogados, ¿no? Siempre diciendo que no podemos hacer esto o aquello. Y eran los abogados quienes estaban yendo a las reuniones, lo que contribuyó para el impase. Esto se solucionó cuando llegamos a los directivos.

Logramos un buen avance, pero desde el punto de vista político, sin la participación de Levy habría sido complicado o por lo menos no habría salido con la misma velocidad.

CAF: ¿Y el Código de Autorregulación del *E-Mail Marketing*?

JW: La elaboración del Código fue el segundo trabajo más importante que desarrolló la CT-Spam cuando yo estaba en el CGI.br y también implicó la participación de empresas en torno a una causa común.

Siempre digo que existen varios tipos de *spam*. Uno es el "*spam* bandido", que se estaba combatiendo mediante la gestión del puerto 25; el otro es el "*spam* ingenuo", que se disfraza de marketing. Es el sujeto que compra una base de datos y envía mensajes a todo el mundo, con la mejor de las intenciones y con el objetivo de vender más. Es el caso de algunos pequeños comerciantes que ven en esto una forma de marketing barato. En este caso, los comerciantes tienen un interés legítimo, pero acaban volviéndose *spammers*.

A fin de cuentas es un tiro por la culata, porque la imagen de la empresa termina manchada. Acaba teniendo un 1% de retorno positivo y todo el reso es negativo. Esto es *spam* ingenuo.

¿Qué tratamos de hacer? Invitamos a las empresas que hacían *e-mail marketing* serio para discutir el código de autorregulación. En ese entonces, el Congreso Nacional estaba debatiendo una serie de proyectos de ley sobre *spam*, algunos de los cuales pretendían criminalizar el *spam*. El propio CGI.br estaba involucrándose en el debate y buscando llegar a una redacción que pudiese ayudar a cuidar del problema del *spam* a través de la ley. Algunos proyectos de ley eran bien locos y el CGI.br estaba haciendo un trabajo de

esclarecimiento, junto a los diputados, sobre las implicancias técnicas de la adopción de una u otra definición. Incluso así no había consenso porque el CGI.br aún no había consultado a la propia comunidad afectada por esta regulación, es decir, el conjunto de empresas que usaban este tipo de comunicación. En 2008, 2009, la cantidad de empresas que vivían de esta actividad estaba aumentando. Era un sector prometedor con el que podría acabar un mal proyecto de ley, dificultando así la vida de empresas nacientes, que son de lo que está hecho este mercado: gente joven reunida.

Entonces, ¿qué sucedió? Estaba leyendo un *e-mail* que alguien había enviado al CGI.br criticando nuestro trabajo en la CT. Llamé a esta persona para conversar y buscar una forma de abordar el problema que no fuese por la ley sino por consenso entre los actores involucrados en esta actividad.

En lugar de tratar de caracterizar qué es *spam* como venían haciendo los proyectos de ley, optamos por definir qué sería el *e-mail marketing* legítimo. Todo lo que quedara fuera sería *spam* y podría ser afectado por la ley que se aprobara. Incluso porque definir qué es *spam* es muy complejo.

Trabajamos, entonces, en las reglas de este código y se demoró un año para lograr cerrar un acuerdo entre todos los involucrados. En la conversación estuvieron presentes representantes de entidades representativas de los usuarios, remitentes, proveedores, incluso ABRANET (Asociación Brasileña de Internet). Cuando llegamos a la redacción vimos que se precisaba más que un código, porque este debía ser eficaz.

Si el código no era eficaz, sería letra muerta, sin una instancia que lo promueva. Para ser eficaz, la autorregulación debe funcionar y ser acompañada. Creamos entonces una entidad con los modelos del CONAR (Consejo Nacional de Autorregulación Publicitaria) cuyo nombre se derivaba del propio Código. Surgió así la CAPEM (Código de Autorregulación para la Práctica de *E-Mail Marketing*), cuyo estatuto tenía una serie de normas que impulsaron la aplicación del Código.

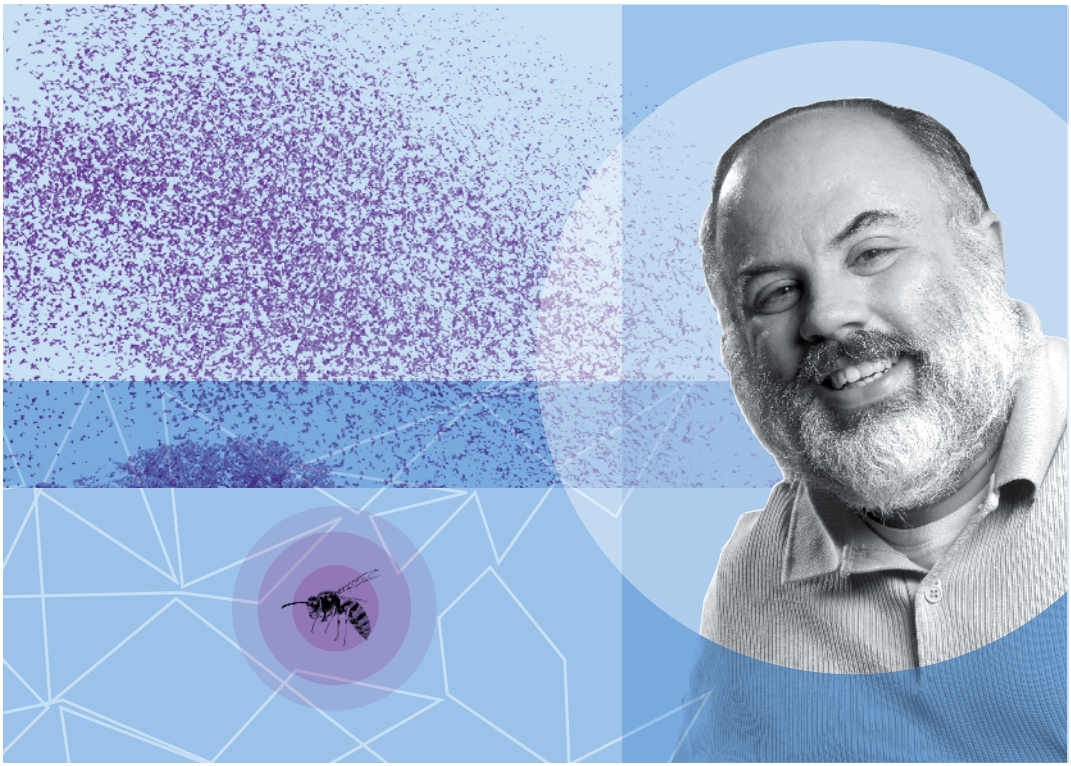
Era un CONAR más sencillo, con menos instancias de recursos y respaldado por un proceso automático de distribución y ayuda al juicio. Trabajamos en esto más de un año y cuando salí del CGI.br la entidad ya existía. Como no fui reelegido, acabé alejándome porque entendía que esta actividad no debía ser desarrollada por mí, sino por quien fuese el representante del sector en el CGI.br.

Cuando salí, la gran cuestión era cómo se financiaría la entidad

y su mantenimiento. Teníamos, entonces, el código y la entidad. Mi idea en aquella época era organizar este lío que existía con la discusión sobre el *spam*, creando incluso una lista negra brasileña cuyo proceso sería más reglamentado que el de las listas que existían por el mundo. Como se sabe, estas listas negras privadas que existen por ahí tienen un criterio técnico para la inclusión de un dominio en la lista, pero retirar el nombre de la lista es una cuestión eminentemente política; se trata de quién conoce a quién para llamar y pedir que la saque, como si fuese en una repartición.

En aquella época escribí un artículo sobre los diferentes tipos de *spam* que fue de ayuda en este trabajo y en las conversaciones para definir lo que sería el *e-mail marketing* profesional. Por ejemplo, una gran empresa de comunicación participó del CAPEM y, por causa de nuestras discusiones, dejó de vender su base de datos y luego empezó a vender un servicio que era la posibilidad de enviar un mensaje a su base de clientes, pero no vender la base como un todo.

Estos fueron algunos efectos interesantes del trabajo de la CT-Spam que yo pude acompañar como consejero del CGI.br, destacando la gestión del puerto 25 y el Código de Autorregulación del *E-mail Marketing*.



11. Entrevista con Marcelo Fernandes

Realizada telefónicamente el 10 de febrero de 2014

Carlos Affonso Pereira de Souza: ¿Podría describir cómo se involucró con el proyecto de gestión del puerto 25?

MF: En 2005, Henrique Faulhaber, Klaus Steding-Jessen y yo participamos de una reunión de la OCDE (Organización para la Cooperación y el Desarrollo Económico), en Ginebra, que abordaría la cuestión del *spam*. Asistimos en representación del CGI.br y nuestra misión era presentar la posición de Brasil en la lucha contra el *spam*. Al llegar en el evento, nos abordó un representante de SpamHauss quién nos dijo "me gustaría matar a los brasileños, especialmente a ustedes que están produciendo esta basura en Internet." Durante la conversación quedó claro que la cuestión del *spam* en Brasil no era solamente un problema nacional, sino también algo que afectaba a otros países y agentes, que sentían los efectos del gran volumen de mensajes enviados desde Brasil. Curiosamente, en la misma reunión notamos que, incluso encon-

trándonos dentro de la OCDE y usando una red oficial, no lográbamos enviar *e-mails*. Klaus prontamente descubrió que la razón era que ellos estaban usando el puerto 587 para el envío de mensajes y con nuestra configuración de ese entonces no era posible enviar mensajes. Esta situación trivial despertó en el grupo las ganas de avanzar en el debate sobre el *spam* en Brasil y ampliar la actuación del Comité Gestor de Internet en Brasil en esta área. La primera medida que tomamos fue la creación de la Comisión de Trabajo sobre *Spam* (la "CT-Spam").

Pero al comienzo nadie quería alborotar este avispero. Fue necesario mucho convencimiento e investigación para entender cuál sería la mejor medida a tomar y a partir de ahí desarrollar las actividades necesarias para revertir el cuadro de envío en masa de *spam* desde computadoras brasileñas. Se luchó durante cinco o seis años para lograr buenos resultados y que el país pudiese llegar en un nivel que los Estados Unidos y Europa ya habían logrado hacía mucho tiempo con una medida como la prohibición de que las conexiones residenciales continuasen usando el puerto 25 para enviar *e-mails*.

En un principio, el objetivo de las actividades consistía en identificar lo que realmente estaba sucediendo: ¿éramos "mulas" o simples disparadores de los *e-mails*? Fue en este momento que se empezó a desarrollar el proyecto de gestión del puerto 25.

Mi papel en esta historia empezó desde el primer momento en Ginebra. Pronto comencé a ayudar al equipo del CERT en una iniciativa que —en mi opinión— es uno de los proyectos más exitosos para la gestión de Internet en Brasil: el proyecto SpamPots. Este proyecto fue determinante porque dejó en claro que las medidas que se estaban adoptando para luchar contra el *spam* no eran tan efectivas como nos hubiera gustado y nos indicó una nueva dirección a seguir que llevó a la gestión del puerto 25. Esta iniciativa del proyecto SpamPots generó incluso trabajos académicos que reflexionaban sobre el impacto de la investigación y cómo fue importante para identificar lo que se debía hacer. Quedó claro que si no abordábamos la gestión del puerto 25 con el apoyo de los operadores estaríamos fritos. Google ya usaba el puerto 587 y Brasil no.

En este punto mi participación se dio en analizar los datos para identificar cuál era nuestro problema, señalar posibles caminos a seguir y a partir de ahí implementar la solución escogida, en este caso la gestión del puerto 25. A partir de aquí empieza la parte de

la historia que involucra las reuniones con los operadores, la reunión con el Ministerio de Justicia, los Procons y las confusiones que ya se imaginan.

CAF: ¿Llegó a participar de las reuniones que se mantuvieron luego de la decisión de implementar el control del puerto 25?

MF: Solo participé de las dos o tres primeras reuniones con terceros que serían agentes en la implementación de la gestión del puerto 25, dado que en esta fase yo acabé dedicándome más a los *spasmpots* y la articulación con los operadores quedó a cargo de Henrique Faulhaber. En seguida empezó a participar Jaime Wagner en el debate que tenía a ver con la creación de un código de autorregulación para el *e-mail marketing*.

CAF: ¿Podría describir un poco más cómo nació esta iniciativa de los *spampots*?

MF: Volvimos de Ginebra con la idea de que todas las denuncias contra Brasil —como la que presenciamos con el representante de SpamHauss— y toda la confusión de listas negras y grises debían acabar. Pero para esto era necesario entender quién, de dónde y hacia qué destino estaban saliendo estos *spams*. Teníamos algunas ideas, algunas pistas, pero en la época puedo decir que aún era una fase de dudas, ya que faltaban datos reales que comprobasen nuestras sospechas de que las computadoras brasileñas estaban siendo abuadas con una finalidad que no era primordialmente enviar *spam* hacia el interior de Brasil.

En una reunión con las personas del CERT, llegamos a la conclusión de que había llegado la hora de mostrar que la impresión que el mundo tenía sobre Brasil era infundada. Fue así que desarrollamos un prototipo de servidor y lo colocamos en diversos puntos de la red en Brasil, tanto corporativos como residenciales, y a partir de ahí pasamos a escuchar. Este servidor se presentaba en la red con sus puertos liberados para quien lo quisiese ver. Empezamos a percibir que rápidamente, incluso el mismo día, los servidores empezaron a recibir tráfico en sus puertos buscando probarlos para ver cuál funcionaba. Pero el *software* que desarrollamos tenía una peculiaridad: informaba a quienes llegaban al servidor queriendo enviar *spam* que el mensaje se estaba entregando normalmente, cuando en realidad este no era el caso. A partir de esta confirmación de que se enviaba a quien tratase de explotar el servidor empezamos a ver volumen. En dos o tres meses tuvimos que hacer un *upgrade* del almacenamiento, ya que era muy grande el volumen de datos que

estaban enviando. El volumen era tan absurdo que incluso siendo solo texto superó la capacidad de almacenamiento.

La pregunta que nos dejó esta prueba fue: ¿cómo demostramos esto ante el mundo? Fue así que contratamos a la Universidad Federal de Minas Gerais, a partir de contactos de Rogério Santana, con sus expertos en *data mining*. El CERT preparó una lista con todo lo que queríamos saber de estos *e-mails*: ¿De dónde venían? ¿En qué idioma estaban escritos? ¿Quién los estaba enviando? Seleccionamos todos los asuntos, por ejemplo, si se trataba de *phishing*. Fue así que se empezó a realizar esta exploración de los datos. Fueron terabytes y más terabytes que mostraron que, por estar abierto el puerto 25, la red brasileña era atractiva para toda la red mundial de *spammer*s. El *spammer* tenía la facilidad de no encontrar bloqueos para enviar sus mensajes. La red brasileña era una red perfecta: los usuarios no estaban acostumbrados a hacer actualizaciones de seguridad y *upgrades*, no usaban antivirus, existía una banda ancha razonablemente adecuada para estos fines. Todo esto explotó y el resultado fue una intensa explotación de la red nacional. El proyecto SpamPots lo mostró claramente.

CAF: ¿Cómo divulgaron esta noticia?

MF: Creo que en mi primera exposición sobre el tema, que mostraba que estábamos sufriendo ataques de usuarios ubicados fuera de Brasil y que la gestión del puerto 25 podría ser la solución, fue en la propia OCDE. Fue interesante ver cómo el efecto de descubrimiento en Brasil acabó generando interés en otros países. Klaus, por ejemplo, fue a Catar e instaló *spampots* allí. Otros países que iban aprendiendo con nosotros tenían exactamente el mismo problema y eran abusados por las mismas redes de *spammer*s. Entonces empezamos a hacer una gestión en base a estas informaciones. Nuestro trabajo tuvo una gran repercusión internacional y acabamos firmando diez o doce acuerdos con otros países y empresas de telecomunicaciones para el uso de la tecnología. Fue interesante ver que algunos eran justamente los mismos países que acusaban a Brasil de ser una de las principales fuentes de *spam* del mundo.

Con las iniciativas a seguir, involucrando al gobierno y a otros órganos, además de la sociedad civil, los Procons y toda una diversidad de actores del sector privado, el resultado fue que logramos sacar a Brasil de las listas de los países que más envían *spam*. Caímos diez o quince puestos solo porque empezamos a hacer la vida difícil a los *spammer*s. Algunos datos de los *spampots* son públicos

y cualquiera los puede consultar. Actualmente no tenemos ningún sensor instalado, pero con este trabajo la UFMG obtuvo laureles, porque fue una gran colaboradora del CGI.br. Siento mucho orgullo de esta iniciativa.

CAF: ¿Recuerda alguna resistencia a la iniciativa de la gestión del puerto 25?

MF: La decisión de que este era el mejor camino a seguir ya había sido tomada. Hubo resistencia de parte de las empresas de telecomunicaciones en el sentido de que no quisieron implementarlo de inmediato debido a su temor de ser demandadas por sus consumidores alegando cambios en sus contratos. Y este debate hizo que todo el proyecto durase cinco años. Aunque apoyó la iniciativa, Anatel acabó no reglamentando por entender que se trataba de una cuestión relacionada con Internet y no con las telecomunicaciones. Mirando atrás, queda claro que este fue uno de los proyectos más complejos en términos de articulación de agentes que haya coordinado el CGI.br.

CAF: ¿Cuáles son las lecciones que aprendió de este proyecto?

MF: Podemos aprender varias lecciones de la iniciativa de la gestión del puerto 25. La primera es comprender que, una vez identificando el problema, buscar datos que permitan comprobar cuál es la mejor solución es más importante que quedarse con dudas o recurrir a índices internacionales. Con los resultados que tenemos hoy, no se puede decir que Brasil es un país que llena la Internet de *spam*. En segundo lugar, es importante saber cuáles son las responsabilidades a asumir y quién las asumirá. Es importante salir de una situación llena de "glamour y romance" y entender que las cosas solo se resuelven con educación. El usuario va a entender, pero solo si las personas que generan y ofrecen al mercado un recurso crítico asumen sus debidas responsabilidades dentro del proyecto. En tercer lugar, creo que la gran diferencia la marca la existencia de una planificación interna con metas y objetivos que tengan en cuenta que, por más importante que sea la iniciativa, esta no va a durar para siempre. Por esta razón no podemos quedarnos esperando y sin actuar. Por último, un factor que no era exactamente lo deseado, fue el tiempo que llevó implementar la gestión del puerto 25. Como habrán visto en otras entrevistas, la articulación entre todos los participantes con sus intereses específicos, está lejos de haber sido algo sencillo.

nic.br